Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

PTC Safety Plan

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	PM	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Wilton Alston Safety Engineer		Wilton D. Alston 2019.08.16 15:24:27 -04'00'
Verified:	Jason Weighley Safety Engineer		Jason W Weighley 2019.08.16 14:42:10 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.08.16 15:00:26 -04'00'
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group		Phil Magloire 2019.08.19 08:35:05 -04'00'
BT/SRA Review:	N/A Title		
BT/SRA Review:	N/A Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3154931

Effective Date:	Revision:	Language:
2019-08-16	_C	EN

Jaclyn Gottschalk 2019.08.19 15:30:22 -04'00'

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2019-05-29	First issue
_A	2019-06-28	Issued for PTCSP Version 14.0
_B	2019-07-25	Issued for FRA Submittal PTCSP Version 15.0
_C	2019-08-16	Updated to expand Attachments

Table of Contents

Section	Subject	Page
1	Executive Summary	4
2	Introduction	4
2.1	Compliance Matrix	4
2.2	Reference Documents	4
2.3	Glossary	4
3	Attachment A – PTCSP Main Body	5
4	Attachment B – PTCSP Documents	6

List of Figures

No table of figures entries found.

List of Tables

Table 1: Reference Documents 4

1 Executive Summary

This document is the cover page for the PTCSP submittal for LIRR. The attachments to this document include the formally released files that the RR will submit to the FRA. These files do not all follow the BT Template as the PTCSP is a combination of writings from LIRR, BT and Siemens.

2 Introduction

The PTCSP is a regulation submission each RR must provide to the FRA to gain type approval of the PTC systems prior to formal operation.

2.1 Compliance Matrix

Not Applicable.

2.2 Reference Documents

Table 1: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms[1].

3 Attachment A – PTCSP Main Body

LIRR PTCSP MAIN BODY Rev 15.2 - Clean- 15-Aug-19

Long Island Rail Road
PTC Safety Plan
(PTCSP)

Docket Number FRA-2010-0031

Date: August 15, 2019
Rev 15.2

DEL 0067

Volume 1 – Main Body

Submitted in fulfillment of 49 CFR Part 236, Subpart I, §236.1015, et.al.

REVISION HISTORY

Date	Revision	Description	Author
July 24, 2019	15.0	LIRR Review	K. Jackson/ W. Alston / J. Weighley
July 25, 2019	15.1	Updated Executive Summary to LIRR comments	J. Weighley/
August 15, 2019	15.2	Update Document to refer to Attachments versus Appendices.	W. Alston/

Preface to PTCSP

This PTCSP (Document ID 3051824) is intended to cover LIRR cab signal equipped Automatic Speed Control (ASC) track segments as overlaid with the vital ACSES II PTC system, and LIRR non-cab-signal equipped (ABS and CMB) track segments as overlaid with the vital ACSES II PTC system.

The entire LIRR territory includes the following three types of FRA compliant vital signaling:

- Cab signaling with Automatic Train Control collectively is referred to as Automatic Speed Control [ASC]. This territory has both cab signal with wayside intermediate signals and cab signaling without intermediate wayside signals.

- Non-cab signaled Automatic Block Signal (ABS) signaling with wayside signals-only. This territory has continuous vital track circuit and hand operated switch indication control of all signal aspects.

- Non-cab signaled Controlled Manual Block (CMB) signaling with continuous vital track circuit and hand operated switch indication control of Manual Block Signal aspects.

The use of ACSES II by the LIRR in the non-cab signal territory is already governed by the "Type Approved" ACSES II per the PTCDP submittal made and granted FRA Type Approval (FRA-TA-2013-04) for territories without cab signaling. The ASC territories are covered by the ACSES II Type Approval **FRA-TA-2010-001** originally granted to AMTRAK.

The use of ACSES II by the LIRR in non-cab signal territory is already considered a "Type Approved" ACSES II implementation and is supported by an type approved PTCDP for ABS/CMB territory under Type Approval **FRA-TA-2013-04**.

Table of Contents

1 Executive Summary i

LIRR Mainline Territory iv
LIRR Rolling Stock vi
LIRR Mainline Track Exclusion Addendum (MTEA) vi
Signal Territories and Rules vii
Tenants x
LIRR ACSES II System x
Functions List xiii
Database Engineering xv
Configuration Management xv
Variances to Type Approvals xvi
Amtrak FRA-TA-2010-00 ACSES II xvi
LIRR Type Approval FRA-TA-2013-04 xvii
Testing Program xvii
Regression Testing xx
Failure Reporting Analysis and Corrective Action System (FRACAS) xx
Penn Station, NY through Harold Interlocking xxii
Operations and Maintenance of ACSES II xxii
Train Crews xxiii
TSR Application and Annulment xxiii
Training xxiv
Operating Rules xxiv
Maintenance of ACSES II xxiv

2 Introduction 2-1

2.1 Document Overview 2-2
2.1.1 Use of the Terms "PTC System" in this PTCSP 2-4
2.1.2 49 CFR Part 236, Subpart I Cross Reference to PTCSP 2-4
2.1.3 Goals and Objectives 2-30
2.1.4 Success Criteria 2-30
2.2 Update of This PTCSP 2-32
2.3 Acronyms and Definitions 2-32

3 Applicable Reference Documents 3-1

4 Confirmation of FRA Vital Overlay Designation For Long Island Rail Road ACSES II PTC System [§236.1015(e)(2), §236.1031(d)] 4-1

4.1 Reliably Execute PTC Functions 4-1
4.2 Analysis of System Risk As It Applies to Appendix C Safety Principles 4-2
4.3 Justification of Non-Vital Classification of the Communications Segment 4-3

5 Type Approval Reference [§236.1009(d)(1), §236.1015(b), §236.1023] 5-1

5.1 Type Approval Referenced and Utilized in This PTCSP 5-1
5.2 PTC Product Vendors List (PTCPVL) [§236.1015(b)(1), §236.1015(b)(3), §236.1023(a)] 5-1
5.3 PTC System Vendor Quality Control System [§236.1015(b)(2)] 5-1
5.3.1 Applicable Licensing Information [§236.1015(b)(3)] 5-1
5.3.2 Version Control for Subsystems of the ACSES II System on LIRR 5-2

6 PTCDP Reference And Identification Of Any Variances [§236.1009(d)(1), §236.1015(c), §236.1015(d)] 6-1

6.1 PTCDP and Type Approval References [§236.1015(c)(1), §236.1015(d)] 6-1
6.2 Variances from PTCDP (As Approved) [§236.1015(c)(2)] 6-2
6.3 Attesting to Compliance with Referenced PTCDP [§236.1015(c)(3)] 6-2

7 LIRR PTC System Implementation [§236.1005(a), §236.1005(f), §236.1015(d)] 7-1

7.1 LIRR Operating Environment 7-1
7.2 Information Required For PTCDP Under §236.1013(a) 7-2
7.2.1 Incorporate PTCDP by Reference 7-2
7.2.2 Final Human Factors Assessment 7-2
7.3 LIRR PTC System Implementation 7-2
7.3.1 LIRR PTC Implementation Plan (PTCIP) 7-2
7.3.2 LIRR-Specific PTC System Functions Implementation, If Any 7-3
7.4 PTC Architecture 7-4
7.5 Safety Assurance Objectives 7-12
7.5.1 Safe Operation 7-13
7.5.2 Tenant Operations on LIRR Territory 7-13
7.5.3 LIRR PTC System Reliability and Availability Goals / Performance 7-13
7.5.4 Reliability and Availability Assumptions 7-15
7.5.5 LIRR PTC System Safety Goals 7-16
7.5.6 Safety Assumptions 7-17
7.5.7 Interoperability 7-19
7.6 System Users 7-19

8 Final Human Factors Analysis [§236.1015(d), Part 236 Appendix C(b)(5)] 8-1

8.1.1 Design of Office Segment 8-1
8.1.2 Design of ACSES II Display Unit 8-1
8.1.3 Mounting of the ADU in the LIRR Revenue Vehicles 8-1
8.1.4 Design of the RWPS 8-2
8.1.5 Design for Maintainability 8-2
8.2 Ergonomic Analysis of ADU Placement 8-2

9 Safety Assessment, V&V Processes and Appendix C Safety Principles [§236.1015(d)(5)] 9-1

9.1 Industry Standards for Safety Assessment and V&V Processes 9-2
9.1.1 System Safety Scope 9-2
9.1.2 System Safety Organization 9-3
9.1.3 Roles and Responsibilities 9-4
9.1.4 System Safety Certification Board 9-5
9.2 System Safety Program for ACSES II 9-5
9.2.1 System Lifecycle and Safety Tasks 9-5
9.2.2 ACSES II System Safety Targets 9-11
9.2.3 Hazard Management 9-11
9.2.4 Safety Principles, Architecture, and Requirements 9-11
9.2.5 Interoperability 9-13
9.2.6 Operations and Maintenance Readiness 9-16
9.3 Companion Program of Safety Activities 9-17
9.3.1 Software and Data Maintenance Facility (SDMF) 9-17
9.3.2 Wayside Diagnostic and Programming Tool 9-18
9.3.3 STS Programming Tool 9-18
9.4 System Safety Certification 9-19
9.4.1 Methodology 9-21
9.4.2 Safety Compliance Assessment 9-21
9.4.3 Safety Certification Policy 9-22

9.4.4 Final Safety Report ... 9-23
9.5 Hazard and Risk Mitigation Plan ... 9-24
9.5.1 Hazard and Risk Resolution Process ... 9-30
9.5.2 Hazard Identification ... 9-31
9.5.3 Hazard Log ... 9-31
9.5.4 Evaluation of Supplier Provided Hazard Analysis ... 9-31

10 Hazard Log [§236.1015(d)(1)] ... 10-1

10.1 Hazard Log Overview ... 10-1
10.1.1 Sources of Hazards in the Hazard Log ... 10-1
10.1.2 Hazard Tracking Log Attributes ... 10-2
10.2 Hazard Log Tools Used ... 10-2
10.3 Maintenance of the Hazard Log ... 10-2
10.3.1 During Development and Deployment Phases ... 10-2
10.3.2 During Post-Deployment Phase ... 10-3

11 Safety Assurance Concepts [§236.1015(d)(2) and Part 236 Appendix C(b)] ... 11-1

11.1 Safety-Critical Performance and Fallback Procedures ... 11-2

12 Risk Assessment [§236.1015(d)(3), Part 236 Appendix B] ... 12-1

12.1 Risk Assessment Approach ... 12-1
12.2 Appendix C Safety Principle Compliance Conclusions ... 12-1
12.3 Residual Risk Impact Assessment Conclusions ... 12-1

13 Hazard Mitigation Analysis [§236.1015(d)(4)] ... 13-1

13.1 Hazard Assessment ... 13-1
13.1.1 Hazard Assessment of ACSES II Introduction ... 13-2
13.1.2 Hazard Identification and Mitigation ... 13-3
13.1.3 Hazard Severity Classifications ... 13-3
13.2 System Safety Design ... 13-7
13.2.1 Detailed Hazard Descriptions and Mitigation Techniques ... 13-7
13.2.2 Safety Design Order of Precedence ... 13-8
13.2.3 Analysis of PTC System Components ... 13-8

14 Verification and Validation Processes [Part 236, Appendix C, §236.1015(d)(5), §236.1015(d)(7), §236.1015(f)] ... 14-1

14.1 PTC System Verification and Validation Processes ... 14-1
14.1.1 Review ... 14-2
14.1.2 Analysis ... 14-3
14.2 PTC Master Test Plan ... 14-3
14.2.1 Testing Scope ... 14-3
14.3 Testing and Commissioning ... 14-3
14.3.1 Test Strategies ... 14-3
14.3.2 Use of Automated Testing ... 14-4
14.3.3 Test Metrics and Completion Criteria ... 14-4
14.3.4 Requirements Traceability ... 14-5
14.3.5 Test Documentation ... 14-5
14.3.6 Test Documentation Development, Storage, and Submittal ... 14-6
14.3.7 Test Plans ... 14-6
14.3.8 Test Results, Records, and Reports ... 14-6
14.4 Interoperability Testing ... 14-6

15 Training Plan [§236.1015(d)(6), §236.1041, §236.1043, §236.1045(a), §236.1047(a), (b) and (d), §236.1049]

15-1

15.1 Training and Qualification Program Requirements 15-1
15.2 Locomotive Engineer Training 15-2
15.3 Train Dispatchers and Chief Train Dispatcher Training 15-2
15.4 Signal Personnel Training 15-2
15.5 Communications Office Personnel Training 15-2
15.6 Communications Field Personnel Training 15-3
15.7 Mechanical Department Personnel Training 15-3
15.8 Maintenance of Way Personnel Training 15-3
15.9 Rules Examiners Training 15-3
15.10 Operations Managers Training 15-3
15.11 Front Line Supervisors Training 15-3
15.12 SI Training 15-4
15.13 Emergency Preparedness Drills 15-4
15.14 Tenant Train Crew Training 15-4
15.15 Train Crew Training for Operation on Amtrak Tracks 15-4

16 Procedures, Test Equipment, And Operations And Maintenance Manual [§236.1015(d)(7) and §236.1039, Appendix C (b)(7)] 16-1

16.1 Operations and Maintenance Procedures and Documentation 16-1
16.1.1 Test Equipment 16-1
16.2 O&MM Document Access and Control 16-1
16.3 Change Control of O&MM Documents 16-1

17 Warnings and Warning Labels [§236.1015(d)(8)] 17-1

18 Configuration Management and Revision Control Measures [§236.1015(d)(9) and §236.1023(c)(2)] 18-1

18.1 Configuration Management Plans 18-1
18.1.1 Project and Product Configuration Management 18-2
18.1.2 LIRR PTC Configuration Management 18-2

19 Initial Implementation Procedures [§236.1015(D)(10) and §236.1015(d)(5), §236.1015(f)] 19-1

19.1 Testing Requirements 19-1
19.1.1 Component Testing 19-1
19.1.2 Subsystem Testing 19-2
19.1.3 Integration Testing 19-2
19.1.4 Field and Commissioning Testing 19-2
19.2 LIRR ACSES II Laboratory Testing 19-2
19.3 LIRR GIS Database 19-3
19.4 LIRR Field Testing 19-3
19.5 Revenue Service Demonstration (RSD) Report 19-4
19.6 Interoperability Testing (Amtrak) 19-4

20 Post-Implementation Testing (Validation) and Monitoring Procedures [§236.1015(d)(11)] 20-1

20.1 Post-Implementation Test Procedures 20-2
20.2 Test and Demonstration with Tenant Onboard Equipment 20-6
20.3 Post Implementation Monitoring Activities 20-6

21 Records [§236.1015(d)(12), §236.1023(b)(1), §236.1023(e), §236.1037, §236.1043(b)] 21-1

21.1 Records Retention 21-1
21.1.1 Product Vendor Notification 21-1
21.1.2 Action Upon Product Vendor Notification 21-2

21.1.3 Configuration Management Upon Product Vendor Notification 21-2
21.1.4 Procedures for Product Vendor Notification 21-2
21.2 Records Operation and Maintenance 21-2
21.3 Data Retention Management 21-2

22 Safety Analysis Of Work Zone Incursion Protection from Human Error [§236.1015(D)(13)] 22-1

23 Alternative Arrangements for Rail At-Grade Diamond Crossings [§236.1005 (a)(1)(i), §236.1015(d)(14)] 23-1

24 Authority And Signal Enforcement and Switch Position [§236.1015(d)(15)] 24-1

***25* Compliance with Stated MTEA [§236.1015(d)(16), §236.1019(f)] 25-1**

26 Deviation in Operational Requirements for En Route Failures of PTC System [§236.1006, §236.1015(d)(17), §236.1015(d)(21), §236.1023(f), §236.1023(j), §236.1029] 26-1

26.1 Operating Provisions in Event of PTC System En Route Failure 26-1
26.2 Failure Detection and Report 26-2
26.3 Temporary Exception Provisions 26-5

27 Enforcement of Hazard Detectors [§236.1005(a)(4)(v), §236.1005(c)(1), §236.1005(c)(2), §236.1015(d)(18)] 27-1

28 Emergency and Planned Maintenance – Temporary Rerouting Plan [§236.1005(g) – (k), §236.1033(f), §236.1029] 28-1

28.1 Emergencies – Temporary Rerouting 28-1
28.2 Rerouting Request Content Requirement 28-1
28.3 Service Restoration Plan 28-1

***29* High Speed Service Requirements [§236.1005(c)(3), §236.1007, §236.1015(d)(20)] 29-1**

30 Communication and Security Requirements [§236.1015(d)(20), §236.1033] 30-1

30.1 LIRR PTC System Security Management Plan 30-1
30.2 Security Requirements 30-1
30.3 Security Measures 30-2

31 List of Each Location Where a Locomotive with a Failed Onboard Apparatus will be Regularly Exchanged or Repaired [§236.1029(b)(6)] 31-1

32 PTC System Safety Audits 32-1

33 Potential Data Errors and Their Mitigation [§236.1015(h)] 33-1

33.1 Sources of Potential Data Errors 33-1
33.2 Hazard Capture and Mitigation References Related to Data Errors 33-1
33.3 Mitigations of Hazards from Potential TSR Data Errors 33-1

34 Third Party Safety Assessment [§236.1017] <Reserved> 34-1

35 Event Recorders [§229.135, §236.1005(d)] 35-1

35.1 LIRR PTC Data Recorder 35-1
35.1.1 Physical Connection 35-1
35.1.2 CHMM 35-1
35.2 Storage and Retention of LIRR PTC Data 35-1

36 Errors and Malfunctions [§236.1015(c)(1), §236.1023(e)(3), §236.1023(f), §236.1023(g), §236.1023(j), §236.1037(d)] 36-1

36.1 Product Vendor List 36-1
36.2 Failure Reporting and Change Notification Process 36-1

36.2.1 Failure Reporting and Corrective Action System 36-3
36.2.2 Planned Modification 36-3
36.3 PTC Restoration Process 36-3

37 Role of Office Automation Systems in the PTC System [§236.1027(a)] 37-1

38 Novel Technology Employed in Highway Crossing Protection for PTC [§234.275(c)] 38-1

39 Justification for LIRR PTCSP Redaction 39-1

List of Tables

TABLE EX-1: KEY PTC FUNCTION COMPLIANCE MATRIX II
TABLE EX-2: LIRR TERRITORY DATA OVERVIEW BY SEGMENT V
TABLE EX-3: ROLLING STOCK TO EQUIP WITH ACSES VI
TABLE EX-4: MTEA CLASSIFICATIONS VI
TABLE EX-5: LISTING OF MTEAS VII
TABLE EX-6: ROLES AND SUPPLIERS XI
TABLE EX-7: LIST OF MTTHE CALCULATIONS XII
TABLE EX-8: ACSES FUNCTIONS LIST XIII
TABLE EX-9: TYPE APPROVAL FRA-TA-2010-001 VARIANCES XVI
TABLE EX-10: TYPE APPROVAL FRA-TA-2010-001 LIRR VARIANCES XVI
TABLE EX-11: SUMMARY TEST PROGRAM XIX
TABLE 2-1: 49 CFR PART 236, SUBPART I CROSS-REFERENCE TO PTCSP 2-4
TABLE 7-1: COMPLETE LIRR ACSES II SYSTEM RAM REQUIREMENTS 7-14
TABLE 7-2: COMPLETE LIRR ACSES II SYSTEM RAM PERFORMANCE 7-14
TABLE 7-3: INDIVIDUAL LIRR ACSES II SYSTEM RAM REQUIREMENTS 7-14
TABLE 7-4: INDIVIDUAL LIRR ACSES II SYSTEM RAM PREDICTION RESULTS 7-15
TABLE 8-1: DRAWING NUMBERS ERGONOMIC ANALYSIS OF ADU PLACEMENT 8-2
TABLE 9-1: ACCOUNTABLE POSITIONS IN LIRR SAFETY ORGANIZATION 9-4
TABLE 9-2: SAFETY ACTIVITIES 9-9
TABLE 9-3: SAFETY PRINCIPLE CHECKLIST 9-12
TABLE 9-4: RISK ASSESSMENT CRITERIA CHECKLIST 9-25
TABLE 9-5: SI-PERFORMED HAZARD ANALYSES 9-32
TABLE 9-6: PROCEDURE NEEDS FROM MTEA AND PHA 9-34
TABLE 10-1: HAZARD SOURCES 10-2
TABLE 11-1: FALL-BACK RELEVANT PROCEDURES, IDENTIFIED VIA OHA 11-3
TABLE 12-1: LIST OF MTTHE CALCULATIONS 12-2
TABLE 13-1: HAZARD SEVERITY CLASSIFICATIONS 13-4
TABLE 13-2: HAZARD PROBABILITY CLASSIFICATIONS 13-5
TABLE 13-3: MAPPING OF ACSES II PROBABILITY CATEGORIES INTO LIRR CATEGORIES 13-6
TABLE 13-4: HAZARD RISK ASSESSMENT MATRIX 13-7
TABLE 13-5: HAZARD RISK INDEX (HRI) 13-7
TABLE 13-6: SAFETY DESIGN ORDER OF PRECEDENCE 13-8
TABLE 20-1: MAINTENANCE SCENARIOS, IN SUPPORT OF POST-IMPLEMENTATION TESTING 20-2
TABLE 21-1: RECORD LOCATIONS 21-1
TABLE 21-2: RETAINED DOCUMENTS 21-3
TABLE 25-1: MTEA TRACK CLASSIFICATIONS 25-1
TABLE 25-2: MTEA DESCRIPTION/TRACKAGE LOCATION 25-1
TABLE 26-1- PTC SUBSYSTEM FAILURE AND BACKUP OPERATION PROCEDURE 26-1
TABLE 26-2: PTC FAILURE DETECTION AND REPORT PROCEDURE 26-2
TABLE 31-1: PTC FAILURE DETECTION AND REPORT PROCEDURE 31-1

List of Figures

FIGURE EX-1: SCHEMATIC MAP OF LIRR MAINLINE TERRITORY IV
FIGURE EX-2: LIRR SIGNAL TERRITORY OVERVIEW VIII
FIGURE EX-3: SCHEMATIC MAP OF LIRR MAINLINE TERRITORY IX
FIGURE EX-4: OVERVIEW BLOCK DIAGRAM OF ASCES II X
FIGURE EX-5: FRACAS PROCESS MAP XXI
FIGURE EX-6: AMTRAK / LIRR JOINT OPERATING TERRITORY XXII
FIGURE EX-7: SELECT-CHECK-EXECUTE PROCESS, TSR REQUEST (SAME FOR ANNULMENT) XXIII
FIGURE EX-8: ALLOCATION OF ACSES II COMPONENTS TO LIRR MAINTENANCE DEPARTMENTS XXV
FIGURE 7-1: SYSTEM ARCHITECTURE CONTEXT DIAGRAM 7-6
FIGURE 7-2: OFFICE SUBSYSTEM CONTEXT DIAGRAM 7-7
FIGURE 7-3: ONBOARD SUBSYSTEM CONTEXT DIAGRAM 7-8
FIGURE 7-4: WAYSIDE SUBSYSTEM CONTEXT DIAGRAM 7-9
FIGURE 7-5: COMMUNICATION SUBSYSTEM CONTEXT DIAGRAM 7-10
FIGURE 7-6: ACSES II PTC BLOCK DIAGRAM FOR ABS TERRITORY 7-11
FIGURE 7-7: ACSES II PTC BLOCK DIAGRAM FOR CMB TERRITORY 7-11
FIGURE 9-1: ACSES II SYSTEM SAFETY SCOPE 9-3
FIGURE 9-2: LIRR PTC SYSTEM SAFETY ORGANIZATION 9-4
FIGURE 9-3: LIRR'S IMPLEMENTATION PROCESS 9-9
FIGURE 9-4: SAFETY CASE DEVELOPMENT 9-20
FIGURE 9-5: PROCESS FOR HAZARD ANALYSIS, HAZARD MITIGATION AND RISK ASSESSMENT 9-30
FIGURE 13-1: PROJECT HAZARD TRACKING PROCESS 13-2
FIGURE 26-1: ERRORS AND MALFUNCTION PROCESS FLOW 26-4
FIGURE 35-1: ACSES II OBC TO EVENT RECORDING DEVICE CONNECTIONS 35-1
FIGURE 35-2: EVENT RECORDER OUTPUT DISPLAY ON LAPTOP 35-2
FIGURE 35-3: SCREEN SHOT OF EVENT RECORDER MONITORED DATA 35-3
FIGURE 36-1: FRACAS PROCESS FLOW 36-3

1 Executive Summary

This document is the Long Island Rail Road (LIRR) Positive Train Control Safety Plan (PTCSP) for the LIRR Positive Train Control system implemented on the LIRR service territory.

The LIRR currently deploys the following types of 49 CFR Parts 234, 235, and 236 FRA compliant vital signaling:

- Cab signaling with Automatic Train Control (referred to as Automatic Speed Control [ASC]). This territory has both cab signal with wayside intermediate wayside signals and cab signaling without intermediate wayside signals.
- Non-cab signaled Automatic Block Signal (ABS) signaling with wayside signals-only. This territory has continuous vital track circuit and hand operated switch vital indication control of all signal aspects.
- Non-cab signaled Controlled Manual Block (CMB) signaling with continuous vital track circuit and hand-operated switch vital indication control of Manual Block Signal aspects.

This PTCSP does not detail the vitality of the existing LIRR vital cab Signal/ATC and wayside signaling systems as these are long standing systems that LIRR has operated, maintained and modified for many decades in compliance with 49 CFR Parts 234, 235, and 236.

PTC compliance on LIRR mainline trackage by territory is summarized below by the two main types of LIRR signaled territories: ASC and non-ASC adding ACSES II as a vital overlay:

1) ASC mainline trackage by: **Cab Signal/ATC + ACSES II** – per Amtrak Type Approved **FRA-TA-2010-00** ACSES II (ASC includes territory with and without intermediate automatic wayside Signals)

2) Non-ASC ABS & CMB mainline trackage by: **Wayside Signaling + ACSES II** – per LIRR PTCDP Type Approval **FRA-TA-2013-04**

Note, this LIRR PTCSP incorporates both of the above Type Approved ACSES II applications on LIRR. The PTCSP also addresses LIRR's Roadway Worker Protection System (RWPS) being implemented as a result of agreements between the railroad and the FRA regarding LIRR's Type Approval **FRA-TA-2013-04** for use of ACSES II in non-ASC territory. The RWPS is not a PTC requirement, but is addressed in this PTCSP inasmuch as it is an adjunct to, and substantially implemented by LIRR's ACSES II system.

Table EX-1 on the following page summarizes the allocation of PTC enforcement and compliance to the various vital signaling and train control systems implementing PTC functionality.

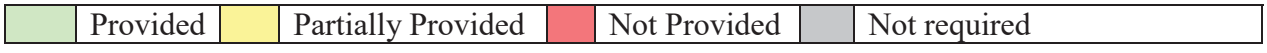
PTC Regulatory Functional Requirements

1: Prevent train-to-train collisions
2: Prevent overspeed derailments
3: Prevent unauthorized incursions into work zones
4: Prevent movements over switch in wrong position
5: Protect highway-crossing activation failures

Table Ex-1: Key PTC Function Compliance Matrix



Color Key:







Throughout implementation of ACSES II as documented within the latest revision of LIRR's FRA-approved PTCIP, LIRR has generated specific actions and compiled critical evidence to address the requirements of 49CFR Part 236 Subpart I for PTC. In documenting the body of evidence to support this safety plan, as detailed in the References and Attachments attached hereto, LIRR has:

1. Described the LIRR rail environment and application of its PTC system to its subdivisions, shown Section 1 of this PTCSP.
2. Referenced applicable industry and safety standards and regulations, provided in Section 3 of this PTCSP.
3. Provided FRA with the required regulatory submittals. Refer to SIR site contents as previously submitted to FRA under separate cover.
4. Performed a Risk Assessment identifying the residual risk remaining with ACSES II; attesting that it satisfies the level required for a vital overlay PTC system, summarized in **Section 12** and fully described in **Attachment K** of this PTCSP.
5. Identified hazards, defined hazard mitigations and performed or sponsored creation of various system-level hazard and safety analyses, as given in **Attachment L** – **Attachment P** of this PTCSP, to attest to the implementation of ACSES II as a vital overlay. The hazard analyses specific to the RWPS are found in **Attachment U** – **Attachment W** of this PTCSP.
6. Identified processes and procedures employed to perform functional and safety verification and validation of the implemented PTC system over its useful life cycle, provided in Sections 8 and 13 of this PTCSP.
7. Provided the planning, curriculum, management of, and results of a PTC Training program, as summarized in Section 15 of this PTCSP and presented in detail in the Detailed Master Training Plan **[35]**.
8. Provided results of all verification and validation activities performed as submitted to the SIR site under separate cover.
9. Identified how LIRR is maintaining proper configurations, managing safety related records, as well as changes to PTC system components, as summarized in Section 18 and fully described in the Configuration Management Plan **[29]** and the Long Island Rail Road PTC Configuration Management Plan **[69]**.
10. Identified the means by which LIRR is addressing special operational scenarios (e.g., Human Errors affecting Work Zones), as described in Section 22 as well as in **Attachment W** of this PTCSP.
11. Identified how LIRR will address impacts to operations in the light of system degraded modes or failures, as provided in **Attachment DD** of this PTCSP.

Working closely with its interoperability partners in confirming proper operation in applicable host/tenant scenarios.

LIRR Mainline Territory



Figure Ex-1: Schematic Map of LIRR Mainline Territory

Table Ex-2: LIRR Territory Data Overview by Segment

Branch/Segment	From (Station or Interlocking*)	To (Station or Interlocking*)	Length Miles	QTY Passenger Stations	QTY H'Way Xings	QTY Hand Op Switches	Signal Territory type (rule)	QTY[1] WkD[2] revenue trains	QTY[1] WkE[3] revenue trains
Montauk	Babylon	Patchogue (pilot 1)	18.1	5	31	7	ABS/CMB	42	41
Port Wash	Woodside	Port Washington (P2)	16.3	12	1	17	ASC (410)	103	75
West Hempstead	Valley	West Hempstead	4.7	5	8	0	ASC (410)	42	36
Main Line	Ronkonkoma	Greenport	46.1	6	58	34	Non-signaled	9	8
Babylon	Jamaica	Babylon	27.8	14	0	4	ASC (410)	163	102
Oyster Bay	Mineola	Oyster Bay	14.3	10	16	9	ABS/CMB	35	22
Central	Bethpage	Babylon	8.2	0	8	5	ABS	14	6
Port Jefferson	Hicksville	Port Jefferson	32.6	10	34	31	ASC (410)	192	147
Long Beach	Valley	Long Beach	7.3	6	8	0	ASC (410)/CMB	105	82
Far Rockaway	Valley	Far Rockaway	5.0	11	14	5	ASC (410)/CMB	122	85
Hempstead	Valley	Hempstead	6.5	6	6	8	ASC (410)	63	44
Atlantic	Atlantic Terminal	Jamaica	15.8	3	0	0	ASC (409)	141	79
Main Line	Long Island City	Jamaica	8.5	6	1	11	ASC (409/410)	457[A]	378[A]
Main Line	Jamaica	Ronkonkoma	39.9	9	34	43	ASC (410)	77	44
Montauk	Patchogue	Montauk	61.4	11	64	27	ASC (410)	48	43

NOTES
[1] From May 2018 public timetables. Some revenue trains originate or terminate at stations on the segment other than the designated end of segment station.
[2] WkD – Week day Revenue Trains
[3] WkE – Weekend Revenue Trains
[A] Includes: LIRR Port Washington trains (103 WkD, 75 WkE) and Amtrak trains through Harold (40 WkD, 30 WkE)

LIRR Rolling Stock

LIRR rolling stock is composed of the following rolling stock:

Table Ex-3: Rolling Stock to Equip with ACSES

ACSES-Equipped LIRR Rolling Stock Types
DC electric M9 multiple units (MU) married pairs
DC electric M7 multiple units (MU) married pairs
DC electric M3 multiple units (MU) married pairs
MP15AC work locomotives
DE30 diesel electric locomotives
DM30 dual mode DC Electric / diesel locomotives
C-3 Cab Cars

All units where the brakes of a train are controlled from will have operative ACSES II equipment per 49 CFR Part 236, Subpart I when operating in PTC territory and will have successfully completed a departure test less than 24 hours from the time of departure from its initial terminal. En route failures of ACSES II equipment shall be reported and managed by operating rules that are compliant with §236.1029.

LIRR has 6 SW1001 (E10) switcher locomotives that are confined to yards and will therefore not be ACSES II equipped. Tenant rolling stock will be fully equipped for PTC compliance and interoperability before being permitted to operate on LIRR mainline trackage.

LIRR Mainline Track Exclusion Addendum (MTEA)

LIRR PTCIP[1] approved by the FRA under §236.1019 includes MTEAs listed and summarized below – see PTCIP section 13 for additional detail. LIRR's PTC systems enforce a maximum speed of 15 mph within MTEAs and protect the exit point of the MTEAs to protect against train-to-train collisions.

Table Ex-4: MTEA Classifications

Classification	Description
A.	Non-signaled Restricted Speed running track on which passenger trains operate.
B.	Non-Signaled main line with Manual Block rules on which passenger and non-passenger trains operate.
C.	Non-signaled passenger-train terminal with hand-operated switches. May include short running track between the End-of-Block sign and the station. The 15-mph Restricted Speed is and will be enforced.
D.	Signaled and interlocked 15-mph passenger-train terminal with 15-mph cab signaling enforced by ATC.

Table Ex-5: Listing of MTEAs

Type	MTEA Description/Trackage Location
A / LOE	Revenue passenger trains operating on bidirectional 15-mph maximum-speed non-signaled running tracks. LIRR LOEs include the following trackage based on 49 CFR 236.1019(c)(1): 1 Hunterspoint Avenue Lead Tracks 2 Belmont Race Lead Track
B / LOE	Revenue passenger trains and non-passenger trains operating on bidirectional track under Manual Block Rules. Temporal Separation pursuant to 40 CFR 236.1019(c)(ii) will be employed by LIRR to provide protection against train-to-train collisions of passenger and non-passenger trains. Risk Mitigation [236.1019(c)(iii)] includes PTC system overspeed enforcement, reported highway grade crossing failure restriction enforcement and DSIs and derails for protection of non-interlocked switches. LIRR LOEs include the following trackage: 1 Mainline from Ronkonkoma (KO) to Greenport (GY)
C / LOE	For non-signaled 15-mph (or less) terminals and terminal areas. LIRR LOEs include the following trackage based on 49 CFR 236.1019(c)(1). 1 Long Island City Station & Yard 2 Belmont Race Track Station & Yard 3 Long Beach Station & Yard 4 Far Rockaway Station & Yard 5 **Port Washington Station & Yard** 6 Hempstead Station & Yard 7 Oyster Bay Station & Yard 8 Port Jefferson Station & Yard 9 Montauk Station & Yard 10 Greenport Station & Yard
D / PTE	For signaled 15-mph (or less) terminals and terminal areas. LIRR PTEs include the following trackage based on 49 CFR 236.1019 (b) (1) (2) and (3): 1 Jamaica Passenger-only Zone 2 GCT Terminal & Interlocking (future) 3 Brook Interlocking 4 West Hempstead Station & Yard 5 Dunton Zone 15-mph
D / LOE	For signaled 15-mph (or less) terminals and terminal areas. LIRR LOE includes the following trackage based on 49 CFR 236.1019(c)(1): 1 Jamaica freight routes

Signal Territories and Rules

The following figures identifies the the signaling territories, interlockings, yards and applied signaling rules.



Figure Ex-2: LIRR Signal Territory Overview

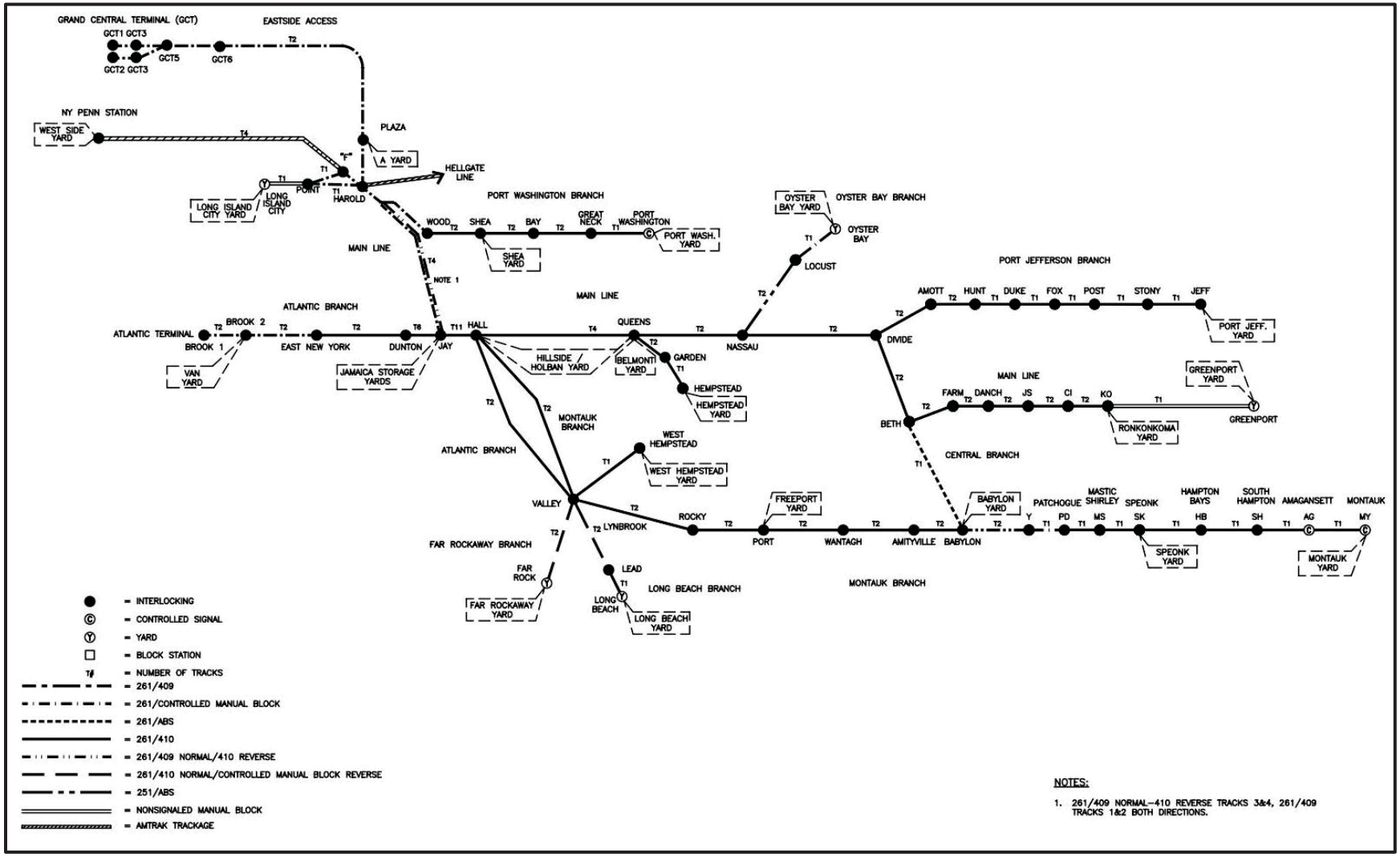


Figure Ex-3: Schematic Map of LIRR Mainline Territory

Tenants

LIRR has two tenants: New York & Atlantic Railway (NYAR) and Amtrak. New York and Atlantic Railway has operating agreements to operate freight trains over LIRR mainline trackage. Amtrak operates passenger and work trains through LIRR's Harold interlocking. All tenant trains operating in LIRR territory will be PTC compliant and interoperable with LIRR's PTC systems.

LIRR ACSES II System

Level 0 ACSES II System Block Diagram is depicted below.

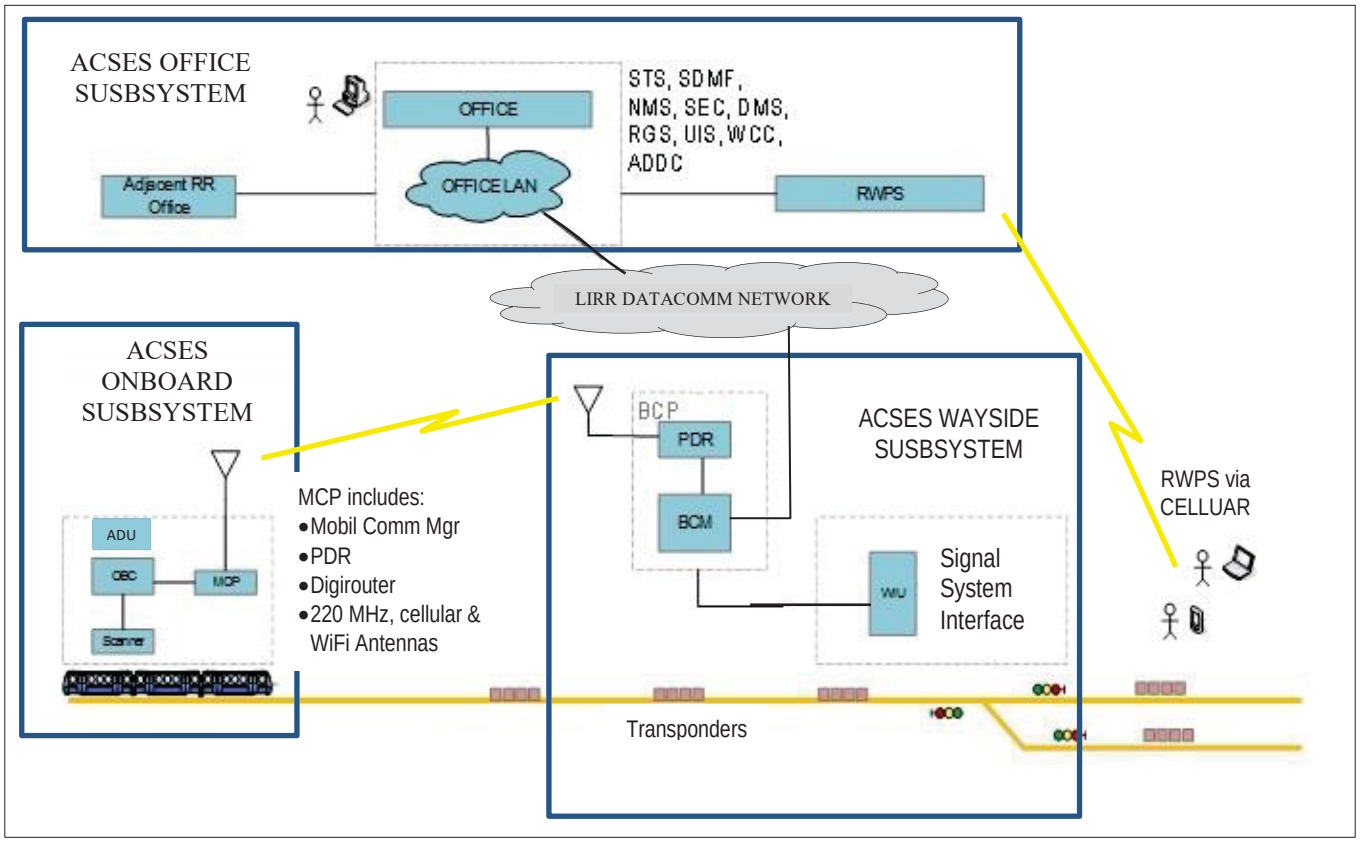


Figure Ex-4: Overview Block Diagram of ASCES II

The LIRR ACSES II System is made up of the following major subsystems and main components:

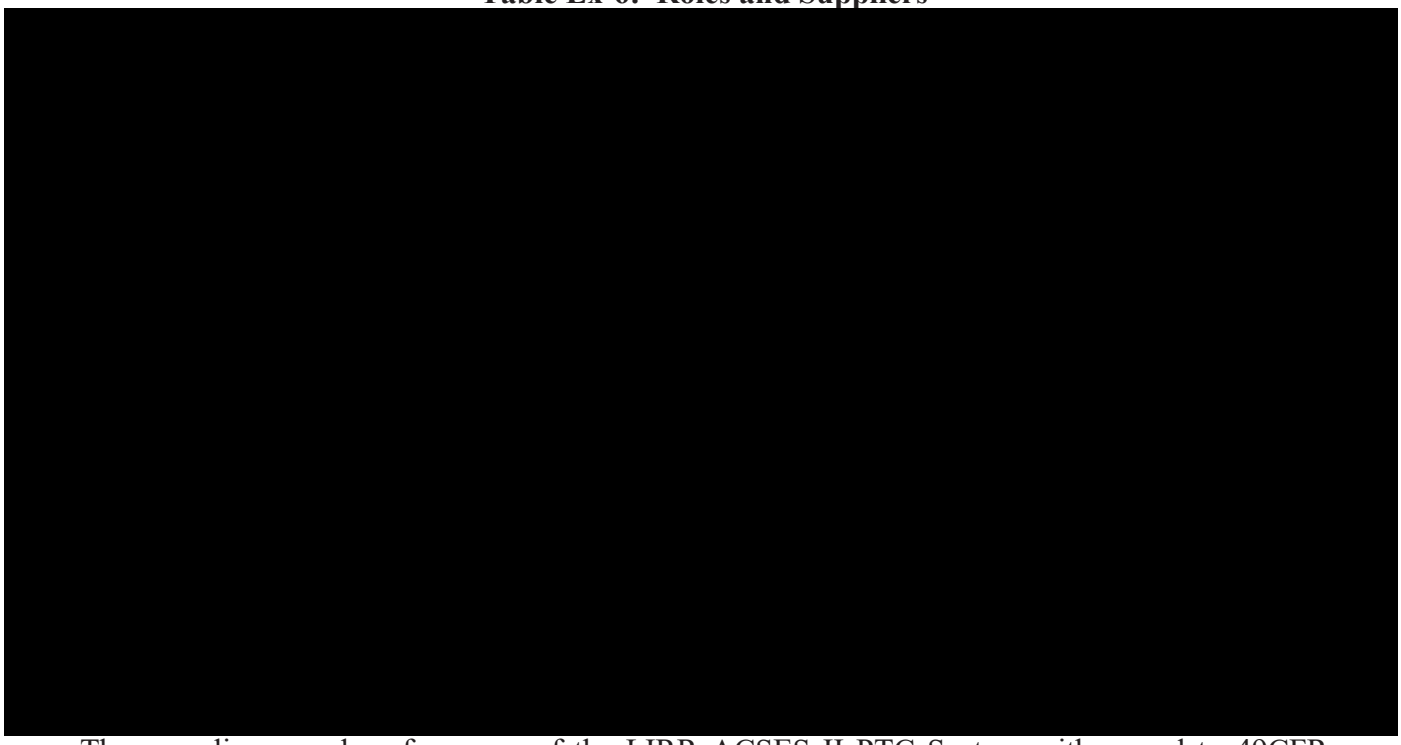
- **Onboard Subsystem**: Includes ACSES II Onboard Computer, Aspect Display Unit (ADU), CTV and Transponder Scanner, ATC Interfaces (AIU), Mobile Communications Manager (MCM).
- **Wayside/Signals Subsystem**: Includes Wayside Interface Units (WIUs) and WIU connectivity to ACSES networks, and Transponders.
- **Communications Subsystem:** Includes networks and network connectivity, Base Communications Packages, PTC Data Radios
- **Office Subsystem**: Includes Redundant Network, Safety TSR Server (STS), Software and Data Maintenance Facility (SDMF), Network Monitoring System (NMS), Active Directory

Domain Controller (ADDC), Security Server, Data and Maintenance System (DMS), Railroad Gateway Server (RGS), User Interface System (UIS), and Wayside Communication Controller (WCC).

- **RWPS Subsystem**: Includes RWPS Server, RWPS Workstations, Truck Mounted EIC Terminals, Handheld EIC Devices, Redundant Network, Network Monitoring System, Active Directory Domain Controller, Security Server, Data and Maintenance System.

A consortium of Bombardier Transportation (BT) and Siemens Rail Automation (SRA), with Wabtec as a communications subcontractor supplier, is designing and commissioning LIRR's ACSES II vital overlay to LIRR's existing signaling systems. The high level roles and scope of supply are listed below.

Table Ex-6: Roles and Suppliers



The compliance and performance of the LIRR ACSES II PTC System with regard to 49CFR §236Appendix C has been fully analyzed via the Risk Assessment included in **Attachment K** of this PTCSP and summarized in Section 11. As such, for each safety-critical function provided by the ACSES II PTC System, the following Appendix C Safety Principles have been addressed:

- System safety under normal operating conditions;
- System safety under failures;
- Closed loop principle;
- Safety assurance concepts;
- Human factor engineering principle;

[1] LIRR has conducted Safety Audits. The audits are on file.

- System safety under external influences; and,
- System safety after modifications.

As part of substantiating the designation of vital overlay PTC system, evidence is reviewable for Appendix C compliance verification for non-vitally implemented safety-critical functions as well.

The PTC system vitality is supported by the safety analysis and supporting documents contained in the pertinent References and Attachments.

The nominal entries in the System Hazard Log results are specifically being managed through the specification of safety requirements by the LIRR.

Table Ex-7: List of MTTHE Calculations



Section 7.3 of this PTCSP describes the manner by which the fulfillment of the FRA Rule is achieved by the ACSES II PTC System's design and implementation.

Functions List

The major PTC functions implemented by the existing LIRR signaling with ACSES II overlay are provided above at the start of section. The ACSES II Functions List is provided in table below. Each function is identified by one of four classifications:

1) Type Approved ACSES II used unmodified – **TA A2**
2) Type Approved ACSES II Modified – **TM**
3) Type Approved LIRR PTCDP – **TA DP**
4) Enhanced Train Control Function – **EF** (Enhancement of ACSES capabilities particular to the high-density commuter railroad application.)

Table Ex-8: ACSES Functions List

Function ID	ACSES II PTC Functionality	Approval Type
OBSx	**Onboard Specific functionality**	
OBS1	ACSES II Modes	TA A2
OBS2	Location Determination	TA A2
OBS3	Front of Train Offset by Direction	EF
OBS4	Distance Calculation	TA A2
OBS5	Wheel Diameters	TA A2
OBS6	Wheel Wear Compensation	TA A2
OBS7	Slip/Slide Compensation	TM
OBS8	Rollaway Protection	TA A2
OBS9	V-zero Determination	TA A2
OBS10	ATC Status	TA A2
OBS11	Cab Signal Failure Enforcement	TA A2
OBS13	Full Service Brake Application	TA A2
OBS14	Brake Curve Compensation	TM
OBS15	ACSES Brake Assurance	EF
TEIx	**Train Engineer Interface**	
TEI1	ACSES Display	TM
TEI3	Acknowledge	TA A2
TEI4	No TSR Data Status	TA A2
TEI5	No Transponder Status	TM
TEI6	ACSES Status	TM
TEI7	ATC Status	TM
TEI8	Absolute Stop Bypass Pushbutton	TA A2
DTx	**Departure Testing**	
DT1	Departure Test	TM
DT2	Radio Transmission Departure Test	EF
IPRx	**Interlocking Protection**	

Table Ex-8: ACSES Functions List

Function ID	ACSES II PTC Functionality	Approval Type
IPR1	PTS Enforcement	TM
IPR2	LoMA	TM
IPR13	Line Boundaries	EF
IPR4	PTSO	TA A2
IPR6	C Signal Function	TA A2
IPR7	Interlocking Exit determination	TM
IPR8	ACSES II Terminate 15 MPH ASB enforcement when TP missed	EF
IPR11	Stopping Accurately at Stations Close to HS	EF
IPR12	ACSES II 8 Track Limit	TM
RCx	**Wireless Communications**	
RC1	220 MHz Data Radio Transmission	TM
RC3	220 MHz Data Radio	EF
RC5	TDMA Radio Messaging	EF
RC9	OBC Location Report to MCM	EF
RC10	Report Train Distance to Home Signal	EF
RC12	Data Radio Termination	TM
RC13	BCP Interlocking Configurations	EF
RC14	Nested ILKs with Different Radio Channels	EF
RC15	Cellular	EF
TSRMx	**Temporary Speed Restriction**	
TSRM1	User Input to Safety TSR Server	TM
TSRM4	TSR Select-Check-Execute	TM
TSRM5	TSR List Management	TM
TSRM6	Memorize A TSR in TSR List	TA A2
TSRM7	Delete A TSR from TSR List	TA A2
TSRM8	Approve TSR	TA A2
TSRM10	Output TSR List	TM
TSRM11	TSRs Through Junctions	EF
TSRM12	Shadow (Duplicate) TSRs	TM
TSRM13	Railroad Gateway Server	EF
TSRM15	Increase OBC TSR Storage	TM
TSRM18	Multi-STS Segment Control	EF
TSRM19	TSR Data Request (preload)	TM
TSRM20	Announced Line Boundary	EF
SENx	**Speed Enforcement**	
SEN1	Vitally Encoded Transponder data	TA A2
SEN2	Onboard Read of TP Data	TA A2
SEN3	Alert Curve	TA A2
SEN4	MAS Enforcement	TA A2

Table Ex-8: ACSES Functions List

Function ID	ACSES II PTC Functionality	Approval Type
SEN5	PSR Enforcement	TA A2
SEN6	TSR Enforcement	TM
SEN8	"0" Speed TSR	TM
SEN9	Stop & Release TSR	TM
SEN10	Interlocking PSR	TA A2
SEN11	Route Dependent Speed Restriction	TA A2
SEN13	Route Dependent PTS	EF
TBNCx	**Territory Boundaries & Non-PTC territories**	
TBNC1	Yard & Siding Entry Protection	TM
TBNC2	PTS Enforcement at ABS/CMB Signals w/o cab signaling	TA DP
TBNC3	MTEA	EF
TBNC4	Protection of MTEA Boundaries	EF
TBNC5	Exiting ACSES Territory	TM
DIAGx	**Diagnostics**	
DIAG1	Maintenance and Error Messages	TM
DIAG2	OBC Event Logging	TM
DIAG3	DMS Event Logging	TM
DIAG4	Network Management System	TM
DIAG5	Event Recorder Memory Module	EF
DIAG9	OBC Remote Diagnostics	EF
MISCx	**Additional System**	
MISC1	Configuration Management	EF
MISC2	System Initialization	TM
MISC3	Security	EF
MISC4	ADDC and Single Sign-on	EF
RWPx	**Roadway Worker Protection System**	
RWP1	Roadway Worker Protection System	TA DP

Database Engineering

The LIRR ACSES II topographic database used for the transponders layout and programming, STS database, and WIU route elements are built and output with a CENELEC T3 certified software development tool for database engineering known as SDMT. Database changes implemented during system implementation and future life-cycle maintenance, such as modification for infrastructure changes are implemented through the SDMT tool in the Software Data Maintenance Facility (SDMF). The work is conducted per the railroad's Configuration Management Plan and under oversight of a Configuration Manager.

Configuration Management

LIRR has two relevant Configuration Management Plans (CMP) for controlling versions of hardware and software:

1) The System Integrator's CMP for controlling versions of hardware and software from the Design phase through all phases of testing and commissioning - see Section 17 of this PTCSP for the governing CMP during development and implementation.
2) LIRR has developed its own Configuration Management Plan and established a Configuration Manager position (and have filled the position) for controlling software and hardware versions and modifications during the operation and maintenance phase of the ACSES II System - see Section 17 of this PTCSP.

All ACSES II system changes are approved by a Change Control Board (CCB) consisting of the relevant departments of the railroad and the SI. In addition to the CCB, the railroad calls a System Safety Control Board (SSCB) whenever changes occur in safety-critical software.

Variances to Type Approvals

Amtrak FRA-TA-2010-00 ACSES II

In its application of the Amtrak Type Approval, LIRR's ACSES II system incorporates the variances identified in the Table below (see **Table Ex-9** and for descriptions)

Table Ex-9: Type Approval FRA-TA-2010-001 Variances

Variance #	Type Approved Item	Variance Item
1	Ansaldo Transponder	Bombardier Transponder
2	No TSR data light only illuminated without a TSR List	No TSR Light plus Alternating Dash-Dash Rate on ADU without a TSR List
3	New Siemens ADU	LIRR-specific Siemens ADU configuration
4	220 MHz Radio migration, Updated Siemens OBC. New Lilee MCM, BRCM for data radio message management	Updated 220 MHz radio and updated Siemens OBC. Wabtec MCM and BCM for data radio message management
5	New Alstom WIU and Lilee BCM	New Siemens WIU & Wabtec BCM
6	Amtrak STS, D&MS, OCM and datacomm. Network	Bombardier STS, COTS D&MS, Wabtec WCC (OCM) and LIRR datacomm network

Table Ex-10: Type Approval FRA-TA-2010-001 LIRR Variances

Variance #	Type Approved Item	Variance Item
1	Vzero detection at 3 mph to 5 mph depending on vehicle type	Vzero reduced to under 1.0 mph for all vehicle types
2	ACSES II miss PTS and/or TSR enforcement in some complex	RD-PTS and ALB functionality added as necessary B2B configurations.

Table Ex-10: Type Approval FRA-TA-2010-001 LIRR Variances

Variance #	Type Approved Item	Variance Item
	multi-interlocking configurations without pocket tracks between the interlockings (referred to as Back-to-Back Interlocking [B2B])	
3	In close transponder set configurations, ACSES II could incorrectly transponder data due to processing delays, referred to as TP out of order.	Corrected
4	No over-the-air cryptic security	Over-the-air cryptic security added
5	No cross-railroad boundary TSR enforcement (interoperability)	Cross-railroad boundary TSR enforcement (interoperability)
6	Protection of trains turning back when a train run terminates on the mainline and a new train run originates in the opposite direction.	Turnback added to enforce a stop until safe to move in the opposite direction
7	Protection of Highway Crossings with credible reports of activation failures not provided	Stop and Release TSR added providing ACSES enforcement of trains stopping prior to the edge of road, required Engineer acknowledgment of the stop to advance the train to and over the road, and speed restriction enforcement across the road.

It should be noted that variance 5 is not currently released and is still ongoing development and testing but will be implemented.

LIRR Type Approval FRA-TA-2013-04

No variances are requested for LIRR's Type Approval using ACSES in conjunction with non-ASC ABS and CMB wayside signaling.

Testing Program

The ACSES test program includes factory testing conducted at the contractor's facilities and field testing on LIRR – see Section 18 of this PTCSP for detail on the testing program and test records. All test reports are available to the FRA upon request. Test cases are tracked by the Contractor in their RQM database tool. Test procedures and test cases are traced to requirements within the

Requirements Traceability Matrix (RTM) at both the System Level (SLR) and Subsystem Level (SSLR) from Rational Quality Manager (RQM) to Dynamic Object Oriented Requirements System (DOORS) (the contractor's requirements tracking tool).

A FRACAS (Failure Reporting Analysis and Corrective Action System) has been implemented to track variances and corrections. Change Control Boards are activated to control and approve all changes during development and testing of the system.

Database data engineering processes are audited for conformance with approved practices.

LIRR PTC test program has been engaged in factory and field testing since 2nd quarter of 2017. Field testing on pilot lines is conducted under LIRR's FRA-approved test waiver[7]. LIRR has met the 19 conditions set out in the test waiver in the conduct of the field testing.

The main elements of testing underway are identified in the table below. The table aligns LIRR test program elements with the FRA recommended test program.

Table Ex-11: Summary Test Program

	LIRR Test Type	FRA Testing Terminology	Brief Description
Factory Tests	Factory Acceptance Tests (FAT)	Laboratory Segment Testing	Each of the subsystems are tested for functions and performance. External interfaces are emulated with simulators and test tools.
	Factory Integrated System Test (IST)	Laboratory Integration Testing	Subsystems are interconnected and all functions are demonstrated. System performance and stress testing are conducted. Unstructured tests are also performed. External simulators are used to represent the external interfaces. A 96 hour stability test is conducted after the IST.
	Database Safety Verification	Laboratory Track Database Validation	The topographic database is checked first as an engineering process and then after input to the database tool as outputs of the tool. All devices, topographic features, stationing, grades, etc. are checked; naming conventions validated with Transportation.
Field Tests	SPT Database verification	Field WIU Validation, Field Critical Feature Validation	The database is V&V'd in the field with test train operation and measurements.
	Site Installation Tests (SIT)	Field WIU Validation	Each Wayside and office location and devices at the location including WIUs, Radios, Comm Cases, Office cabinets, and remote workstations get a Post Installation Check Out (PICO) for proper installation, power up, and proof of connectivity.
	Site Performance Tests (SPT).	Field Integration Testing (FIT), Field Brake Testing	System functions are demonstrated in the field including PTS, MAS, PSR, and TSR enforcement and their application to PTC compliance. Prior to SPT each wayside location undergoes Site Installation Test (SIT). Each test vehicle undergoes static and dynamic tests.
	Site Integration System Test (SIST) Part 1Repeatability Part 2 Integration	Field Qualification Testing (FQT)	Part 1: quantity of repetitions of critical functions necessary to achieve a 95% confidence level. Includes the Critical Function Repeatability Analysis assessing the necessary quantities Part 2: Fully connected and operational system level load and performance testing is conducted.
	Site Installation Tests: Rolling Stock Static Tests	Field Locomotive Post-Installation Testing	All rolling stock installations are checked in the shop with a PICO test and departure test.
	Rolling Stock Dynamic Tests (pre-SPT)	Field Locomotive Class/Interface Testing	All rolling stock performance are tested dynamically on a test track to verify proper reading of transponders, data radio communications between train and wayside, and Positive Stop enforcement.
	Availability/Reliability Demonstration	No Equivalent	Minimum 24 month period of reliability/availability analysis of full system operation. System maintainability is also demonstrated.

Regression Testing

Regression testing has been integral to the development of the ACSES system. Regression tests are conducted following any modification to the hardware or software subsequent to formal testing. For each modification, an analysis is performed to determine the scope of the regression testing based on the change being implemented. The regression test documentation captures the test cases and procedures that must be rerun to properly verify that the modifications achieved their intended purpose and no unintended consequences resulted. This testing is performed during the Site Update Period (SUP) of the testing program.

Each FAT Plan (System and subsystem) must identify the test cases that are necessary as part of any regression test activity. These tests are those that test the fundamental functionality of the system that provide the full PTC regulatory compliance. .

Retesting is performed as deemed necessary by the Change Control Board (CCB) to any portion of the ACSES II system, including that which has been accepted by the Engineer, due to changes or additions to the Master Test Plan, test specific Test plans, or any test procedure documentation. Regression testing has been performed as necessary through the life of the system through the end of warranty and transfer of ownership.

Failure Reporting Analysis and Corrective Action System (FRACAS)

Corrective actions to the ACSES II system that arise as a result of failures witnessed during system testing are managed under the FRACAS process implemented during the system life-cycle. The FRACAS Process Map is depicted in the following figure. All variances are input to Rational Team Concert tool and are available to the FRA upon request. FRACAS provides data for the Availability, Reliability, and Maintainability calculations.

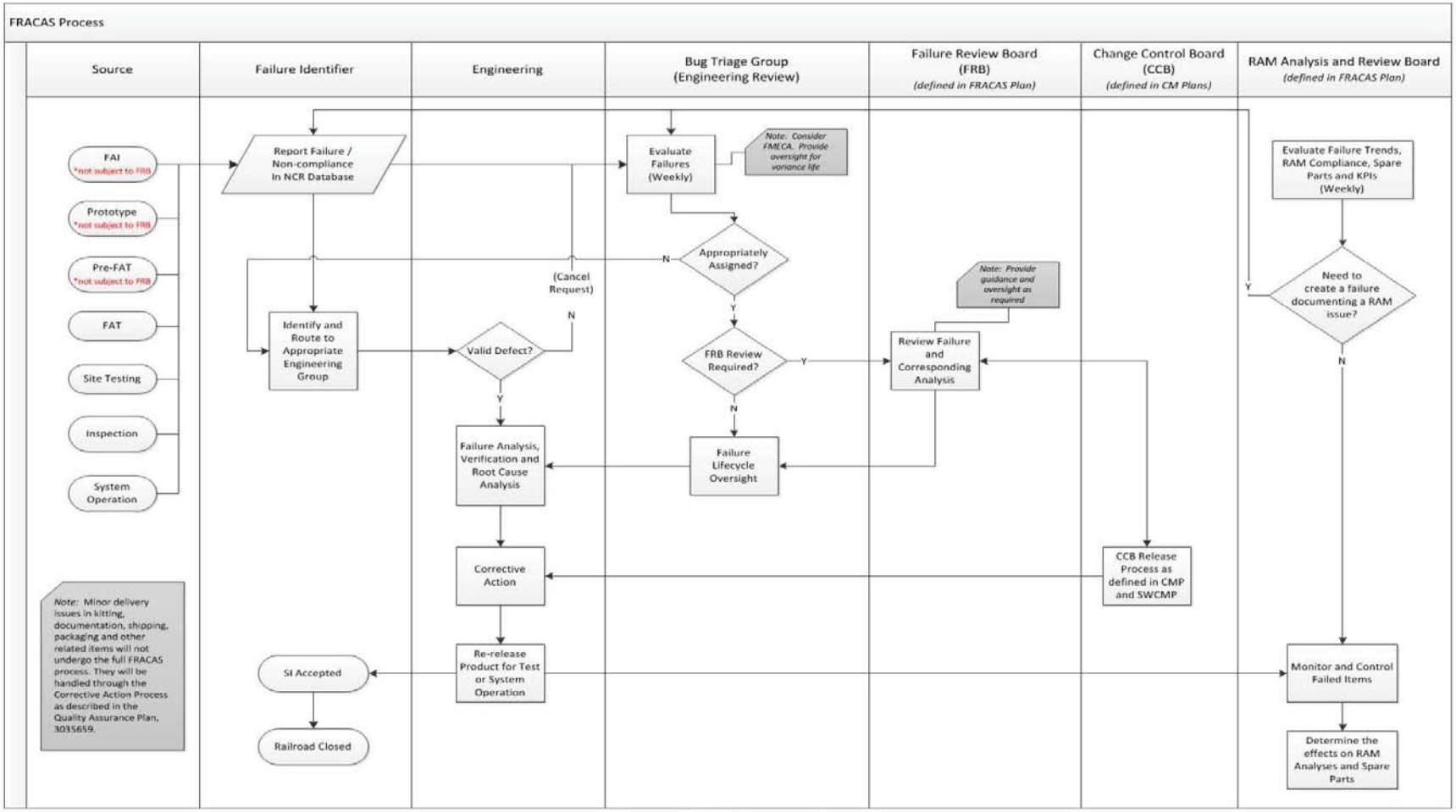


Figure Ex-5: FRACAS Process Map

Penn Station, NY through Harold Interlocking

LIRR operates over Amtrak territory from LIRR's Harold interlocking to and from Amtrak's Penn Station, NY. The territory is dispatched from Amtrak's Penn Station Central Control (PSCC) under joint operating agreement with LIRR. The boundaries between LIRR's Harold interlocking and Amtrak's adjacent territory are extremely complex – see figure below.

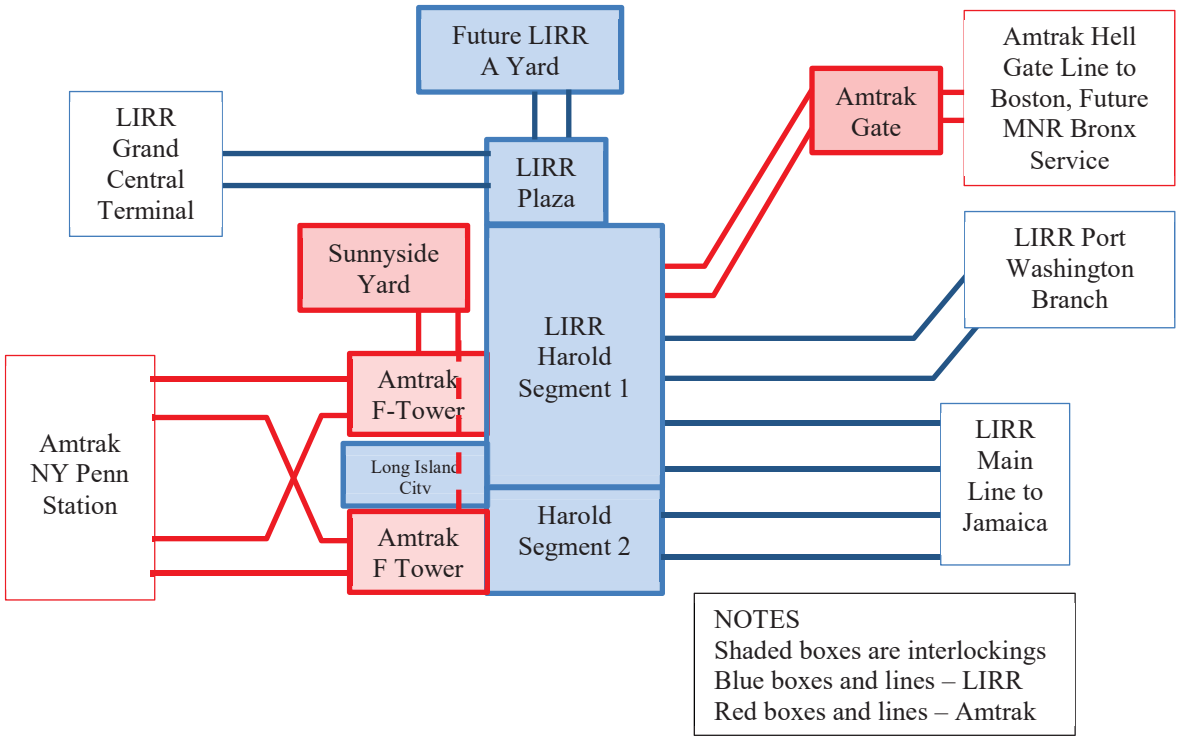


Figure Ex-6: Amtrak / LIRR Joint Operating Territory

The lowest risk systems engineering solution for implementation of ACSES II in the joint operating territory was determined to be incorporation of the Amtrak territory into the LIRR Safety TSR Server (STS). This approach greatly reduces the line segment boundaries in the congested areas and reduces the disparate supplier STS interfaces between the railroads; LIRR's STS being form Bombardier and Amtrak's from Hitachi. All trains operating through the territory will receive TSRs from the LIRR STS. Dispatchers controlling the territory will input TSRs to the LIRR STS.

Operations and Maintenance of ACSES II

LIRR has included as attached to this PTCSP an Operations and Maintenance Procedures and Documentation Manual – see Section 15 of this PTCSP. Key LIRR users of the ACSES II system include:

- Transportation Supervisors, Train Dispatchers, Approvers and Tower Operators.
- Train Engineers.

- Maintenance of Equipment personnel.
- Engineering personnel.
- Configuration Manager

Train Crews

All LIRR trains have a Train Engineer who operates the train, and a Conductor and Assistant Conductors as-required, who are responsible for the safe movement of the train, fare collection and on-board customer service. In addition, a train may have one or more assistant conductors to assist with fare collection and other duties. Passenger trains on LIRR are operated by a one-person crew in the cab of locomotives, MU units, and cab cars. The train conductor is physically located in the passenger coaches of the trains. Freight and work trains operate with two crew members in the lead locomotive.

TSR Application and Annulment

The application of TSRs via the ACSES II system includes a Select-Check-Execute (SCE) process. Annulment of TSRs implemented in ACSES II uses the same SCE process. The SCE process requires independent approval of TSRs, i.e., an Authorized User selecting application or annulment of a TSR **cannot also Execute** any TSR operation they selected. The Execute element of the TSR process must be by a different Authorized User.

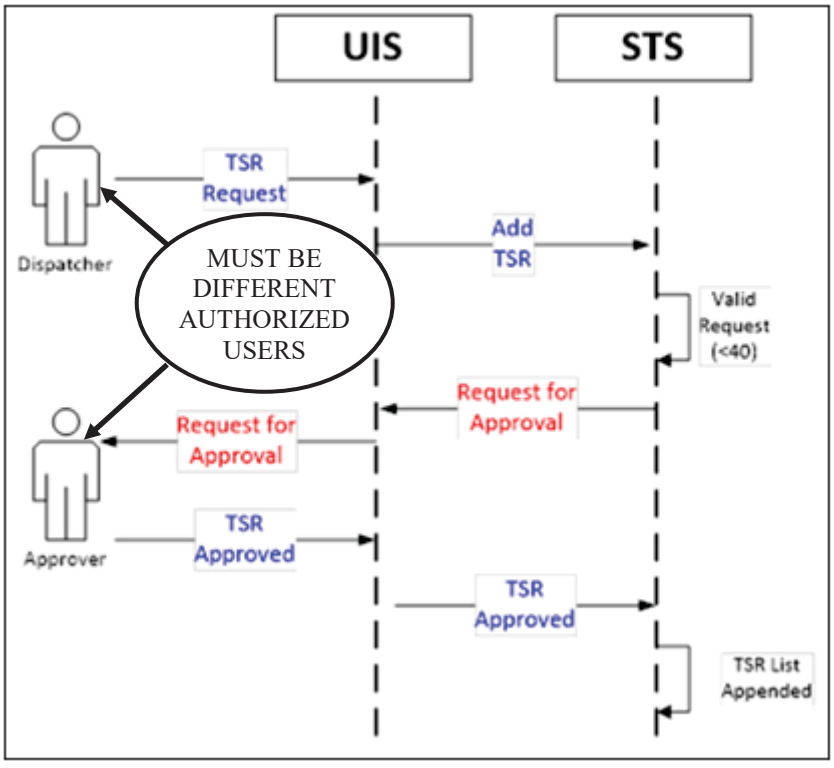


Figure Ex-7: Select-Check-Execute Process, TSR Request (Same for Annulment)

ACSES Dispatchers and Transportation Supervisors utilize the ACSES User Interface System (UIS) workstations to implement and annual TSRs.

Roadway Workers In-Charge (RWIC) will be able to use handheld terminals at work zone locations to implement TSRs for their work zones. RWPS utilizes the ACSES II SCE process for TSR application and annulment with a difference being that the Select portion originates in the RWPS terminal. Also, ACSES II prevents initiation of annulment of a TSR that was implemented by a RWIC using their RWPS terminal by anyone except the RWIC of the work zone.

RWPS also permits protection of secondary work crews within an established work zone and prevents removal of the protecting TSR until all secondary crews are reported clear.

Training

The LIRR SI has developed a comprehensive training curriculum for life-cycle maintenance of the ACSES II system hardware and software modifications – see The Training Section 14 of this PTCSP. The Training Program is based on Train-the-Trainer concept in which LIRR trainers are trained to conduct the training of Transportation and Maintenance Department personnel to operate and provide lifecycle maintenance of the ACSES II system. A complete set of Training Manuals is part of the training Program. All Training Manuals are available for review upon request.

As the workforce changes through normal attrition, new employees receive PTC training as part of their job training. When changes are made to the signal system or any work takes place which affects the PTC system, the PTC changes are coordinated as part of the signal cutover or as part of the modifications to the infrastructure. The PTC changes are implemented when modified track is returned to service.

Operating Rules

LIRR has supplemented its operating rules for en route ATC failures to also include en route failures of onboard ACSES II equipment in compliance with §236.1029. LIRR Rules of the Transportation Department are available upon request.

In addition a Service Restoration Plan has been implemented – see the Section 27.3 of this PTCSP.

Maintenance of ACSES II

LIRR has developed a Maintenance Concepts Document that allocates to maintenance departments the ACSES II equipment and subsystems. The Maintenance Concepts Document is available for FRA review upon request. The high level allocation is represented in the figure below.

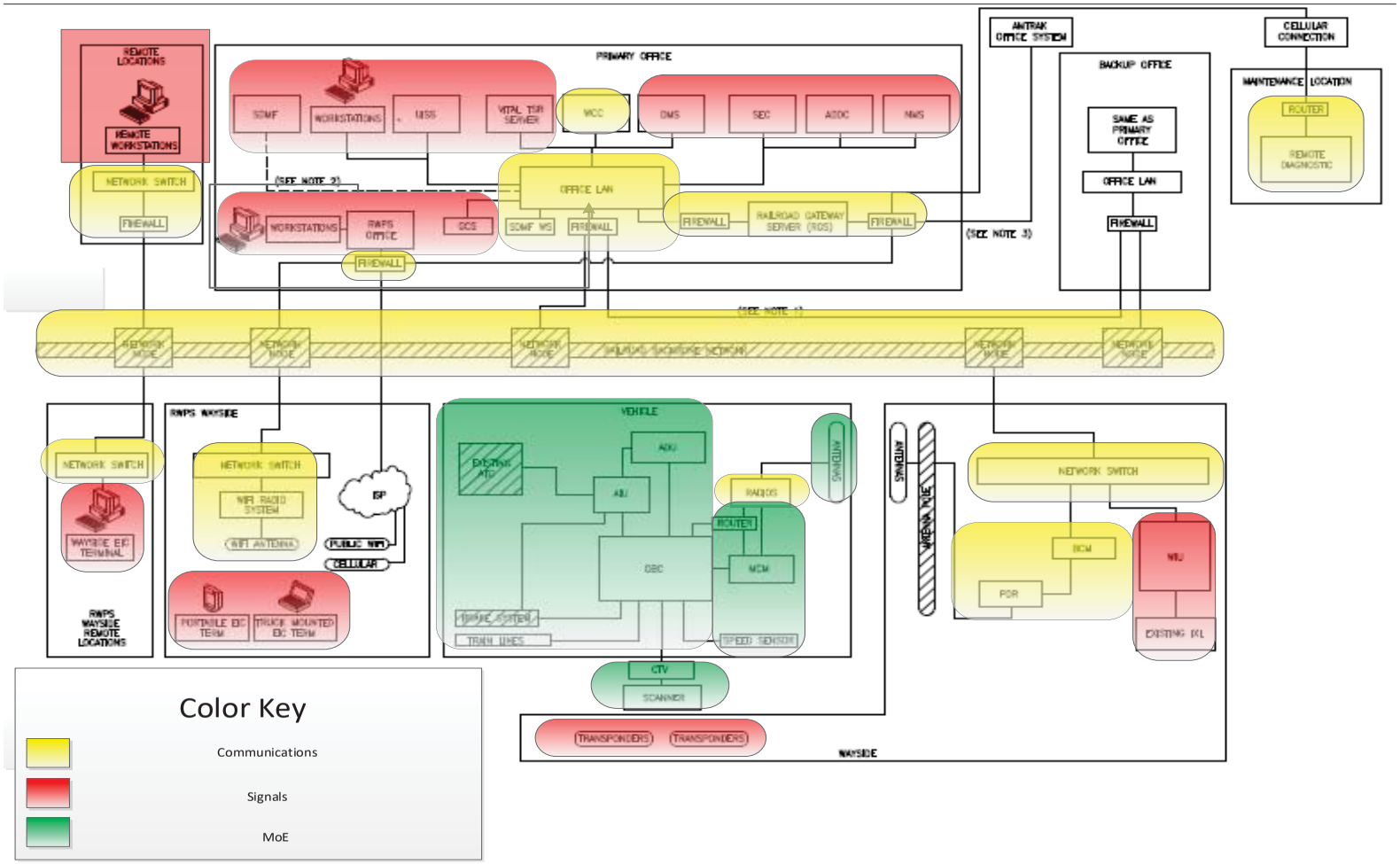


Figure Ex-8: Allocation of ACSES II Components to LIRR Maintenance Departments

[redacted]

[redacted]

4 Attachment B – PTCSP Documents

Attachment ID	Document Name	Document ID	Revision
B	System Final Safety Report	3035838	_F
C	Transponder Final Safety Report	3037458	_B
D	WIU Final Safety Report	3037456	_A
E	Office Final Safety Report	3037452	_E
F	Onboard Final Safety Report	3051179	_V
G	Comms Final Safety Report	3037454	__
H	RWPS Finals Safety Report	3037460	_A
I	System Database Safety Verification Report	3035832	_C
J	System Hazard Log	3035819	_N
K	System Risk Assessment	3155231	__
L	System Operating Hazard Analysis (OHA)	3035826	_C
M	System Hazard Analysis	3035823	_A
N	System Interface Hazard Analysis	3035828	_D
O	System Fault Tree Analysis	3035830	_E
P	System Preliminary Hazard Analysis (PHA)	3035821	_D
Q	System Operations and Maintenance Manual	(LIRR Operation and Maintenance Manual.PDF	1.0
R	System Warnings and Labels Description Document	(LIRR System Warnings and Labels Description.pdf)	0.1
S	RWPS Subsystem Design Description (SDD)	3035851	_C
T	RWPS System Safety Concept Document	3036417	_C
U	RWPS Operating Hazard Analysis	3037424	_A
V	RWPS Preliminary Hazard Analysis	3036416	_D
W	RWPS Subsystem Hazard Analysis (SSHA)	3037395	__

X	RWPS Interface Hazard Analysis	3037436	_C
Y	RWPS Work Zone Safety Analysis	(Work Zone Incursion.pdf)	15 Aug 2019
Z	System Vulnerability Assessment	3035840	_F
AA	Site Security Control Plan	3035470	_A
BB	Security Management Plan	S-L 0530	April 2019
CC	LIRR Communication Security Addendum	3041191	_B
DD	PTC Restoration Plan (Service and Communications)	(PTC Restoration Plan.pdf)	0.1

Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

System
Final Safety Report
CDRL 2-136-20

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	PM	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Jason Weighley Safety Engineer		Jason W Weighley 2019.07.18 10:24:39 -04'00'
Verified:	Aaron Graham Safety Engineer		Aaron Graham 2019.07.18 10:27:25 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.07.22 12:20:04 -04'00'
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group		Phil Magloire 2019.07.18 14:22:47 -04'00'
BT/SRA Review:	NA Title		
BT/SRA Review:	NA Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3035838

Effective Date:	Revision:	Language:
2019-07-18	_F	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
Draft	2017-05-19	First issue
__ Draft 1	2017-05-22	Second Draft
_ Draft.2	2017-05-24	Third Draft _ Split Test Track details to separate document.
Draft 3	2017-05-25	Fourth Draft
Draft.4	2017-05-25	Fifth Draft – Update of PW Transponder Test Reports and OBC Statements
__	2017_05-26	First Release
_A	2018-11-21	System Baseline 3.2 - RSD
_B	2018-12-06	System Baseline 3.3.2 - RSD
_B1	2019-02-28	System Baseline 3.4 - RSD
_C	2019-03-07	System Baseline 3.4 – RSD Final
_D	2019-03-27	Updated to Resolve SCCB commnets on Baseline and 3.4 and respond to comments from SI-RVVW-0774
_E	2019-06-06	System Baseline 3.5 - RSD
_F	2019-07-18	Updated for PTCSP comments still basline 3.5

Table of Contents

Section	Subject	Page
1	**Executive Summary**	7
1.1	**Changes From Prior Revision**	7
2	**Introduction**	7
2.1.1	Office Subsystem	8
2.1.2	Onboard Subsystem	8
2.1.3	Wayside Subsystem	9
2.1.4	Communication Subsystem	9
2.1.5	Roadway Worker Protection Subsystem	10
2.2	**System Interfaces**	10
2.2.1	External Interface to the System	10
2.2.2	Internal Interface to the System	11
2.2.2.1	Onboard Subsystem	11
2.2.2.2	Wayside Interface Unit Subsystem	12
2.2.2.3	Office Subsystem	12
2.2.2.4	Transponder Subsystem	12
2.2.2.5	Communications Subsystem	12
2.2.2.6	RWPS Subsystem	12
2.3	**System Functions**	13
2.3.1	Office Subsystem	13
2.3.1.1	Safety TSR Server (STS)	13
2.3.1.2	Data & Maintenance System (DMS)	13
2.3.1.3	Network Management System (NMS)	14
2.3.1.4	Wayside Communication Controller (WCC)	14
2.3.1.5	User Interface System Server	14
2.3.1.6	Security Server (SEC)	15
2.3.1.7	Railroad Gateway Server (RGS)	15
2.3.1.8	Active Directory Domain Controller (ADDC)	15
2.3.2	Roadway Worker Protection System	15
2.3.3	On Board	15
2.3.3.1	Onboard ACSES II Computer	15
2.3.3.2	Transponder Scanner and CTV Antenna Interface	16
2.3.3.3	Aspect Display Unit	17
2.3.3.4	Speed Sensor Units	17
2.3.3.5	Vital Interface to the ATC	17
2.3.3.6	AIU	17
2.3.3.7	Decelerometer	17
2.3.3.8	Event Recorder Unit	18
2.3.4	Wayside Subsystem	18
2.3.4.1	Wayside Interface Unit (WIU)	18
2.3.4.2	Passive Transponders	18
2.3.5	Communication Subsystem	18
2.3.5.1	Base Communication Package	18
2.3.5.2	Mobile Communication Manager	19

2.3.6 System Database 19
2.4 Compliance Matrix 21
2.5 Reference Documents 25
2.6 Glossary 27
3 Summary of Safety Analysis and Evidences 28
3.1 System Hazard Analysis 29
3.1.1 Closure of all Hazards 29
3.2 Fault Tree Analysis 29
3.3 Operation Hazard Analysis 30
3.4 Interface Hazard Analysis 30
3.5 System Configuration 30
3.6 Subsystem Final Safety Reports 31
3.6.1 Onboard Final Safety Report 31
3.6.2 Office Final Safety Report 33
3.6.3 Communication Final Safety Report 35
3.6.4 WIU Final Safety Report 35
3.6.5 Transponder Final Safety Report 35
3.6.6 RWPS Final Safety Report 36
3.6.7 Database Safety and Verification Report 36
3.7 System Integration Test Reports 39
3.7.1 LIRR Factory Integration Test Report 39
3.7.2 SPT Site Integration Test Reports 40
3.7.2.1 SPT Vehicle Qualification Test Report 40
3.7.2.2 SPT Communication Qualification Test Report 40
3.7.2.3 Interlocking Status and Control Test Report 40
3.7.2.4 Pilot Line 1 Database Verification Test Report 40
3.7.2.5 Pilot Line 2 Database Verification Test Report 40
3.7.2.6 SPT Temporary Speed Restriction Test Report 40
3.7.2.7 SPT Integrated System Test Report 40
3.7.3 SUP 3.1 Site Integration Test Reports 41
3.7.3.1 SUP 3.1 Pilot Line 1 Database Verification Test Report 41
3.7.3.2 SUP 3.1Pilot Line 2 Database Verification Test Report 41
3.7.4 SUP 3.2 Site Integration Test Reports 41
3.7.4.1 SUP 3.2 Vehicle Qualification Test Report 41
3.7.4.2 SUP 3.2 Communication Qualification Test Report 41
3.7.4.3 SUP 3.2 Interlocking Status and Control Test Report 41
3.7.4.4 SUP 3.2 Pilot Line 1 Database Verification Test Report 41
3.7.4.5 SUP 3.2 Pilot Line 2 Database Verification Test Report 42
3.7.4.6 SUP 3,2 Temporary Speed Restriction Test Report 42
3.7.4.7 SUP 3.2 Integrated System Test Report 42
3.7.5 Office Factory Integration Testing 42
3.7.6 SUP Baseline 3.4 Testing 42
3.7.6.1 SUP 3.4 Vehicle Qualification Test Report 42
3.7.6.2 SUP 3.4 Communication Qualification Test Report 42

3.7.6.3 SUP 3.4 Interlocking Status and Control Test Report 43
3.7.6.4 SUP 3.4 Pilot Line 1 Database Verification Test Report 43
3.7.6.5 SUP 3.4 Pilot Line 2 Database Verification Test Report 43
3.7.6.6 SUP 3.4 Temporary Speed Restriction Test Report 43
3.7.6.7 SUP 3.4 Integrated System Test Report 43
3.7.7 SUP Baseline 3.5 Testing 43
3.7.7.1 SUP Baseline 3.5 Interlocking Status and Control Test Report 43
3.7.7.2 SUP Baseline 3.5 Temporary Speed Restriction Test Report 43
3.7.7.3 SUP Baseline 3.5 Integrated System Test Report 44

3.8 System Verification and Validation 44
3.8.1 System SVVR 44
3.8.2 Onboard SVVR 44
3.8.3 WIU SVVR 44
3.8.4 Office SVVR 45
3.8.5 Transponder Validation 45
3.8.6 RWPS SVVR 45
3.8.7 Communication Subsystem SVVR 45
3.8.8 System Database and Safety Verification Report 45

4 Calculation of MTTHE 45

5 Safety Certification Process 46

5.1 Safety RTM 46

5.2 Remaining Open Items 47
5.2.1 Remaining NCR 47
5.2.2 Remaining Variances 47
5.2.3 Restrictions to Mitigate Open Items 50
5.2.4 Schedule to Remove Restrictions 54

6 Conclusion 54

6.1 Limitations From the PVI 54

7 Attachment A - List of Remaining Variances 55

8 Attachment B - List of Open NCR 56

List of Figures

Figure 1: PTC ACSES II System Architecture 8
Figure 2: Database Generation and Maintenance Process 21

List of Tables

Table 1: List of ACSES II External elements 10
Table 2: Compliance Matrix 21
Table 3: Reference Documents 25

Table 4: Terms Specific to this Document 28
Table 5: Acronyms Specific to this Document 28
Table 6 Safety CDRL Status 28
Table 7 Office Variances 34
Table 8 Transponder List of Open Variance 36
Table 9: NCRs from Verified Reports 37
Table 10: Variances from Verified Reports 37

1 Executive Summary

The System Final Safety Report documents the closure of all hazards assigned to the ACSES System and evidence of closure of all assigned safety requirements to the ACSES system.

This revision of the Final Safety report is to authorize revenue service demonstration (RSD) on the Pilot Line 1 and 2 with System Baseline 3.5. Factory Testing, SUP Testing Evidence, OBC Safety Report and Office Safety reports updated to allow this.

1.1 Changes From Prior Revision

This revision of the document Updates Variance and NCR Lists to show the full list of variances and NCRs for the system. It also corrects the listing of Safety Critical variances as reviewed in the SCCB.

2 Introduction

Long Island Rail Road (LIRR) is implementing supplemental Positive Train Control (PTC) ACSES II system capabilities to their existing train control and signaling systems. In this regard, the protection afforded for the trains, Office, Communication and wayside equipment are accomplished by a cooperative operational design between ACSES II and the existing train control system.

The LIRR ACSES II enforces positive stop at home signals and enforces permanent and temporary speed restrictions. ACSES II uses data obtained from passive track-mounted transponders and a data radio to impose permanent and temporary speed limits. The Onboard System responds to data acquired from transponders and through the data radios. The Onboard System calculates a speed profile for both warning and enforcement from the track profile and vehicle performance characteristics.

The ACSES II System Architecture for LIRR can be divided into equipment systems, such as:

- Office Subsystem (STS vital component)
- Onboard Subsystem (OBC/AIU vital component)
- Wayside Subsystem
    - Transponder Subsystem
    - WIU Subsystem (vital component)
- Communication Subsystem
- RWPS Subsystem

Since all these subsystems are already in use for the existing ASC system, except for the STS, Transponder and RWPS subsystems, the system implementation requires updates/development to support PTC ACSES II System functionalities. Each subsystem, Office, Onboard, Wayside, Transponder, Communication and RWPS project team shall produce a Subsystem Product Safety Plan to produce a comprehensive set of Subsystem Safety Reports which then will be used to develop the overall PTC ACSES II System Product Safety Report.

The ACSES II system basic architecture and interfaces between the subsystems is presented in Figure 1 below. The System Architecture Drawing Package defines the formal architecture of ACSES II for LIRR. The system design is documented by the System Design Description.

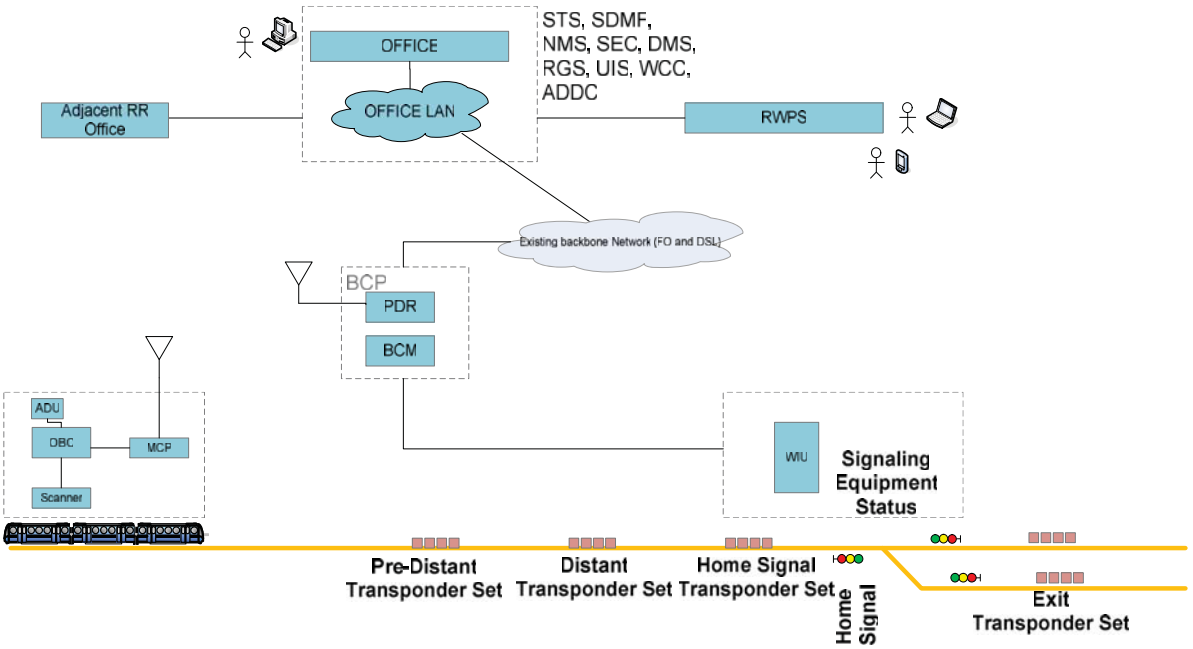


Figure 1: PTC ACSES II System Architecture

2.1.1 Office Subsystem

The Office Subsystem includes all ACSES II components necessary to integrate the dispatcher and field functions in order to issue Temporary Speed Restrictions, store vital and non-vital data, provide maintenance and reporting functions, and provide all interfaces to the Wayside Systems for ACSES II operations. The Office subsystem is fully described by the Office SDD This office equipment set includes:

- Safety TSR Server (STS) –Vital
- Wayside Communication Controller (WCC)
- Data & Maintenance System (DMS)
- ACSES II Network Management System (ACSES II NMS)
- User Interface System (UIS)
- ACSES II Office Local Area Network (ACSES II LAN)
- Active Directory Domain Controller (ADDC)
- Railroad Gateway Server (RGS)
- Software and Data Maintenance Facility (SDMF)
- Security Server (SEC)

The Safety TSR Server (STS) will be the single point of execution for office safety critical logic functions and will calculate all safety critical parameters for the ACSES II System.

2.1.2 Onboard Subsystem

The onboard is a vital subsystem that is located in the train and controlling the train's movement through requesting an application of the train's brakes upon detecting unsafe/undesirable conditions. The onboard platform supports both Cab Signal System functions with and ACSES II functions as an overlay to the existing cab signaling system. The onboard system is described by the Onboard SDD. The Onboard ACSES II system equipment set consists of the following key elements:

- Onboard Computer –Vital
- Transponder Antenna and CTV
- Speed Sensor
- Decelerometer- Vital
- Vital interface to ATC (via AIU where applicable)- Vital
- Train Engineer Aspect Display Unit (ADU)
- Acknowledge Switch
- Event Recorder System
- ACSES Alerter – for providing audible alerts to the train engineer.
- Stop and Release pushbutton
- Cut-out switch

2.1.3 Wayside Subsystem

The wayside components will be installed at the existing interlocking locations and integrated with the communications network. These wayside components include:

- Wayside Interface Unit (WIU) -Vital
- Track-mounted passive transponder
  - The validation of the data in the transponder is Vital
- Data radio
- Communication Managers
- Interfaces to the existing signal logic and communications network and
- Any necessary supporting equipment (power supplies, etc.).

Additional wayside components include passive track-mounted apparatus (transponders), and data radio antenna installations, both of which will be installed based upon site-specific requirements determined during system design. The WIU is described by the WIU SDD. The transponder is described by the Transponder SDD.

2.1.4 Communication Subsystem

The communication components will be installed at the existing interlocking locations and integrated with the communications network. The communication system is described by the Comms SDD which includes the type of communication (open and/or closed media) is using by the PTC ACSE II system. These components include:

Wayside

- Data radio
- Base Communications Manager (BCM)
- Base Radio Communication Manager (BRCM)
- RTU – Remote Terminal unit for monitoring status
- μRTU – micro Remote Terminal Unit for monitoring status in the CIL
- L2 and L3 network switches
- Any necessary supporting equipment (power supplies, antennae, filters, fibers, etc.).

Onboard

- Data Radio
- Mobile Communications Manager (MCM)
- Any necessary supporting equipment (power supplies, antennae, filters, fibers, etc.)

2.1.5 Roadway Worker Protection Subsystem

The roadway worker protection subsystem (RWPS) is required to provide a means to protect the boundaries of work zones and any worker with the zone. The RWPS will be connected to the Office sub system to allow roadway workers to request TSR's and determine the active TSR's on the system. The RWPS is described by the RWPS SDD. The RWPS system components include:

- Roadway Worker Protection Server
- Employee In Charge Terminal
- Data & Maintenance System (DMS)
- ACSES II Network Management System (ACSES II NMS)
- User Interface System (UIS)
- ACSES II Office Local Area Network (ACSES II LAN)
- Active Directory Domain Controller (ADDC)

2.2 System Interfaces

The interface descriptions between subsystems are described in detail in the ICDs. The interface descriptions are divided into two sections. The first section describes the External interfaces which are external to the BT/Siemen's scope of work and the second section is the internal interfaces which are the interfaces within each subsystem. The following sections present a brief description of each interface.

The type of interface, i.e. between vital subsystem(s) and/or user relevant (human machine) shall be identified during the Interface Hazard Analysis (IHA). The security relevant hazards shall be identified during the System Vulnerability Assessment (SVA). The details about the IHA is presented in section 3.4 below.

2.2.1 External Interface to the System

The system is bound by the external entities which mean that the interfaces between the system of the contract and the LIRR environment are specified in

Table **1** below.

Table 1: List of ACSES II External elements

External Entity	Interface Type	Description
Rolling Stock	Equipment	The collection of equipment, used for transportation, comprising propelled vehicles on running wheels. Safety Critical interfaces include: Emergency Brake, Tachometer, Active Cab, Train direction trainlines.

External Entity	Interface Type	Description
Cab Based Signaling System	Equipment	System that provides safe operating speed based on track occupancies and signaling status to equipped trains. Safety Critical interfaces include: ATC Healthy, and ATC Enforced Speed.
Signaling Equipment	Equipment	System comprised of mechanical, electromechanical and computer-based equipment that is responsible for the safe movement of trains. Safety Critical inputs include: C-Signal, Switch Position, Signal Status
Power Supply Equipment	Equipment	Various equipment that is responsible for supplying electrical power to the system.
System Administrator	Human	Human entity that is responsible for authorizing access to the system and administering roles and security functions.
Dispatcher	Human	Human entity that is responsible for requesting and approving Temporary Speed Restrictions. Also responsible for authorizing operation in degraded modes.
System Maintainer	Human	Human entity that is responsible for the maintenance, installation and testing of any part of the equipment that comprises the system.
Configuration Engineer	Human	Human entity that is responsible for performing and managing the configuration of the system.
Train Engineer	Human	Train Engineers will interact with the PTC system to operate trains in accordance with the speed enforcement functionality of LIRR's ACSES II PTC system.

2.2.2 Internal Interface to the System

The internal interfaces between subsystems of the contract are described in detail below. The interfaces were determined from a review of the System Architecture Drawing Package.

2.2.2.1 Onboard Subsystem

The On-Onboard Computer (OBC) is interfaced internally within OBC and externally to vehicle equipment including Aspect Display Unit (ADU), Mobile Communication Management (MCM), CTV and Transponder Scanner, Speed Sensor, and Train Line equipment. The detailed information about the interface descriptions are presented in the Onboard Subsystem Description Document.

2.2.2.2 Wayside Interface Unit Subsystem

The WIU is a vital subsystem that is located in the wayside equipment rooms and/or signal cases and interfaces with the signal system to provide interlocking status to the ACSES II system such as signal status, exit track and route, civil speed limit based on switch alignment, etc. The WIU interfaces to other WIU units on nested and complex interlockings to share switch position and signal status between WIU's. The WIU interfaces to a Base Communications Manager (BCM) to provide internal interfaces between the WIU and Onboard subsystems as well as alarm and status reporting to the Office sub systems. The detailed information about the interface description is presented in the WIU Subsystem Description Document.

2.2.2.3 Office Subsystem

The Office Subsystem consists of the following components: STS, WCC, NMS, UISS, RGS, SEC, ADDC, DMS, and SDMF. The Office Subsystem is installed in the Central Control centers to collect and authorize the Temporary Speed Restriction (TSR) orders from dispatchers and external railroads. The STS is a vital component of the Office Subsystem.

Interfaces of the office subsystem include: Office to Comms, Office to OBC, Office to RWPS, Office to WIU, Primary Office to Backup Office, Office to Adjacent Railroad, and user interfaces to office.

The Office Subsystem Design Description Document covers the interfaces between the Office Subsystem and the other PTC subsystems.

2.2.2.4 Transponder Subsystem

The transponder is passive equipment that is mounted between the rails. Transponders are installed in sets of two to four. The passive transponders are energized by the onboard transponder scanner (located beneath the train). The energized transponders return the railroad, line, track number and milepost. The ACSES II onboard system maintains the absolute location of the last transponder and tracks the distance traveled from it, to the nearest tenth of a mile. ACSES II additionally tracks the instantaneous distance to the next transponder which may represent a target location. The detailed information about the interfaces description is presented in the Transponder Subsystem Description Document.

2.2.2.5 Communications Subsystem

The Communications subsystem is the network and radio equipment used to connect the ACSES II subsystems together. Interfaces of the Communications subsystem include: Comms to office, Comms to OBC, Comms to WIU, Comms to RWPS, and Comms to Adjacent Railroads. The detailed information about the interfaces is presented in the Comms Subsystem Description Document.

2.2.2.6 [redacted]

[redacted]

2.3 System Functions

The ACSES II system provides a set of primary safety critical functions using the configuration of equipment, databases, and I/O, which make up the LIRR PTC system. The details of the ACSES II functions are described in SDD. The primary functions of the ACSES II system are:

1. Enforcement of Permanent Speed Restrictions (PSR).
2. Enforcement of passenger and freight TSRs received through the data radio network.
3. Enforcement of PTS at HS's displaying a Stop aspect.
4. Enforcement of Stop and Release at reliable reporting of failed highway grade crossings.
5. Enforcement of Temporary Speed Restrictions (TSRs) to protect Roadway Workers.
6. Release or override of the PTS (PTS Override or PTSO) for either HS not displaying a Stop aspect when cab signal is inoperative or is restricting the interlocking signal status allows the train to move.
7. Enforcement of a civil speed received by radio which is based on switch alignment at an interlocking. This speed corresponds to the diverging or crossover civil speed (Interlocking PSR).
8. Route dependent speed enforcement based on selected exit track (Route Dependent PSR).
9. Utilize the communications network to report and record ACSES II specific maintenance messages from all ACSES II Subsystems to the Office Subsystem.

ACSES II subsystems, working independently and as an integrated whole, support the safety critical objectives and functions described above. The specific functions performed by each ACSES II subsystem are described below.

2.3.1 Office Subsystem

2.3.1.1 Safety TSR Server (STS)

The STS is a vital component of the ACSES II office subsystem. Its functions include:

i. Two physically diverse processors executing logically identical executive programs; 2 out of 2 (2oo2) input and output data cross checks must be identical before issuing a permissive output.
ii. TSR Generation and Management which includes maintaining lists of active and inactive TSRs, creating duplicate TSRs at boundaries, and adding and deleting TSRs from lists.
iii. Interface with User Interface System (UIS) includes sending and receiving messages for TSR addition/deletion following the "SELECT-CHECK-EXECUTE" process.
iv. Responding to TSR requests from trains based on train location (BCP zone), three-zone look ahead including possible diverging routes, and TSR duplicates at line boundaries.
v. Interface with boundary STS, external to LIRR provide TSR updates at/near line boundaries.
vi. Vital timing and scheduling of time dependent TSR's.
vii. Executive program and fixed database version checks at startup and verification across two processors.

2.3.1.2 Data & Maintenance System (DMS)

The Data & Maintenance System (DMS) is a significant component of the ACSES II office subsystem. Its functions include:

i. Record every transmission occurring on the PTC office Local Area Network (LAN) between the STS, UIS, WCC, RGS, SEC, ADDC, WIU, and OBC.
ii. Use redundant DMS servers to host Structured Query Language (SQL) databases for logging and reporting of transmission data.
iii. Manage and interrogate the SQL databases.

2.3.1.3 Network Management System (NMS)

The NMS is a Commercial Off The Shelf (COTS) component system of the ACSES II office subsystem. Its functions include:

i. Poll the ACSES II equipment including network equipment and displays information assurance alerts and alarms.
ii. Collect, manage, and report ACSES II equipment status.
iii. Provide logging of all maintenance and status data received as well as provide statistics and status reports.
iv. Monitor the health of all ACSES II equipment servers.
v. Monitor and provide manual control of the A/B switch position.
vi. Monitor and provide manual control of wayside Radio Transfer Switches.
vii. Generate SNMP alarms and maintenance information on the operational status of the all ACSES II networked equipment (WIU, Office, Onboard, Comms, and RWPS equipment).

2.3.1.4 Wayside Communication Controller (WCC)

The WCC is a significant component of the ACSES II office subsystem. Its functions include:

i. Process all ACSES II messages and perform addressing and routing of all messages between ACSES II Office (STS, DMS) and Wayside and Onboard equipment (BCP, WIU, OBC).
ii. Maintain a table of all trains currently communicating including entries for each train comprised of the train address, location (BCP number), Received Signal Strength Indicator reported by each BCP, and the time the entry has been in the list.
iii. Centralize ACSES II messaging and overlapping BCP coverage to assure that duplicate messages are not sent to the train.

2.3.1.5 User Interface System Server

The User Interface System Server (UISS) is a significant component of the ACSES II office subsystem. Its functions include:

i. Provide TSR status and information to dispatchers.
ii. Allow dispatchers to generate TSR requests.
iii. Allow supervisors to approve and validate TSR requests from STS verification requests.
iv. Allow dispatchers to update train orders, work orders, and other Railroad forms used for non TSR Mandates.
v. Interface with the Fax Server to support faxing TSR forms and lists to LIRR personnel.

2.3.1.6 Security Server (SEC)

The security server (SEC) is a significant component of the ACSES II office subsystem. The security server is responsible for managing security software on the Office subsystem, denial of service protection, and intrusion detection.

2.3.1.7 Railroad Gateway Server (RGS)

The Railroad Gateway Server is a significant component of the ACSES II office subsystem. The RGS is responsible for managing connections with adjacent railroads and the RWPS subsystem.

2.3.1.8 Active Directory Domain Controller (ADDC)

The Active Directory Domain Controller (ADDC) is a component of the ACSES II office subsystem. Its functions include:

i. Authenticate user information and grant functional rights with the Office Subsystem based on user privilege.
ii. Gate and enforce user access rights in the Office subsystem.

2.3.2 Roadway Worker Protection System

The Roadway Worker Protection System (RWPS) is a significant subsystem of the ACSES II system. The RWPS subsystem is comprised of the following components: EIC, RWPS Server, ADDC, SEC, NMS, and DMS. Its functions include

i. Allowing EIC to request TSR's for work zone protection.
ii. Checking input integrity of work zone protection TSRs.
iii. Maintaining copies of in progress work zone TSRs.
iv. Handling assignments of EIC's to work zone TSRs.

2.3.3 On Board

2.3.3.1 Onboard ACSES II Computer

The OBC is a Vital component of the ACSES II onboard subsystem. Its functions include:

i. Support all LIRR rolling stock types.
ii. Calculate Alert & Braking Profile for all train types.
iii. Calculate over-speed Alert & Braking Profiles.
iv. Determine ACSES II MODE 1 & 2 operation as well as ACSES II Cut-In & Cut-Out conditions.
v. Perform construction zone transition.
vi. Detect reverse movements and trailing.
vii. Provide trailing unit location retention.
viii. Detect direction of movement and establishes ACSES II direction of travel.
ix. Interface with the directional train line.
x. Determine front of train by direction.
xi. Monitor cab signal and detect ATC cab signal Cut-Out.
xii. Send stop request to ATC.
xiii. Interface with the braking system and speed sensors.
xiv. Monitor and interface with MCM.
xv. Send train location and distance to approaching signal to MCM.
xvi. Provide scanner antenna control.

xvii. Interface with the vehicle power supply.
xviii. Monitor radio and detect missed radio messages/timeout.
xix. Detect partial or missing transponder sets.
xx. Detect linking transponders.
xxi. Decode and store transponder messages.
xxii. Perform transponder milepost conversion.
xxiii. Request, decode and store TSR data from STS.
xxiv. Request, decode and store interlocking status.
xxv. Request interlocking status on power up.
xxvi. Send onboard maintenance messages to DMS.
xxvii. Receive DMS acknowledgment.
xxviii. Provide speed processing function and detect speed threshold.
xxix. Provide wheel wear compensation function.
xxx. Identify and detect target speed.
xxxi. Perform PTS.
xxxii. Prevent train type routing to East Side Access (ESA) to avoid tunnel collision.
xxxiii. Provide penalty request forestall.
xxxiv. Determine and detect over-speed points.
xxxv. Detect downgrade speed change.
xxxvi. Determine train speed under alert curve and train speed hitting alert curve.
xxxvii. Allow speed increase after restriction zone ends.
xxxviii. Provide penalty brake running release.
xxxix. Provide Stop signal enforcement.
xl. Handles “C” signals (Clear Block).
xli. Enforce interlocking and route dependent PSRs.
xlii. Enforce TSR.
xliii. Provide Stop and Release enforcement of 5MPH TSR.
xliv. Enforce Maximum Authorized Speed (MAS) on ATC failure.
xlv. Enforce single and nested interlocking PTS.
xlvi. Manage onboard communications processor messages.
xlvii. Provide Pre-Distant Signal (PDS) Read ID of approaching BCP and PDS Read ID of next BCP in direction of travel.
xlviii. Provide PDS Read of distance to stop signal.
xlix. Detect train past Stop signal.
l. Provide brake assurance determination.
li. Provide route management and handle route not available conditions.
lii. Provide slip/slide compensation.
liii. Perform Departure Test (Non-Vital)
liv. Interface to ADU.

2.3.3.2 Transponder Scanner and CTV Antenna Interface

The scanner antenna is a significant component of the ACSES II onboard subsystem. Its functions include:

i. Energize the passive transponders laid on the tracks as it passes over them.
ii. Receive messages from transponders and transmits them to the OBC.

2.3.3.3 Aspect Display Unit

The ADU is a significant component of the ACSES II onboard subsystem. It is the operator's primary interface to the ATC and PTC systems. The speed limits from both the ATC and ACSES II systems are shown on the ADU. The ADU functions as an ATC signal aspect display and displays ACSES II related information. Its additional functions include:

i. Displays Civil Speed.
ii. Provides Visual and Audible Alert Curve Violation Displays.
iii. Allows Audible Alarm acknowledgments.
iv. Displays ACSES II Status.
v. Displays TSR Data Status as available or not.
vi. Displays "STOP" Target.
vii. Provides Test Inputs and Display.

2.3.3.4 Speed Sensor Units

The speed sensor is a significant component of the ACSES II onboard subsystem. Its main function is to convert speed sensor outputs to wheel rotation and deduce train speed from wheel rotation.

2.3.3.5 Vital Interface to the ATC

The OBC has capability of providing two vital outputs:

- Service penalty
  The service penalty output drives a non-vital relay interfacing with existing brake system circuitry on brake assurance capable vehicles. The same service penalty output drives a vital relay on vehicles without brake assurance.
- Emergency penalty
  The emergency penalty output drives a vital relay interfacing with existing brake system circuitry on brake assurance capable vehicles.

2.3.3.6 AIU

AIU is used to interface a non-Siemens ATC to an ACSES unit and an ADU. The AIU monitors the aspects that the ATC is enforcing and delivers these values to the ADU. This unit is also used to interface to the brake system used for Penalty and Emergency Brake (as applicable) to enforce a PTS (Positive Train Stop).

2.3.3.7 Decelerometer

The decelerometer is a vital, microcontroller-based device whose primary function is to provide grade-compensated deceleration sensing in railroad applications. It is designed to operate, and report deceleration measured within the range of a typical service brake rate.

It utilizes an inclinometer and automatically performs certain self-tests and diagnostics to monitor its integrity, checking its calibration and dynamic range. The ACSES II OBC uses decelerometer input to implement spin/slide compensation, brake assurance (where applicable), and cross check with speed sensor.

The function will be implemented as per the Type Approved ACSES II System with the exception of the decelerometers themselves, which are particular to the LIRR system design.

2.3.3.8 Event Recorder Unit

The Event recorder unit will store the vital, non-vital train control data, text messages conveying mandatory directives, alarms, etc. The stored data can be retain for various reasons by authority personnel. The format and duration for retention of such data shall be specified in the Onboard System design document.

2.3.4 Wayside Subsystem

2.3.4.1 Wayside Interface Unit (WIU)

The WIU is a vital component of the ACSES II wayside subsystem. Its functions include:

i. Read the real time status of all interlocking signals (More permissive stop and Clear Block Signal) and all interlocked switch positions (normal or reverse).
ii. Transmit interlocking route status messages to trains via data radio.
iii. Provide information regarding the interlocking exit track of routes.
iv. Provide civil speeds for an established route.
v. Provide distance from the HS to the diverging switch.
vi. Provide distance from the facing point of the diverging switch to the trailing point of the switch on the exit track.
vii. Provide a list of the tracks the train will cross during its move through the interlocking.
viii. Provide LoMA information.

2.3.4.2 Passive Transponders

The transponders are a safety significant component of the ACSES II wayside subsystem. However, the data within the transponder is vital and protected by the CRCs. The transponder functions include:

i. Stores track topographic data, signal, and communications information.
ii. “Broadcasts” the stored information upon being energized by the trains passing over them.
iii. Provides the actual distance to the beginning of the next speed restriction(s), or speed change.
iv. Provides the target speed of all restrictions between this transponder set and the next transponder set.
v. Provides all speed upgrades between this transponder set and the next in the direction of train travel.
vi. Provides the worst-case grade over the distance to the next transponder in the direction of train travel.
vii. Provides Transponder type, location, and track number.
viii. Provides the actual distance to the next transponder location and necessary sync and
ix. Check bytes to transmit a vital, failsafe message.
x. Provides the distance to the next Interlocking Home Signal.
xi. Provides the radio channel assignment for communications between the wayside BCP and the onboard MCP.

2.3.5 Communication Subsystem

2.3.5.1 Base Communication Package

The BCP is a significant component of the ACSES II wayside subsystem. Their functions include:

i. BCM with WIU and office subsystem interfaces.
ii. BRCM with PTC data radio interface.
iii. PTC data radio.

2.3.5.2 Mobile Communication Manager

The MCM is a significant component of the ACSES II onboard subsystem. Its functions include:

i. Handle radio messaging between OBC and ACSES II office subsystem.
ii. Handle radio messaging between OBC and ACSES II wayside subsystem.
iii. Manage TDMA scheme.
iv. Manage mobile radio power.

2.3.6 System Database

Topographic Database – All data characteristics necessary to describe the detailed topography to support ACSES II database and data programming, is maintained in Topographic database. All data within the TopoDB is created and modified using SDMT provided within SDMF. SDMT provides an authorized user with capabilities to generate a graphical map that includes both a tabular and a graphical representation of the ACSES II database. This generated map is linked within the TopoDB to allow users to modify either the database or the map directly. The Topographic database is stored and version managed using the configuration tools provided by SDMF. The following databases are generated using a version of TopoDB:

A. ACSES II safety-critical data is generated using the SDMF and its associated system data maintenance tool (SMDT) following specific generation and verification processes for each of the following data elements:
    a. Transponder Location Specific Telegram files
    b. Safety TSR Server Fixed Database
    c. Encoder (WIU) Location Specific Configuration files: SDMT generates intermediate configuration data file, using this intermediate file with manual data entry and applying design rules, a route table is created. This route table data is manually entered using DT (diagnostic Tool) to generate location specific configuration files for WIU. Generated location specific configuration files are configuration managed within SDMF. WIU dash board tool provided within SDMF provides an authorized user with capability to modify WIU configuration data and store newly generated configuration files back under version control using configuration tools provided within SDMF.
B. SDMT provided within the SDMF is used to produce non-vital data files required by the UIS subsystem application software. Details of the database schema can be found in the UIS subsystem database design document. Microsoft SQL Server is used to manage this database. SDMT generated data files (SQL queries) are used to populate database structure with static topographical data.
C. Configuration Files for Communications Subsystems – MCM, BCM, RCF, WCC, RGS and IP & ATCS Addresses for ACSES II System. Note: Input of these data elements are controlled through specific processes relative to the subsystem. See SDMT Verification and Test Plan for the specific subsystem. SDMT generated intermediate file (infrastructure data), manual data entry along with design rules, configuration files are generated/modified using text editor or XML editor.

The process of system data generation is shown in Figure 2. Inputs are verified and captured in the SDMT to generate or modify the TopoDB. Any modification to data files, part of TopoDB, are version controlled and the results are captured in a new version of the TopoDB. Using a version of TopoDB, the SDMT generates databases or data files in the format required by each subsystem. For the format and description of the database and data files refer to the SDMF ICD. The data files generated by the SDMT (intermediate files), as applicable to the subsystem, are used along with manual data entry (where applicable), and design rules to generate input data as required for subsystem specific intermediate tools.

In the case of the WIU, an intermediate file is generated by SDMT with all infrastructure data. Manual data entry per design rules are used to generate routing tables, which are then entered into DT (WIU compiler tool) to generate location specific configuration files. Once verified, the WIU configuration files are version controlled within SDMF.

In the case of the OBC, vehicle configuration items are set on the train using ACSESView (PTE application). The ACSESview application generates a log file with all parameters used to configure the specific vehicle. This log file is saved and version controlled within SDMF.

In the case of the communication subsystems, the SDMT generates intermediate files and a manual data entry process is followed per design rules. Configuration files are generated or modified using a text editor or XML editor. These modified configuration files are verified and version controlled within SDMF.

Note: The subsystem specific database and data files generated, either using an SDMT generated intermediate file or not, follow subsystem specific verification processes.

A new baseline of ACSES II configuration is (BaseDB) is created with generated subsystem database/data files.



2.4 Compliance Matrix

Table 2: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part I	12.10.12.A	Final Safety Report	Final Safety Report shall provide a summary of the results on the overall safety analysis, safety verification, and system safety demonstration	All
Vol 2 Part I	12.10.12.B		Final Safety Report shall contain evidence of safety analysis	3

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part I	12.10.12.C	MTTHE	Document the calculation and methodology to show the MTTHE requirements in 9.1 have been achieved	3.7.4.1
Vol 2 Part I	12.10.12.D	Risk Reduction Actions	Address all risk reduction actions taken during design, test, operation and maintenance to mitigate faults caused by Operating Scenarios, Failures, Latent Design Errors, Installation errors, Human Reaction, Post implementation changes to SW or HW, or Interoperability and compatibility issues.	3.3
Vol 2 Part I	12.10.12.E	Information in Report	Describes the Safety Certification process and issues encountered during certification. Describes certification status Describes remaining restrictions / open issues and actions / work arounds to ensure acceptable level of safety is maintained. Provides a schedule for eliminating restrictions / workarounds. As appropriate. Includes Certificate of Compliance	5

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part 1	12.10.12.F	Resolution of all Hazards	Report shall contain evidence of the resolution of all hazards. Evidence of resolution shall consist of satisfactory closure of the items as listed in the Project Hazard Log and achievement of the items listed in the Certified Item List	3.1.1
	12.10.12.G	Approved by Engineer	Report format will be approved by the Engineer and submitted in draft form at FDR. Report will stay draft until final system certification is achieved.	5
	12.10.12.H	Approval of Final Safety Report	Report is to be submitted to SSCB prior to Completion of Pilot Phase commissioning and testing. Once approved by SSCB then submitted to the FRA and revised to address comments with a disposition per FRA comment. The report will be revised when characteristics of any territory, TP interface or the TP is modified in a way that impacts the safety of the system.	3

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part I	9.1.E	MTTHE	The SI shall provide a quantifiable analysis of the safety of each of the ACSES II Subsystems and the ACSES II System as a whole. The minimum level of safety that the SI shall demonstrate through calculated Mean-Time-To-Hazardous-Event (MTTHE) is 10^{-9} hours. The MTTHE and the complete safety analysis and calculations for each ACSES II Subsystem and the ACSES II system shall be provided as part of the Final Safety Report, CDRL 2-136.	3.7.4.1
Vol 2 Part I	9.5.F	MTTHE	Final Safety Report shall document the complete safety analysis and calculations to support the MTTHE of the Transponder Subsystem	3.7.4.1

2.5 Reference Documents

Table 3: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624
[2]	LIRR Project Hazard Log (CDRL 2-126-20)	3035819
[3]	Certifiable Item List (CDRL 2-125-20)	3035818
[4]	System Fault Tree (CDRL 2-132-20)	3035830
[5]	LIRR Transponder Final Safety Report	3037458
[6]	LIRR OBC Phase 3 Software Safety Report	3051179
[7]	LIRR WIU Final Safety Report	3037456
[8]	LIRR SRAC	3045431
[9]	LIRR Office Final Safety Report	3037452
[10]	System Description Document (CDRL 2-027)	3035724
[11]	LIRR System PVI	3050637
[12]	LIRR System Validation Report	3035712
[13]	LIRR SPT Vehicle Qualification Test Report CDRL 2-090-202	4009311
[14]	SPT Communication Qualification Test Report CDRL 2-090-203	4009312
[15]	SPT Interlocking Status and Control Test Report CDRL 2-090-204	4009313
[16]	LIRR SPT Database Verification Test Report CDRL 2-090-205	4009314
[17]	LIRR – L1 Pilot Line SPT Database Verification Test Report Addendum 2 to CDRL 2-090-205	4009316
[18]	LIRR – L2 Pilot Line SPT Database Verification Test Report Addendum 1 to CDRL 2-090-205	4009315
[19]	SPT Temporary Speed Restriction Operation Test Report CDRL 2-090-206	4009317
[20]	SPT Integrated System Test Report CDRL 2-090-207	4009318
[21]	SUP Baseline 3.1 Database Verification Test Report CDRL 2-090-210	4009465
[22]	SUP Baseline 3.1 Pilot L2 Database Verification Test Report Addendum 1 to CDRL 2-090-210	4009466

Reference Number	Document Name	Identification Number
[23]	SUP Baseline 3.1 Pilot L1 Database Verification Test Report Addendum 2 to CDRL 2-090-210	4009467
[24]	SUP Baseline 3.2 Vehicle Qualification Test Report CDRL 2-090-211	4009565
[25]	SUP Baseline 3.2 Communication Qualification Test Report CDRL 2-090-212	4009566
[26]	SUP Baseline 3.2 Interlocking Status and Control Test Report CDRL 2-090-213	4009567
[27]	SUP Baseline 3.2 Database Verification Test Report CDRL 2-090-214	4009568
[28]	SUP Baseline 3.2 Pilot L2 Database Verification Test Report Addendum 1 to CDRL 2-090-214	4009569
[29]	SUP Baseline 3.2 Pilot L1 Database Verification Test Report Addendum 2 to CDRL 2-090-214	4009570
[30]	SUP Baseline 3.2 Temporary Speed Restriction Test Report CDRL 2-090-215	4009571
[31]	SUP Baseline 3.2 Integrated System Test Report CDRL 2-090-216	4009572
[32]	Integrated ACSES II System FAT Test Results (LIRR)	4009092
[33]	System Database Safety Verification Report CDRL 2-133	3035832
[34]	Onboard SVVR	3039733
[35]	WIU SVVR	3050366
[36]	Transpondeur Validation Report Port Washington	3043407
[37]	Transponder Validation Report Montauk	3046231
[38]	Office SVVR	3052060
[39]	LIRR System SRTM	3153121
[40]	System Vulnerability Assessment	3035840
[41]	System Operating Hazard Analysis	3035826
[42]	System Preliminary Hazard Analysis	3035821
[43]	System Interface Hazard Analysis	3035828
[44]	Office 3.3.0 and Office 3.3.1 Factory Integration Test Report	4009697
[45]	SUP Baseline 3.4 Vehicle Qualification Test Report	4009745
[46]	SUP Baseline 3.4 Comms Test Report	4009746

Reference Number	Document Name	Identification Number
[47]	SUP Baseline 3.4 Interlocking Status Test Report	4009747
[48]	SUP Baseline 3.4 Database Verification Test Report	4009748
[49]	SUP Baseline 3.4 Database Verification – Addendum 2 Test Report	4009778
[50]	SUP Baseline 3.4 TSR Operation Test Report	4009749
[51]	SUP Baseline 3.4 Integrated System Test Report	4009750
[52]	Variances Analysis Process	3153502
[53]	ACSES II Message Description Document	3041417
[54]	Office Interface Control Document (CDRL 6-018)	3035958
[55]	MCM – OBC Interface Control Document	3040403
[56]	RWPS Interface Control Document (CDRL 2-225)	3035874
[57]	Transponder Interface Control Document (CDRL 4-002)	3035877
[58]	WIU Interface Control Document (CDRL 4-016)	3035890
[59]	Onboard Interface Control Document (CDRL 5-002)	3035903
[60]	PCC and BCC Office Split for Non-Revenue Service Verification	3153856_Rev_A
[61]	Communication SVVR	3036422
[62]	RWPS SVVR	3036418
[63]	SUP Baseline 3.5 Interlocking Status and Control Test Report	4001031_Rev__
[64]	SUP Baseline 3.5 Temporary Speed Restriction Test Report	4001032_Rev__
[65]	SUP Baseline 3.5 Integrated System Test Report	4001033_Rev__
[66]	LIRR System Hazard Analysis CDRL 2-128-20	3035823

2.6 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in Table 4 and Table 5 respectively.

Table 4: Terms Specific to this Document

Term	Definition
Segment	A section of the railroad defined by the railroad authority and engineering in the design of the transponder design.

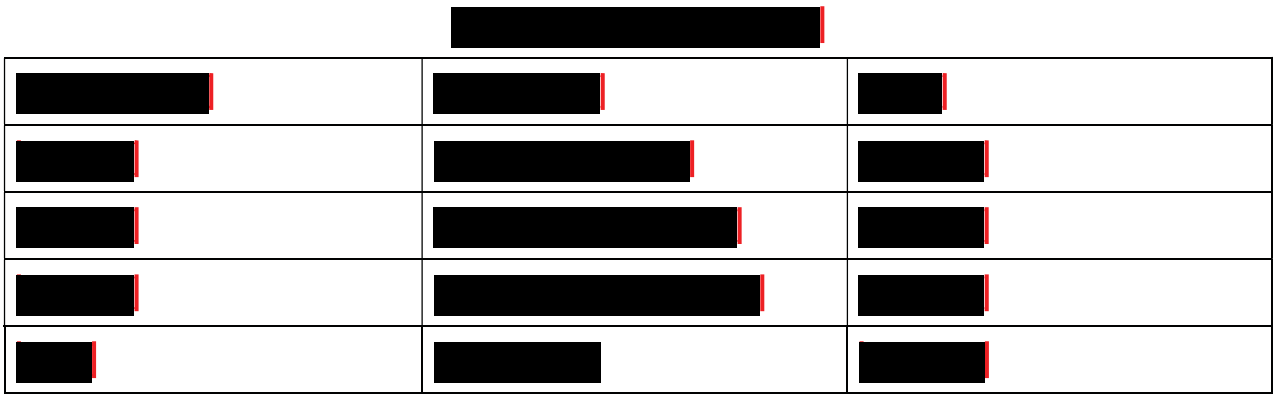
Table 5: Acronyms Specific to this Document

Acronym	Definition
EMC	Electromagnetic Compatibility
FAT	Factory Acceptance Test
IHA	Interface Hazard Analysis
MAS	Maximum Authorized Speed
OHA	Operational Hazard Analysis
RTC	Rational Team Concert
SDMT	Software Data and Maintenance Tool
SSHA	Subsystem Hazard Analysis
Topo DB	Topographical Database
TP	Transponder

3 Summary of Safety Analysis and Evidences

Safety analysis of the system was performed by analyzing the functions performed by the system within the overall system. The analysis performed for the system were the Interface Hazard Analysis, Operations Hazard Analysis and Fault Tree.

The safety CDRL's listed below are intended for the full ACSES.



[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

3.1 System Hazard Analysis

The first analysis performed was the Preliminary hazard analysis focusing on system functionality within the system. The PHA analysis results were latter included and refined in the system hazard analysis. In both of these analysis additional hazards were transferred where applicable to the system hazard log where mitigations to the hazards was incorporated into other system functionality.

3.1.1 Closure of all Hazards

All the hazards from the IHA [43], OHA [41], and SHA [66] analysis were added to the system hazard analysis report. A hazard control board will be held to review the hazards defined in the subsystem hazards analysis report. This review will focus on a review of the safety requirements mitigating the hazards defined in the subsystem hazard analysis report. The review will also confirm that test evidence was available to provide closure evidence for each safety requirement was properly implemented in the final system including hazards mitigated by functionality of other subsystems.

The SI will prioritize the closure of all hazards as quickly as possible while the system is within the Revenue Service Demonstration. System functions not yet tested and interoperability hazards may not be closed prior to FRA submittal.

3.2 Fault Tree Analysis

The fault tree defines the failures that can cause the top level system hazards.

This document will be finalized as soon as possible.

Some fault tree mitigations are not complete with this system design. Specifically, mitigations to prevent non equipped trains from entering ACSES territory and some specific scenarios where a train exists temporary speed restrictions at higher speeds than restricted will need further discussion with the railroad. ACSES does not protect these scenarios and additional manual mitigations may need to be documented by the System Fault Tree.

3.3 Operation Hazard Analysis

Operational and maintenance impacts to the safety of the system were analyzed in the Operation Hazard Analysis.

The SRAC also contains restrictions for human reaction to failures and events. Failures considered:

Transponder Missed or No Transponder Read – SRC_L5 and SRC_L6

OBC Failure – SRC_L6

Entry / Exit to Test Track – SRC_L15

3.4 Interface Hazard Analysis

The System IHA is approved. All interface hazards have been defined and mitigations are in place. Testing and analysis confirm that mitigations have been implemented by the assigned subsystems.

3.5 System Configuration

The System configuration analyzed is defined in LIRR System PVI [11]

The following table shows the subsystem configuration defined by this System PVI Rev_Q (Baseline 3.5). Only the RSD Revisions are noted in this report and the related evidence for the Pilot Lines 1 and 2 only. The Non_RSD versions will be approved when that functionality is approved for service.



[redacted]

3.6 Subsystem Final Safety Reports

3.6.1 Onboard Final Safety Report

Onboard SW Safety Report [6]–Released.

The functionality of the ACSES II meets all requirements for LIRR OBC functionality for System Baseline 3.5. The train types covered by this Safety report are the M7, M9, MP15, M3, C3, DE/DM, TC-82, NYAR GP 38, NYAR MP 15, and NYAR PR20B.

All onboard safety activities and documents have been completed and reviewed with the safety working group or are in review.

BT safety does acknowledge open variances that prevent the operation of M3 trains in RSD operations.

Safety has reviewed the Onboard SVVR [34]. BT Safety and validation had determined that this revision of this report covers all components and the correct version of software tested.

The safety report does list a number of variances not corrected in this software release. Eight safety variances are CAT 2 and listed in this report. The constraints listed by this report are included in the SRAC. These constraints must be approved with the railroad prior to operation.

[redacted]





3.6.2 Office Final Safety Report

Office Final Safety Report [9].

Based upon

- positive conclusion of System Database Safety Verification Report
- positive conclusion of Office SVVR
- implementation of System SRACs, and
- implementation of OBC functional safety requirements per Table 10 herein

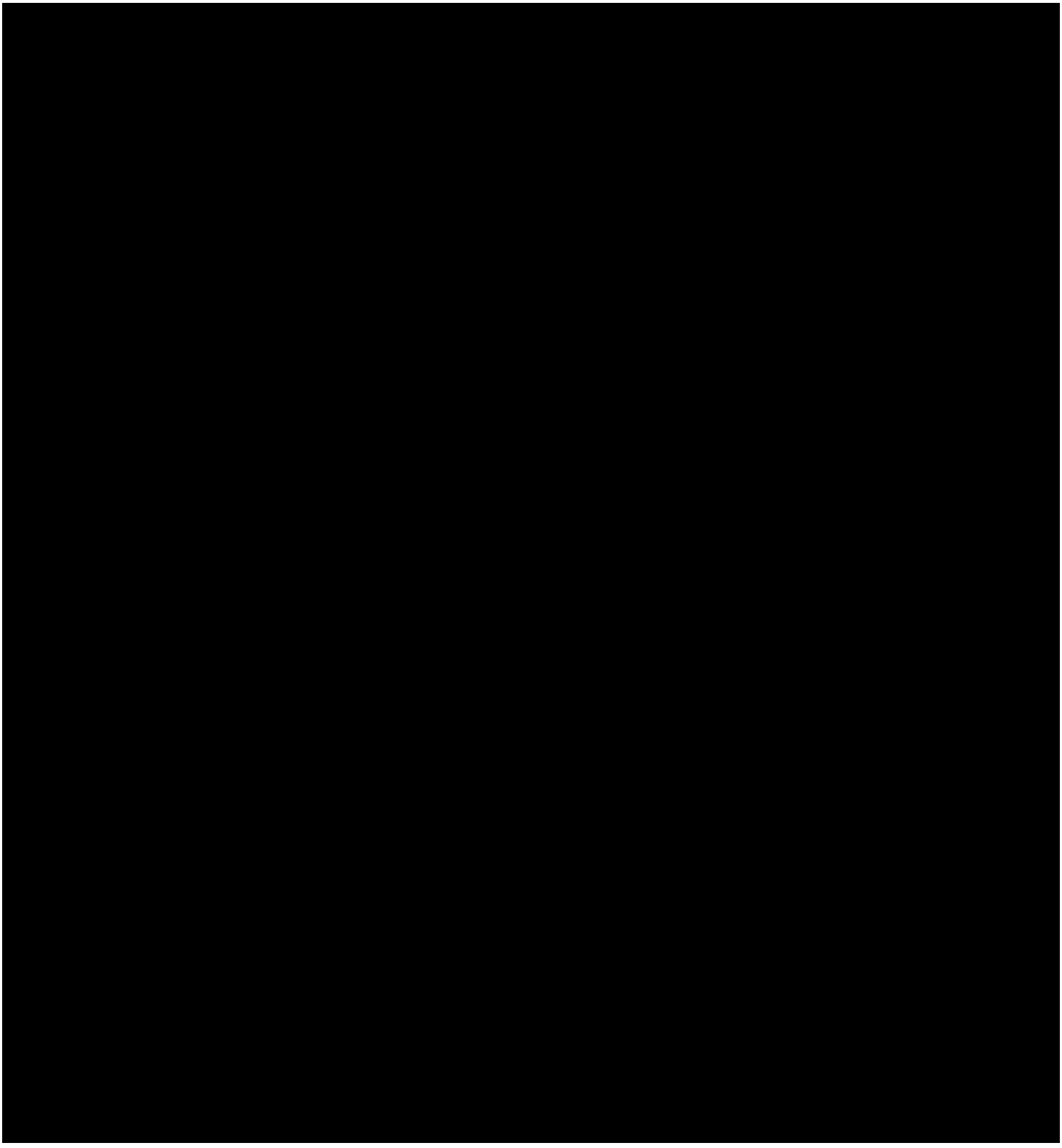
BT-RCS concludes that there is no known safety issue that would operation in RSD.

The System Database Safety Verification Report has been released and its conclusion indicate in this report. No issues that are not mitigated by SRACs.

Implementation of Office and System SRAC. – All office SRAC are covered currently by the System SRAC. A few Office SRAC are covered by other subsystem requirements and coverage of these are provided in the SRTM section. No open issues remain based on the current evidence that impact RSD.

Implementation of OBC Functional Requirements. All tracked Office Safety requirements to system requirements are properly tested and reported. No untested

List of Safety Critical variances and Justifications. The other issues have been mitigated as shown.





3.6.3 Communication Final Safety Report

3037454 – CDRL 2-135-23 – Communications Final Safety Report.

Communication analysis has been performed all hazards identified are properly mitigated and handled by the vital subsystems that can impact vital functionality. A few remaining safety requirements require the proper operation of system with continuous communication and will be mitigated by alternative barer frequencies that is not yet implemented. Maintenance protections and restrictions will need to be analyzed in the next release of this document.

The Communication Verification and validation report [35] has been released and reviewed by BT safety and BT Validation.

List of Safety Critical variances and Justifications. The other issues have been mitigated as shown. No variances remain for the communication subsystem. The configuration management error identified in the report have been explained by engineering as errors comparing SDMT stored files to the actual executable file. SDMT has been corrected to fix the error (corruption of CRC by the addition of a tag to the executable file).

3.6.4 WIU Final Safety Report

3037456 – 2-136-24 – WIU Final Safety Report [7] – Released

All non-conformities have been corrected with the WIU portion of System Release 3.2 by the WIU software and the implementation of the identified constraints. Resolution of non-safety related nonconformities will continue for those that have been deferred until future releases. This revision is to be cut-in and operation for Revenue Service Demonstration and testing on approved pilot lines. V&V has concluded with no issues. A list of constraints was added to the BT SRAC based a list emailed from the Siemens Safety lead

The WIU Verification and validation report [35] has been released and reviewed by BT safety and BT Validation. No open issues remain and the WIU software may be placed into Revenue service.

3.6.5 Transponder Final Safety Report

– Transponder Final Safety Report [5]– Released.

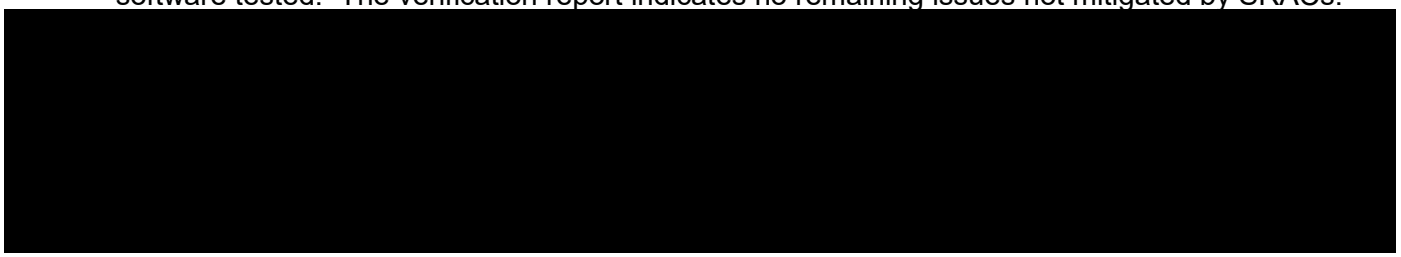
The functionality of the Transponder and the Transponder Application data meets all requirements for LIRR Transponder functionality for System Baseline 3.4.

All Transponder safety activities and documents have been completed and reviewed with the safety working group or are in review.

Safety has reviewed the Port Washington Validation Report.[36] BT Safety and validation had determined that this revision of this report covers all components and the correct version of software tested. The verification report indicates no remaining issues not mitigated by SRACs. The most relevant restrictions are the NCR 256628 – Discrepancy between TP and Office DB SDMT.

Release 3.4 also indicate SRAC opened to close track 3S and 8S to resolve assigned variances.

Safety has reviewed the Montauk Validation Report. [37] BT Safety and validation had determined that this revision of this report covers all components and the correct version of software tested. The verification report indicates no remaining issues not mitigated by SRACs.



The safety report does list a number of variances not corrected in this software release. Six safety variances are listed in this report.

As all open NCRs and Variances are mitigated by SRAC or closed. The SRAC's identified in must be agreed with railroad operations to ensure the safety of the system. The safety engineer supports the operations of Pilot Line 1 and Pilot Line 2 in Revenue Service Demonstration.

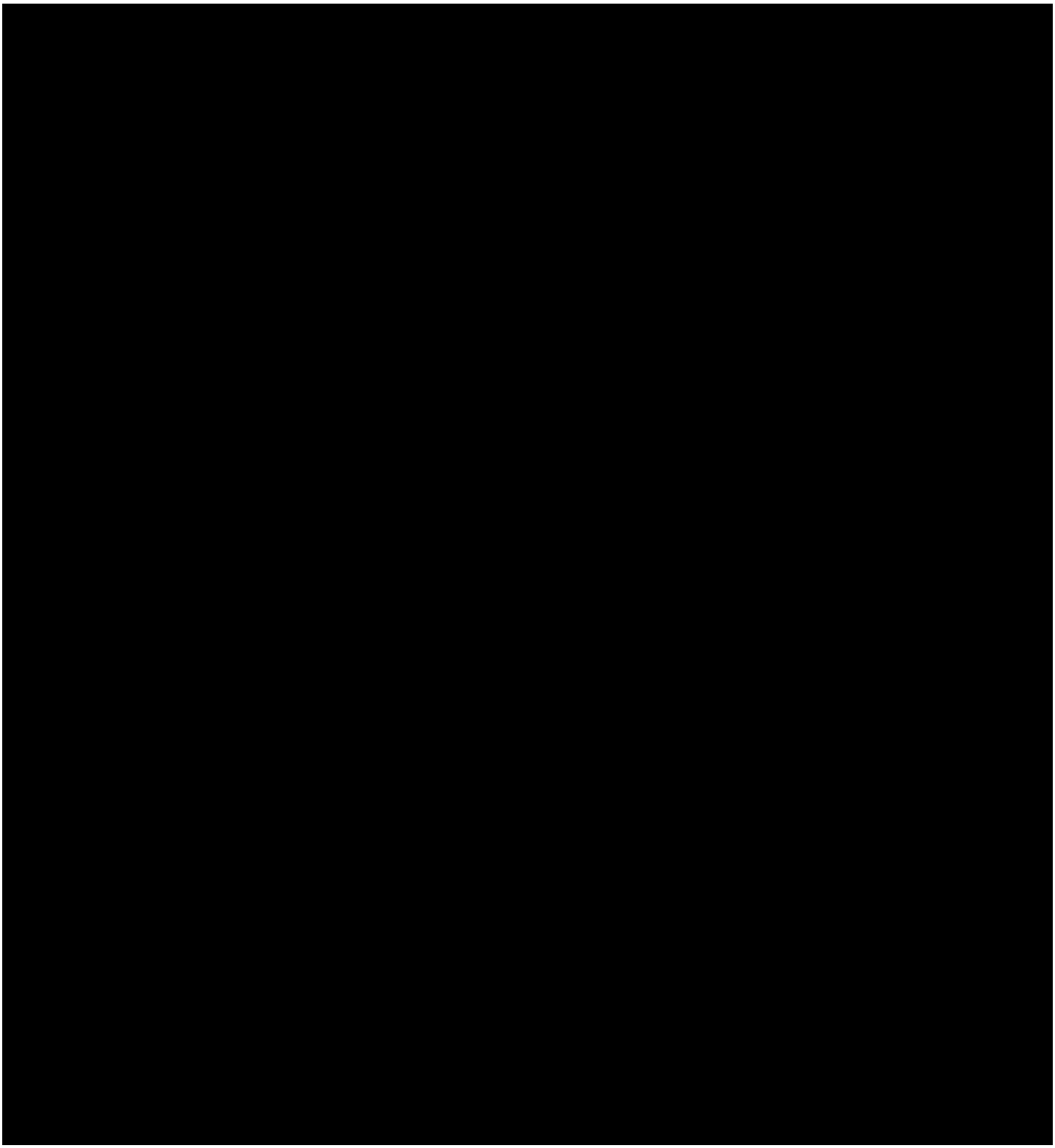


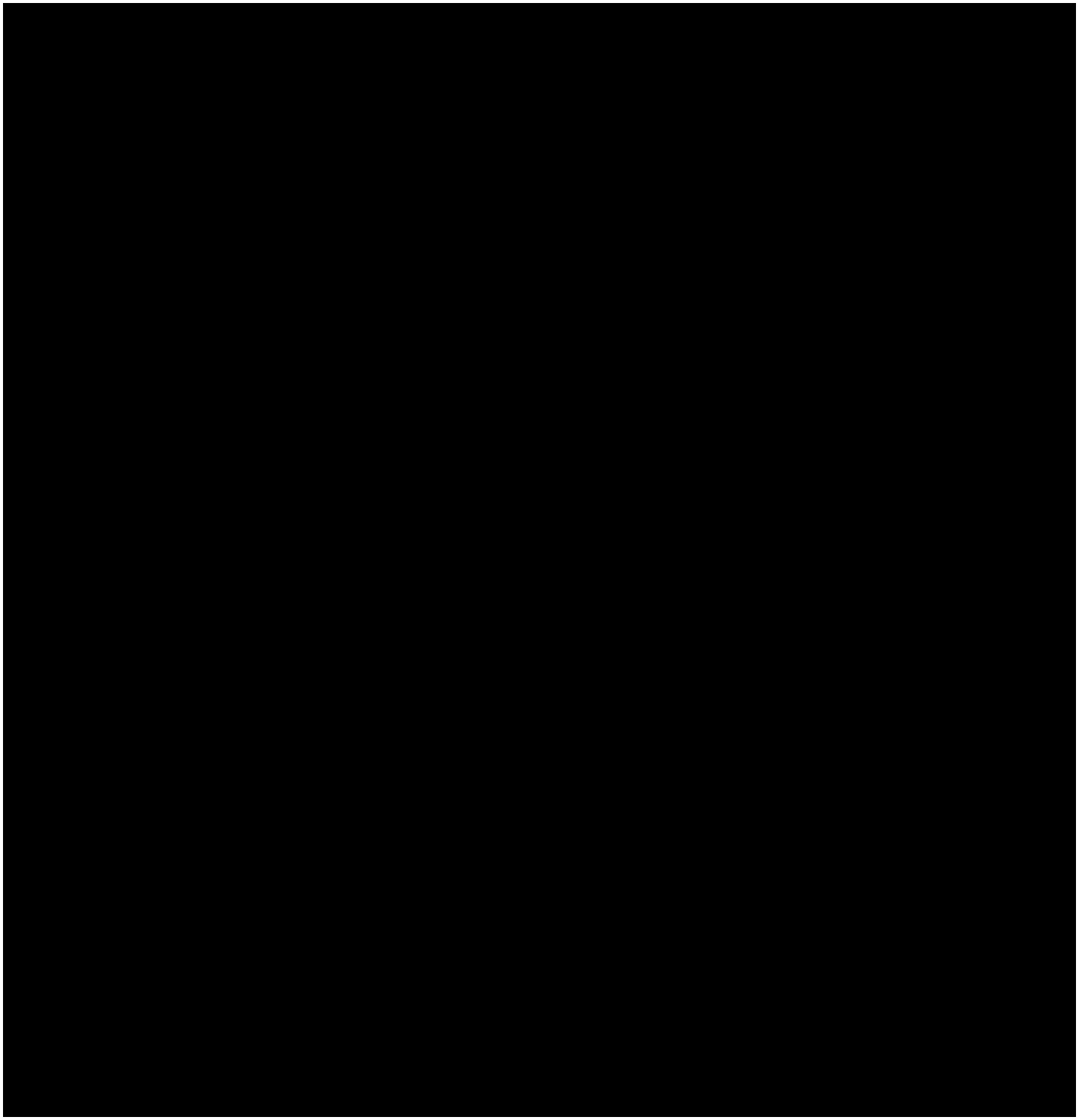
Once the Validator recommends the subsystem baseline 2.4.1 for revenue service in the Validation Report, the subsystem can then support revenue service demonstration.

3.6.7 Database Safety and Verification Report

LIRR Database Safety and Verification Report [33] provides an overview of the safety activities and verification activities performed during the development of the ACSES system database. This evidence concludes that the process defined in the SDMF Verification and Test plan has been completed and properly followed.

The Following Tables show open issues from the verified reports that have been referenced, as well as a Safety Justification for each issue. All safety NCRs and Variances in the below tables from referenced documents are justified.







3.7 System Integration Test Reports

3.7.1



3.7.2 SPT Site Integration Test Reports

Safety reviewed SPT testing results and open variances from SPT testing. Safety finds that the system lacks sufficient evidence from this round of testing to start revenue service. Additional software revisions will be required to correct these issues and additional testing required to approve revenue service demonstration.

3.7.2.1 SPT Vehicle Qualification Test Report

The SPT Vehicle Qualification Test Report [13] provides the evidence of the test cases integrating the OBC onto the specific train types to prove ACSES functionality related to onboard. Four test cases marked deferred, one retest, and two failed. 19 Test cases passed. The variances from this test report have been analyzed and reviewed.

3.7.2.2 SPT Communication Qualification Test Report

The SPT Communication Qualification Test Report [14] provides the evidence of the test cases ACSES functionality related to communication functions. Ten test cases marked deferred, three marked pass and two failed. The variances from this test report have been analyzed and reviewed.

3.7.2.3 Interlocking Status and Control Test Report

The SPT Interlocking Status and Control Test Report [15] provides the evidence of the test cases related to the interlocking status and control functions of ACSES II. One test case marked deferred, sixteen marked pass and six failed. The variances from this test report have been analyzed and reviewed.

3.7.2.4 Pilot Line 1 Database Verification Test Report

Pilot Line 1 Database Verification Test Report [17] provides the evidence of the test cases verifying specific data programmed into the system. Many test cases failed and many more were not fully tested or deferred.

3.7.2.5 Pilot Line 2 Database Verification Test Report

Pilot Line 2 Database Verification Test Report [18] provides the evidence of the test cases verifying specific data programmed into the system. Many test cases failed and many more were not fully tested or deferred.

3.7.2.6 SPT Temporary Speed Restriction Test Report

SPT Temporary Speed Restriction Test Report [19] provides the evidence of the test cases with temporary speed restriction functionality. Two test cases marked deferred, four marked retest, twenty two marked pass and two failed. The variances from this test report have been analyzed and reviewed.

3.7.2.7 SPT Integrated System Test Report

SPT Integrated Test Report [20] provides the evidence of the test cases with ACSES functionality. Nine test cases marked deferred, one marked retest, four marked pass and three failed. The variances from this test report have been analyzed and reviewed.

3.7.3 SUP 3.1 Site Integration Test Reports

Safety reviewed SUP 3.1 testing results and open variances from this round of testing. Safety finds that the system lacks sufficient evidence from this round of testing to start revenue service. Additional software revisions will be required to correct these issues and additional testing required to approve revenue service demonstration

3.7.3.1 SUP 3.1 Pilot Line 1 Database Verification Test Report

Pilot Line 1 Database Verification Test Report [23] provides the evidence of the test cases verifying specific data programmed into the system. Fewer failures but still several test cases not performed.

3.7.3.2 SUP 3.1Pilot Line 2 Database Verification Test Report

Pilot Line 2 Database Verification Test Report [22] provides the evidence of the test cases verifying specific data programmed into the system. Fewer failures but still several test cases not performed.

3.7.4 SUP 3.2 Site Integration Test Reports

Safety reviewed SUP 3.2 testing results and open variances from this round of testing. Safety found that additional Office changes are required to correct the variances related to proper reporting of the grade to the onboard. Once this variance is approved sufficient evidence exists for Line 2 to enter Revenue Service Demonstration with the listed SRACs approved.

3.7.4.1 SUP 3.2 Vehicle Qualification Test Report

The Vehicle Qualification Test Report[24] provides the evidence of the test cases integrating the OBC onto the specific train types to prove ACSES functionality related to onboard. Only one test case deferred as its not applicable to baseline 3.2.

3.7.4.2 SUP 3.2 Communication Qualification Test Report

The Communication Qualification Test Report [25] provides the evidence of the test cases with communication functions. Five test cases marked deferred, but all other test passed. The variances from this test report have been analyzed and reviewed.

3.7.4.3 SUP 3.2 Interlocking Status and Control Test Report

The Interlocking Status and Control Test Report [26] provides the evidence of the test cases for interlocking status and status functionality. Two test cases marked failed (variance 262675 and 262678). The variances from this test report have been analyzed and reviewed.

3.7.4.4 SUP 3.2 Pilot Line 1 Database Verification Test Report

Pilot Line 1 Database Verification Test Report [29] provides the evidence of the test cases verifying specific data programmed into the system. Seventeen test cases deferred that do not impact the ability to start RSD. Two test cases failed tracked by Variances 262679 and 262783.

3.7.4.5 SUP 3.2 Pilot Line 2 Database Verification Test Report

Pilot Line 2 Database Verification Test Report [28] provides the evidence of the test cases verifying specific data programmed into the system. Twenty-eight test cases deferred that do not impact RSD and 1 test case failed. The variance for the failure is 262559.

3.7.4.6 SUP 3,2 Temporary Speed Restriction Test Report

Temporary Speed Restriction Test Report [30] provides the evidence of the test cases with ACSES functionality. One test case deferred, and the rest passed. The deferred test case does not impact RSD. The variances from this test report have been analyzed and reviewed.

3.7.4.7 SUP 3.2 Integrated System Test Report

SUP Integrated Test Report [31] provides the evidence of the test cases with ACSES functions. Three test cases marked deferred and two marked failed. The remaining 11 test cases have passed. The variances from the failed test cases are 262742 and 262593 have been analyzed and reviewed

3.7.5 [redacted]



3.7.6 SUP Baseline 3.4 Testing

The remaining variances have been reviewed by Safety. Mitigations have been applied and are documented at the end of this report to mitigate any open safety critical variances found during the site integration testing. With the mitigations identified and the functional limitations applied in the conclusion of this report against functionality not fully tested, the safety engineer approves the factory test report and finds no issues that would prevent Revenue Service Demonstration for either Line 1 or Line 2 Pilot Lines.

3.7.6.1 SUP 3.4 Vehicle Qualification Test Report

The Vehicle Qualification Test Report[45] provides the evidence of the test cases integrating the OBC onto the specific train types to prove ACSES functionality related to onboard. Twenty-five test cases passed with no reported failures. One test case was reported as deferred related to ESA tunnel protection and is included in the System PVI as functions not available.

3.7.6.2 SUP 3.4 Communication Qualification Test Report

The Communication Qualification Test Report [46] provides the evidence of the test cases with communication functions. Eight test cases passed, and five test cases are deferred. The deferred test cases are from alternative radios not currently supported by the Baseline.

3.7.6.3 SUP 3.4 Interlocking Status and Control Test Report

The Interlocking Status and Control Test Report [47] provides the evidence of the test cases for interlocking status and status functionality. Twenty-two test cases pass and only one test case failed. The failure is tracked by Variance 263478.

3.7.6.4 SUP 3.4 Pilot Line 1 Database Verification Test Report

Pilot Line 1 Database Verification Test Report [49] provides the evidence of the test cases verifying specific data programmed into the system. All test cases except Line Boundary test cases which were not run are now passed. All prior variances and NCR's addressed.

3.7.6.5 SUP 3.4 Pilot Line 2 Database Verification Test Report

No database elements changed for Line 2 so no report was generated for Baseline 3.4. Please refer to baseline 3.2 Report.

3.7.6.6 [redacted]

[redacted]

3.7.6.7 SUP 3.4 Integrated System Test Report

SUP Integrated Test Report[51] provides the evidence of the test cases with ACSES functions. Eleven test cases pass out of sixteen total test cases. Three test cases deferred due to line boundary functionality and the remaining two test cases failed. Both failed test cases are tracked by Variance 263104 but does not impact safety

3.7.7 SUP Baseline 3.5 Testing

The remaining variances have been reviewed by Safety. Mitigations have been applied and are documented at the end of this report to mitigate any open safety critical variances found during the site integration testing. With the mitigations identified and the functional limitations applied in the conclusion of this report against functionality not fully tested, the safety engineer approves the factory test report and finds no issues that would prevent Revenue Service Demonstration for either Line 1 or Line 2 Pilot Lines.

3.7.7.1 SUP Baseline 3.5 Interlocking Status and Control Test Report

The Interlocking Status and Control Test Report[63] provides the evidence of the test cases for interlocking status and status functionality. Of the one regression tests performed for this system configuration, one test cases passed. Variance 263478 was verified in this report.

3.7.7.2 SUP Baseline 3.5 Temporary Speed Restriction Test Report

Temporary Speed Restriction Test Report[64] provides the evidence of the test cases for TSR speed restriction functionality. Of the nine test cases retested for changes, nine passed. One test case remains deferred from the prior revision. The deferred test case is due to Line Boundary functionality and will not impact RSD. [redacted]

3.7.7.3 SUP Baseline 3.5 Integrated System Test Report

Integrated System Test Report[65] provides the evidence of the test cases for ACSES system functionality. Of the four regression tests performed for this system configuration, three test cases passed and one failed. [redacted]

3.8 System Verification and Validation

Safety has reviewed the Verification and Validation of the system, system database and overall system. This review ensures that the proper process was defined and followed. The review also reviewed the evidence from each verification report and ensured that all open issues were properly documented and if appropriate mitigations put in place to protect the system until the issues are corrected.

3.8.1 System SVVR

The Safety engineer reviewed the System SVVR[12] to determine if the SVVP was properly fully implemented and all open issues identified and mitigated. The safety engineer finds that after reviewing all verification activities have been completed with the exception of requirements verified by analysis this will be completed shortly.

The report supports Revenue Service Demonstration and indicates that all remaining open issues are mitigated by SRACs captured in the current LIRR SRAC[8] document.

The report does have an error as it indicates that C3 and DE/DM trains are not permitted in RSD operations. This will be corrected and was based on SRAC L106 that is now closed.

The report does prohibit RWPS from RSD operations due to a number of variances.

3.8.2 Onboard SVVR

Safety has reviewed the Onboard SVVR [34]. BT Safety and validation had determined that this revision of this report covers all components and the correct version of software tested. BT safety confirms that FSTV and GSTV results have been completed on identified safety critical software and this report states no open issues with this version of software.

3.8.3 WIU SVVR

Safety reviewed the WIU SVVR [35] to determine that the WIU SVVP was fully implemented and that all outstanding findings from the verification were closed. The WIU SVVR provide evidence for hardware verification and specific data application verification. The specific application data is covered by proper engineering review records as indicated in the plan and all findings from the review have been justified or closed. The hardware verification evidence include peer review records as well as First Article inspection evidence, and the FMECA. The Generic product verification for the WIU is covered under the Siemens safety certificate and is out of scope for the system safety engineer.

3.8.4 Office SVVR

Safety reviewed the Office SVVR[38] to ensure that all verification activities have been completed and that no open items exist in the design. Safety engineer does note at the current revision of this document is providing evidence for only the vital subsystem (STS). The verification reports indicate that that there are currently open NCRs due to test failures, questions about proper linkage of requirements, and other reasons. However, these have been analyzed and do not pose a hazard for RSD, except for NCR 261693. The report also indicates a note on the PVI that has been corrected in System Baseline 3.5.

[redacted]

3.8.5 Transponder Validation

Safety reviewed the Port Washington Transponder Validation Report[36] to confirm that all verification activities are complete and implemented per the SDMT Verification and Test Plan. The safety engineer also reviewed if all open issues were justified and covered by SRACs.

Safety Reviewed the Montauk Transponder Validation Report [37] to confirm that all verification activities are complete and implemented per the SDMT Verification and Test Plan. The safety engineer also reviewed if all open issues were justified and covered by SRACs.

3.8.6 RWPS SVVR

Safety reviewed the RWPS SVVR[61] to ensure that all verification activities have been completed and all outstanding findings are closed.

[redacted]

3.8.7 Communication Subsystem SVVR

Safety reviewed the Comms SVVR[62] to ensure that all verification activities have been completed and all outstanding findings are closed. The Safety engineer found that all requirements that required testing were properly tested except requirements linked to the alternate barer methods (Wi-Fi and Cellular). The report also indicated open variances for site testing on the configuration of the communication subsystem. Engineering has since responded to the variance in the report and indicated that this is due to SDMT errors that are now addressed. The correct software has been confirmed to be installed at site.

3.8.8 System Database and Safety Verification Report

See section 3.6.6.

4 Calculation of MTTHE

[redacted]

[redacted]

5 Safety Certification Process

The safety analysis of the system is competed and the current status of the approval of the safety documentation is shown in Table 6. The hazards from these analyses are tracked by the Project Hazard Log. All hazards have identified mitigations, and these have been fully linked to safety requirements and system requirements. In addition, safety has analyzed the tracing of safety related system requirements to the testing and analysis evidence to confirm the mitigation has been properly implemented.

Safety has also confirmed that Verification has been performed to the proper process defined for each subsystem and at the system level. All verification findings have been analyzed and where necessary mitigations applied to correct any open remaining safety critical variances for those findings.

Issues found by safety or verification have been added as NCR's and tracked through the RCT tool. Each issue includes a justification of the impact of that issue on operations. The justifications are presented in the Attachments. Where necessary Safety Related Application Conditions (SRAC) have been added and agreed with the railroad to provide further mitigation until the issues are corrected.

5.1 [redacted]

[redacted]

[redacted]

5.2 Remaining Open Items

5.2.1 Remaining NCR

See Attachment B - List of Open NCR

All NCRs are covered by existing SRAC or function restrictions.

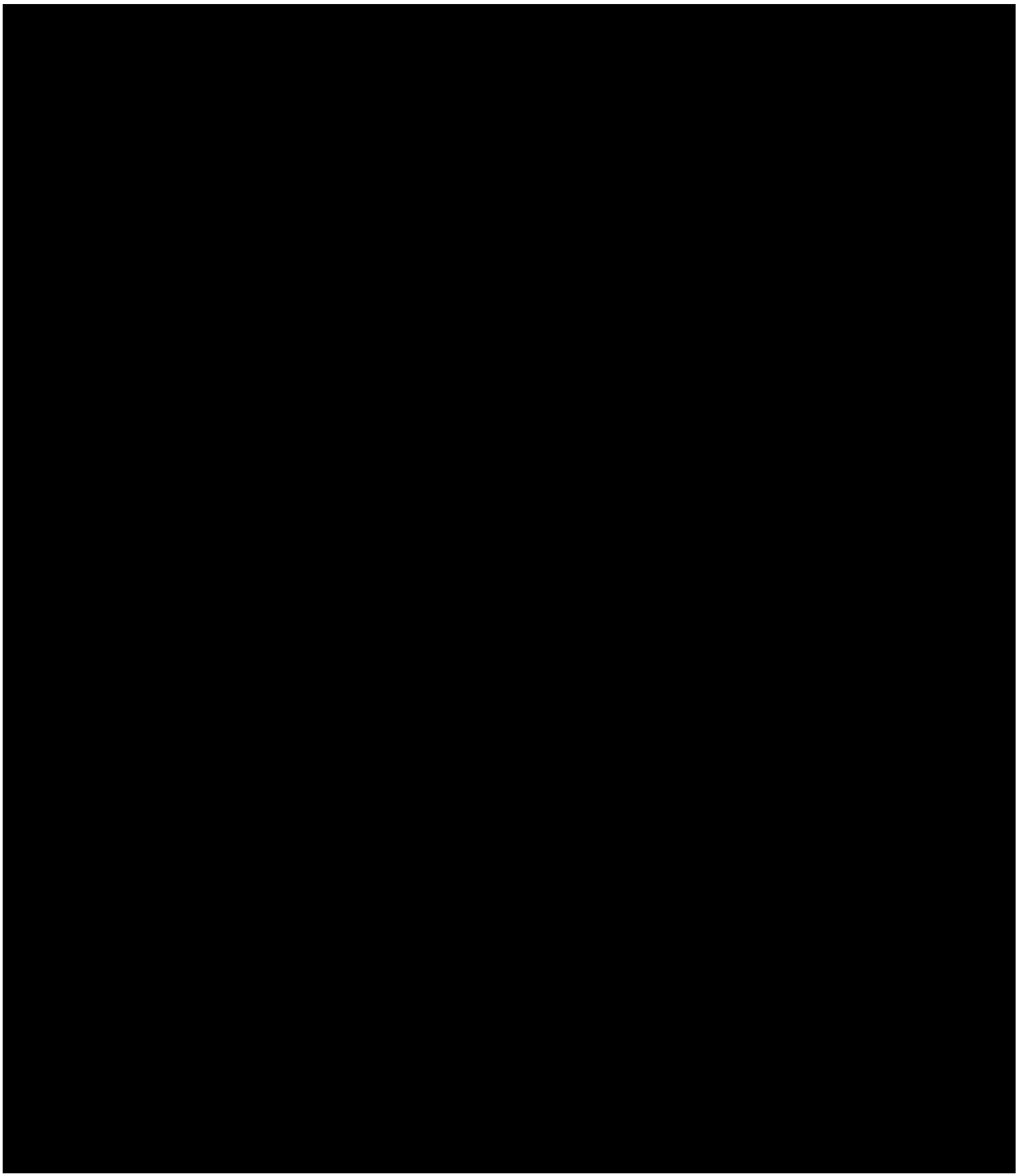
5.2.2 Remaining Variances

See Attachment A - List of Remaining Variances

Currently we have 21 Cat 2 or Cat 3 Open Variances that impact Pilot Line 1 or Line 2. The Cat 2 variances are listed below the appropriate mitigations listed in the table.

[redacted]



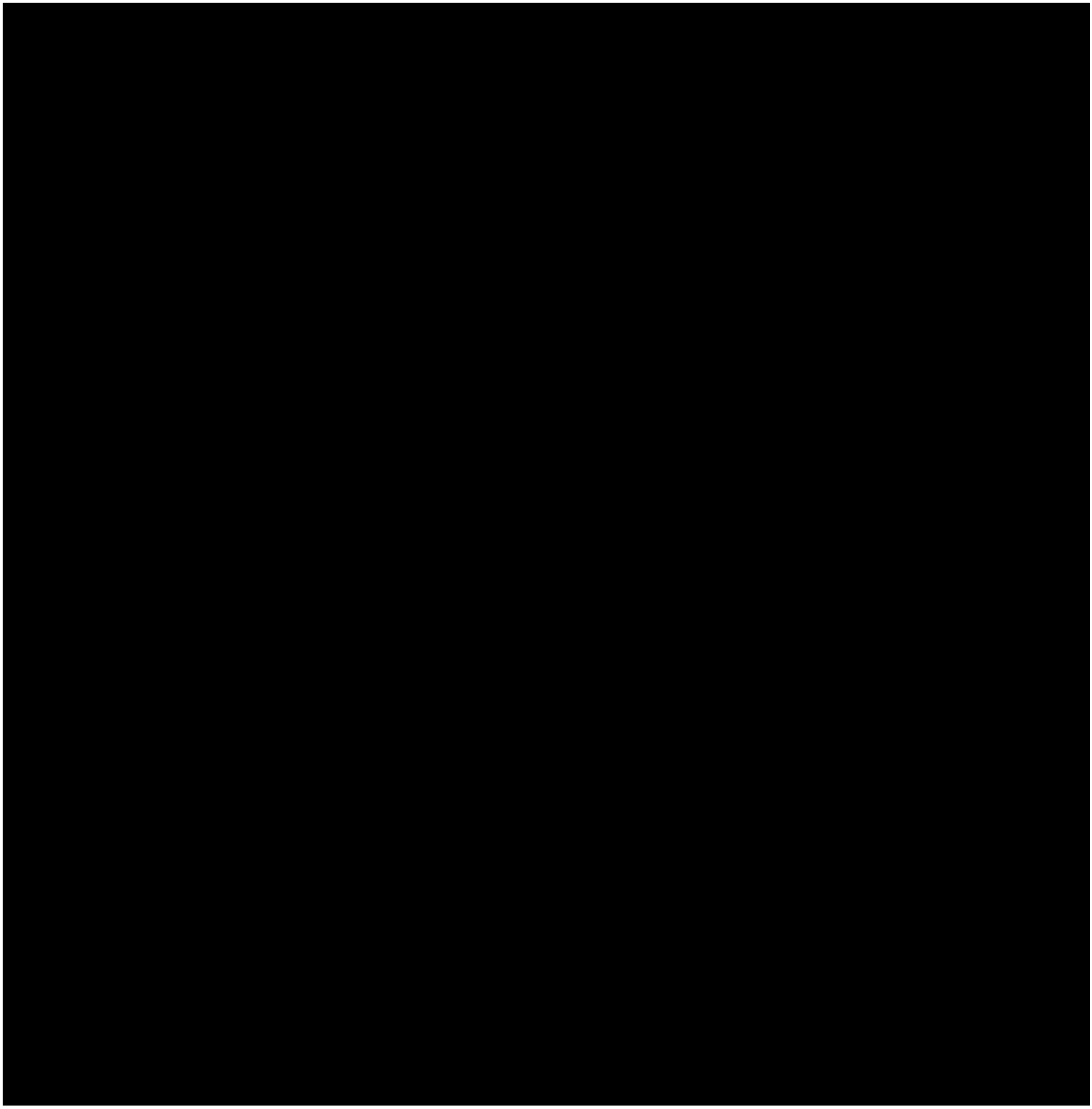


[redacted]

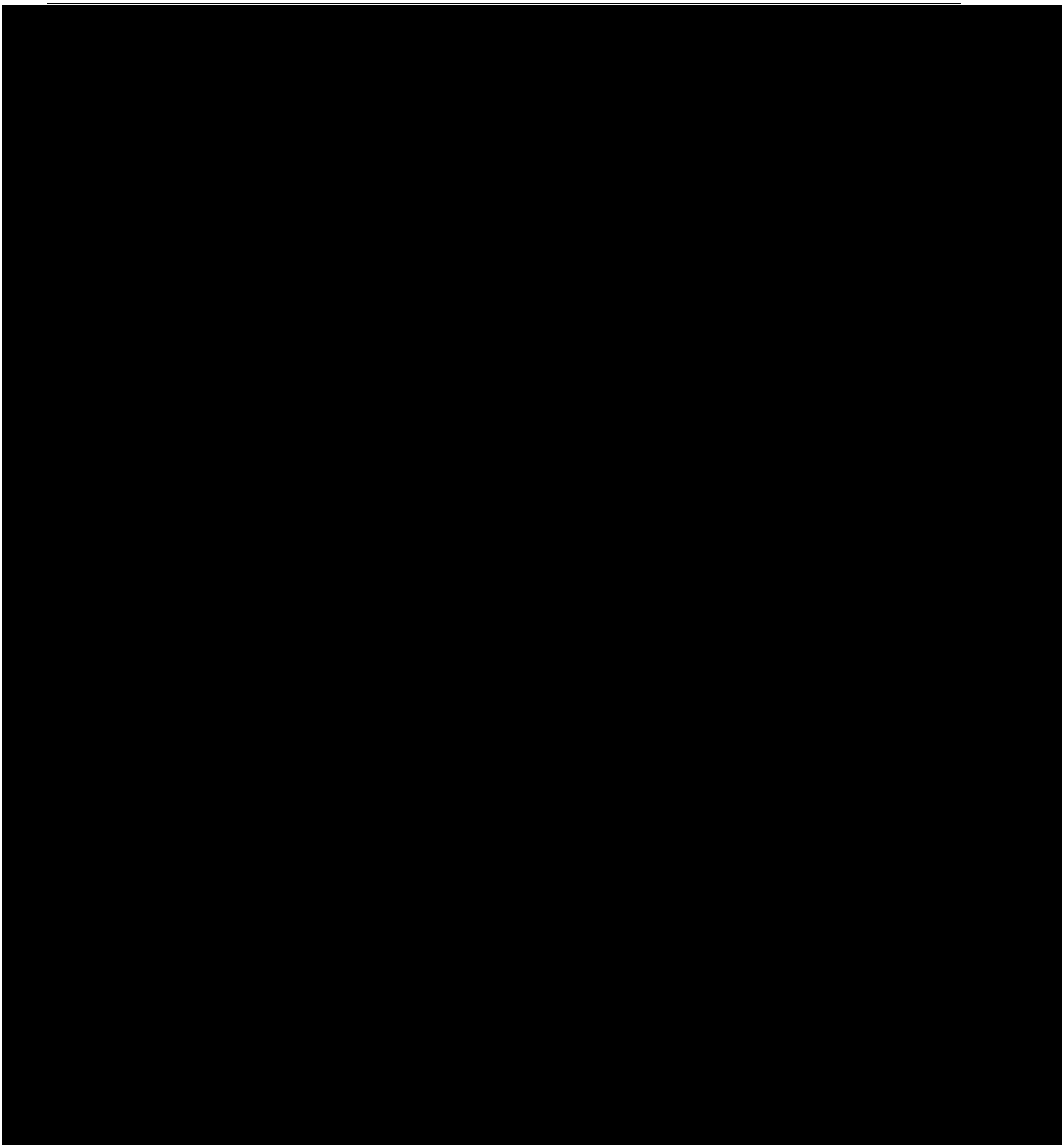
5.2.3 Restrictions to Mitigate Open Items

See LIRR SRAC [8]. All variance and NCR restrictions have been checked.

[redacted]







[redacted]

5.2.4 Schedule to Remove Restrictions

Restrictions above will be evaluated for each software release of each subsystem to the system.

6 Conclusion

The current status of the system safety analysis is represented in section 3.

[redacted]

6.1 Limitations From the PVI

As part of the System Safety Analysis to allow RSD the following system functions identified from the System PVI were not included in the system safety analysis for revenue service demonstration. Additional testing and/or verification is required to implement these functions.

[redacted]

7 Attachment A - List of Remaining Variances

See 3035838_Rev_E_Attachment_A

8 Attachment B - List of Open NCR

See 3035838_Rev_E_Attachment_B

Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

Transponder
Final Safety Report
CDRL 2-136-25

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	PM	Report	Project	Released

Prepared:	Jason Weighley Safety Engineer	Jason Weighley	2019.03.27 10:27:20 -04'00'
Verified:	Francis Tabi Safety Engineer	T. Tabi	2019.03.27 11:32:06 -04'00'
Approved:	Anthony DeFrancisco Project Director	Anthony DeFrancisco	3/28/19
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group	P. Magloire	2019.04.03 10:51:29 -04'00'
BT/SRA Review:	N/A Title		
BT/SRA Review:	N/A Title		
	Name / Title, Group	**Signature**	**Date**

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3037458

Effective Date:	Revision:	Language:
2019-03-27	_B	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2018-11-13	First issue
__1	2019-02-19	Updated the FSR with updates to Montauk Pilot Line 1 and Port Washington Pilot Line 2
_A	2019-02-27	Released for Baseline 3.4
_B	2019-03-27	Updated to Resolve comments from SCCB and address comments from SI-RVW-00873

Table of Contents

Section	Subject	Page
1	**Executive Summary**	5
1.1	**Changes to this version of the Report**	5
2	**Introduction**	5
2.1	**Compliance Matrix**	7
2.2	**Reference Documents**	11
2.3	**Glossary**	12
3	**Summary of Safety Analysis and Evidences**	12
3.1	**Evidence of Closure of Items from Certified Item List**	13
3.1.1	Port Washington Verification Evidence.	14
3.1.1.1	Port Washington FAT Test Reports – 4008751_Rev_D	14
3.1.1.2	Port Washington SIT and PICO Test Results – 4007924_rev_E	17
3.1.1.3	PICO Test	18
3.1.1.4	Port Washington Validation Report – 3043407 Rev _J	18
3.1.2	Montauk Verification	19
3.1.2.1	Montauk Factory Test Report	19
3.1.2.2	Montauk PICO Test Report	22
3.1.2.3	Site Testing	22
3.1.2.4	Montauk Validation Report.	23
4	**Calculation of MTTHE**	26
5	**Safety Certification Process**	26
5.1	**SRTM**	26
5.2	**FMECA**	26
5.3	**Remaining Open Items NCR**	27
5.4	**Remaining Variances**	29
5.4.1	Restrictions to Mitigate Open Items	32
5.4.2	Schedule to Remove Restrictions	34
6	**Conclusion**	34
7	**Attachment A – R2215P Bombardier 4.5Mhz Transponder Report**	36
8	**Attachment B – REC – E703892**	37

List of Figures

Figure 1 - Transponder Interface 6

List of Tables

Table 1: Compliance Matrix 7
Table 2: Reference Documents 11
Table 3: Terms Specific to this Document 12
Table 4: Acronyms Specific to this Document 12
Table 5: Test Tools for LIRR_L2_009_REL 14
Table 6: FAT Results for LIRR_L2_009_REL 15
Table 7: Verified Variance/NCR 16
Table 8: New NCR/Variance for LIRR_L2_008 17
Table 9: Outstanding Transponders for Test Case 1 for LIRR_L2_009_REL 17
Table 10: Test Environment/Test Tools for LIRR_L1_007_REL 20
Table 11: FAT Test Results for LIRR_L1_007 20
Table 12: Resolved/Verified NCRs for FAT LIRR_L1_007_REL 21
Table 13: Failed PICO Testing for LIRR_L1_007_REL 22
Table 14: Outstanding Test Case 1 for LIRR_L1_007_REL 22
Table 15: Failed Transponders for LIRR_L1_007_REL 23
Table 16 List of Open NCR 27
Table 17 List of Open Variances 29
Table 18 List of SRAC 32

1 Executive Summary

The Transponder Final Safety Report documents the closure of all hazards assigned to the transponder subsystem and evidence of closure of all assigned safety requirements to the Transponder subsystem. The report also details the calculation of the MTTHE rates for the Transponder subsystem and how this calculation meets the targets defined for this subsystem by the System Integrator.

This version of the report is focused on the requirements and hazards of the full ACSES functionality of the contract. The scope of this version of the report is reduced to analysis of Pilot Line 1 and Pilot Line 2. The Safety Engineer finds from the evidence provided and contingent upon acceptance of the identified SRACs that Revenue Service Demonstration can be performed on both Pilot Line 1 and Pilot Line 2.

1.1 Changes to this version of the Report

Updated Section 3.1.2 to include changes to Updated Montauk Validation Report. Updated Section 5 conclusion to include requested changes. Aligned listed variances and NCR's in Section 5.4 to align with current RCT status.

2 Introduction

The transponders, which are mounted in the gauge of the rails, interface with scanner antennas mounted on the underside of trains. Each transponder is configured to convey information to the on-board computer (OBC) specific to that transponder's location and purpose. Information is passed through the air gap to the OBC as a single telegram consisting of a set of packages that are pre-programmed into the transponder. The Transponder Interface Control Document [13] describes the structure and content of each package in detail.

The communication between the transponder and the on-board scanner antenna is based on inductive coupling. The scanner antenna transmits a signal with a frequency of 27 MHz in order to power up the transponder electronics. The transponder then transmits the pre-programmed information at a rate of 50 kHz by means of 4.5 MHz bursts, as illustrated below in Figure 1.

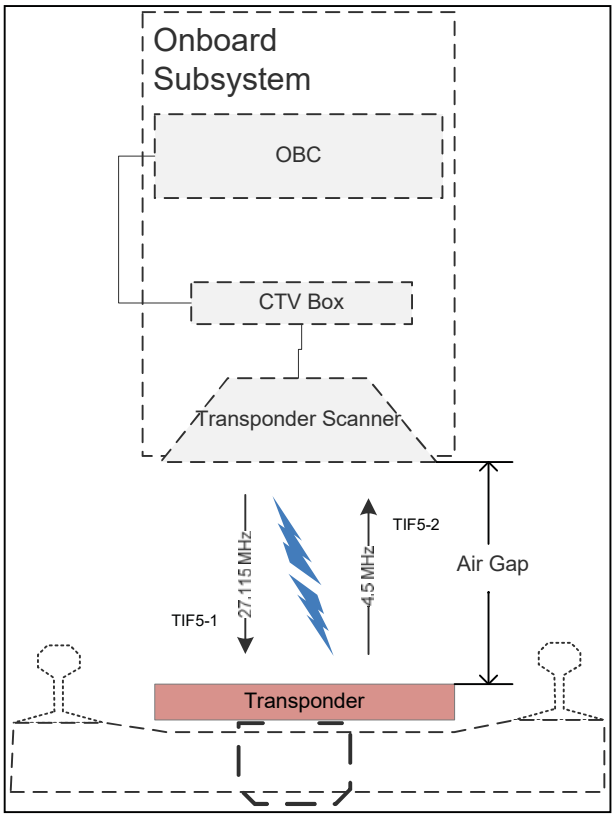


Figure 1 - Transponder Interface

Transponders are strategically placed and programmed to provide the train with advance notice of PTC information specific to the transponder's location and purpose. The transponders are programmed with telegrams composed of two or more "packages" of information – a base information package and one or more operational-specific packages. The telegrams are subject to a 180-bit data limit (with the remaining bits constituting a 72-bit CRC and 3 filler bits. Each telegram package conveys information specific to that package type, as described in the Transponder Interface Control Document [13].

Transponders are grouped into sets when placed on the track. A transponder set has a minimum of two transponders in order to provide direction to the passing train. Additional transponders are added, as needed, up to a maximum of four transponders per set.

Please refer to Transponder Subsystem Design Description [12] for further details.

This analysis is limited to the base packets and MAS packets. The complete review of the full functionality of the transponder will be provided in a future update of this document.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part I	12.10.12.A	Final Safety Report	Final Safety Report shall provide a summary of the results on the overall safety analysis, safety verification, and system safety demonstration	All
Vol 2 Part I	12.10.12.B		Final Safety Report shall contain evidence of safety analysis	3
Vol 2 Part I	12.10.12.C	MTTHE	Document the calculation and methodology to show the MTTHE requirements in 9.1 have been achieved	4
Vol 2 Part I	12.10.12.D	Risk Reduction Actions	Address all risk reduction actions taken during design, test, operation and maintenance to mitigate faults caused by Operating Scenarios, Failures, Latent Design Errors, Installation errors, Human Reaction, Post implementation changes to SW or HW, or Interoperability and compatibility issues.	5
Vol 2 Part I	12.10.12.E	Information in Report	Describes the Safety Certification process and issues encountered during certification.	5

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
			Describes certification status Describes remaining restrictions / open issues and actions / work arounds to ensure acceptable level of safety is maintained. Provides a schedule for eliminating restrictions / workarounds. As appropriate. Includes Certificate of Compliance	
Vol 2 Part 1	12.10.12.F	Resolution of all Hazards	Report shall contain evidence of the resolution of all hazards. Evidence of resolution shall consist of satisfactory closure of the items as listed in the Project Hazard Log and achievement of the items listed in the Certified Item List	5.1
	12.10.12.G	Approved by Engineer	Report format will be approved by the Engineer and submitted in draft form at FDR. Report will stay draft until final system certification is achieved.	5

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.12.H	Approval of Final Safety Report	Report is to be submitted to SSCB prior to Completion of Pilot Phase commissioning and testing. Once approved by SSCB then submitted to the FRA and revised to address comments with a disposition per FRA comment. The report will be revised when characteristics of any territory, TP interface or the TP is modified in a way that impacts the safety of the system.	5

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part I	9.1.E	MTTHE	The SI shall provide a quantifiable analysis of the safety of each of the ACSES II Subsystems and the ACSES II System as a whole. The minimum level of safety that the SI shall demonstrate through calculated Mean-Time-To-Hazardous-Event (MTTHE) is 10^{-9} hours. The MTTHE and the complete safety analysis and calculations for each ACSES II Subsystem and the ACSES II system shall be provided as part of the Final Safety Report, CDRL 2-136.	4
Vol 2 Part I	9.5.F	MTTHE	Final Safety Report shall document the complete safety analysis and calculations to support the MTTHE of the Transponder Subsystem	4

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624
[2]	LIRR Project Hazard Log (CDRL 2-126-20)	3035819
[3]	Certifiable Item List (CDRL 2-125-20)	3035818
[4]	Transponder FMECA (CDRL 2-129-05)	3037411
[5]	Transponder Subsystem Hazard Analysis (CDRL 2-128-05)	3037394
[6]	Transponder Fault Tree (CDRL 2-132-05)	3037447
[7]	LIRR Port Washington Transponder Validation Report CDRL 2-12	3043407_Rev_J
[8]	LIRR Montauk Pilot Line 1 Transponder Validation Report CDRL 2-12	3046231_Rev_J
[9]	Transponder EMI/EMC Test Report	REC-E703982
[10]	Transponder LIRR Operation Hazard Analysis CDRL 2-130-25	3037422
[11]	LIRR SRAC	3045431
[12]	Transponder Subsystem Description Document (CDRL 4-001)	3035876
[13]	Transponder Interface Control Document (CDRL 4-002)	3035877
[14]	Serial Transponder JGA 29001/6 Environmental Test Results and Analysis	EH 140030
[15]	Construction Transponder Test Report	4007070
[16]	LIRR Port Washington FAT Test Report	4008751_Rev_D
[17]	LIRR Port Washington SIT Test Report	4007924_Rev_E
[18]	LIRR Port Washington PVI	3046615_Rev_H
[19]	LIRR Montauk TP FAT Report	4008795_Rev_G
[20]	LIRR Montauk TP SIT Report	4009101_Rev_E
[21]	LIRR Montauk TP PVI	3045945_Rev_G
[22]	Transponder SRTM	3153122_Rev__
[23]	Transponder IHA	3037434 Rev _A

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in Table 3 and Table 4 respectively.

Table 3: Terms Specific to this Document

Term	Definition
Segment	A section of the railroad defined by the railroad authority and engineering in the design of the transponder design.

Table 4: Acronyms Specific to this Document

Acronym	Definition
EMC	Electromagnetic Compatibility
FAT	Factory Acceptance Test
FMECA	Failure Mode and Effects Criticality Analysis
IHA	Interface Hazard Analysis
MAS	Maximum Authorized Speed
OHA	Operational Hazard Analysis
RTC	Rational Team Concert
SSHA	Subsystem Hazard Analysis
TP	Transponder

3 Summary of Safety Analysis and Evidences

Safety analysis of the transponder was performed by analyzing the functions performed by the transponder subsystem within the overall system. The analysis performed for the transponder subsystem were the Subsystem Hazard Analysis, Fault Tree Analysis, IHA, OHA, and FMECA. The Fault Tree, OHA and SSHA are still under review with the RR safety working group. If the status is noted as Approved this indicates the Safety working group review was completed and the document was formally submitted to the Railroad.





Hazard Status:

The SSHA contained 72 hazards when this report was written. All of the hazard are mitigated by identified safety Requirements. Please refer to the SRTM section for closure status of the hazards. The SSHA updates to reflect this status will be updated in the next release of the CDRL. Updates to the Hazard Log to ensure proper closure of hazards will be completed shortly to align with the goals of revenue service demonstration.

3.1 Evidence of Closure of Items from Certified Item List

EMI/EMC Evidence:

R-2215P – Retlif Test Report on FCC Part 15 Section 15.223 for 4.5Mhz Transponder FCC ID: 2AC9HJGA29001-6. All tests results passed.

REC – E703892 Delta Test Report for EMC Test of Transponder JGA 290 01/4 HW Revision 1.7. This report indicates two failures. One in Immunity to RF electromagnetic fields between 176 and 182 MHz, and the other in Measurement of RF electromagnetic field 30Mhz to 1GHz. It should be noted the immunity tests were compliant to IEC 62236-4 2008 Std but not the requirements of the contract. Emissions and Immunity failures will be mitigated as the Transponder does not constantly transmit and only transmits once a train is over the transponder. The metallic body of the train will shield the emissions of the transponder and scanner. Years of service of both equipment is a proof of this compliance.

Climate Test Reports

EH 140030 – Shock and Vibration Testing for Bombardier for 17 Transponder Assemblies

This report indicates the transponders were tested to the contractual limits and continued to function after the shock and vibration tests. The units were found to develop cracks near the mounting holes during the testing. This cracking has been confirmed not to cause the transponders to fail.

Construction TP Test Report – 4007070 Rev __

Provides evidence that Construction Transponder Packets and layout provides mitigations to equipped trains reading and reacting to installed transponders without proper testing confirming correct speed enforcement and placement. This report indicates tests confirming that the construction zone transponder packets prevent the onboard from reading programmed transponders with valid telegrams.

Transponder Simulator Verification Report:

The transponder simulator verification report reviews the requirements of the transponder simulator and provides inspection, demonstration or test results of the simulator release to the simulator requirements. No errors were found in this release of the report.

3.1.1 Port Washington Verification Evidence.

3.1.1.1 Port Washington FAT Test Reports – 4008751_Rev_D

FAT testing for Pilot line (L2) has been completed by using the transponder simulator. Below is the table for tools used for the FAT testing and the results for Pilot line (L2) LIRR_L2_009_REL.

Table 5: Test Tools for LIRR_L2_009_REL

PTC - LIRR		
Software Configuration/ Version Control		
Pilot L2 (Port Washington) MP2 to MP17 Branch of LIRR		
Pittsburgh Test Lab/Desktop PC		
Simulators	**PVI Version**	**S/W Version**
Transponder Simulator	3049678 Rev_G	Rev 3.2.1
TPLV Tool	3047093_Rev_D	Rev 3.1
Software		
LIRR_L2_009.zip	3046615_Rev_H	L2#1

Table 6: FAT Results for LIRR_L2_009_REL

#	TC Result ID	Test Case ID	Test Case / Test Script	Actual Result	Variance/NCR ID
1.	7500	13691	Movement of train of type B in UP direction for all tracks of Port Washington	Passed	263005 (NCR Verified) 262432 (NCR Verified) 263019 (Variance Verified) 262557 (Variance Verified) 263027 (NCR Verified)
2.	7501	13692	Movement of train of type B in DOWN direction on all tracks of Port Washington	Passed with comments	263005 (NCR Verified) 262432 (NCR Verified) 263019 (Variance Verified) 262557 (Variance Verified) 263027 (NCR Verified) 262428 (Variance Open)
3.	7502	13693	Movement of train of type E in UP direction for all tracks of Port Washington	Passed	263005 (NCR Verified) 262432 (NCR Verified) 263019 (Variance Verified) 262557 (Variance Verified) 263027 (NCR Verified)
4.	7503	13694	Movement of train of type E in DOWN direction on all tracks of Port Washington	Passed with comments	263005 (NCR Verified) 262432 (NCR Verified) 263019 (Variance Verified) 262557 (Variance Verified) 263027 (NCR Verified) 262428 (Variance Open)

The following NCRs/Variances were fixed/resolved during the FAT testing for LIRR_L2_009_REL



There were new NCRs/Variances indicated in the results for LIRR_L2_009_REL FAT report [16]. Below are the new NCRs/Variances that were discovered while using LIRR_L2_009_REL for FAT testing.

[redacted]

Variance 262428 affects the transponders in the sidings that have electronic lock switches. These transponders have been turnback packages with Encoder 14, signal 8 which acts as a Forward PTS, should a train actually do a turnback. Trains won't do turnbacks here and are protected by the derails, but if they would do it a PTS would be enforced resulting in a required ASB pushbutton.

~~NCR 262432 is raised for documentation issues with the drawings for Port Washington Pilot Line L2.~~

3.1.1.2 Port Washington SIT and PICO Test Results – 4007924_rev_E

Site testing will be completed for Port Washington Pilot Line L2 and The Port Washington Transponder Site Installation Test Report [17] will be updated for LIR_L2_009_REL. Below are the results for Site testing in Port Washington Pilot Line L2 for LIRR_L2_009_REL.

Table 9: Outstanding Transponders for Test Case 1 for LIRR_L2_009_REL

Set ID	Justification	Variance/NCR
3S-0714 UP/DOWN	Outstanding Item – to be tested. Track closed before this transponder set	NCR 256628
8S-0710 UP/DOWN	Outstanding Item – to be tested Track unavailable	NCR 256628
8S-0711 UP/DOWN		
8S-0712 UP/DOWN		
8S-0713 UP/DOWN		
8S-0715 UP/DOWN		

NCR 256628 is raised for the untested transponders (SRAC SRC-L175).

The validator reviewed the site test procedure and site test report to ensure that he correct tools were used for site testing. The validator found no other issues in the SIT report for Port Washington Pilot Line L2.

3.1.1.3 PICO Test

The validator reviewed Port Washington Site Installation Test Report and procedure which included both PICO and Site testing activities. The Port Washington Transponder Site Installation Test Report includes 5 test runs that were completed on the Port Washington Pilot line L2 branch. PICO testing activities were completed in Tracks 1, 2, 3S and 8S.

All PICO testing for Port Washington Pilot Line L2 passed on all the tracks and no Variance was raised as a result. The validator found no issues or inconsistencies. The details of the PICO testing activities are in the Port Washington Transponder Site Installation Test Report [17]

3.1.1.4 Port Washington Validation Report – 3043407 Rev _J

All transponders on Port Washington Pilot Line L2 have been installed and site tested, see sections 6 and 7 for details. Tracks 3S and 8S have been included in the SRAC [11] document and are restricted from RSD in LIRR Port Washington Pilot line 2. All other tracks can be used for RSD.

The validation conditions for the Signaling System based on the above results are listed as follows:





No Test Report was found documenting the required subsystem factory test prior to integration test to be performed according to the Master Test Plan. Safety / validation do not recommend testing in the field prior to all possible factory testing being completed.

3.1.2 Montauk Verification

3.1.2.1 Montauk Factory Test Report

FAT testing for Montauk Pilot line (L1) has been completed using LIRRL1_007_REL.

Below is the table for tools used for the FAT testing and results for Montauk Pilot line (L1) as indicated in the LIRR - L1 Pilot Line Transponder FAT Test Report [19]

Table 10: Test Environment/Test Tools for LIRR_L1_007_REL

Test Environment on Transponder Simulator/Real OBC		
PTC - LIRR		
Software Configuration/ Version Control		
Pilot L1 (Mon_L1_007)		
Pittsburgh Test Lab/Desktop PC		
Simulators	**PVI Version**	**S/W Version**
Transponder Simulator	3049678 Rev_G	Rev 3.2.1
TPLVT	3047093 Rev_D	3.1
Transponder Software		
Mon_L1_007.zip	3045945_Rev_G	I1#1

Table 11: FAT Test Results for LIRR_L1_007

#	TC Result ID	Test Case ID	Test Case / Test Script	Actual Result	Variance ID
1	7606	13695	Movement of train of type B in UP direction for all tracks of Montauk from MP 31 to MP 56	Passed	263019 (Variance Verified) 262819 (Variance Verified) 255593 (NCR Verified) 263164 (NCR Verified) 263270 (NCR Verified)
2	7607	13696	Movement of train of type B in DOWN direction for all tracks of Montauk from MP 56 to MP 31	Passed	263019 (Variance Verified) 262819 (Variance Verified) 255593 (NCR Verified) 263164 (NCR Verified) 263270 (NCR Verified)
3	7608	13697	Movement of train of type E in UP direction for all tracks of Montauk from MP 31 to MP 56	Passed	263019 (Variance Verified) 262819 (Variance Verified) 255593 (NCR Verified)

#	TC Result ID	Test Case ID	Test Case / Test Script	Actual Result	Variance ID
					263164 (NCR Verified) 263270 (NCR Verified)
4	7609	13698	Movement of train of type E in DOWN direction for all tracks of Montauk from MP 56 to MP 31	Passed	263019 (Variance Verified) 262819 (Variance Verified) 255593 (NCR Verified) 263164 (NCR Verified) 263270 (NCR Verified)

The following NCRs/Variances were fixed/resolved during the FAT testing for LIRR_L1_007_REL



There were no new NCRs/Variances indicated in the results for LIRR_L1_007_REL FAT [19] report. Hence this release can be used for field testing in Montauk Pilot Line L1.

The validator reviewed the Transponder FAT test procedure and report documents for LIRR_L1_007_REL and had no questions/comments. The validator checked and verified that the FAT test tools used for FAT testing for Montauk Pilot Line L1 was the current tool stated in the FAT test procedure. No issues were found by the validator.

3.1.2.2 Montauk PICO Test Report

PICO testing for Montauk Pilot line L1 release LIRR_L1_007_REL has been completed and results has been updated in the Transponder SIT Test Report Pilot Line 1- LIRR CDRL 2-057-202 [20]. Below are the results for PICO testing.

Table 13: Failed PICO Testing for LIRR_L1_007_REL

Set ID	Index	Comments	Variance/NCR
8-3662	1	Set moved 18 feet west due to rotten ties and frog	VAR 263537
8-3662	2		
8-3349	1	Moved due to construction/freight facility	VAR 263536
8-3349	2		
8-3425	1	Moved due to frog	VAR 263535
8-3425	2		

ACSES track 8 in Babylon Yard (8-3662) is tracked by the variance 263537 and ACSES track 8 in the Central branch portion of Montauk Pilot Line 1 (8-3349, 8-3525) is tracked by variances 263536 and 263535 respectively. These does not impact RSD and will be corrected in upcoming releases.

3.1.2.3 Site Testing

Site acceptance testing for Montauk Pilot Line L1 has been completed for LIRR_L1_007_REL has been updated in the Transponder SIT Test Report Pilot Line 1- LIRR CDRL 2-057-202 [20]. Below are the results from the Sit report for Montauk Pilot Line L1.





This NCR will be tracked till closure. The validator found no other site testing issues in the SIT report for Montauk Pilot Line L1. For the full functionality of transponders in Montauk Piot Line L1, all transponders should be tested, and all NCRs and Variances should be closed

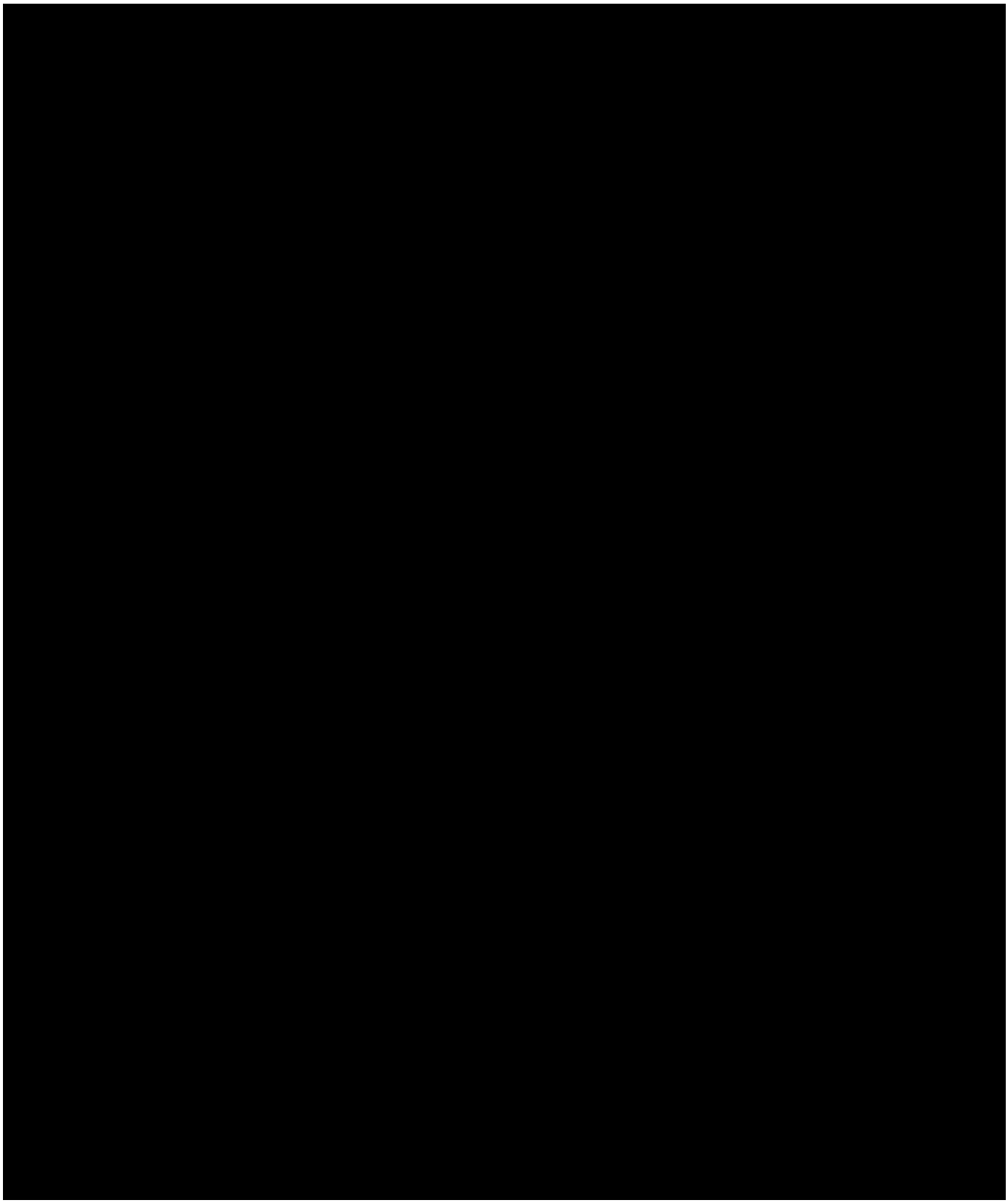
3.1.2.4 Montauk Validation Report.

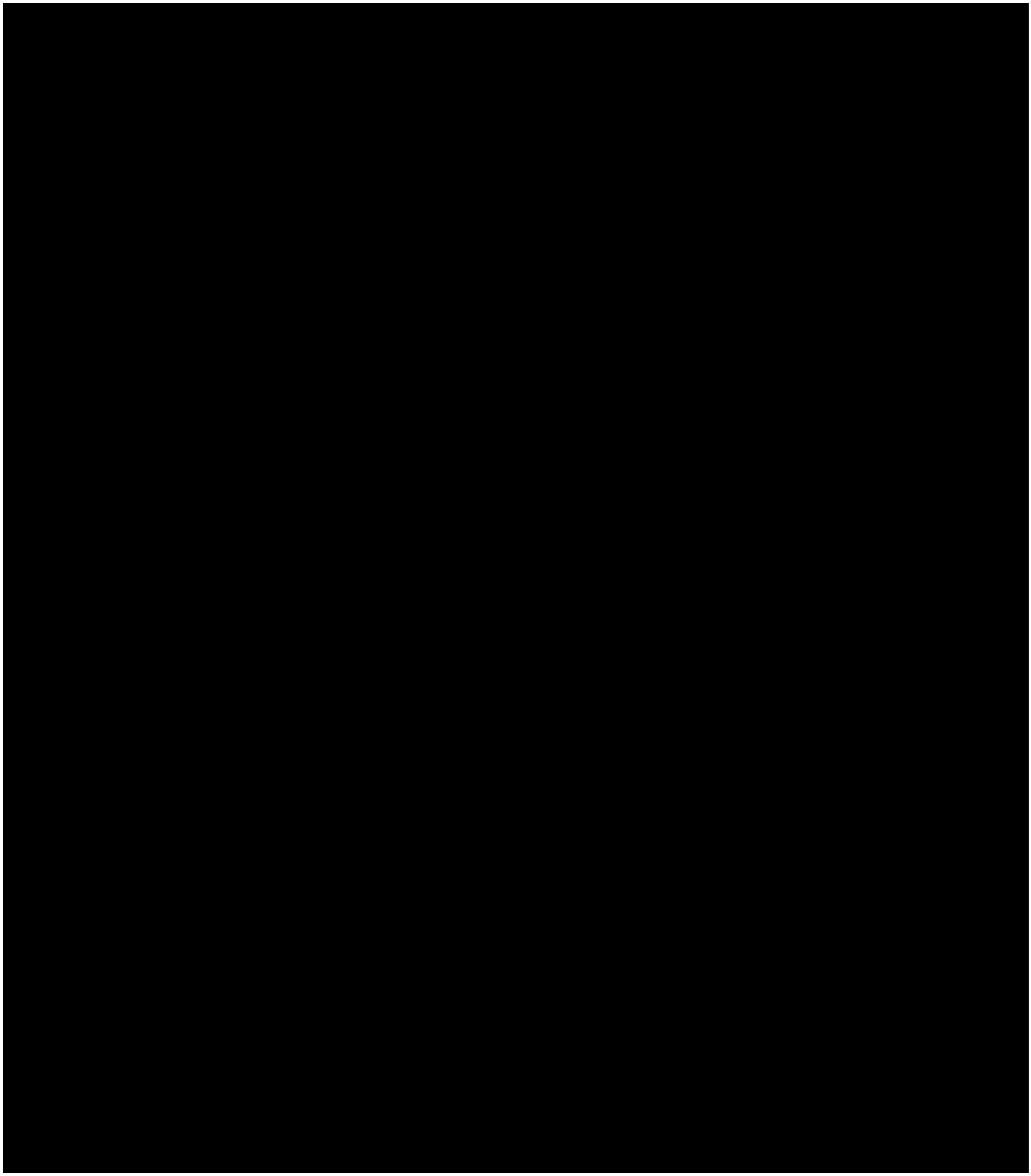
Verification artifacts has been validated and properly configuration managed, all safety related issues are tracked by NCR/Variances in this report and mitigated by SRACs in the LIRR SRAC document.

LIRR Montauk Pilot Line 1 can be used for RSD with the considerations of the SRACs for this pilot line.

The validation conditions for the Signaling System based on the above results are listed as follows:









4 Calculation of MTTHE

From the Fault Tree document and the defined failures contributing to the top hazard failure rates the Transponder MTTHE is 1.389E-13 for the defined mission.

5 Safety Certification Process

5.1 SRTM

Safety has completed the linking of the hazards to the subsystem requirements that define the mitigations that are relevant for the civil speed enforcement functionality. Safety has reviewed that the factory testing in the Rules based testing confirms that these requirements have been tested by the test cases defined in the test procedures.



5.2 FMECA

The FMECA and fault tree have been reviewed and approved. The FMECA concludes that no single points of failures exist in the transponder design. The onboard mitigations required by the FMECA for alarms for missing transponders have been confirmed to be in the type approved onboard design. These alarms will not be sent to the office as the radio system is not in place and will require the railroad to periodically inspect train data files to determine if a failed transponder set exists until the full system is installed.

5.4.2 Schedule to Remove Restrictions

The above restrictions should be removed when the next transponder release is made to the Port Washington line.

6 Conclusion

The following table lists the evidence from the safety analysis that concludes that the Transponder subsystem can support Revenue Service Demonstration on the Pilot Lines

Safety Activity	Evidence Cited	Comments
Safety Analysis	See Section 3 Certifiable Item List CDRL 2-125[3] Transponder SSHA[5] Transponder OHA[10] Transponder IHA[23] Project Hazard Log[2]	Closure of hazards to be prioritized during RSD.
Safety Analysis HW Compliance	EMI/EMC Test Report – Attachment A See Section 7 Environmental Test Report – Attachment B See Section 8	Warranty extended to cover cracking issue. No known transponder failure was shown from the cracking.
Safety Analysis FAT and SIT Reports	Port Washington Validation Report[7] Port Washington TP FAT Test Report[16] Port Washington TP SIT Test Report[17] Montauk Validation Report[8] Montauk TP FAT Test Report[19] Montauk TP SIT Test Report[20]	
Calculation of MTTHE	Transponder FTA[6]	
Safety Requirement Traceability	Transponder SRTM[22]	Three missing Test links for Line Boundary Functions to be added prior to 3.5.

		Safety to analyze Four missing links and link to Analysis evidence. All hazards linked to Safety requirements and fully linked to subsystem requirements.
FMECA	Transponder FMECA[4]	
Open NCR	Table 16 Table 18	All remaining NCR covered by SRAC
Open Variances	Table 17 Table 18	All remaining Variances covered by SRAC

As all open NCRs and Variances are mitigated by SRAC or closed. The SRAC's identified in Section Table 18 must be agreed with railroad operations to ensure the safety of the system. The safety engineer supports the operations of Pilot Line 1 and Pilot Line 2 in Revenue Service Demonstration.

7 Attachment A – R2215P Bombardier 4.5Mhz Transponder Report

See 3037458_Rev_B_Attachment_A

RETLIF TESTING LABORATORIES | Put Us To The Test℠
3131 Detwiler Road
Harleysville, PA 19438 USA
Tel: (215) 256-4133 • Fax: (215) 256-4130 • www.retlif.com

FCC Part 15, Subpart C, Section 15.223
Test Report

On

4.5 MHz Transponder
FCC ID: 2AC9HJGA29001-6

Customer Name:	Bombardier Transportation
Customer P.O:	4500740877-P1U
Date of Report:	October 21, 2014
Test Report No:	R-2215P
Test Technician:	Brian Freedman
EMC Test Engineer:	David Rybicki, Dean Landers
Approved By:	Richard C. Gaynor
Report Prepared By:	C. Reitz

Our letters, procedures and reports are for the exclusive use of the customer to whom they are addressed and their communication or the use of the name of Retlif Testing Laboratories must receive our prior written approval. Our letters, procedures and reports apply only to the sample tested and are not necessarily indicative of the qualities of apparently identical or similar products. The letters, procedures and reports and the name of Retlif Testing Laboratories or insignia are not to be used under any circumstances in advertising to the general public. This test report shall not be reproduced, except in full, without the written approval of Retlif Testing Laboratories.

Technical Information

Report Number:	R-2215P
Customer:	Bombardier Transportation
Address:	1501 Lebanon Church Road
	Pittsburg, PA 15236
Manufacturer:	Bombardier Transportation
Manufacturer Address:	1501 Lebanon Church Road
	Pittsburg, PA 15236
Test Sample:	4.5 MHz Transponder
Model Number:	JGA29001/6
FCC ID:	2AC9HJGA29001-6
Power Requirements:	Derived from a 27.1 MHz RF Signal
Frequency of Operation:	4.44 MHz
Equipment Class:	DXX
Equipment Use:	Fixed

Test Specification:
FCC Rules and Regulations Part 15, Subpart C, Section 15.223

Test Procedure:
ANSI C63.4:2003

Test Facility:
Retlif Testing Laboratories
3131 Detwiler Road
Harleysville, PA 19438

Tests Performed

The test methods performed on the 4.5 MHz Transponder are shown below:

FCC Part 15, Subpart C	Test Method
15.223(a)	Bandwidth
15.223(a)	Field Strength of Fundamental / In Band Emissions
15.223(b) / 15.209	Out of Band / Band Edge Radiated Emissions (9 kHz to 272 MHz)

General Test Requirements

1. The measurement procedures of ANSI C63.4:2003 were utilized as specified in FCC Part 15, Subpart C, Section 15.31(a)(3).
2. All radiated emissions measurements were performed on an Open Area Test Site (OATS), listed with the FCC, in accordance with FCC Section 15.31(d).
3. The level of the fundamental field strength was measured with the position of the EUT over the scanner varied.
4. All measurements were performed at the specified 3 and 10 meter test distance as required by FCC Section 15.31(f).
5. The EUT was rotated throughout 360 degrees for all radiated emissions measurements as specified in FCC Section 15.31(f)(5).
6. All readily accessible EUT controls were adjusted in such a manner as to maximize the level of emissions in accordance with FCC Section 15.31(g).
7. Appropriate accessories were attached to all EUT ports during the performance of radiated emissions measurements as required by FCC Section 15.31(i).
8. The EUT operated at the frequency range of 4.44 MHz in accordance with FCC Section 15.31(m).
9. The frequency spectrum was investigated from the lowest frequency generated in the device up to the 10th harmonic of the highest fundamental frequency in accordance with FCC Section 15.33(a)(1).
10. All measurements were taken with an average detector function as specified in FCC Section 15.223(a). An additional peak measurement was made in accordance with FCC Section 15.35(c), with the average limit increased by 20 dB.

Certification and Signatures

We certify that this report is a true representation of the results obtained from the tests of the equipment stated. We further certify that the measurements shown in this report were made in accordance with the procedures indicated and vouch for the qualifications of all Retlif Testing Laboratories personnel taking them.

David Rybicki
EMC Test Engineer
NVLAP Approved Signatory

Richard C. Gaynor
Laboratory Manager
iNARTE Certified Engineer EMC-000214-NE
NVLAP Approved Signatory

Non-Warranty Provision
The testing services have been performed, findings obtained and reports prepared in accordance with generally accepted laboratory principles and practices. This warranty is in lieu of all others, either expressed or implied.

Non-Endorsement
This test report contains only findings and results arrived at after employing the specific test procedures and standards listed herein. It is not intended to constitute a recommendation, endorsement or certification of the product or material tested. This test report must not be used by the client to claim product endorsement by NVLAP or any agency of the U.S. Government.

Requirements and Test Results

Requirement:
FCC Section 15.223 – Operation in the band 1.705 – 10.0 MHz
(a) The field strength of any emission within the band 1.705 – 10.0 MHz shall not exceed 100 microvolts/meter at a distance of 30 meters. However, if the bandwidth of the emission is less than 10% of the center frequency, the field strength shall not exceed 15 microvolts/meter or (the bandwidth of the device in kHz) divided by (the center frequency of the device in MHz) microvolts/meter at a distance of 30 meters, whichever is the higher level. For the purposes of this section, bandwidth is determined at the points 6 dB down from the modulated carrier.

(b) The field strength of emissions outside of the band 1.705 – 10.0 MHz shall not exceed the general radiated emission limits in Section 15.209.

- Results:
  The 6 dB bandwidth was measured and found to be 117 kHz, 2.6 % of the center frequency.

Requirement:
FCC Section 15.209(a) - Radiated Emission Limits, General Requirements
Except as provided elsewhere in this subpart, the emissions from an intentional radiator shall not exceed the field strength levels specified in Table 1.

Table 1 - Radiated Emission Limits

Frequency of Emission (MHz)	Field Strength (microvolts/meter)	Measurement Distance (meters)
1.705 to 30	30	30
30 to 88	100	3
88 to 216	150	3
216 to 960	200	3
Above 960	500	3

The Fundamental and Harmonic Emissions limits for a device operating at 4.44 MHz are listed in Table 2. This limit is derived from FCC Section 15.223(a).

Table 2 - Fundamental and Harmonic Limits

Frequency of Operation MHz	Fundamental µV/m	Harmonics µV/m
Average - 4.44	26.38	26.38
Peak – 4.44	263.8	263.8

- Results:
  The Fundamental and Harmonics field strengths did not exceed the limits specified in Table 2 at a test distance of 3 and 10 meters, taken with an Average and Peak Detector. See Table 3 for the Fundamental and Harmonic emissions test results.

Table 3 - Fundamental and Harmonics Test Results

Fundamental Frequency MHz	Maximum Fundamental µV/m	Maximum Harmonics µV/m
Average - 4.44	25.23	7.87
Peak – 4.44	12.5	0.99

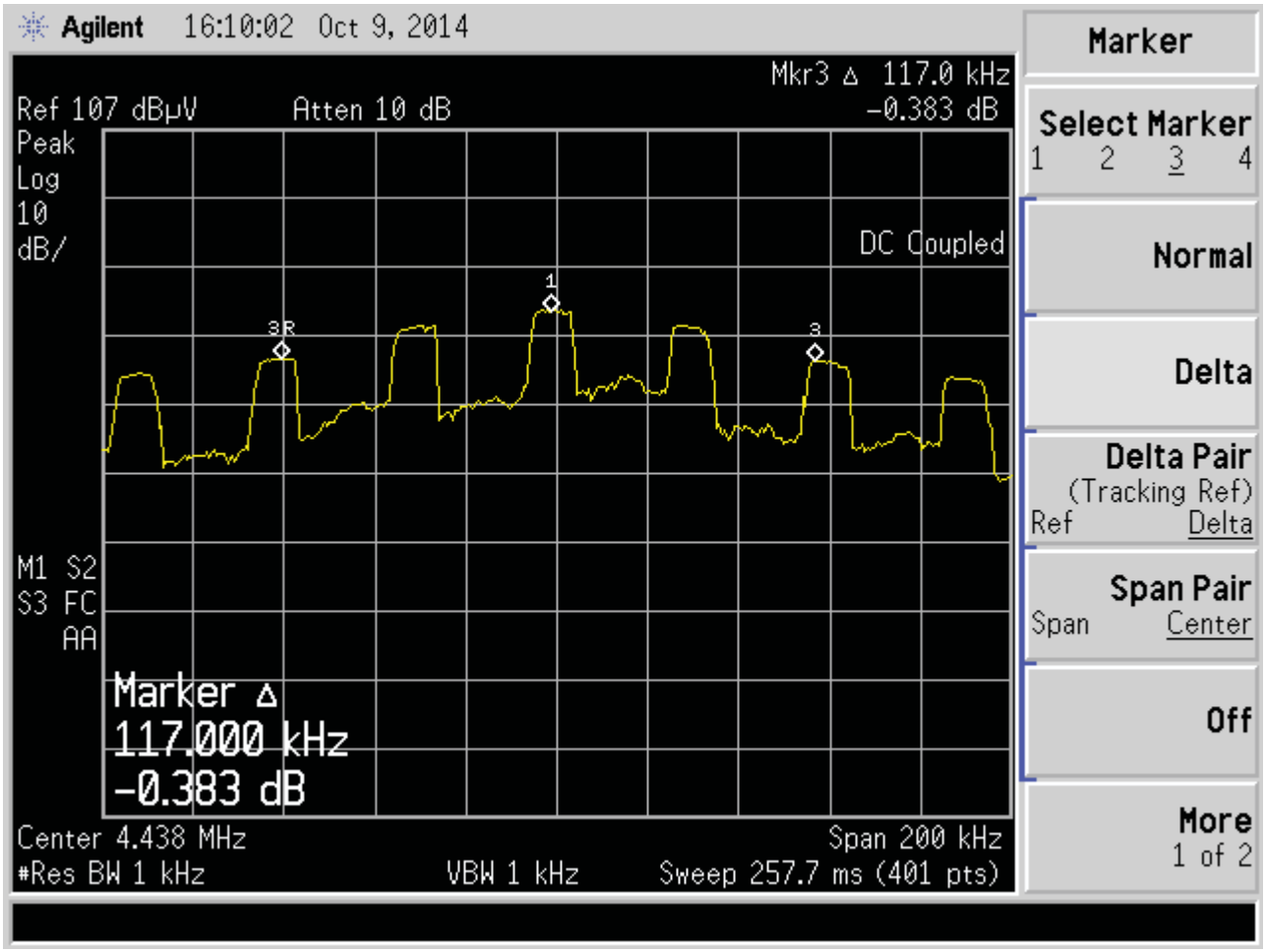
Equipment Lists

FCC Section 15.223(a) - Bandwidth
FCC Section 15.223(a) – Field Strength of Fundamental / In Band Emissions
FCC Section 15.223(b) – Out of Band / Band Edge Radiated Emissions (9 kHz to 272 MHz)

EN	Manufacturer	Description	Range	Model No.	Cal Date	Due Date
3207	EMCO	ACTIVE LOOP	10 KHZ- 30 MHZ	6502	1/22/2014	1/31/2015
8076	AGILENT / HP	SPECTRUM ANALYZER	100 Hz - 1.5 GHz	8568B	10/18/2013	10/31/2014
8077	AGILENT / HP	SPECTRUM ANALYZER		85662A	10/18/2013	10/31/2014
8079	ROHDE & SCHWARZ	EMI TEST RECEIVER		ESH3	6/30/2014	6/30/2015
8080	ROHDE & SCHWARZ	EMI TEST RECEIVER	20-1300 MHz	354-3000.56ESVP	12/16/2013	12/31/2014
8411	SONOMA INSTRUMENT	PRE-AMPLIFIER	9 kHz - 1 GHz	310N	9/4/2013	9/30/2014
8433	ETS LINDGREN	BICONILOG	20 - 6000 MHz	3142D	3/10/2014	9/30/2015

FCC Part 15, Subpart C
15.223(a), Bandwidth
4 MHz to 10 MHz
Test Data

EMISSIONS TEST DATA SHEET	
Test Specification:	**FCC Part 15, Subpart C**
Method:	15.223(a) Bandwidth
Job Number/Customer:	R – 2215P / Bombardier Transportation
Test Sample:	4.5 MHz Transponder
Model Number:	JGA 29001/6
Serial Number:	E1514000001
Operating Mode:	Continuously Sending Data
Technician:	D. Rybicki
Date(s):	10/10/14
Temperature:	15.6 ºC
Relative Humidity:	50 %



FCC Part 15, Subpart C
15.223 (b), Out of Band / Band Edge Radiated Emissions
9 kHz to 1.705 MHz
10 MHz to 272 MHz
Test Data

EMISSIONS TEST DATA SHEET

Test Specification:	**FCC Part 15, Subpart C**
Method:	15.223(a) Field Strength of Fundamental/In Band Emissions
Job Number/Customer:	R – 2215P / Bombardier Transportation
Test Sample:	4.5 MHz Transponder
Model Number:	JGA 29001/6
Serial Number:	E1514000001
Operating Mode:	Continuously Sending Data
Technician:	D. Rybicki
Date(s):	10/10/14
Temperature:	15.6 ºC
Relative Humidity:	50 %
Test Distance:	10 m converted to 30m
Detector:	Average

TEST PARAMETERS

Frequency	Antenna Polarization	EUT Orientation	Meter Reading	Correction Factor	Corrected Reading	Corrected Reading	Limit
MHz	**Horizontal / Vertical**	**Degrees**	**dBuV**	**dB**	**dBuV/m**	**uV/m**	**uV/m**
4.00							26.38
I							I
4.4039	Parallel	109.6	27.5	-9.36	18.14	8.07	I
4.4039	Perpendicular	98.0	15.9	-9.36	6.54	2.12	I
I							I
4.4357	Parallel	125.9	31.3	-9.36	21.94	12.50	I
4.4357	Perpendicular	152.0	12.4	-9.36	3.04	1.42	I
I							I
4.4684	Parallel	103.7	27.9	-9.36	18.54	8.45	I
4.4684	Perpendicular	106.0	11.3	-9.36	1.94	1.25	I
I							I
4.4998	Parallel	98.2	24.0	-9.36	14.64	5.40	I
4.4998	Perpendicular	104.7	14.5	-9.36	5.14	1.81	I
I							I
8.8714	Parallel	88.4	7.2	-9.28	-2.08	0.79	I
8.8714	Perpendicular	132.7	9.2	-9.28	-0.08	0.99	I
I							I
10.00							26.38

The frequency range was scanned from 4 MHz to 10 MHz
The emissions observed from the EUT do exceed the limits specified. All emissions not recorded were more than 20dB below the specified limit

EMISSIONS TEST DATA SHEET

Test Specification:	**FCC Part 15, Subpart C**
Method:	15.223(a) Field Strength of Fundamental/In Band Emissions
Job Number/Customer:	R – 2215P / Bombardier Transportation
Test Sample:	4.5 MHz Transponder
Model Number:	JGA 29001/6
Serial Number:	E1514000001
Operating Mode:	Continuously Sending Data
Technician:	D. Rybicki
Date(s):	10/10/14
Temperature:	15.6 ºC
Relative Humidity:	50 %
Test Distance:	10 m converted to 30m
Detector:	Peak

TEST PARAMETERS

Frequency	Antenna Polarization	EUT Orientation	Meter Reading	Correction Factor	Corrected Reading	Corrected Reading	Limit
MHz	**Horizontal / Vertical**	**Degrees**	**dBuV**	**dB**	**dBuV/m**	**uV/m**	**uV/m**
4.00							263.8
I							I
4.4039	Parallel	109.6	33.5	-9.36	24.14	16.11	I
4.4039	Perpendicular	98.0	29.9	-9.36	20.54	10.64	I
I							I
4.4357	Parallel	125.9	37.4	-9.36	28.04	25.23	I
4.4357	Perpendicular	152.0	28.1	-9.36	18.74	8.65	I
I							I
4.4684	Parallel	103.7	37.3	-9.36	27.94	24.94	I
4.4684	Perpendicular	106.0	28.4	-9.36	19.04	8.95	I
I							I
4.4998	Parallel	98.2	36.8	-9.36	27.44	23.55	I
4.4998	Perpendicular	104.7	34.0	-9.36	24.64	17.06	I
I							I
8.8714	Parallel	88.4	22.3	-9.28	13.02	4.48	I
8.8714	Perpendicular	132.7	27.2	-9.28	17.92	7.87	I
I							I
10.00							263.8

The frequency range was scanned from 4 MHz to 10 MHz
The emissions observed from the EUT do exceed the limits specified. All emissions not recorded were more than 20dB below the specified limit

FCC Part 15, Subpart C
15.223 (b), Out of Band / Band Edge Radiated Emissions
9 kHz to 1.705 MHz
10 MHz to 272 MHz
Test Data

EMISSIONS TEST DATA SHEET

Test Specification:	**FCC Part 15, Subpart C**
Method:	15.223(b) Out of Band / Band Edge Radiated Emissions
Job Number/Customer:	R – 2215P / Bombardier Transportation
Test Sample:	4.5 MHz Transponder
Model Number:	JGA 29001/6
Serial Number:	E1514000001
Operating Mode:	Continuously Sending Data
Technician:	B. Freedman / D. Rybicki
Date(s):	10/10/14
Temperature:	20.3 ºC
Relative Humidity:	47 %
Test Distance:	10 m converted to limit specified distance
Detector:	Quasi-Peak

TEST PARAMETERS

Frequency	Antenna Polarization	EUT Orientation	Meter Reading	Correction Factor	Corrected Reading	Corrected Reading	Limit
MHz	Horizontal / Vertical	Degrees	dBuV	dB	dBuV/m	uV/m	uV/m
0.009							266.67 @ 300m
I							I
0.490							4.90 @ 300m
0.490							48.97 @ 30m
I							I
1.705							14.08 @ 30m
10.00							30.00 @ 30m
I							I
13.3071	Parallel	180.0	13.1	1.26	14.36	5.16	I
13.3071	Perpendicular	180.0	9.0	1.26	10.26	3.26	I
I							I
17.7428	Parallel	180.0	10.5	1.15	11.65	3.82	I
17.7428	Perpendicular	180.0	8.0	1.15	9.15	2.87	I
I							I
22.1785	Parallel	180.0	7.5	0.61	8.11	2.54	I
22.1785	Perpendicular	180.0	6.1	0.61	6.71	2.17	I
I							I
26.6142	Parallel	180.0	4.8	-0.12	4.68	1.71	I
26.6142	Perpendicular	180.0	18.3	-0.12	18.18	8.11	I
I							I
30.00							30.00 @ 30m

The frequency range was scanned from 9 kHz to 10 MHz and from 10 MHz to 30 MHz
The emissions observed from the EUT do not exceed the limits specified. All emissions not recorded were more than 20dB below the specified limit

EMISSIONS TEST DATA SHEET

Test Specification:	**FCC Part 15, Subpart C**
Method:	15.223(b) Out of Band / Band Edge Radiated Emissions
Job Number/Customer:	R – 2215P / Bombardier Transportation
Test Sample:	4.5 MHz Transponder
Model Number:	JGA 29001/6
Serial Number:	E1514000001
Operating Mode:	Continuously Sending Data
Technician:	B. Freedman / D. Rybicki
Date(s):	10/10/14
Temperature:	20.3 ºC
Relative Humidity:	47 %
Test Distance:	3 m
Detector:	Quasi-Peak

TEST PARAMETERS

Frequency	Antenna Polarization	EUT Orientation	Meter Reading	Correction Factor	Corrected Reading	Corrected Reading	Limit
MHz	Horizontal / Vertical	Degrees	dBuV	dB	dBuV/m	uV/m	uV/m
30.00							100.00
I							I
31.0499	H / 1.00	180.0	11.7	17.56	29.26	29.07	I
31.0499	V / 1.00	180.0	20.1	17.56	37.66	76.38	I
I							I
34.4856	H / 1.00	180.0	9.9	15.68	25.58	19.01	I
34.4856	V / 1.00	180.0	20.8	15.68	36.48	66.68	I
I							I
39.9213	H / 4.00	180.0	10.7	12.84	23.54	15.03	I
39.9213	V / 1.00	180.0	17.4	12.84	30.24	32.51	I
I							I
44.3570	H / 4.00	180.0	15.3	10.97	26.27	20.58	I
44.3570	V / 1.00	180.0	19.3	10.97	30.27	32.62	I
I							I
88.00							100.00
88.00							150.00
I							I
216.00							150.00
216.00							200.00
I							I
272.00							200.00

The frequency range was scanned from 30 MHz to 272 MHz
The emissions observed from the EUT do not exceed the limits specified. All emissions not recorded were more than 20dB below the specified limit

8 Attachment B – REC – E703892

See 3037458_Rev_B_Attachment_B

We help ideas meet the real world

DELTA Test Report

TEST REPORT issued by an Accredited Testing Laboratory

1688
ISO/IEC 17025

EMC test of Transponder JGA 290 01/4

Performed for Bombardier Transportation

REC-E703892
Project no.: E703892

30 January 2015

DELTA Development Technology AB
Finnslätten
Elektronikgatan 47
721 36 Västerås
Sweden

Tel. 021-31 44 80
Fax 021-31 44 81
info@delta-dt.se
www.delta-dt.se

Bankgiro 5534-7728
VAT SE 556556207001

DELTA Development Technology AB
is a subsidiary company of DELTA

This report is issued under the rules of SWEDAC (Swedish Accreditation) and ILAC (International Laboratory Accreditation Cooperation) including its MRA (Mutual Recognition Arrangement). Further information can be found at www.swedac.se and www.ilac.org.
The report must not be reproduced, except in full, without the written approval of DELTA.

Title	EMC test of Transponder JGA 290 01/4
Test object	Transponder JGA 290 01/4
Report no.	REC-E703892
Project no.	E703892
Test period	4 June 2014 to 9 June 2014
Client	Bombardier Transportation Box 42505 SE 12 616 Stockholm Sweden Tel.: +46 10 852 5000
Contact person	Mikael Matsson E-mail: mikael.matson@se.transport.bombardier.com
Client observers	Mikael Mattsson and Johan Nilsson
Manufacturer	Bombardier Transportation
Specifications	IEC 62236-4:2008 and LIRR/MNR Contract 1712 Positive Train Control
Results	The test object did not fulfil part(s) of the requirements, please refer to Section 1
Test personnel	Daniela Coman
Date	30 January 2015

Project Manager

Daniela Coman Specialist
DELTA

Responsible

Ulf Bjerke Technical Manager
DELTA

Table of contents

		Page
1.	**Summary of tests**	**4**
2.	**Test object and auxiliary equipment**	**5**
2.1	Test object	6
2.2	Auxiliary equipment	7
3.	**General test conditions**	**10**
3.1	Measurement procedure for ESD test	10
3.2	Measurement procedure for Radiated Immunity tests	11
3.3	Measurement procedure for Radiated emission tests	12
3.3.1	Measurement procedure for Radiated emissions tests 30 MHz to 1 GHz	12
3.3.2	Measurement procedure for Radiated emissions tests above 1 GHz	14
3.4	EUT test setup	15
3.4.1	Description and intended use of test object, operation mode	16
3.5	Criteria for compliance during immunity test	16
3.6	Modifications of the test object	16
3.7	Test sequence	17
4.	**Test results**	**18**
4.1	Immunity to electrostatic discharges	18
4.2	Immunity to RF electromagnetic field 80 MHz – 6 GHz	25
4.3	Measurement of RF electromagnetic field 30 MHz – 1000 MHz	33
4.4	Measurement of RF electromagnetic field 1 – 6 GHz	38
5.	**National registrations and accreditations**	**42**
5.1	SWEDAC Accreditation	42
5.2	FCC Registrations	42
5.3	IC Registrations	42
6.	**List of instruments**	**43**

1. Summary of tests

Tests	Test methods	Results
Immunity to electrostatic discharges	IEC 61000-4-2:2009	Passed, see Note 1
Immunity to RF electromagnetic fields 80 MHz – 6 GHz	IEC 61000-4-3:2006+A1+A2	Partly compliant, Note 1 Failed between 176-182 MHz. Passed the rest of the tested frequency range.
Immunity to fast transients	IEC 61000-4-4:2012	Not relevant, see Note 2
Immunity to surge transients	IEC 61000-4-5:2005	Not relevant, see Note 2
Immunity to conducted RF disturbances	IEC 61000-4-6:2009	Not relevant, see Note 2
Immunity to fluctuations, dips and short interruptions	IEC 61000-4-29:2000	Not relevant, see Note 2
Immunity to polarity reversal	EMI/EMC Control Plan CDR 2-98 Identity No: 3035790	Not relevant, see Note 2
Measurement of RF voltage on power port	CISPR 16-2-1:2008+A1 IEC 61000-6-4:2006+A1	Not relevant, see Note 2
Measurement of RF voltage on telecommunication port	CISPR 22:2008	Not relevant, see Note 2
Measurement of RF electromagnetic field 30 MHz – 1 GHz 1GHz – 6 GHz	CISPR 16-2-3:2010+A1 Limits according to IEC 61000-6-4:2006+A1 IEC 61000-6-4:2006+A1	 Failed Passed

Note 1: Higher test level were applied, according to document LIRR/MNR Contract 1712 Positive Train Control

Note 2: They are no cables connected to the Transponder. The Transponder is powered from the carrier of a 27.095 MHz transmitter (Scanner).

Conclusion

The test object mentioned in this report meets the requirements of the standard stated below, except for Radiated emission between 30 and 1000 MHz.

- IEC 62236-4 Edition 2.0 2008-12
  "Railway applications - Electromagnetic compatibility - Part 4: Emission and immunity of the signalling and telecommunications apparatus".

Note: The test object mentioned in this report is partly compliant with the document LIRR/MNR Contract 1712 Positive Train Control due to more severe test levels.

The test results relate only to the object tested.

2. Test object and auxiliary equipment

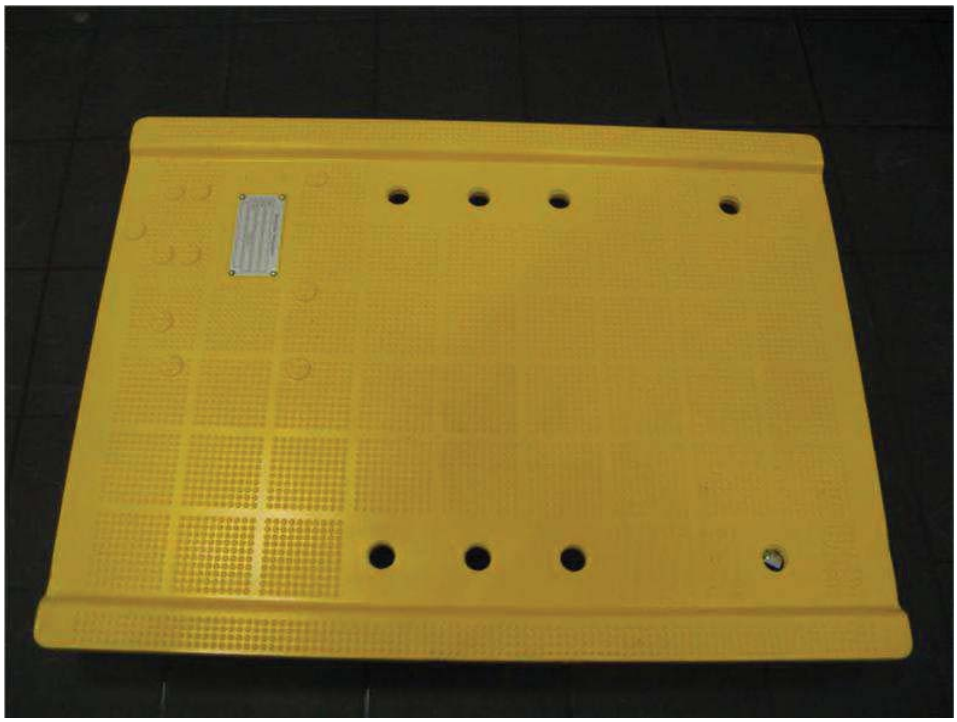


Photo 2.1.1 Test object i.e. JGA 290 01/4 Transponder, view of upper side.



Photo 2.1.2 Test object i.e. JGA 290 01/4 Transponder, view of bottom side.

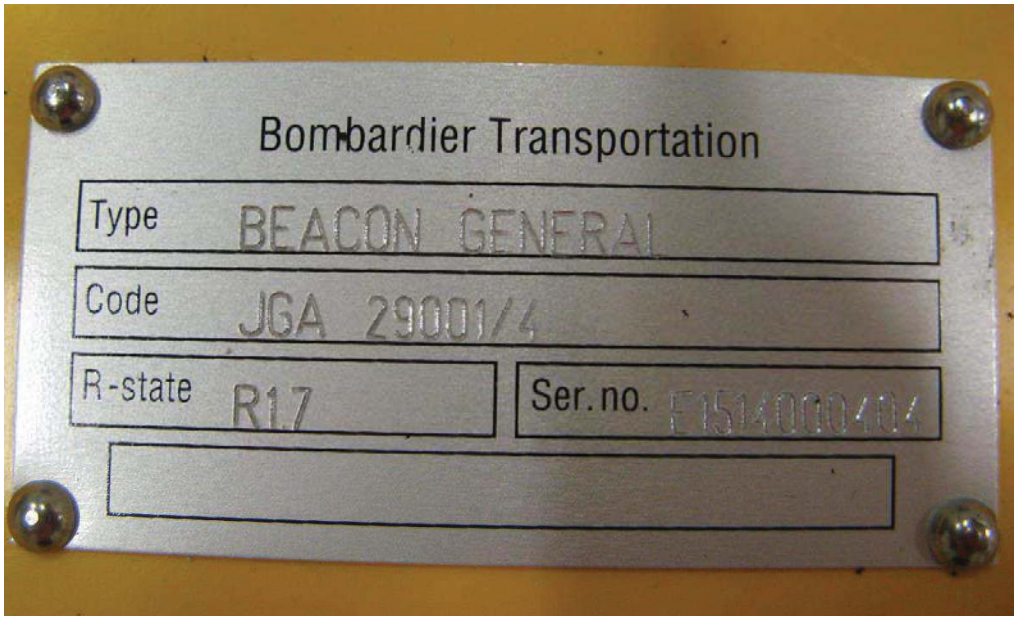


Photo 2.1.3 Label on test object.

2.1 Test object

Test object 2.1.1

Name of test object	Transponder
Model / type	JGA 290 01/4
Part no.	-
Serial no.	E1514000404
FCC ID	-
Manufacturer	Bombardier Transportation
Supply voltage	Energized from the carrier of a 27.095 MHz transmitter (Scanner)
Software version	-
Hardware version	R1.7
Highest generated frequency	4.4 MHz
Received	Date: 2014-05-28 Status: Used

2.2 Auxiliary equipment

Auxiliary equipment 2.2.1

Name of auxiliary equipment	Personal computer
Model / type	HP 6730b
Manufacturer	HP
Supply voltage	230 VAC
	Auxiliary equipment supplied by the client, who also has the responsibility for its correct function and set up.
Comment	Equipped with SW for test: BTIT client lab v8.6

Auxiliary equipment 2.2.2

Name of auxiliary equipment	BTM 2000
Model / type	BTM 2000 V3.3 (Low Voltage)
Part no.	3NSS001688-01
Serial no.	E40800725
FCC ID	-
Manufacturer	Bombardier Transportation
Supply voltage	Powered with 48 VDC from Power supply Mascot 8921
	Auxiliary equipment supplied by the client, who also has the responsibility for its correct function and set up.

Auxiliary equipment 2.2.3

Name of auxiliary equipment	Scanner
Model / type	GPA 2000
Part no.	3NSS000311-01 V2.1
Serial no.	E41400126
FCC ID	-
Manufacturer	Bombardier Transportation
Highest frequency generated or used	27.095 MHz
	Auxiliary equipment supplied by the client, who also has the responsibility for its correct function and set up.
Comment	Used to energize the Transponder.

Auxiliary equipment 2.2.4

Name of auxiliary equipment	Modem
Model / type	Access MA-42
FCC ID	-
Manufacturer	Westermo
	Auxiliary equipment supplied by the client, who also has the responsibility for its correct function and set up.
Comment	RS 422 to RS 232

Auxiliary equipment 2.2.5

Name of auxiliary equipment	Reference Loop
Model / type	-
Part no.	3NSS001152-01
Serial no.	A1295
FCC ID	-
Manufacturer	Bombardier
	Auxiliary equipment supplied by the client, who also has the responsibility for its correct function and set up.
Comment	Used instead of Transponder JGA 290 01/4, in order to measure the radiated emission from the environment (without the test object).



Photo 2.2.1 Photos of the Scanner which during tests, was placed inside the test chamber.



Photo 2.2.2 Auxiliary equipment used during the tests, placed outside test chamber.



Photo 2.2.3 Photo illustrating the Reference Loop tested with Scanner.

3. General test conditions

3.1 Measurement procedure for ESD test

The Transponder was tested as a tabletop equipment on an ESD table.
The test setup consisted of a wooden table, 0.8 m high, standing on the ground reference plane. A horizontal coupling plane was placed on the table and was connected to the GRP via a cable with 470 kW resistor located at each end.
The Transponder was isolated from the coupling plane by an insulating support 0.5 mm thick.

An example of the test set-up for tabletop equipment is given in figure below.

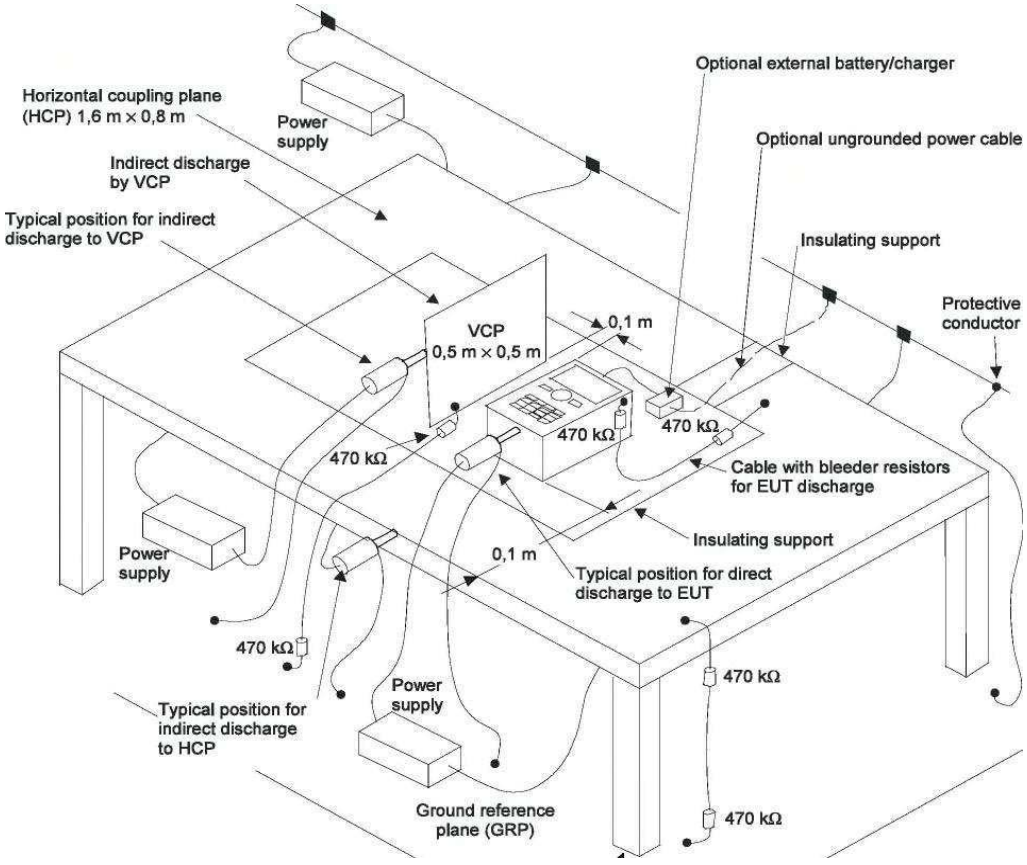


Figure 3.1.1 : General setup for ESD test

The test voltage was increased from a minimum test level to the required test level for air discharge test. The test levels below the required test levels are selected from the following levels: +/-4 kV, 8 and 15 kV. The test level shall not be increased before all the selected test points of the EUT are exercised using one test level.
Contact discharge test was applied with +/- 6 and 8 kV test level.

Indirect discharges was also performed by applying ESD discharge to a Vertical Coupling Plane placed 10 cm from the EUT.

3.2 Measurement procedure for Radiated Immunity tests

The Transponder was tested as a tabletop equipment, placed on a non-conductive table with a height of 0.8m above the ground reference plane.

No consideration for arrangement of cables was taken during test of Transponder, for no cables were connected to it.

The chosen dwell time was 3 sec and the step size 1% of the preceding frequency value.

The carrier signal was 80% amplitude modulated with a 1 kHz sine wave.
The tests were carried out in the full anechoic chamber in the frequency range 80 MHz – 1000 MHz, at 3 m test distance and in the semi-anechoic chamber for test between 1GHz to 6 GHz which was carried out at 1.5 m test distance.

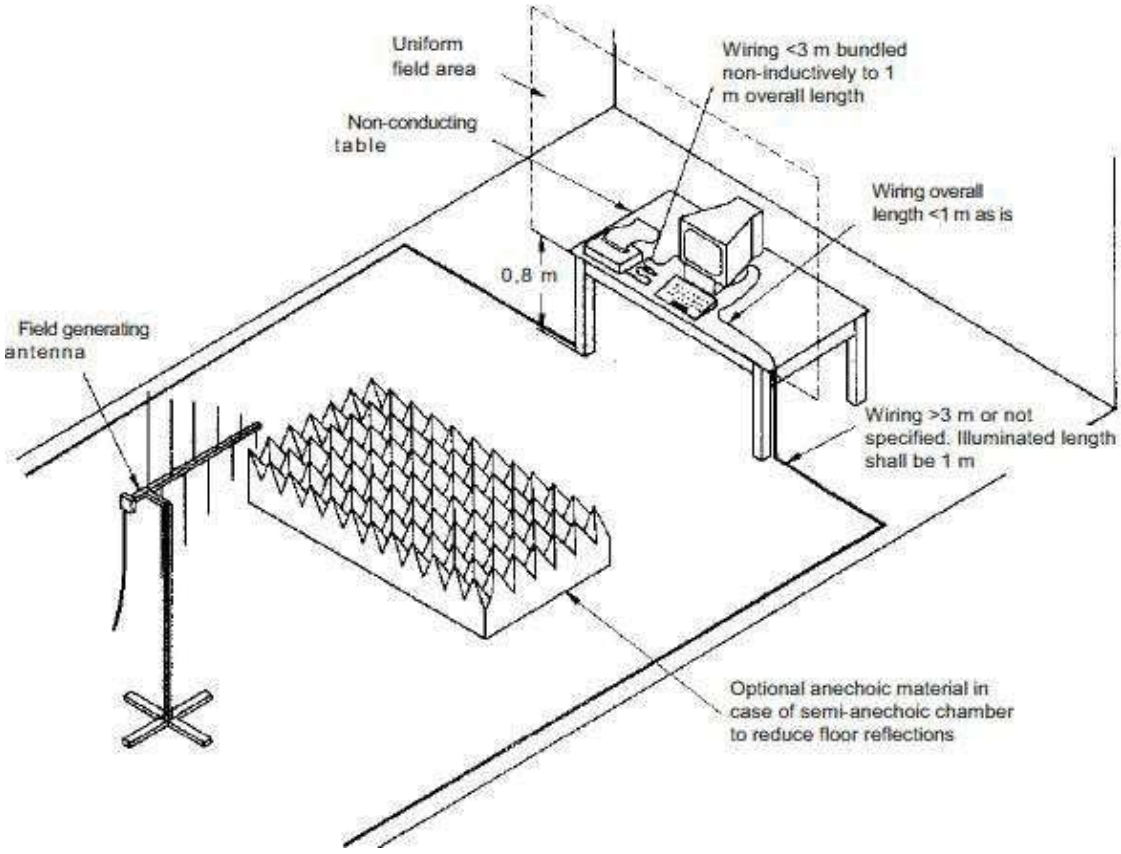


Figure 3.2.1 : General setup for Radiated RF immunity test

3.3 Measurement procedure for Radiated emission tests

The measurement facility is a semi-anechoic chamber, validated according to CISPR 16 and ANSI C63.4. The volumetric Normalized Site Attenuation, NSA, satisfy the ± 4dB criterion, in the frequency range 30 MHz to 1000 MHz, in a cylinder with diameter of 3 m and height of 2 m at 3 m and 10 m measurement distance.

The chamber is validated according to CISPR 16-1-4 VSWR method and complies with the 6 dB requirements in a cylinder with diameter of 3m and a height of 2,3 m with 3 m measurement distance.

The operation of the EUT shall be as identical as possible as the normal operation of it. The configuration of it shall be selected such that the emission is maximized. Measurements shall be made such that the maximum radiated emission level can be detected.

3.3.1 Measurement procedure for Radiated emissions tests 30 MHz to 1 GHz

The general test setup for a table top equipment is given in figure here below. If floor standing equipment is measured, it is placed on the floor, electrical insulated from it by up to 12 mm.

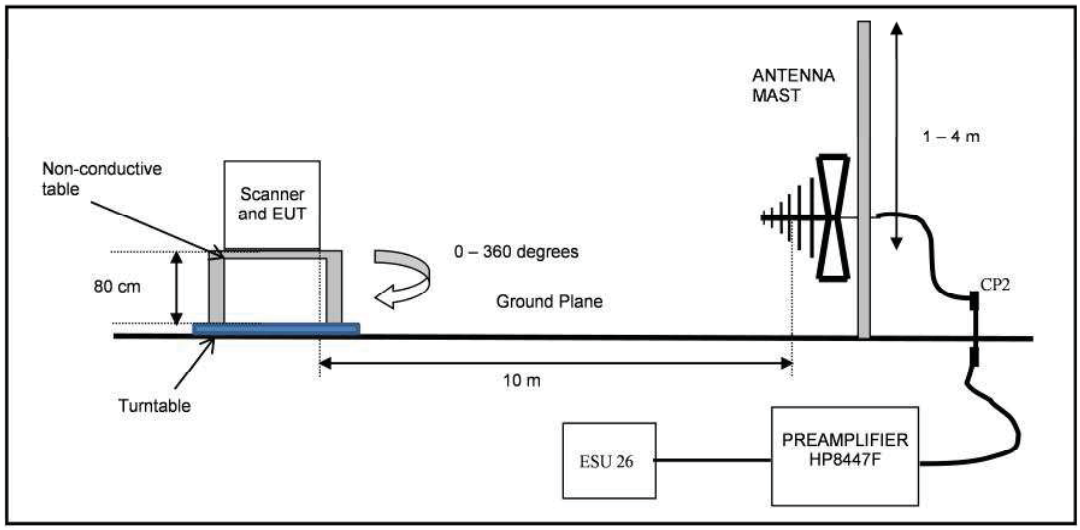


Figure 3.3.1 : Setup for measurements in the frequency range 30 MHz to 1 GHz.

The details of used test equipment are shown in section 6 List of instruments.

The Transponder was tested as a tabletop equipment, which means that it was placed on a non-conductive table, 80 cm above the ground reference plane. The Scanner was mounted 35.5 cm above the Transponder oriented facing down.

The screened cable from the Scanner was connected to the Auxiliary equipment, BTM 2000, placed outside the test chamber.

During the emission tests performed on Transponder JGA 290 01/4, the test setup was configured as described in section 3.1.
The measurements sequence was automatic and controlled from a computer.
The measurement resolution bandwidth of the analyzer/receiver is 120 kHz and the used detectors are Peak and Quasi Peak.

A biconical-log/ hybrid antenna was used and the measurements were carried out 10 m from the periphery of the EUT, by varying the antenna height from 1 m to 4 m.
The measuring instrument was in Peak mode during the pre-scan measurements and the maximization procedure and in Quasi Peak mode when final measurements were performed.

During the initial characterization of the EUT, pre-scan measurements in 64 positions were performed, at antenna heights of 1, 2, 3 and 4 m and azimuth angles of 0, 45, 90, 135, 180, 225, 270 and 315 degrees. See Figure 2.1.2 regarding angles of turntable.
The measurements were carried out in horizontal as well as vertical orientation of the antenna.
After these initial measurements, at each critical frequency, closer than 20 dB from the limit line, first the turntable angle and then the antenna height were varied within a certain range (+/- 45 degrees for turntable and +/-100 cm for the antenna), in order to found the maximum emission more precisely.
The measurements were performed in both horizontal and vertical orientation of the antenna.

When the direction of highest emission in Peak mode was found, final measurement with Quasi-Peak detector with a measurement time of at least 1s was performed.

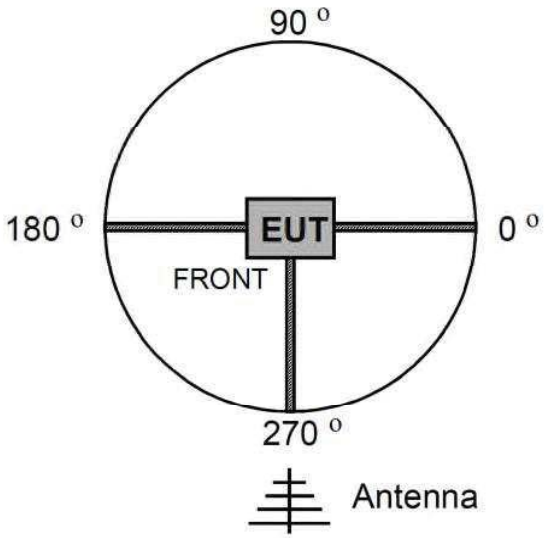


Figure 3.3.2 : Position of EUT on turntable referring.

3.3.2 Measurement procedure for Radiated emissions tests above 1 GHz

The general test setup for a table top equipment is illustrated in the figure here below.

The Radiated emission measurement above 1GHz was performed in the semi-anechoic chamber with the floor covered with absorbers.

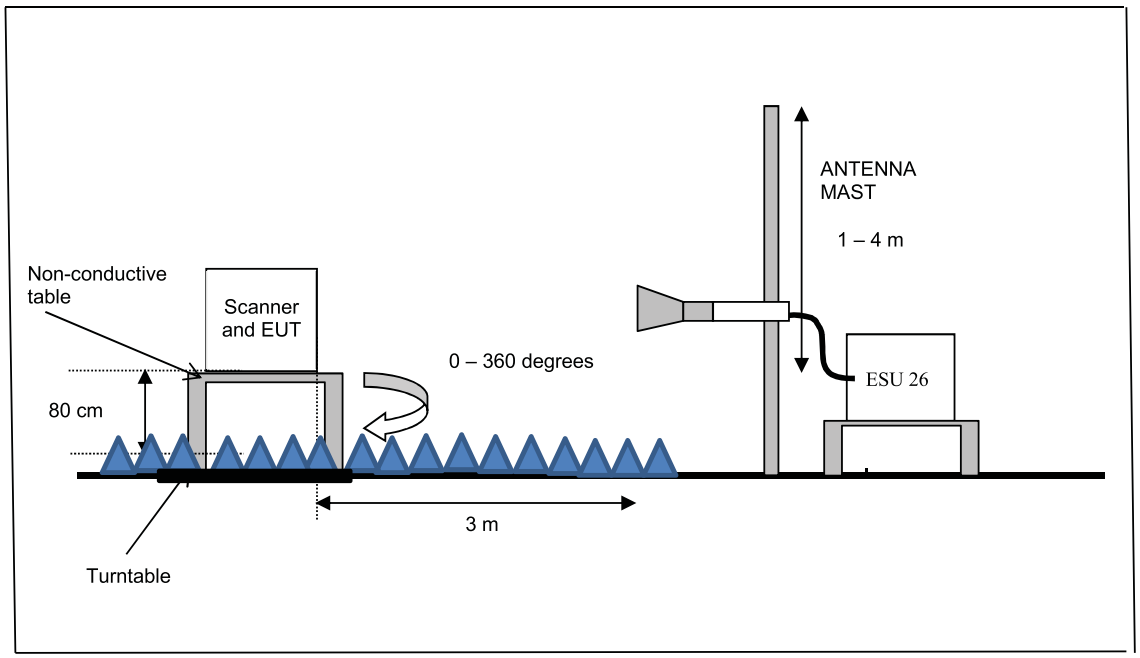


Figure 3.3.3 Setup for measurements in the frequency range 1 GHz - 6 GHz.

The measurement distance is normally 3 m and that was the distance for the measurements on Transponder. A horn antenna DRG-118 (E-I839) was used .
If the lobe of the antenna does not cover the whole EUT in height, more than one position shall be used. The lobe of the antenna at 3m measurement distance is 1 m.

The measurements sequence was automatic and controlled from a computer on the same way as measurement below 1 GHz.
The measurement resolution bandwidth is normally 1 MHz and the used detectors of the analyzer/receiver are Peak and Average.

During the initial characterization of the EUT, pre-scan measurements in 16 positions were performed, at antenna heights of 1 m and azimuth angles of 10, 55, 100, 155, 190, 235, 280 and 325 degrees. See Figure 2.1.2 regarding angles of turntable.
The measurements were carried out in horizontal as well as vertical orientation of the antenna.

After these initial measurements, at each critical frequency, closer than 20 dB from the limit line, first the turntable angle and then the antenna height were varied within a certain range (+/- 45 degrees for turntable and +/-100 cm for the antenna), in order to found the maximum emission more precisely.

The measurements were performed in both horizontal and vertical orientation of the antenna.

When the direction of highest emission in Peak and Average mode were found, final measurement with the same detectors but with a measurement time of at least 1s was performed.

3.4 EUT test setup

The block diagram below illustrates the test setup of the EUT and its auxiliary equipment.

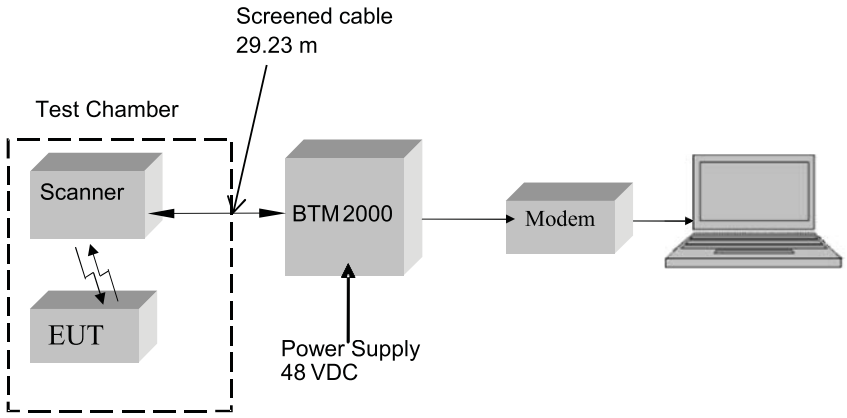


Figure 3.4.1 Block diagram of test object with auxiliary equipment.

During the tests, no cable was connected to the Transponder, which is the test object, but following cable was connected to the Scanner:

Port	**Type/ Length**	**Remarks**
Cable (connecting Scanner placed in the test chamber and the BTM placed outside the test chamber), equipped with ferrites	Screened/ 29.23 m	3NSS006298-2923 VR0.64 5

3.4.1 Description and intended use of test object, operation mode

The test object JGA 290 01/4 is a transponder operating in duplex. It receives on 27.095 MHz and transmits on around 4.4 MHz.

The Transponder is mounted on the sleeper in the railroad track, between the rails.
It is a passive device until it's energized from the carrier of a 27.095 MHz transmitter in the train, Scanner GPA 2000.

3.5 Criteria for compliance during immunity test

Performance criteria according to corresponding standard were applied during immunity tests as follows:

General

The equipment shall not become dangerous or unsafe as a result of the application of the tests.

Performance criterion A:

- The equipment shall continue to operate as intended during the test.
- The acceptable Level for the BER (**LA**$_{BER}$) recorded during the immunity test shall not be more than 500 errors during 3 s.
- The Transponder is not allowed to change operating mode.

Performance criterion B:

- The equipment shall continue to operate as intended after the test.
- Temporary degradation or loss of function or performance which is self-recoverable is allowed:
  For errors occurring during the test more than "**LA.**$_{BER}$", the performance of the Transponder shall be re-verified with a new test without disturbance.
  For this second test, the error limit for criteria A shall be respected.
  The bit string programmed in the Transponder telegram memory shall remain unchanged.

Performance criterion C:

- The equipment is allowed to have temporary degradation or loss of function or performance which requires operator intervention or systems reset.

During Radiated RF immunity tests, the Transponder shall meet performance criterion A, and during the ESD tests at least criterion B shall be fulfilled.

3.6 Modifications of the test object

No modification was implemented to the test object.

3.7 Test sequence

The tests described in this test report were performed in the following sequence:

1. Measurement of RF electromagnetic field 30-1000 MHz
2. Measurement of RF electromagnetic field 1-6 GHz
3. Immunity to RF electromagnetic fields 80 – 1000 MHz
4. Immunity to RF electromagnetic fields 1-6 GHz
5. Immunity to electrostatic discharges

4. Test results

4.1 Immunity to electrostatic discharges

Test object	Transponder	Sheet	ESD-1
Type	JGA 290 01/4	Project no.	E703892
Serial no.	E1514000404	Date	09 June 2014
Client	Bombardier Transportation	Initials	DAC
Specification	IEC 62236-4:2008	Required Perf. criter.	B

Test method	EN/(IEC) 61000-4-2:2009	Temperature	23 °C
Characteristics	Discharge network: 150 pF, 330 Ω	Humidity	48 % RH
Test equipm.	EMC Test site C Västerås Setup VIC1	Uncertainty	1.1 dB

Surface under test	Test standard's name of surface	Coupling of discharges	No of disch. each combin.	Amplitude [kV]	Passed	Remarks
Several test points on bottom side EUT	Enclosure	Direct air	10	+/- 4, 8 and 15	Yes	See Photos 4.1.3 and 4.1.4
Several test points on upper side EUT	Enclosure	Direct air	10	+/- 4, 8 and 15	Yes	See Photos 4.1.4 and 4.1.5
Mounting screws and label	Metallic	Direct contact	10	+/- 6 and 8	Yes	See Photos 4.1.6 and 4.1.7
10 cm from Transponder	Metallic	VCP contact	10	+/- 6 and 8	Yes	See Photo 4.1.8

Note 1:

Criteria for compliance: See Section 3.2

Test result: The discharges caused no malfunctions

Compliant: Yes

Comments: IEC 62236-4: 2008 standard specifies test with 6 kV contact discharge and up to 8 kV air discharge.
Higher test levels were applied, according to the document "LIRR/MNR Contract 1712 Positive Train Control".



Photo 4.1.1 Test setup regarding immunity to electrostatic discharges.
Vie of bottom side of Transponder.



Photo 4.1.2 Test setup regarding immunity to electrostatic discharges.
View of upper side of Transponder.



Photo 4.1.3 Test points regarding immunity to electrostatic discharges.
Air discharge test.



Photo 4.1.4 Test points regarding immunity to electrostatic discharges.
Air discharge test.



Photo 4.1.5 Test points regarding immunity to electrostatic discharges. Air discharge test.



Photo 4.1.6 Test points regarding immunity to electrostatic discharges. Contact discharge test.

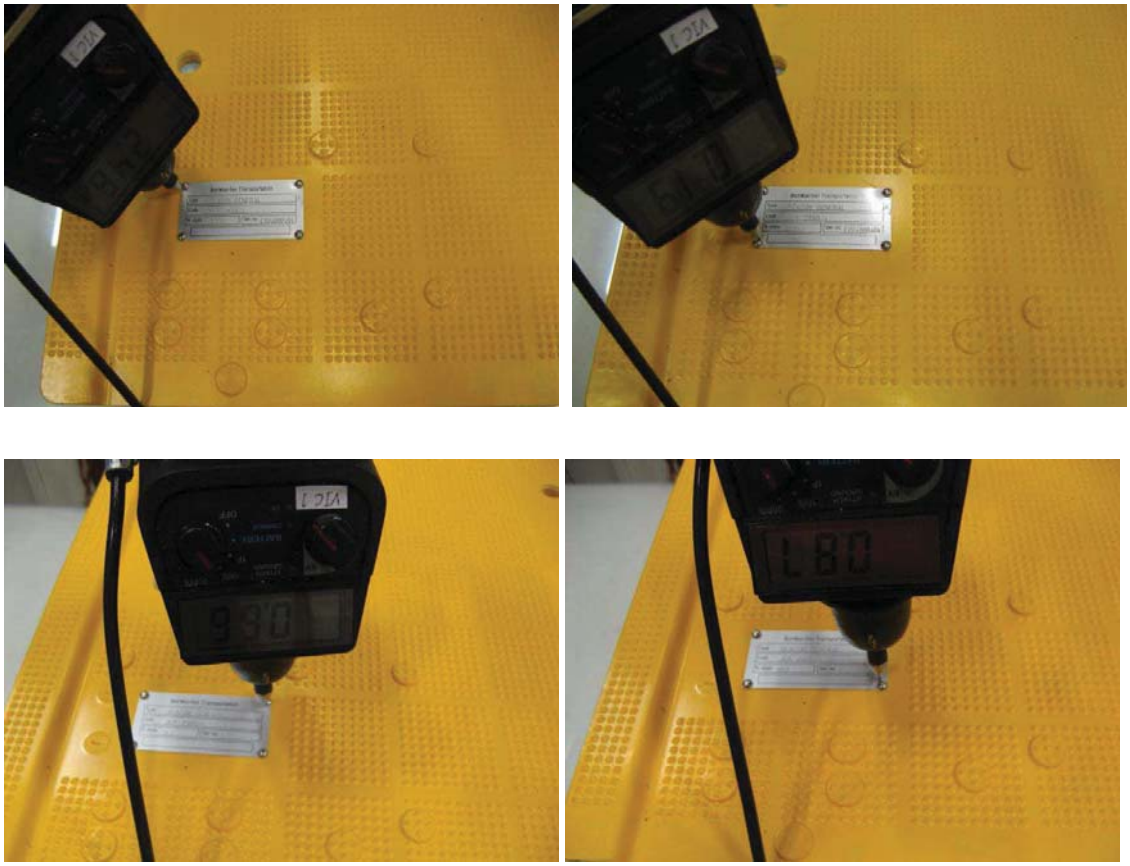


Photo 4.1.7 Test points regarding immunity to electrostatic discharges.
Contact discharge test.

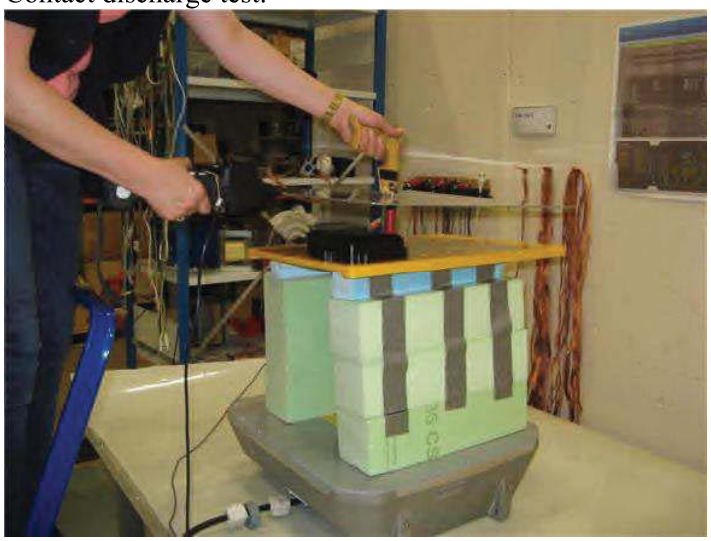


Photo 4.1.8 Test setup regarding immunity to indirect electrostatic discharges.

4.2 Immunity to RF electromagnetic field 80 MHz – 6 GHz

Test object	Transponder	Sheet	RF Field-1
Type	JGA 290 01/4	Project no.	E703892
Serial no.	E1514000404	Date	05 June 2014
Client	Bombardier Transportation	Initials	DAC
Specification	IEC 62236-4:2008	Required Perf. criter.	A

Test method	EN/(IEC) 61000-4-3:2006+A1+A2	Temperature	21 °C
Characteristics	16 point pre-Calibration	Humidity	43 % RH
Test equipm.	EMC Hall B Västerås Setup VIE2 Test between 80-1000 MHz	Uncertainty	1.9 dB

Frequency range	Modulation	Field direction	Amplitude [V/m]	Passed	Remarks
First side of Transponder exposed to the field					
80-1000 MHz	80 % AM 1 kHz	Horizontal	20	Yes	
80-1000 MHz	80 % AM 1 kHz	Vertical	20	Yes	
Second side of Transponder (GPA Scanner cable outlet exposed to the field)					
80-1000 MHz	80 % AM 1 kHz	Horizontal	20	Yes	
80-1000 MHz	80 % AM 1 kHz	Vertical	20	Yes	
Third side of Transponder exposed to the field					
80-1000 MHz	80 % AM 1 kHz	Horizontal	20	Yes	
80-1000 MHz	80 % AM 1 kHz	Vertical	20	Yes	
Fourth side Transponder exposed to the field					
80-1000 MHz	80 % AM 1 kHz	Horizontal	20	Yes	
80-1000 MHz	80 % AM 1 kHz	Vertical	20	Yes	
Bottom side of Transponder exposed to the field					
80-177 MHz	80 % AM 1 kHz	Horizontal	20	Yes	
177-182 MHz	**80 % AM 1 kHz**	**Horizontal**	**20**	**No**	
177-182 MHz	80 % AM 1 kHz	Horizontal	16	Yes	
182-1000 MHz	80 % AM 1 kHz	Horizontal	20	Yes	
80-1000 MHz	80 % AM 1 kHz	Vertical	20	Yes	
Upper side of Transponder exposed to the field					
80-177 MHz	80 % AM 1 kHz	Horizontal	20	Yes	
176-180 MHz	**80 % AM 1 kHz**	**Horizontal**	**20**	**No**	
176-180 MHz	80 % AM 1 kHz	Horizontal	16	Yes	
182-1000 MHz	80 % AM 1 kHz	Horizontal	20	Yes	
80-1000 MHz	80 % AM 1 kHz	Vertical	20	Yes	

Test method	EN/(IEC) 61000-4-3:2006+A1+A2			Temperature	22 °C
Characteristics	4 points pre-Calibration			Humidity	45 % RH
Test equipm.	EMC Hall A Västerås Setup VIE1 Test between 1-6 GHz			Uncertainty	1.9 dB
Frequency range	Modulation	Field direction	Amplitude [V/m]	Passed	Remarks
Side of Transponder exposed to the field					
1-6 GHz	80 % AM 1 kHz	Vertical	20	Yes	
1-6 GHz	80 % AM 1 kHz	Horizontal	20	Yes	
Second side of Transponder exposed to the field					
1-6 GHz	80 % AM 1 kHz	Horizontal	20	Yes	
1-6 GHz	80 % AM 1 kHz	Vertical	20	Yes	
A third side of Transponder exposed to the field					
1-6 GHz	80 % AM 1 kHz	Vertical	20	Yes	
1-6 GHz	80 % AM 1 kHz	Horizontal	20	Yes	
Fourth side of Transponder exposed to the field					
1-6 GHz	80 % AM 1 kHz	Horizontal	20	Yes	
1-6 GHz	80 % AM 1 kHz	Vertical	20	Yes	
Bottom side of Transponder exposed to the field					
1-6 GHz	80 % AM 1 kHz	Vertical	20	Yes	
1-6 GHz	80 % AM 1 kHz	Horizontal	20	Yes	
Upper side of Transponder exposed to the field					
1-6 GHz	80 % AM 1 kHz	Vertical	20	Yes	
1-6 GHz	80 % AM 1 kHz	Horizontal	20	Yes	

Criteria for compliance	See Section 3.2
Test result	The radio frequency electromagnetic field caused malfunctions in the frequency range 176 MHz to 182 MHz but passed the test in the rest of the frequency range from 80 MHz up to 6 GHz. Test between 176 – 182 MHz Passed with a test level of 16 V/m.
Compliant	Yes, according to IEC 62236-4: 2008 Partly compliant according to document LIRR/MNR Contract 1712 Positive Train Control.
Setup comments	Frequency step: 1 %, dwell time: 3 second
Comments	IEC 62236-4: 2008 standard specifies test with 10 V/m between 80-800 MHz and 1.4-2.1 GHz, 20 V/m between 800-1000 MHz and 5 V/m between 2.1-2.5 GHz. Higher test levels were applied, according to the document “LIRR/MNR Contract 1712 Positive Train Control”.

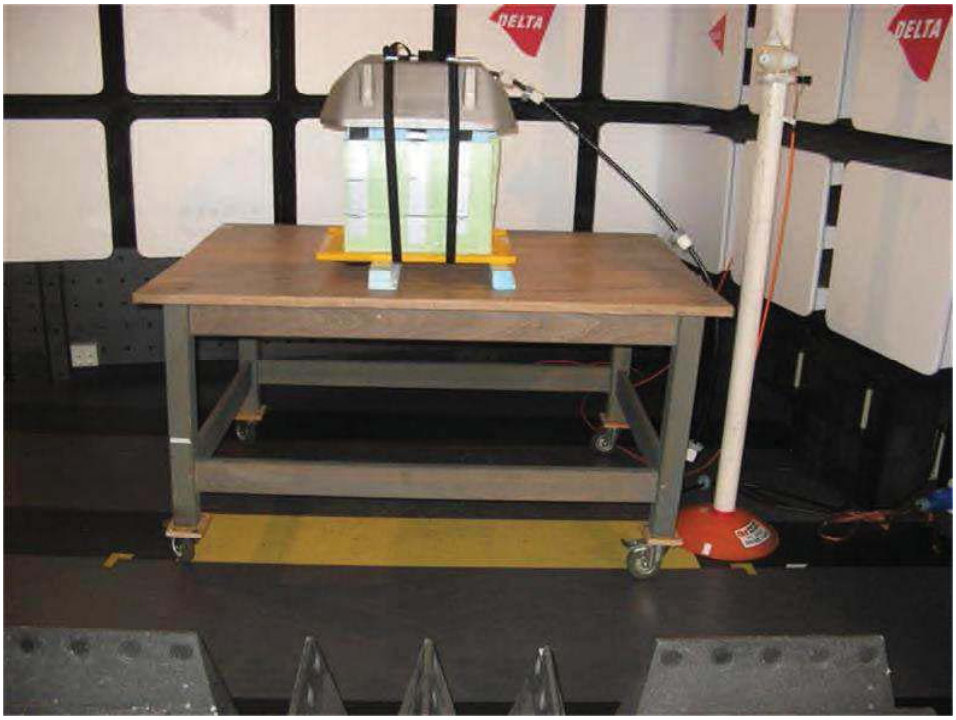


Photo 4.2.1 Test setup regarding immunity to RF electromagnetic field.80-1000 MHz. First side of Transponder exposed to the field.



Photo 4.2.2 Test setup regarding immunity to RF electromagnetic field.80-1000 MHz. Second side of Transponder exposed to the field.

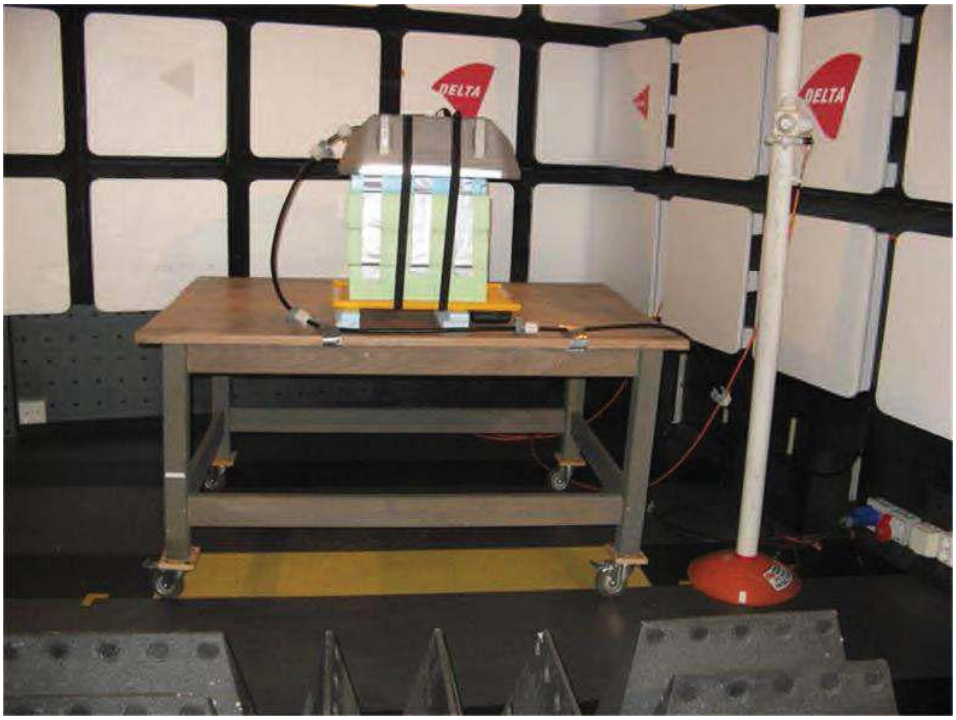


Photo 4.2.3 Test setup regarding immunity to RF electromagnetic field.80-1000 MHz. Third side of Transponder exposed to the field.

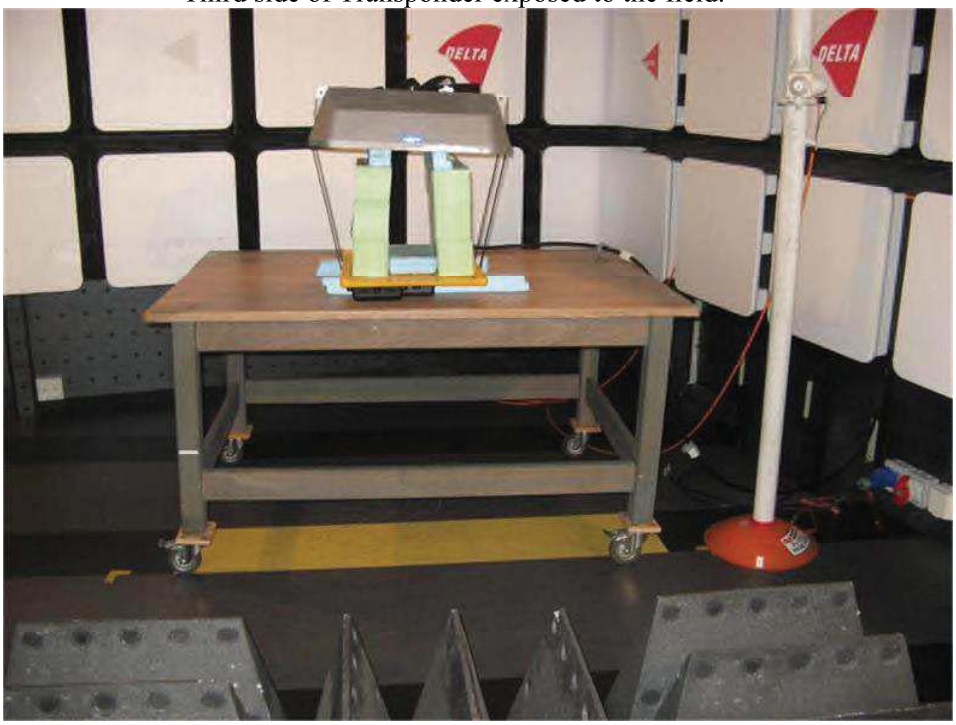


Photo 4.2.4 Test setup regarding immunity to RF electromagnetic field.80-1000 MHz. Fourth side of Transponder exposed to the field.

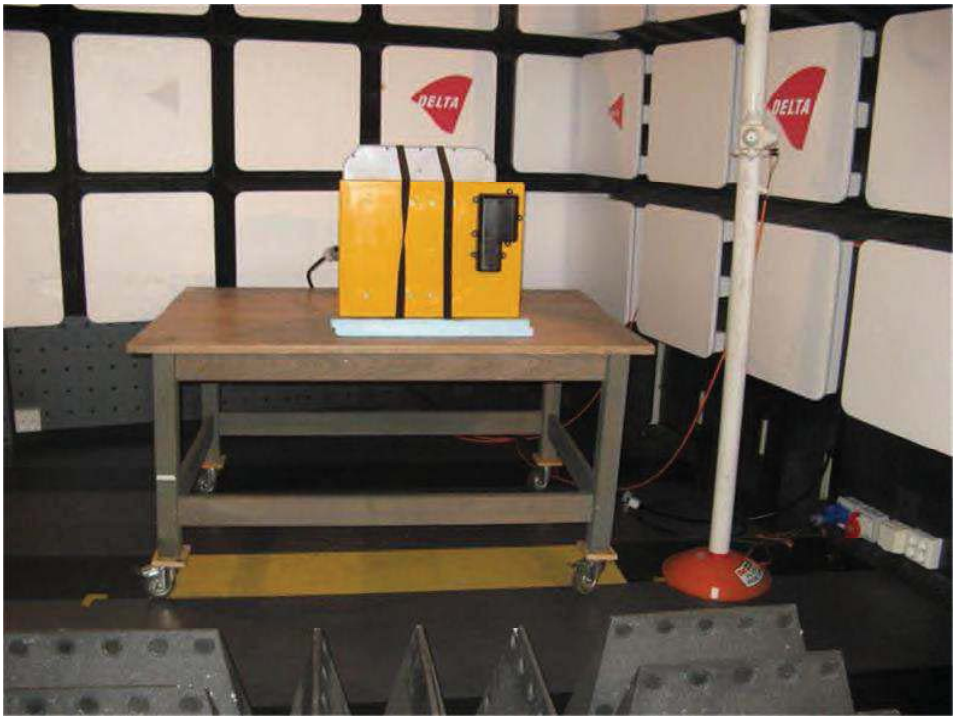


Photo 4.2.5 Test setup regarding immunity to RF electromagnetic field.80-1000 MHz. Fifth side (bottom side) of Transponder exposed to the field.

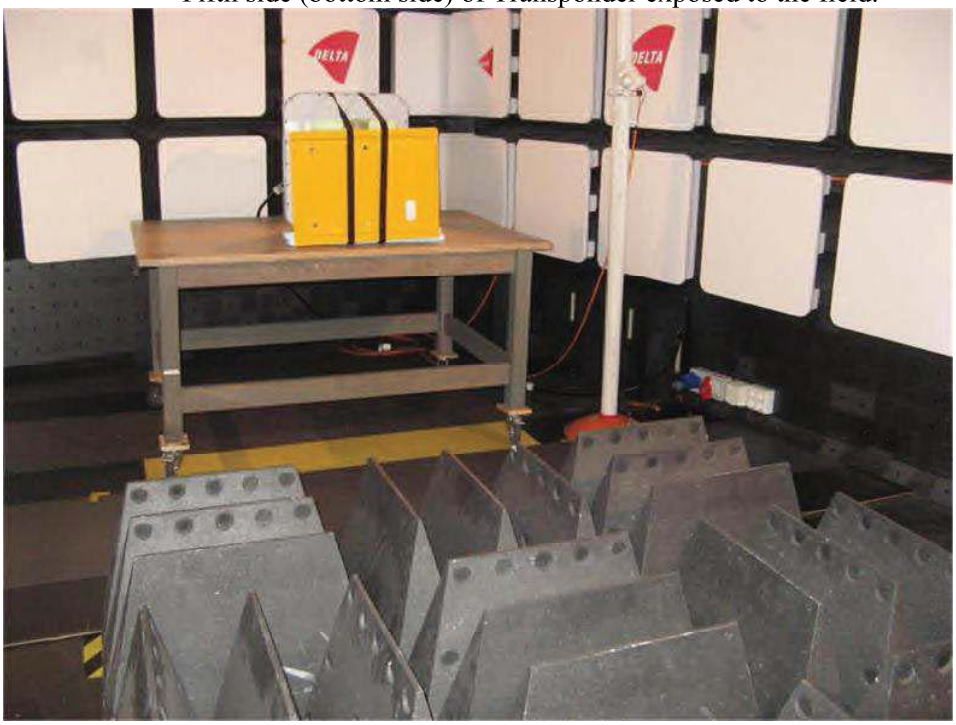


Photo 4.2.6 Test setup regarding immunity to RF electromagnetic field.80-1000 MHz. Sixth side (upper side) of Transponder exposed to the field.

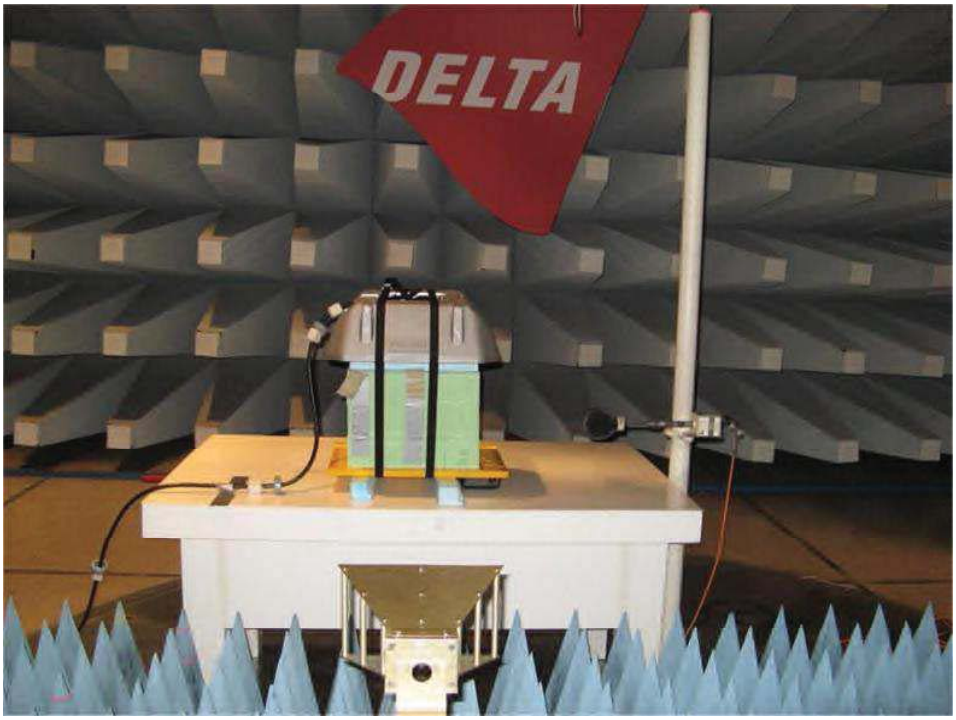


Photo 4.2.7 Test setup regarding immunity to RF electromagnetic field. 1-6 GHz. First side of Transponder exposed to the filed.

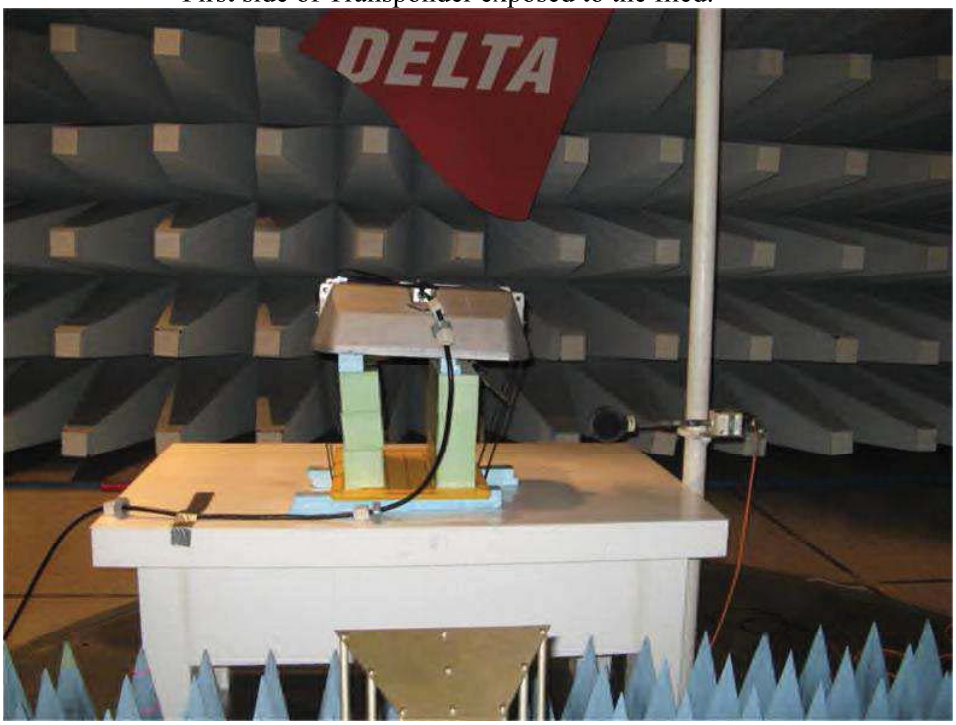


Photo 4.2.8 Test setup regarding immunity to RF electromagnetic field. 1-6 GHz. Second side of Transponder exposed to the filed.

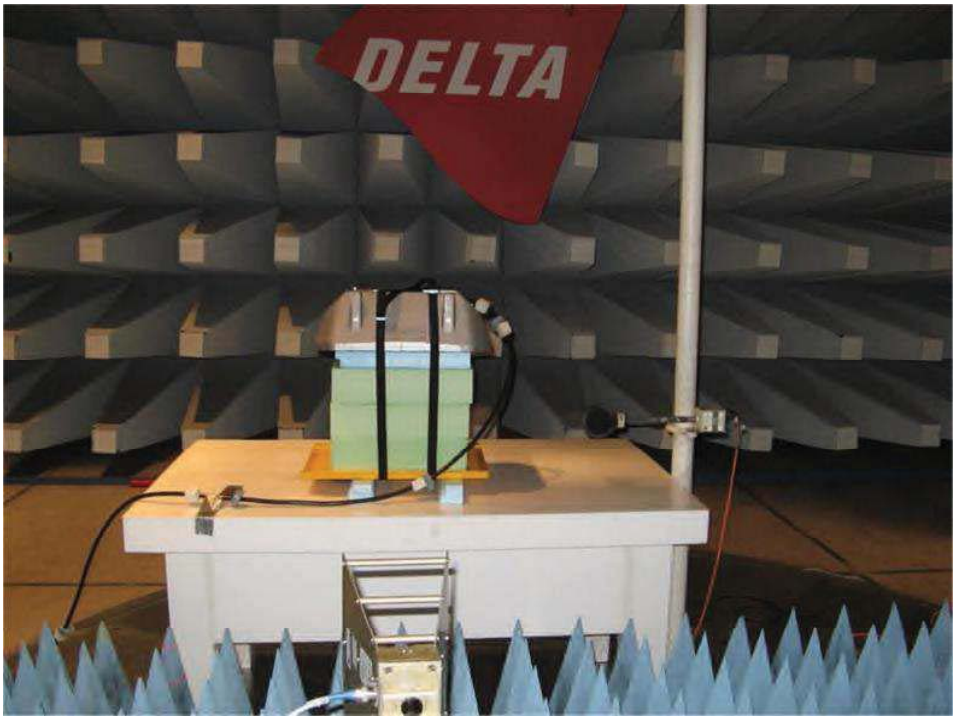


Photo 4.2.9 Test setup regarding immunity to RF electromagnetic field. 1-6 GHz. Third side of Transponder exposed to the filed.



Photo 4.2.10 Test setup regarding immunity to RF electromagnetic field. 1-6 GHz. Fourth side of Transponder exposed to the filed.

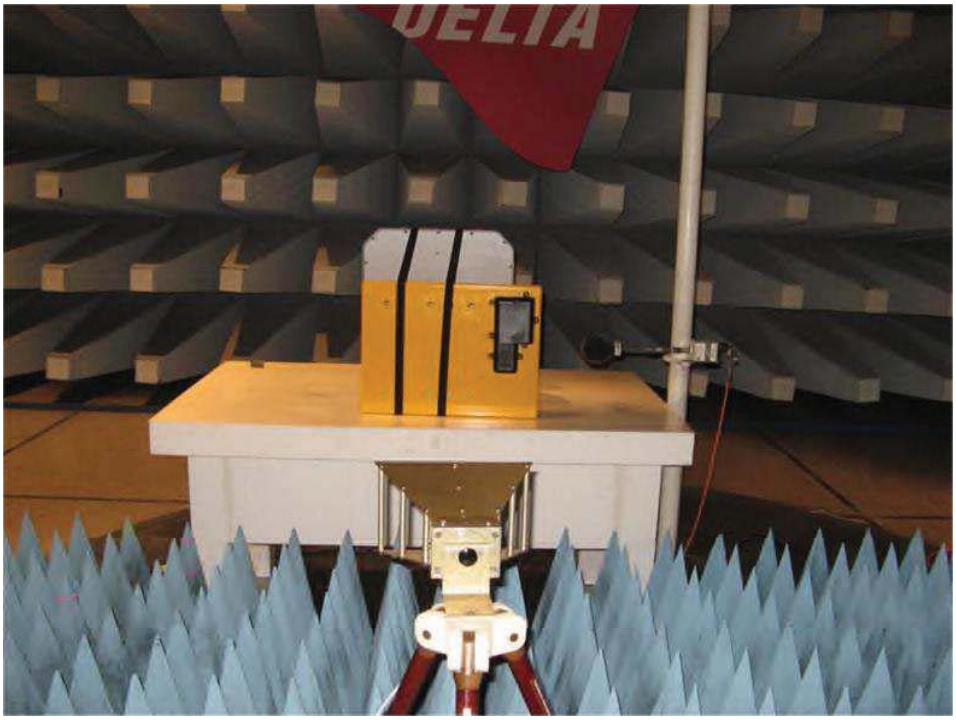


Photo 4.2.11 Test setup regarding immunity to RF electromagnetic field. 1-6 GHz. Bottom side of Transponder exposed to the filed

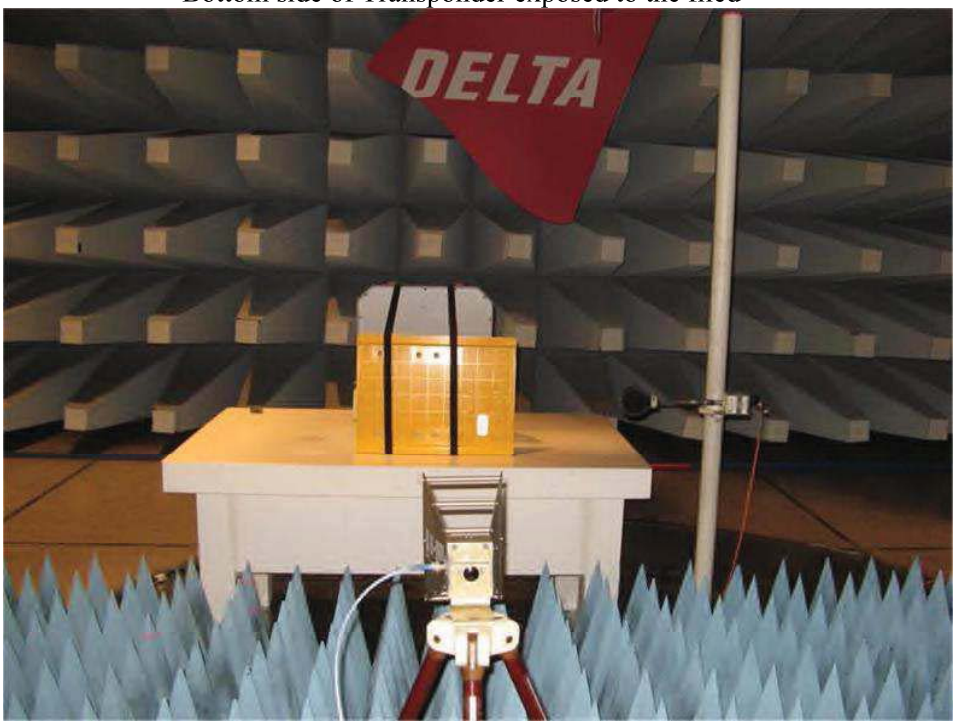


Photo 4.2.12 Test setup regarding immunity to RF electromagnetic field. 1-6 GHz. Upper side of Transponder exposed to the filed.

4.3 Measurement of RF electromagnetic field 30 MHz – 1000 MHz

Test object	Transponder	Sheet	RE-1
Type	JGA 290 01/4	Project no.	E703892
Serial no.	E1514000404	Date	04 June 2014
Client	Bombardier Transportation	Initials	DAC
Specification	IEC 62236-4:2008	Frequency	30-1000 MHz

Test method Characteristics	CISPR 16-2-3:2010+A1 Complete search, antenna distance 10 m	Temperature Humidity	21 °C 43 % RH
Detector	Peak and quasi peak	Bandwidth	120 kHz
Test equipm.	EMC Hall A Västerås Setup VEC1	Uncertainty	5.1 dB

Test result	The measured field strengths were exceeded the limits of IEC 62236-4 and IEC 61000-6-4: 2007 + A1. The measured field strengths were exceeded the limit of IEC 62236-2 Ed. 2 reduced by 6 dB at 894.12 MHz and at 948.3 MHz with 0.34 dB respectively 2.0 dB.
Compliant	No
Comments	Final maximal measurements by variation of turntable azimuth, antenna height, and antenna polarisation

Test Description:	Radiated emission. Complete measurement 30 - 1000 MHz
Date:	2014-06-04
EUT Name:	JGA 29001/4 Transponder
Manufacturer:	Bombardier Transportation
Operating Conditions:	27.095 MHz
Test Site:	DELTA Development Technology AB
Operator Name:	Daniela Coman
Test Specification:	IEC 61000-6-4:2006+A1
Comment:	Pset=100

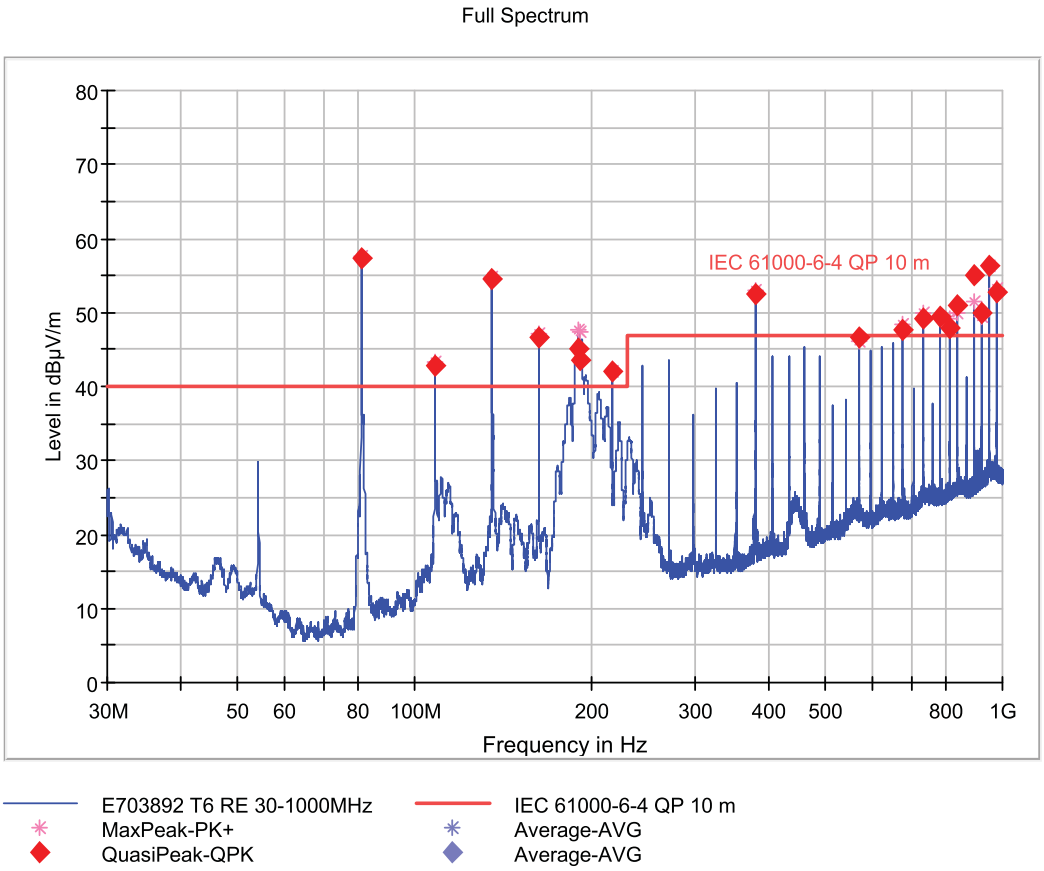


Figure 4.3.1 : Radiated emission measurement 30 MHz – 1 GHz according to IEC 61000-6-4 and IEC 62236-4.

Final_Result

Frequency (MHz)	QuasiPeak (dBµV/m)	Limit (dBµV/m)	Margin (dB)	Meas. Time (ms)	Bandwidth (kHz)	Height (cm)	Pol	Azimuth (deg)	Corr. (dB)
81.270000	57.32	40.00	-17.32	1000.0	120.000	400.0	H	320.0	-18.8
108.390000	42.86	40.00	-2.86	1000.0	120.000	400.0	H	12.0	-14.8
135.480000	54.43	40.00	-14.43	1000.0	120.000	400.0	H	261.0	-13.9
162.570000	46.63	40.00	-6.63	1000.0	120.000	400.0	H	298.0	-15.1
189.660000	45.14	40.00	-5.14	1000.0	120.000	325.0	H	86.0	-16.4
190.740000	43.60	40.00	-3.60	1000.0	120.000	324.0	H	86.0	-16.4
216.750000	42.13	40.00	-2.13	1000.0	120.000	337.0	H	96.0	-15.8
379.320000	52.36	47.00	-5.36	1000.0	120.000	219.0	H	50.0	-9.6
568.980000	46.52	47.00	0.48	1000.0	120.000	134.0	H	129.0	-5.0
677.340000	47.61	47.00	-0.61	1000.0	120.000	124.0	H	134.0	-4.3
731.550000	49.08	47.00	-2.08	1000.0	120.000	108.0	H	137.0	-2.5
785.730000	49.49	47.00	-2.49	1000.0	120.000	122.0	H	81.0	-2.3
812.820000	47.95	47.00	-0.95	1000.0	120.000	100.0	H	91.0	-1.8
839.910000	51.08	47.00	-4.08	1000.0	120.000	108.0	H	98.0	-0.9
894.120000	55.14	47.00	-8.14	1000.0	120.000	105.0	H	109.0	-0.9
921.210000	49.82	47.00	-2.82	1000.0	120.000	100.0	H	104.0	0.1
948.300000	56.38	47.00	-9.38	1000.0	120.000	117.0	H	81.0	1.3
975.390000	52.81	47.00	-5.81	1000.0	120.000	103.0	H	100.0	1.4

Test Description:	Radiated emission. Complete measurement 30 - 1000 MHz
Date:	2014-06-04
EUT Name:	JGA 29001/4 Transponder
Manufacturer:	Bombardier Transportation
Operating Conditions:	27.095 MHz
Test Site:	DELTA Development Technology AB
Operator Name:	Daniela Coman
Test Specification:	IEC 62236-2 Ed. 2 reduced by 6 dB
Comment:	Pset=100

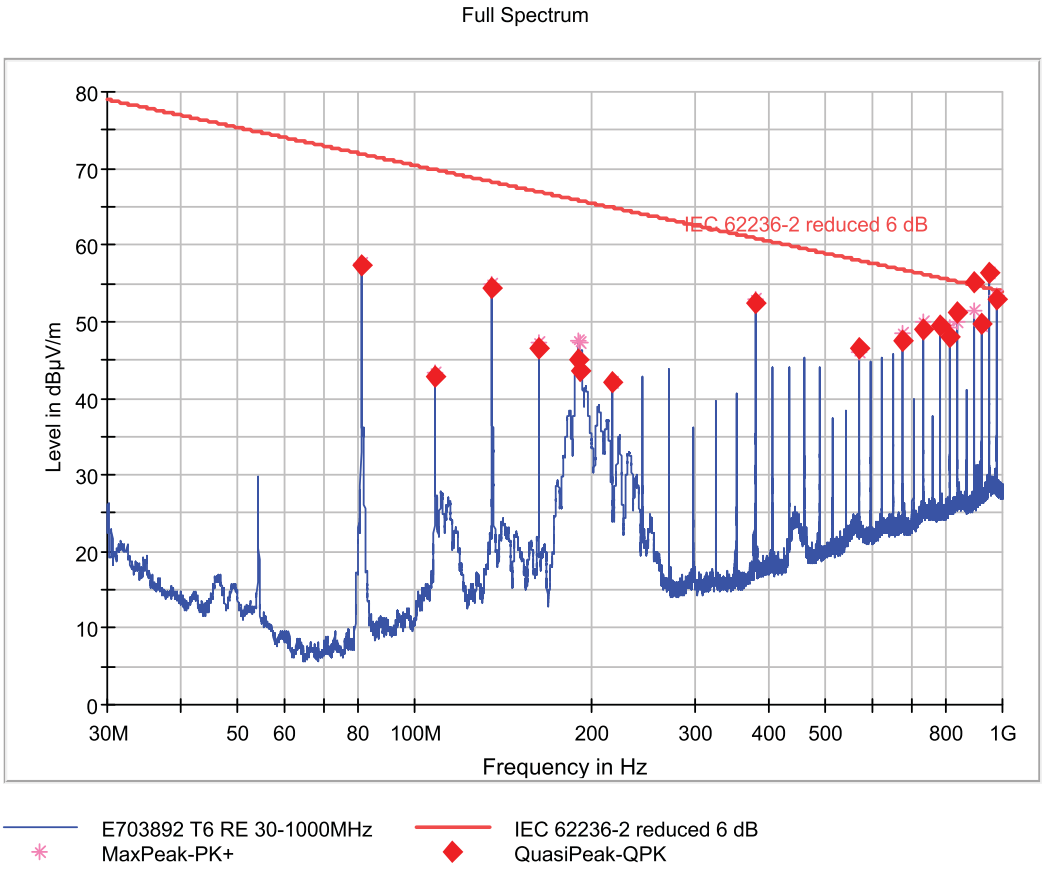


Figure 4.3.2 : Radiated emission measurement 30 MHz – 1 GHz according to IEC 62236-2 reduced by 6 dB

Frequencies above limit IEC 62236-2 reduced by 6 dB

Frequency (MHz)	QuasiPeak (dBµV/m)	Limit (dBµV/m)	Margin (dB)	Meas. Time (ms)	Bandwidth (kHz)	Height (cm)	Pol	Azimuth (deg)	Corr. (dB)
894.120000	55.14	54.80	-0.34	1000.0	120.000	105.0	H	109.0	-0.9
948.300000	56.38	54.38	-2.00	1000.0	120.000	117.0	H	81.0	1.3



Photo 4.3.1 Test setup regarding measurement of radio frequency electromagnetic field.



Photo 4.3.2 Test setup regarding measurement of radio frequency electromagnetic field.

4.4 Measurement of RF electromagnetic field 1 – 6 GHz

Test object	Transponder	Sheet	RE-2
Type	JGA 290 01/4	Project no.	E703892
Serial no.	E1514000404	Date	04 June 2014
Client	Bombardier Transportation	Initials	DAC
Specification	IEC 62236-4:2008	Frequency	1-6 GHz

Test method Characteristics	CISPR 16-2-3:2010+A1 Complete search, antenna distance 3 m	Temperature Humidity	21 °C 43 % RH
Detector	Peak and average	Bandwidth	1 MHz
Test equipm.	EMC Hall A Västerås Setup VEC1	Uncertainty	4.5 dB

Test result	The measured field strengths were below the limit of IEC 62236-4 and IEC 61000-6-4:2006 + A1.
Compliant	Yes
Comments	Final measurements by variation of turntable azimuth and antenna polarisation

Test Description:	Radiated emission. Complete measurement 1-6 GHz
Date:	2014-06-04
EUT Name:	JGA 29001/4 Transponder
Manufacturer:	Bombardier Transportation
Operating Conditions:	27.095 MHz
Test Site:	DELTA Development Technology AB
Operator Name:	Daniela Coman
Test Specification:	IEC 61000-6-4:2006+A1
Comment:	

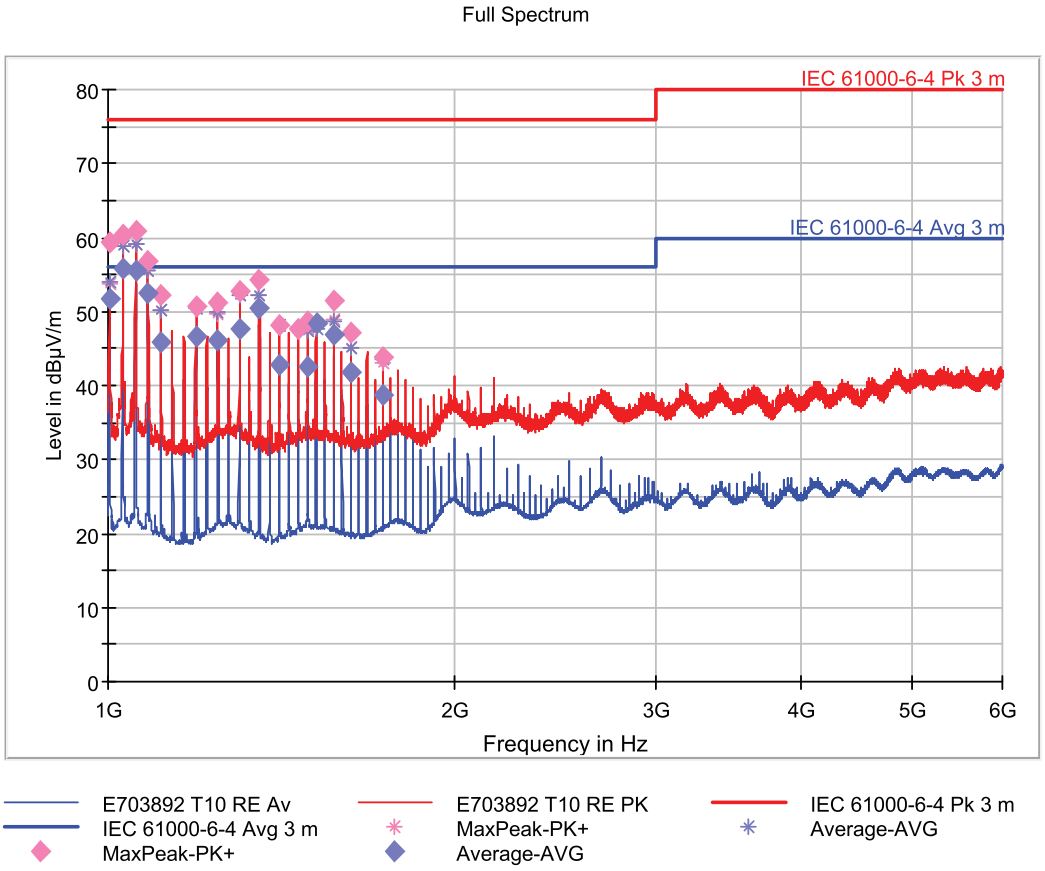


Figure 4.4.1 : Radiated emission measurement 30 MHz – 1 GHz according to IEC 61000-6-4:2006+A1

Final_Result

Frequency (MHz)	MaxPeak (dBµV/m)	Average (dBµV/m)	Limit (dBµV/m)	Margin (dB)	Meas. Time (ms)	Bandwidth (kHz)	Height (cm)	Pol	Azimuth (deg)	Corr. (dB)
1002.500000	59.35	---	76.00	16.65	1500.0	1000.000	130.0	H	123.0	-17.3
1002.500000	---	51.76	56.00	4.24	1500.0	1000.000	121.0	H	63.0	-17.3
1029.500000	---	55.78	56.00	0.22	1500.0	1000.000	115.0	H	126.0	-17.4
1029.500000	60.41	---	76.00	15.59	1500.0	1000.000	115.0	H	126.0	-17.4
1056.750000	60.98	---	70.00	9.02	1500.0	1000.000	120.0	H	76.0	-17.3
1056.750000	---	55.51	56.00	0.49	1500.0	1000.000	127.0	H	77.0	-17.3
1083.750000	56.69	---	76.00	19.31	1500.0	1000.000	118.0	H	101.0	-17.2
1083.750000	---	52.61	56.00	3.39	1500.0	1000.000	118.0	H	100.0	-17.2
1111.000000	52.19	---	76.00	23.81	1500.0	1000.000	118.0	H	122.0	-17.2
1111.000000	---	45.97	56.00	10.03	1500.0	1000.000	204.0	V	324.0	-17.2
1192.250000	50.62	---	76.00	25.38	1500.0	1000.000	108.0	H	328.0	-16.8
1192.250000	---	46.64	56.00	9.36	1500.0	1000.000	106.0	H	328.0	-16.8
1246.250000	---	46.18	56.00	9.82	1500.0	1000.000	103.0	H	21.0	-16.8
1246.250000	51.16	---	76.00	24.84	1500.0	1000.000	103.0	H	23.0	-16.8
1300.500000	---	47.68	56.00	8.32	1500.0	1000.000	106.0	H	187.0	-16.6
1300.500000	52.81	---	76.00	23.19	1500.0	1000.000	103.0	H	186.0	-16.6
1354.750000	---	50.45	56.00	5.55	1500.0	1000.000	103.0	H	176.0	-16.7
1354.750000	54.20	---	76.00	21.80	1500.0	1000.000	103.0	H	177.0	-16.7
1409.000000	---	42.77	56.00	13.23	1500.0	1000.000	106.0	V	328.0	-16.8
1409.000000	48.09	---	76.00	27.91	1500.0	1000.000	100.0	V	331.0	-16.8
1463.250000	47.58	---	76.00	28.42	1500.0	1000.000	106.0	H	56.0	-16.8
1490.250000	---	42.66	56.00	13.34	1500.0	1000.000	103.0	H	328.0	-16.5
1490.250000	48.62	---	76.00	27.38	1500.0	1000.000	103.0	H	61.0	-16.5
1517.250000	---	48.51	56.00	7.49	1500.0	1000.000	106.0	H	171.0	-16.4
1571.500000	51.48	---	76.00	24.52	1500.0	1000.000	103.0	H	93.0	-16.3
1571.500000	---	46.76	56.00	9.24	1500.0	1000.000	103.0	H	94.0	-16.3
1625.750000	---	41.84	56.00	14.16	1500.0	1000.000	100.0	H	40.0	-16.1
1625.750000	47.15	---	76.00	28.85	1500.0	1000.000	103.0	H	40.0	-16.1
1734.000000	---	38.85	56.00	17.15	1500.0	1000.000	119.0	V	324.0	-15.9
1734.250000	43.81	---	76.00	32.19	1500.0	1000.000	129.0	V	233.0	-15.9

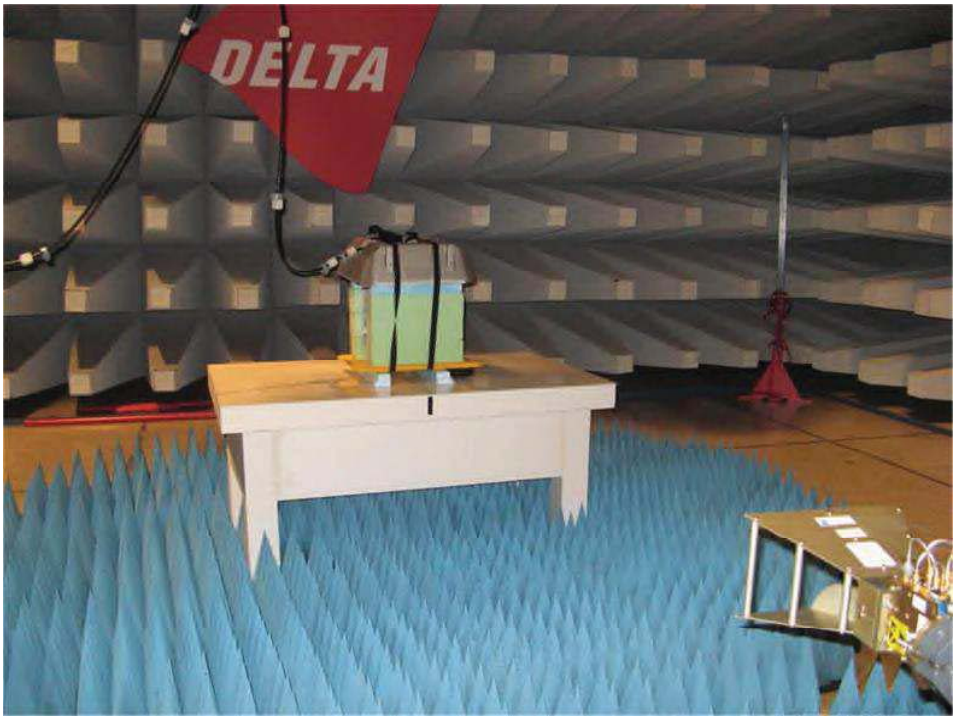


Photo 4.4.1 Test setup regarding measurement of radio frequency electromagnetic field (above 1 GHz).

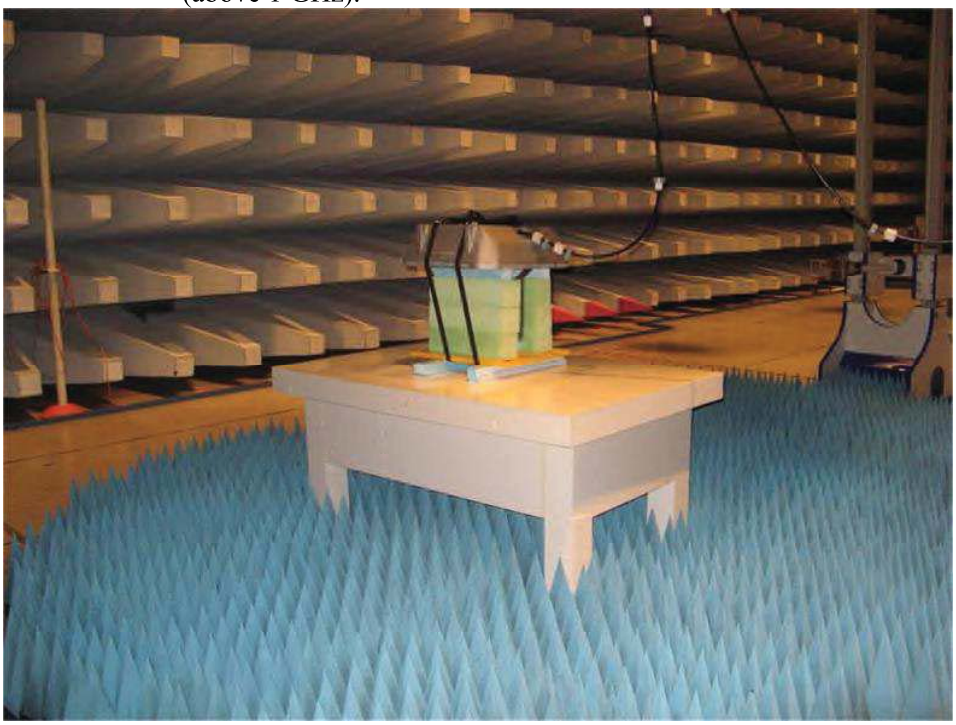


Photo 4.4.2 Test setup regarding measurement of radio frequency electromagnetic field (above 1 GHz).

5. National registrations and accreditations

5.1 SWEDAC Accreditation

Organization: Swedish Board for Accreditation and Conformity Assessment - SWEDAC, see www.swedac.se and www.ilac.org

Registration Number: 1688

SWEDAC is part of ILAC (International Laboratory Accreditation Cooperation) including its MRA (Mutual Recognition Arrangement).

5.2 FCC Registrations

Organization: Federal Communications Commission, USA

Registration Number: 516880

Facilities: EMC chamber A 3 and 10 m

5.3 IC Registrations

Organization: Industry Canada, Certification and Engineering Bureau

Registration Number: 9347A

Facilities: EMC chamber A (9347A-1)

6. List of instruments

Setup VEC1							
Measurement of radio frequency electromagnetic field							
Used	***ID no.***	***Description***	***Manufacturer***	***Type no.***	***Cal Date***	***Due Date***	***Setup uncertainty***
☒	36070	Software	Rohde & Schwarz	EMC32 ver. 9.0.10	-		5.1 dB 30-1000 MHz (10 m) 4.5 dB 1-6 GHz (3 m)
☒	36020	Measuring receiver	Rohde & Schwarz	ESU26	07/08/2013	07/08/214	
☒	IE-B928	Antenna Bilog	Chase	CBL6111A	31/07/2013	31/07/2014	
☒	IE-B758	Preamplifier	HP	8447F	08/08/2013	08/08/2014	
☒	E-I839	Horn antenna 1-18GHz	ARA	DRG-118/A	30/07/2013	30/07/2014	
☒	36021	Preamplifier	Quinstar	QLJ-01184040-J0	30/05/2014	30/05/2015	
☒	36022	Power supply	DELTA	UVB	-	-	
☒	36071	Controller	Maturo	NCD	-	-	
☒	36072	Tilt antenna mast	Maturo	TAM 4.0-E	-	-	
☒		Turntable	Heinrich Deisel	DT 440	-	-	

Setup VIC1							
Immunity to electrostatic discharges							
Used	***ID no.***	***Description***	***Manufacturer***	***Type no.***	***Cal Date***	***Due Date***	***Setup uncertainty***
☒	35064	ESD simulator	KeyTek	MiniZap MZ-15/EC	22/10/2013	22/10/2014	1.1 dB

Setup VIE1					
Immunity to radio frequency electromagnetic fields					
Used	***ID no.***	***Description***	***Manufacturer***	***Type no.***	***Setup uncertainty***
☒	36070	Software	Rohde & Schwarz	EMC32 ver. 9.12.00	1.9 dB
☒	36001	Signal generator	Hewlett-Packard	HP 83620A	
☒	36003	Arbitrary generator	Thurlby Thandar	TGA1241	
☒	IE-B884	Field Strength Meter	Amplifier Research	AR-FM 2000	
☒	IE-B885	E-field Sensor	Amplifier Research	FP 2000	
☒	36004	Field probe	Holaday	HI-4450	
☒	36027	RF Power Meter	Rohde & Schwarz	NRP-B2	
☒	36028	Thermal Power Sensor	Rohde & Schwarz	NRP-Z51	
☒	E-I017	RF Power Meter	Hewlett-Packard	E4418B	
☒	E-I018	RF Power Sensor	Hewlett-Packard	8482A	
☒	36006	Directional Coupler	Pasternack	PE2228-30	
☒	36085	Directional Coupler	R&D Microwaves	C1-A84	
☒	36005	Amplifier	Ophir	5162F	
☒	s/n101649	Amplifier	Rohde & Schwarz	BBA 150	
☒	36007	Antenna Log Periodic	Schwarzbeck	STLP 9148	
☒	E-I839	Antenna Horn 1-18 GHz	ARA	DRG-118/A	
☒	36086	Coaxial Rotary Joint	Diamond Antenna	18-2120-0	
☒	36036	GPIB Bus extender Vagn	ICS	4897-B	
☒	36024	GPIB Bus extender (A)	ICS	4897-B	

Setup VIE2					
Immunity to radio frequency electromagnetic fields					
Used	***ID no.***	***Description***	***Manufacturer***	***Type no.***	***Setup uncertainty***
☒	36070	Software	Rohde & Schwarz	EMC32 ver. 9.12.00	1.8 dB
☒	49642	Signal Generator	Marconi	2023	
☒	304	Field Strength Meter	Amplifier Research	AR-FM 2000	
☒	IE-B886	E-field Sensor	Amplifier Research	FP 2000	
☒	TE-T477	RF Power Meter	Rohde & Schwarz	NRVD	
☒	TE-T478	10 V Insertion Unit	Rohde & Schwarz	URV5-Z2	
☒	TE-T479	100 V Insertion Unit	Rohde & Schwarz	URV5-Z4	
☒	36030	Directional Coupler	Amplifier Research	DC 6580A	
☒	49310	Amplifier	BONN Elektronik	BTA 0122-1000	
☒	49353	Amplifier	Amplifier Research	500W1000M7	
☒	35105	Antenna Log Periodic	Rohde & Schwarz	HL 023 A1	
☒	29451	Antenna Tower	EMCO	1050	
☒	29452	Tower Controller	EMCO	1050	
☒		Data Acq./Control Unit	Hewlett-Packard	3497A	

Metropolitan Transportation Authority
Long Island Rail Road PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Number: 1712

WIU
Final Safety Report
CDRL 2-136-24

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	PM	Report	Project	Released

Prepared:	Andrei Edelman Safety Engineer	Edelman Andrei Digitally signed by Edelman Andrei DN: serialNumber=Z003BFUJ, givenName=Andrei, sn=Edelman, o=Siemens, cn=Edelman Andrei Date: 2018.12.13 15:16:33 -05'00'	2018-12-05
Verified:	James Balliet Safety Engineer	James B Balliet Digitally signed by James B Balliet DN: cn=James B Balliet, o, ou, email=jballiet@us.tuv.com, c=US Date: 2018.12.14 11:20:42 -05'00'	2018-12-05
Approved:	Anthony Nolla Wayside Project Manager	Anthony Nolla Digitally signed by Anthony Nolla Date: 2018.12.13 15:19:40 -05'00' Editor Version: PDF-XChange-Pro 6.0.321.0	2018-12-05
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group	2019.01.09 09:49:19 -05'00'	
BT/SRA Review:	Jason Weighley Safety Engineer	2018.12.17 08:04:41 -05'00'	
BT/SRA Review:			
	Name / Title, Group	**Signature**	**Date**

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2018, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2018 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3037456

Effective Date:	Revision:	Language:
2018-12-05	_A	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2018-11-11	To support System Baseline 3.2 - RSD
_A	2018-12-05	Reference table updated

Table of Contents

Section	Subject	Page
1	EXECUTIVE SUMMARY	4
2	INTRODUCTION	4
2.1	Reference Documents	5
3	CONFIGURATION AND VERSIONS	7
3.1	Known Non-Conformities that have not been corrected in this Release	7
4	CONSTRAINTS	8
5	SUMMARY	11

List of Tables

Table 1: Reference Documents 5
Table 2: WIU Software in System Release Level 3.2 7
Table 3: Constraints 8

1 EXECUTIVE SUMMARY

This revision of the WIU Final Safety report is issued to support authorization of integration testing and revenue service demonstration (RSD) on the Pilot Lines with System Baseline 3.2.

A summary of the evidence reviewed and released that ensures the WIU software included in System Baseline 3.2 is ready for field integration and revernue service demonstraction (RSD) and associated testing. Evidence referenced in this report is in configuration management and all documents are signed off.

2 INTRODUCTION

The general application of the WIU Subsystem is being provided for the LIRR PTC Project. Each is comprised of equipment housed within an equipment room which includes peripheral support devices for power and isolation, interface connections to field devices and the core Wayside Interface Unit (WIU) processor using the VIU-20e product.

The WIU Subsystem provides the interface to the existing vital signaling system to represent the status of the wayside signaling system via transmission of the signaling system status over the ground based network (GBN) and data radios to the approaching trains containing On Board PTC subsystem equipment.

The WIU subsystem is compliant with the Advanced Civil Speed Enforcement System (ACSES) II system functionality and contains additional functions when necessary to accommodate LIRR operational rules.

This document is intended to define the evidence to satisfy the safety, RAM, and compliance requirements assigned to the WIU subsystem for the ACSES II system. This WIU release is part of System Baseline 3.2 and is to allow use of fully functional WIU subsystem for field Integration and Revenue Service Demonstration testing under revenue service conditions on Pilot Lines 1 and 2.

2.1 Reference Documents

Please refer to Volume 4 – PTC Wayside System Specifications of the LIRR contract for a comprehensive list of the applicable standards for the WIU [2].

Table 1: Reference Documents

Reference Number	Document Name	Identification Number	Revision
[1]	Dictionary of Terms and Acronyms	3035817	_B
[2]	WIU Subsystem Product Safety Plan, CDRL 2-123-04	3035816	_C
[3]	WIU Subsystem Safety Concepts Document, CDRL 2-124-04	3035817	_C
[4]	WIU Subsystem Preliminary Hazard Analysis, CDRL 2-127-04	3036409	_C
[5]	WIU Subsystem Failure Modes Effects and Criticality Analysis, CDRL 2-129-24	3043761	_A
[6]	WIU Subsystem Operating Hazard Analysis, CDRL 2-130-24	3037420	__
[7]	WIU Subsystem Interface Hazard Analysis, CDRL 2-131-24	3043762	_A
[8]	WIU Subsystem Fault Tree Analysis, CDRL 2-132-24	3043763	_A
[9]	WIU Software Verification and Validation Report; CDRL 2-012-24	3050366	_A
[10]	WIU Software PVI, Master Executive	3050049	_A
[11]	WIU Software PVI, Slave Executive	3050050	_A
[12]	WIU Software PVI, NV Executive	3050051	_B
[13]	WIU Software PVI, MCF Application	3050048	_A
[14]	WIU Software PVI, NV Application	3051237	__
[15]	WIU Software PVI, Vital Configuration PL1	3051028	_C
[16]	WIU Software PVI, NV Configuration PL1	3051042	_B
[17]	WIU Software PVI, Vital Configuration PL2	3051027	_B
[18]	WIU Software PVI, NV Configuration PL2	3051041	_B
[19]	WIU FAT Test Reports, CDRL 2-053-24	4009412	__

Reference Number	Document Name	Identification Number	Revision
[20]	WIU FAT Test Reports, CDRL 2-053-24, Addendum 1	4009406	_A
[21]	WIU FAT Test Reports, CDRL 2-053-24, Addendum 2	4009407	_A
[22]	WIU SAT Test Reports, CDRL 2-057-24	4009413	__
[23]	WIU SAT Test Reports, CDRL 2-057-24, Addendum 1	4009408	_A
[24]	WIU SAT Test Reports, CDRL 2-057-24, Addendum 2	4009409	_A
[25]	LIRR SRAC	3045431	_D
[26]	ACSES II System - WIU Subsystem, Final Safety Report, by RSC/TUV	n/a	2.0

3 CONFIGURATION AND VERSIONS

Table 2: WIU Software in System Release Level 3.2

Document Name	Identification Number	Revision
WIU Software PVI, Master Executive	3050049	_A
WIU Software PVI, Slave Executive	3050050	_A
WIU Software PVI, NV Executive	3050051	_B
WIU Software PVI, MCF Application	3050048	_A
WIU Software PVI, NV Application	3051237	__
WIU Software PVI, Vital Configuration PL1	3051028	_C
WIU Software PVI, NV Configuration PL1	3051042	_B
WIU Software PVI, Vital Configuration PL2	3051027	_B
WIU Software PVI, NV Configuration PL2	3051041	_B

3.1 Known Non-Conformities that have not been corrected in this Release

There are no known non-conformities that are included in this release.

5 SUMMARY

All non-conformities have been corrected with the WIU portion of system 3.2 level release by the WIU software and the implementation of the identified constraints. Resolution of non-safety related nonconformities will continue for those that been deferred until future releases. This revision is to be cut-in and operational for Revenue Service Demonstration and testing on approved pilot lines. V&V has concluded with no issues.

Metropolitan Transportation Authority
Long Island Railroad
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

Office
Final Safety Report
CDRL 2-136-22

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT	ENG	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Theresa Barbour Safety Engineer		Theresa Barbour 2019.06.27 09:29:36 -04'00'
Verified:	Aaron Graham Safety Engineer		Aaron Graham 2019.06.27 09:45:09 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.06.27 09:53:11 -04'00'
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group		Phil Magloire 2019.06.28 07:22:26 -04'00'
BT/SRA Review:	N/A Title		
BT/SRA Review:	N/A Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3037452

Effective Date:	Revision:	Language:
2019-06-27	_E	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2018-11-21	First issue. This version of the report is to support RSD.
_A	2018-12-04	Revised for Office 3.3.1.
_B	2019-03-07	Revised for Office 3.4.4. Office 3.4.4 includes components at the version released in Office 3.3.1 with an updated NMS Version and an updated reference to the RSD map. Also note that change to reference [21] description corrects a typo present in Rev_A of this document, and does not indicate a change in STS software.
_C	2019-05-17	Revised to address typos and address SI-RVW-0775 - Office Final Safety Report 2-136-22 Rev A SA 01919; as well as March14, 2019 audit comments; for Office 3.4.4.
_D	2019-05-31	Revised for Office 3.5.0 and 3.5.1.
_E	2019-06-27	Revised to address applicable comments from LIRR PTCSP - SNCL_Atkins Observations - Final

Table of Contents

Section	Subject	Page
1	Executive Summary	5
2	Introduction	5
2.1	Compliance Matrix	5
2.2	Reference Documents	8
2.3	Glossary	9
3	Office Subsystem	10
3.1	Constraints for RSD	11
4	Summary of Safety Analysis and Evidences	11
4.1	Office PHA. OHA, IHA, FMECA	12
4.2	Office Fault Tree Analysis and Calculation of MTTHE	13
4.3	Office Subsystem Hazard Analysis	13
4.3.1	Closure of all Subsystem Hazards	13
4.4	FAT Results	13
4.5	Safety Critical Office Variances on Office Requirements	16
4.6	Office Safety Requirements	20
4.7	Non-Safety Critical Office Variances on Safety Related Office Requirements	21
4.8	Dependency on Other Subsystems	22
5	Office Software V&V	23
6	SDMT Safety Verification	23
7	Safety Certification Process	23
7.1	Remaining Open Items	24
7.1.1	Restrictions to Mitigate Open Items	24
7.1.2	Schedule to Remove Restrictions	24
8	Conclusion	24

List of Figures

Figure 1 - Safety Analysis Process 12

List of Tables

Table 1: Compliance Matrix 5
Table 2: Reference Documents 8
Table 3: Terms Specific to this Document 9
Table 4: Acronyms Specific to this Document 9
Table 5 - Office Component Functions 10
Table 6 - Office Safety CDRL Status 11
Table 7 - Failed FAT Results 14
Table 8 - Safety Critical Office Variances on Office Requirements 16
Table 9 - Non-Safety Critical Office Variances on Safety Related Office Requirements 21
Table 10 - Non-Office Requirements Necessary for Safety 22

1 Executive Summary

The Office Final Safety Report documents the results of execution of the Office SPSP[4].

The activities in the Office SPSP include hazard identification, determination of mitigations/safety requirements, and the verification of implementation of mitigations (i.e., fulfillment of safety requirements) at the Office subsystem and/or ACSES system level as appropriate to closure of all the records in the Office Hazard Log in the Office SSHA [2].

The Office Final Safety Report documents the closure of all hazards assigned to the Office Subsystem and evidence of closure of all assigned safety requirements to the Office Subsystem.

The report also includes:

- the result of calculation of the MTTHE for the Office subsystem and that this result meets the targets defined for this subsystem by the System Integrator.
- Regression FAT results
- Safety review of open safety critical variance against Office requirements
- Safety review of open non-safety critical variances against Office safety requirements

This revision of the Final Safety report is to authorize revenue service demonstration (RSD) on the Pilot Lines with Office Baseline 3.5.

The Office Final Safety Report will be integrated into the ACSES system safety case.

2 Introduction

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part I	12.10.12.A	Final Safety Report	Final Safety Report shall provide a summary of the results on the overall safety analysis, safety verification, and system safety demonstration	Section 4
Vol 2 Part I	12.10.12.B		Final Safety Report shall contain evidence of safety analysis	Section 4
Vol 2 Part I	12.10.12.C	MTTHE	Document the calculation and methodology to show the MTTHE requirements in 9.1 have been achieved	Section 4.2

Vol 2 Part I	12.10.12.D	Risk Reduction Actions	Address all risk reduction actions taken during design, test, operation and maintenance to mitigate faults caused by Operating Scenarios, Failures, Latent Design Errors, Installation errors, Human Reaction, Post implementation changes to SW or HW, or Interoperability and compatibility issues.	Section 4.3
Vol 2 Part I	12.10.12.E	Information in Report	Describes the Safety Certification process and issues encountered during certification. Describes certification status Describes remaining restrictions / open issues and actions / work arounds to ensure acceptable level of safety is maintained. Provides a schedule for eliminating restrictions / workarounds. As appropriate. Includes Certificate of Compliance	Section 5
Vol 2 Part 1	12.10.12.F	Resolution of all Hazards	Report shall contain evidence of the resolution of all hazards. Evidence of resolution shall consist of satisfactory closure of the items as listed in the Project Hazard Log and achievement of the items listed in the Certified Item List	Office SSHA [2] For CIL, see [3] Certifiable Item List CDRL 2-125-20
	12.10.12.G	Approved by Engineer	Report format will be approved by the Engineer and submitted in draft form at FDR. Report will stay draft until final system certification is achieved.	NA

	12.10.12.H	Approval of Final Safety Report	Report is to be submitted to SSCB prior to Completion of Pilot Phase commissioning and testing. Once approved by SSCB then submitted to the FRA and revised to address comments with a disposition per FRA comment. The report will be revised when characteristics of any territory, TP interface or the TP is modified in a way that impacts the safety of the system.	NA
Vol 2 Part I	9.1.E	MTTHE	The SI shall provide a quantifiable analysis of the safety of each of the ACSES II Subsystems and the ACSES II System as a whole. The minimum level of safety that the SI shall demonstrate through calculated Mean-Time-To-Hazardous-Event (MTTHE) is 10^{-9} hours. The MTTHE and the complete safety analysis and calculations for each ACSES II Subsystem and the ACSES II system shall be provided as part of the Final Safety Report, CDRL 2-136.	Section 4.2
Vol 2 Part I	9.5.F	MTTHE	Final Safety Report shall document the complete safety analysis and calculations to support the MTTHE of the Transponder Subsystem	NA

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624
[2]	Office Subsystem Hazard Analysis (SSHA) CDRL 2-128-12, CDRL 2-128-22	3037391
[3]	Certifiable Item List (CDRL 2-125-20)	3035818
[4]	Office Product Safety Plan CDRL 2-123-02	3036408
[5]	LIRR SRAC	3045431
[6]	Office Subsystem Description Document CDRL 6-001	3035943
[7]	PVI OFFICE-3.5.0, 3.5.1	3049982 Rev AA, AB
[8]	LIRR Office FAT Test Report	4008709
[9]	Office Preliminary Hazard Analysis CDRL 2-127-02	3035822
[10]	(LIRR) Office Subsystem IHA, CDRL 2-131-22	3037428
[11]	(LIRR) Office OHA CDRL 2-130-22	3037416
[12]	Office FTA CDRL 2-132-02	3037440
[13]	(LIRR) Office FMECA CDRL 2-129-22	3037404
[14]	Office Subsystem Safety Concept Document CDRL 2-124-02	3036410
[15]	CDRL 2-133-20 System Database Safety Verification Report	3035832
[16]	CDRL-2-012-02 Office 3.5.0/3.5.1 Software Verification and Validation Report	3052060 Rev_C in progress
[17]	CDRL 2-146 Reliability Calculation	3035848
[18]	Office SRTM	3153123 Rev_A
[19]	PVI Office Specific Application Data (MAP 1.39) (SDMT Tool 9.6)	3050134 Rev_K
[20]	Problem Reports: (Dimensions PTC_STS:STS_LIRR_MNR\STS_Doc\07 Verification\Comp_Test: NCR_PTC_STS.xlsx	

Reference Number	Document Name	Identification Number
[21]	STS PVI 1.1.0, 1.1.1	3038477_P, _Q
[22]	DOORS Office SSLR module	Baseline 8.0
[23]	CDRL 2-126-20-Project Hazard Log	3035819
[24]	CDRL 2-133 Database Safety Verification Report	3035832
[25]	Database Verification Report	3151611
[26]	Civil Data Verification Report Montauk Line (Pilot Line 1)	3051385 Rev_A
[27]	Civil Data Verification Report Port Washington Branch (Pilot Line 2)	3050830 Rev_A

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in Table 3 and Table 4 respectively.

Table 3: Terms Specific to this Document

Term	Definition
None.	

Table 4: Acronyms Specific to this Document

Acronym	Definition
CIL	Certifiable Items List
HL	Hazard Log
RSD	Revenue Service Demonstration
SRAC	Safety Related Application Condition
SRTM	Safety Requirements Traceability Demonstration

3 Office Subsystem

The Office system is fully described by the Office SDD [6]. The SDMF is not included in the scope of this report.

The safety functionality of each Office component is described in The Office SSCD [14].

Table 5 - Office Component Functions

Office Component	Function	SIL
STS	STS is a vital subsystem in the Office to manage the TSR database. STS performs validity check on the TSR data requested from the UIS and performs the execution of the TSR after the approval received from the UIS user. STS vitally manages the start time and end time of every scheduled TSR(s) to enforce them and maintains the TSR end time to notify the control user by the UISS.	SIL 4
UIS	UIS provides user interface to add, delete, and manage TSRs for the Railroad and other non-TSR forms. UIS displays TSR Alerts/events, and RWPS TSR request with notification.	SIL 0
RGS	Provides interface to adjacent railroad for line boundary anticipation zone TSRs. RGS also provides interface between Office and RWPS subsystems.	SIL 0
DMS	Stores all communication messages, Alarms, Events, Notifications, between all the sub-systems. Provides for Data archiving, retrieval, and review. Generate SNMP alarms to NMS for the PTC devices that are not supported SNMP. Generate acknowledgment for the OBC ACSES II maintenance message.	SIL 0
SEC	Provides periodic vulnerability assessments, centralized installation of antivirus software and comprehensive logging for forensic analysis.	SIL 0
ADDC	Authenticates and authorizes all users and computers in both of the PCC and BCC Office subsystem. Authenticates the computer; that is, ensures that the authorized computer and users are part of the domain.	SIL 0
NMS	Monitors the health of all ACSES II networked devices. NMS is also the primary interface for managing maintenance related alarms, Maintainer's workstation is used to display NMS.	SIL 0
WCC	WCC is the communication interface between Office (Particularly STS and DMS) and Onboard. WCC forwards the TSR List requests from OBCs to STS and forwards the List of TSR(s) response from STS to OBCs. WCC interfaces with DMS to log all ACSES II messages that it receives from OBCs, STS and WIU through BCP.	SIL 0

3.1 Constraints for RSD

- ACSES operation of Office from One control center only.
- Manual procedure to share TSR from Adj RR / Amtrak – ACSES sharing of data prohibited.
- Security related requirements are N/A.
- TSR List count limit of 80 is N/A, OBCs cannot handle 80 TSRs. Current max is 40.
- No line boundaries (virtual or real). Therefor no Shadow, Parent, or Child TSRs.
- TSR cannot be placed at track change points.
- Cellular service not supported.

4 Summary of Safety Analysis and Evidences

Safety analysis of the Office subsystem was performed by analyzing the functions performed by the Office within the PTC system.





4.1 Office PHA. OHA, IHA, FMECA

The Office PHA [9]. OHA [11], IHA [10], and FMECA [13] resulted in the identification of hazard and safety requirements. These hazard records have been logged in the Office Hazard Log in the Office SSHA [2] where the related safety requirements are in the process of being tracked to closure.

Anticipated edits to OHA do not affect the conclusions of this report:

- Record Office_OHA_21 has safety requirement which is erroneously using an already taken SR Id: OF-OR-03: “Procedures and training shall be in place for dispatchers to apply and verify application of TSRs to protect a failed highway crossing. Clearly defined procedures and proper training materials/courses for procedures shall be provided.” Needs a new ID number, OF-OR-79.
- Record Office_OHA_24 has safety requirement which is erroneously using an already taken SR Id: OF-OR-71: “Software and data installation procedures will have instructions to verify the data and software files on the final targets. Clearly defined procedures and proper training materials/courses for procedures shall be provided.” Needs a new ID number, OF-OR-80.

- An addendum regarding Select-Check-Execute protocol is to be added to the OHA.

Anticipated edits to FTA do not affect the conclusions of this report:

- Gate STS FAILURE 14 description should remove reference to HL-328-330. These hazard log entries were deleted because it was determined in the course of the Office IHA that the UIS/RGS interface does not support TSR list exchange between STS and Adj STS.
- Event OF_SR40-43, description should cover HLs 233,234,236-238.

There are no anticipated edits for the FMECA or IHA.

4.2 Office Fault Tree Analysis and Calculation of MTTHE

The Office FTA [12] was constructed using Category I hazards (excluding Electrocution and Fire and Smoke) from the Office Hazard Log in the Office SSHA [2]. The FTA concluded that the Office design meets the customers MTTHE requirement, with an MTTHE of 7.731e-10 hrs. There was one previously unidentified hazard record added as a result of the Office FTA to the Office Hazard Log, and one safety requirement added to mitigate this hazard.

4.3 Office Subsystem Hazard Analysis

The Office SSHA [2] includes:

1. Office Hazard Log where the related safety requirements are in the process of being tracked to closure.
2. Safety Analysis of Office Response Timing Analysis – in progress.
3. Safety Analysis of STS Synchronization Under Failure Conditions –in progress. N/A to RSD. As there is only one Central Control sending TSRs to vehicles, synchronization between PCC and BCC is not necessary.
4. Safety Analysis of TSR Transformation

The Office SSHA verifies the implementation of the safety requirements that have been identified in the Office safety analyses. The Office safety requirements are linked to the Office SSLR or, if the requirement is allocated to another subsystem besides the Office, to the System Safety Requirements.

Future revision of the Office SSHA shall include correction of typo risk reclassification of HL-297 and HL-299 in the Office Hazard Log from IC to IE. Note that HL-297, 298, and 299 are three records for three mitigations to a single hazard. The three mitigations taken together mitigate to ‘E’ frequency.

4.3.1 Closure of all Subsystem Hazards

See the Project Hazard Log [23] Attachment C, Office Hazard Log.

4.4 FAT Results

There were 18 failed test cases in Regression FAT of Office 3.5.0 and 3.5.1:

SR_264	Operating Procedure shall instruct the Supervisor to confirm all EIC are clear of a workzone before issuing a TSR Override.
SR_112	Operating Procedures shall be used by the EIC to verify TSR with Dispatcher before entering Railway.
SR_490	All office equipment to be located in secure physical locations
SR_128	The existing "paper" based system of dispatching TSRs shall be maintained in parallel with electronically generated TSR for the ACSES II. Operating procedure is required to record all possible TSR's manually and ensure Train Engineer is updated on TSR list. Train operator shall have paper copy of TSRs. The Train Engineer shall be trained properly to execute TSR based on Dispatcher printout. TSRs added after train is enroute shall be communicated to train operator by the Dispatcher. Confirmation of existing paper documentation of TSRs shall be included in the daily responsibilities of the Train Dispatcher when he/she completes the Train sheet upon taking over a section.

5 Office Software V&V

A positive conclusion of the Office Software V&V Report [16] for Office 3.5.0/3.5.1 is necessary to proceed with revenue service. This report is has been released with positive conclusion.

6 SDMT Safety Verification

[redacted]

7 [redacted]

[redacted]



7.1 Remaining Open Items

See Section 4.5 and 4.7.

7.1.1 Restrictions to Mitigate Open Items

The LIRR SRAC [5] lists all the restrictions to be followed during RSD.

7.1.2 Schedule to Remove Restrictions

Restrictions above will be evaluated for each software release of each subsystem to the system.

8 Conclusion

Based upon

- positive conclusion of System Database Safety Verification Report [15],
- positive conclusion of Office SVVR [16]
- implementation of System SRACs, and
- implementation of OBC functional safety requirements per Table 10 herein

BT-RCS concludes that there is no known safety issue that would affect operation in RSD.

Metropolitan Transportation Authority
Long Island Railroad
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Number: 1712

OBC Phase 3 Software Safety Report

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	PM	Report	Project	Released

		Name / Title, Group	Signature	Date
Prepared:	Robert Kish	Safety Engineer	Robert Kish	5/15/19
Verified:	Rob Vargo	Project Engineer	Robert Vargo	5/15/19
Approved:	Francis Scapellato	Project Manager	Francis Scapellato	5/15/2019
Quality Process:	Stefan Makuch	SRA Quality	Stefan Makuch	5/15/19
BT/SRA Review:	Jason Weighley	BT Safety	Jason W Weighley Jason W Weighley 2019.07.19 16:02:36 -04'00'	
BT/SRA Review:	NA	Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3051179

Effective Date:	Revision:	Language:
2019-05-15	_V	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2017-08-14	First Release
_A	2017-08-17	Title correcteded in Item 4 of Table 1 from QE to QF. Contract number on cover changed to 1712.
_B	2017-08-28	Changed SVVR to Rev F. Added details to Introduction, Section 2. Removed references to OBC software since this release is for AIU and ADU only. Section 4.3: Added additional operation constraints from safety analysis.
_C	2017-09-20	Table 1, Changed Ref 18 Safety Concepts to Rev C, and Ref 19 LIRR Product Safety Plan to Rev D.
_D	2018-01-04	Updated SVVR Rev to K, Reference 6. Added comments to Section 1 to include C3, DE, and DM types. Added Reference 5 and renumbered other references.
_E	2018-02-02	Updated SVVR to Rev M
_F	2018-08-16	Updated for Rev. S release for RSD
_G	2018-08-20	Updated: Rev levels in Section 4, Variances in Sections 4.2.1 and 4.3, Constraints in Section 4.4.
_H	2018-10-09	Updated for Revenue Service Demonstration Release, aded all environmental test references, added variance details
_J	2018-10-25	Revised variance info based on recent updates, revised references to PVI and SVVR for S2A release for RSD testing.
_K	2018-10-26	Revised for S3. Updated the Reference Documents List, Variances, and Constraints.
_L	2018-11-02	Revised for S2A release (Baseline 3.2). Rev _J was the reference. Incorporated BT comments on Rev H and Rev K as appropriate for S2A. Next Rev (M) will include changes applicable to release S3.
_M	2018-11-06	Revised for S3. Changed version of PVI and SVR in reference Table. Updated variances and constraints.
_N	2018-11-16	Revised for S2A release, based on Rev _L. Note that Rev _M changes are not included. Revised [Ref. 8] OBC New Function FAT test report to show testing of additional closed variances. Updated variance lists by adding the last 5 entries of Table 5. Changed FTA revision level to B.
_P	2018-11-21	Revised for S3A. Includes changes made in Rev M and N.
_Q	2019-01-02	Revised based on comments from LIRR, (SI-PVW-0772). Added lines to Table 5 to match the variances in PVI. Section 2.1 changed to limit applicability to M7 vehicles. Added mention of “constraints” and added explanation of the different Phases. Deleted Constraint #18 and added constraints #25, and #26.. Added AIU to Section 4.1. Deleted duplicate and closed issues from Table 5. Revised Section 5 to clarify that variances listed in Table 5 are closed or have a safety justification.

_R	2019-01-02	Revised based on comments from BT (Review Recods for S3A). Not issued to BT.
_S	2019-02-07	Revised for version S4B.
_T	2019-03-21	Corrected to match PVI. Added line 2819/261735 to Table 5. Changed revison of Reference 16 to _C.
_U	2019-04-25	Changed approver M. Arnold to R. Vargo. Updated for version 5.00.0007. Deleted constraints 15, 22, 23, 25 from Rev T. Constraint 24 in rev T is norw 21. Added new constraints 23, 24, 25, 26, 27, and 28. Updated constraint 22.
_V	2019-05-14	Revised for S5D (5.01.0003).

Table of Contents

Section	Subject	Page
1	Executive Summary	4
2	Introduction	4
2.1	Applicability	4
2.2	Reference Documents	5
3	Configuration	8
4	Versions	9
4.1	Safety Critical Software Verification	10
4.2	Known Non-Conformities that have not been corrected with this release	10
4.3	Constraints	14
5	Summary	17

1 Executive Summary

A summary of the evidence reviewed and released that ensures the Onboard software release version “S5D”. This release is for revenue service and RSD testing. Evidence referenced in this report is in configuration management and all documents are signed off. This version contains additional bug fixes and variance close outs that are intended for OBC release version S5D.

2 Introduction

This document is intended to define the evidence to satisfy the safety, RAM, and compliance requirements assigned to the Onboard subsystem for the ACSES II system for release S5D. The S5D release is to allow the use of the fully functional onboard system with the operating constraints described in this document. The OBC will have event recorder functionality when powered on and by-passed. S5D software is released for field Revenue Service Demonstration testing and revenue service.

This software is fit for revenue service. The vehicles are currently operating with installed PTC for limited use. After Phase 3 software is installed and tested, the entire Onboard OBC, including ADU and AIU, can be used for Normal operation. Phase 3 is a general term that identifies the final phase of product development, to be completed after Phase 1 (Civil Speed Enforcement) and Phase 2 (Commissioning).

2.1 Applicability

This safety report is for the ‘S5D” release of software for LIRR Onboard subsystems. The functionality of the ACSES II meets all requirements for LIRR OBC functionality. The document is applicable LIRR M7, DE/DM, C3, M9, M3, TC-82, PR20B (NYAR), GP38 (NYAR), and MP15 vehicles. This version includes bug fixes and variance resolutions specific for the S5D release.

2.2 Reference Documents

Table 1: Reference Documents

Reference Number	Document Name	Identification Number	Revision
[1]	Dictionary of Terms and Acronyms	3035624	_B
[2]	Safety Related Application Conditions	3045431	_G
[3]	OBC Subsystem Software Release Notes	3039709	AJ or higher
[4]	PVI for LIRR Onboard Software Version S	3039835	_X or higher
[5]	Software Verification and Validation Report CDRL 2-012-01	3039733	AC or higher
[6]	Reliability Calculations CDRL 2-146	3035848	_G
[7]	LIRR ACSES Onboard FAT Report, Basic Functions, CDRL 2-061-207	4008562	_H
[8]	LIRR ACSES Onboard FAT Report, New Functions, CDRL 2-061-209	4008570	_M
[9]	LIRR ACSES Onboard FAT Procedure, Radio Functions, CDRL 2-061-208	4008566	_M (S5C) and _N (S5D)
[10]	LIRR ACSES OBC FAT Test Report. C3 Delta Test, CDRL 2-062-212	4008659	_E
[11]	LIRR ACSES OBC FAT Test Report. DE/DM Delta Test, CDRL 2-062-211	4008658	_E
[12]	PTC Onboard Safety Concepts Description CDRL 1-124-01	3036406	_C
[13]	Onboard System Product Safety Plan, LIRR, CDRL 2-123-11	3036424	_D
[14]	Onboard Preliminary Hazard Analysis, LIRR, CDRL 2-127-21	3036405	_D
[15]	Onboard Failure Modes, Effects, and Criticality Analysis, LIRR, CDRL 2-129-21	3039814	_A
[16]	Onboard Fault Tree Analysis, Common LIRR Vehicles, CDRL 2-132-21	3039788	_C
[17]	Onboard Subsystem Hazard Analysis, LIRR, CDRL 2-128-21	3037390	_D
[18]	M7/M7A Undercar Shock and Vibration Test Report	4007147	_A

Reference Number	Document Name	Identification Number	Revision
[19]	Undercar Temperature Qualification Test Report	4007167	_A
[20]	M7/M7A Undercar Ingress Test Report	4007786	_B
[21]	M7 OBC and ADU Humidity Test Report	4007834	__
[22]	Shock and Vibration Test Report for C3 OBC and ADU	4007929	—
[23]	Shock and Vibration Test Report for M9 PTC OBC	4008530	—
[24]	EMI/EMC Qualification Test Report for C3 OBC and ADU	4007931	—
[25]	Temperature Qualification Test Report for the C3 OBC and ADU	4007932	—
[26]	Shock and Vibration Test Report for DEDM30 OBC and ADU	4007855	_A
[27]	DE/DM Undercar Shock and Vibration Test Report	4007856	—
[28]	EMI/EMC Qualification Test Report for DE / DM30 OBC and ADU	4007857	—
[29]	DE/DM30 OBC Temperature Test Report	4007858	_A
[30]	NYAR GP38 Undercar Shock and Vibration Report	4008599	—
[31]	M7 OBC Shock and Vibration Test Report	4007618	_B
[32]	M7 OBC Temperature Test Report	4007784	_A
[33]	EMC/EMI Qualification Test Report for M7 OBC and ADU	4007785	_B
[34]	M9 PTC OBC Shock and Vibration Test Report	4008530	_A
[35]	M9 PTC EMI/EMC Test Report	4008531	__
[36]	M9 PTC OBC Temperature Test Report	4008532	__
[37]	MP15 Undercar Shock and Vibration Test Report	4008600	—
[38]	NYAR Green OBC and ADU Shock and Vibration Test Report	4008585	—

Reference Number	Document Name	Identification Number	Revision
[39]	NYAR Green Undercar Shock and Vibration Test Report	4008586	—
[40]	NYAR Green EMI/EMC Test Report	4008587	—
[41]	NYAR Green OBC and ADU Temperature Test Report	4008588	—
[42]	TC-82 Undercar Shock and Vibration Test Report	4008282	—

Table 2: Applicability of Environmental Tests

LIRR Vehicle	OBC S&V	UC S&V	EMC	TEMP	IP	HUM
M7	Complete	Complete	Complete	Complete	Complete	Complete
M9	Complete	No, KRC responsible	Complete	Complete	No, same as M7	No, same as M7
MP15	No same as NYAR Green	Complete	No same as NYAR Green	No same as NYAR Green	No, same as M7	No, same as M7
C3	Complete	Complete	Complete	Complete	No. Same as M7	No. Same as M7
M3	No. Same as C3	No. Same as C3	No. Same as C3	No. Same as C3	No. Same as M7	No. Same as M7
DE/DM	Complete	Complete	Complete	Complete	No. Same as M7	No. Same as M7
GP38	No same as NYAR Green	Complete	No same as NYAR Green	No same as NYAR Green	No, same as M7	No, same as M7
TC-82	No, same as DEDM	Complete	No, same as DEDM	No, same as DEDM	No, same as M7	No, same as M7
NYAR Green	Complete	Complete	Complete	Complete	No. Same as M7	No. Same as M7

S&V: Shock and Vibration Test

UC: Undercar Equipment

TEMP: Temperature Test

IP: Ingress Test

HUM: Humidity Test

3 Configuration

Table 3: Hardware and Software Configuration

Location	Component Name	Part Number
ACSES Cardfile	LIRR Main PCB	A073G02-A02
ACSES Cardfile	Tach I/O PCB	A073G01-A92
ACSES Cardfile	Aux I/O PCB	A073G01-A93
ACSES Cardfile	Decoder / Transponder Reader PCB	A073G01-A76
ACSES Cardfile	Ethernet S12 PCB	A073G01-A94
ACSES Cardfile	Ethernet Netburner	A075G03-A02
AIU, all types	MTA AIU	A073G01-A97
Decelerometer	MTA Decelerometer	A073G01-A91
CMM	MTA CMM	A073G01-A101
ADU	M7, M9 and TC-82 ADU	A073G01-A104
ADU	DE/DM ADU	A073G01-A105
ADU	C3, M3 and MP15 ADU	A073G01-A98
ADU	NYAR ADU	A073G01-A109
PTE	MTA ACSESVIEW LIRR	A072G01-A43
CHMM (COTS)	Crash Hardened Memory Module	9VD70C:2.2

4 Versions

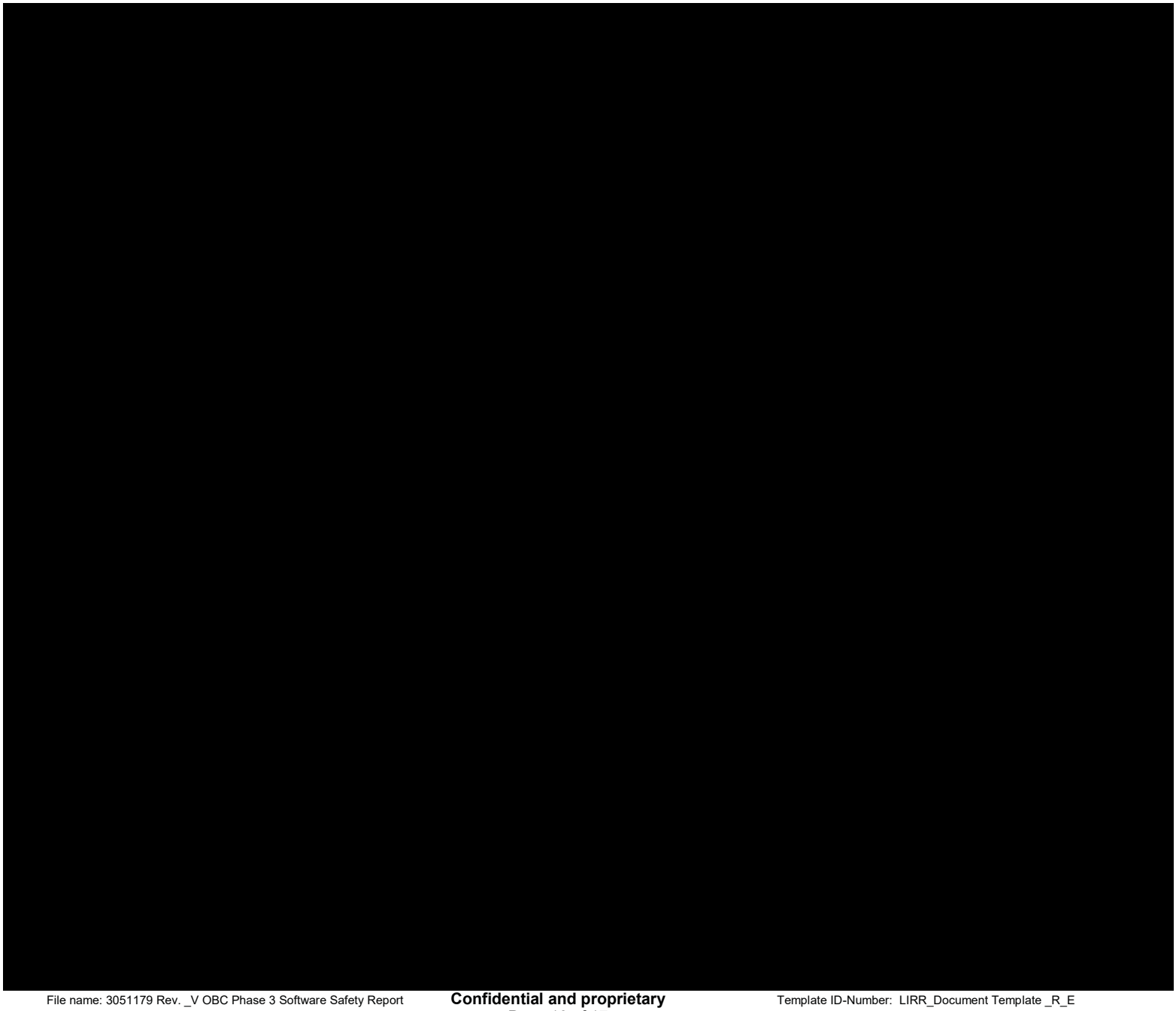
Table 4: Assembly Reference and Build Versions

	Assembly Revision	Date	Build Version	Checksum	Changed From Prior PVI Revision
Main A073G02-A02	8	5/12/19	8.01.0002	$BC1DA8BF	Yes
AuxIO A073G01-A93	1	8/24/16	1.00.0001	$D093913A	No
TachIO A073G01-A92	2	1/16/17	2.00.0000	$3AD9961D	No
Ethernet-S12 A073G01-A94	5	1/22/19	5.00.0000	$905E8DD0	No
Ethernet Netburner A075G03-A02	10	5/14/19	10.01.0003	n/a	Yes
TP Reader A073G01-A76 OR SIMACSES_II	2	4/20/16	n/a	n/a	No
Decel A073G01-A91 Revision 3,4 or 5	3	5/10/17	3.00.0000	$F92423A8	No
	4	5/18/18	4.00.0001	$E49DC1DD	
	5	6/06/18	5.00.0000	$F38C91B7	
Config A073G01-A101	3	8/02/17	2.03.0000	$73F877DD	No
AIU A073G01-A97	3	7/19/17	3.03.0003	$D093913A	No
M7 ADU (also used M9, TC82) A073G01-A104	3	7/06/17	2.00.0002	$375CEF4B7	No
DE/DM ADU A073G01-A105	2	7/06/17	1.00.0002	$92296E71	No
C3 ADU A073G01-A98	5	12/12/18	3.02.0002	$2AFB3D3B	No
M3, MP15 ADU A073G01-A132	0	12/12/18	0.00.0001	$DCAACC9A	No
NYAR ADU A073G01-A109	1	5/04/18	2.00.0001	$C2746EC1	No
ACSESView A072G01-A43	n/a	5/13/19	4.07.0044	n/a	Yes
SimACSES A072G01-A10	n/a	10/29/18	7.19	n/a	No
CHMM (COTS) 9VD70C:2.2	bi	n/a	n/a	n/a	No

4.1 Safety Critical Software Verification

The OBC, AIU, and ADU perform safety-related functions that both require the devices to be fail-safe. The functions are vital under all credible failure conditions of components and circuits, including the ability of the processor to properly execute the software program. Software that is designated as Vital is verified by performing rigorous functional testing, reviews, and verifying that Failsafe Techniques Verification are properly implemented and applied.

4.2 Known Non-Conformities that have not been corrected with this release



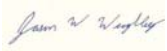
5 Summary

All non-conformities have been corrected with the “S5D” release by the application software or identified as Open with a safety justification for use in RSD. The identified constraints must be implemented as noted. Revision “S5D” is to be cut-in and operational for revenue service on approved lines. This is the release for field installation with full revenue service of RSD testing of the OBC system. V&V has concluded with no issues except the issues noted as variances, “S5D” is fit to be cut-In and operational for revenue service operation.

Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

Communication Subsystem
Final Safety Report
CDRL 2-136-23

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG		Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Jason Weighley Safety Engineer		2019.02.27 15:53:45 -05'00'
Verified:	Aaron Graham Safety Engineer		2019.03.01 08:49:15 -05'00'
Approved:	Anthony DeFrancisco Project Director		Anthony DeFrancisco 2019.05.31 16:58:20 -04'00'
SI Quality Process Review:	Phil Maglorie BT Quality Assurance Group		2019.04.25 13:40:31 -04'00'
BT/SRA Review:	N/A Title		
BT/SRA Review:	N/A Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3037454

Effective Date:	Revision:	Language:
2019-02-27	___	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2019-02-27	First issue

Table of Contents

Section	Subject	Page
1	**Executive Summary**	6
2	**Introduction**	6
2.1	**Ground Based Network (GBN)**	7
2.2	**Wayside Equipment**	7
2.3	**Onboard Equipment**	9
2.4	**Office Equipment**	9
2.5	**Compliance Matrix**	10
2.6	**Reference Documents**	14
2.7	**Glossary**	17
3	**Summary of Safety Analysis and Evidences**	17
3.1	**Comms FAT Tests**	18
3.1.1	Comms Phase 2A FAT Test Results	18
3.1.2	Comms Pre-FAT Certification Phase 2 Release 1.4 Test Report	20
3.1.3	Phase 2 Release 1.6 FAT Results	21
3.2	**Comms Site installation Tests**	21
3.2.1	Comms Baseline Site Installation Test Report	21
3.2.2	L2 Wood C-Case SIT Test Report	22
3.2.3	L1 Network CIL Comms Site Test Report	23
3.2.4	Line 2 Harold 2 Comms Site Installation Test Report	24
3.2.5	L2 Wood 2 Comms Site Installation Test Report	25
3.2.6	L2 Shea C Case Site Installation Test Report	26
3.2.7	L2 Bay C Case Site Installation Test Report	27
3.2.8	L2 Neck 1 C Case Site Installation Test Report	28
3.2.9	L2 Plandome C Case Site Installation Test Report	29
3.2.10	L2 Port Washington C Case Site Installation Test Report	30
3.2.11	L1 Bablyon C Case Site Test Installation Report	31
3.2.12	L1 Babylon 2 C Case Site Installation Test report	32
3.2.13	L1 Babylon Yard C-Case Site Installation Test Report	33
3.2.14	L1 Bayshore C-Case Site Installation Test Report	34
3.2.15	L1 Great River C-Case Site Installation Test Report	34
3.2.16	L1 Sayville C-Case Site Installation Test Report	35
3.2.17	L1 Patchogue C-Case Site Installation Test Report	36
4	**Safety Certification Process**	36
4.1	**SRTM**	36
4.2	**Remaining Open NCR's**	37
4.3	**Remaining Open Variances**	38

5 Conclusion 38
6 Validation Conditions 38
7 Attachment A – Open Variance List 39
8 Attachment B – Open Safety Critical NCR's 40
9 Attachment C Phase 2 Release 1.6 FAT Test Report 41

List of Figures

Figure 1 Communication Subsystem Overview 6

List of Tables

Table 1: Wayside Equipment 8
Table 2: Onboard Equipment 9
Table 3: Office Equipment 10
Table 4: Compliance Matrix 10
Table 5: Reference Documents 14
Table 6: Acronyms Specific to this Document 17
Table 7 Safety Analysis 17
Table 8: Test Tools for Comms 18
Table 9 Pre-FAT Certification Phase 2 Relase 1.4 20
Table 10 Phase 2 Release 1.6 FAT 21
Table 11 4009056 NCR/Variance 21
Table 12 4009190 Wood 2 SIT NCR / Variances 22
Table 13 4009191Variance and NCR 23
Table 14 4009292 Harold 2 SIT NCR / Variance 24
Table 15 4009293 L2 Wood 2 SIT NCR/Variances 25
Table 16 4009294 Shea SIT NCR / Variances 26
Table 17 4009295 Bay SIT NCR/Variances 27
Table 18 4009296 Neck 2 SIT NCR/Variances 28
Table 19 4009297 Plandome SIT NCR / Variances 29

Table 20 4009298 Port Washington SIT NCR / Variances 30
Table 21 4009300 Babylon SIT NCR / Variances 31
Table 22 4009301 Babylon 2 SIT NCR / Variances 32
Table 23 4009302 Babylon Yard SIT NCR / Variances 34
Table 24 4009303 Bayshore SIT NCR / Variances 34
Table 25 4009304 Great River SIT NCR / Variances 35
Table 26 4009305 Sayville SIT NCR / Variances 35
Table 27 4009306 Patchogue SIT NCR / Variances 36
Table 28 Safety Critical NCR 37

1 Executive Summary

The Comms Final Safety Report documents the closure of all hazards assigned to the Comms subsystem and evidence of closure of all assigned safety requirements to the Comms subsystem. As the comms subsystem is not a vital subsystem the MTHE is shown at the system level through the System Fault Tree. All comms subsystem failures and interactions are included in the system fault tree. No specific Comms fault tree was produced.

This version of the report is focused on the requirements and hazards of the full ACSES functionality of the contract. The scope of this version of the report is for Pilot Line 1 and Line 2.

2 Introduction

The Communication subsystem contains four different main components:

1. Onboard MCM
2. Wayside BCM
3. Office (WCC and RGS)
4. Ground Based Network (GBN)

The radios 220MHz and alternate radios (Wi-Fi and Cellular) are also part of the communication subsystem.

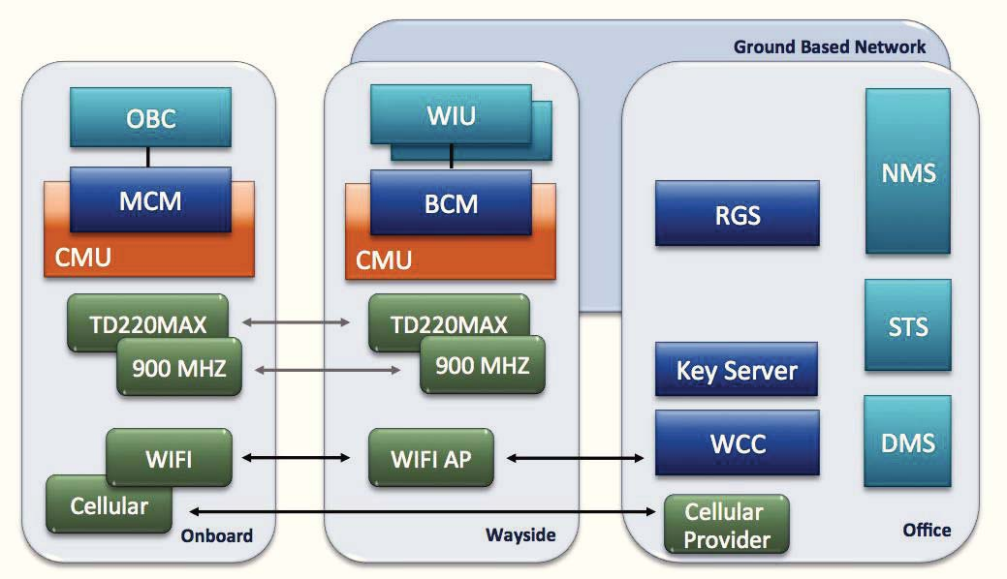


Figure 1 Communication Subsystem Overview

2.1 Ground Based Network (GBN)

The GBN comprises office and field based routers and associated data circuits and connections to interconnect the MTA PTC components and provide the necessary interfaces to other railroads and infrastructures as needed.

2.2 Wayside Equipment

The table below shows the major (Level 1) components of the wayside equipment, and provides a brief description of the function of each. These components are located either in the Comm Hut (C-Case), Radio Case, CIL, or on a radio mast/pole depending on the equipment type or railroad. For details on any of the hardware, refer to the Comms Subsystem Hardware Design description, CDRL 7-002 [40]. A complete functional description of the equipment is provided in later sections of this document.

Table 1: Wayside Equipment

Device	Description
Base Communications Manager (BCM)	Handles the details of the RF protocols and communications failover
Remote Terminal Unit (RTU / µRTU)	Monitors wayside devices via analog and digital inputs, and provides the data to the NMS system via SNMP.
220 MHz PTC Data Radio (PDR)	The primary communications method for transmission of data between the base and mobile objects.
WiFi / Cellular Radio	Provides alternative wireless bearer method.
900 MHz Radio	Provides alternative wireless bearer method.
GPS Receiver	Provides timing pulse to 220 MHz PDR to maintain TDMA clock synchronization.
Layer 3 Network Switch	Provides network connectivity for wayside devices.
Layer 2 Network Switch	Provides network connectivity for wayside devices.
220 MHz / 900 MHz / WiFi / GPS Antennas	Antennas for the various forms of radio communication.
RF Filters	Provide protection for the various forms of radio communication against out-of-band interference.
RF Power Amplifier	Amplifies the 220 MHz RF signal above the 2 Watt output of the PDR.
RF VSWR / Power Monitor	Monitors the condition of the PDR output for failover.
RF Transfer Switch	Connects and switches between the PDR components involved in radio failover. Note: RF Transfer Switch port isolation: 60 dB.
Radiating Cable	Acts as antenna in tunnel locations.

2.3 Onboard Equipment

The following table lists the major (level 1) components of the onboard equipment, and provides a brief description of each. Antennas, Filters, and the 900 MHz radio from the Wayside section 2.2 are functionally equivalent on the vehicle, and are not repeated in this section. For details on the actual vehicle components, please see CDRL 7-002 [40] and CDRL 5-001 [41].

Table 2: Onboard Equipment

Device	Description
Mobile Communications Manager (MCM)	It interfaces between the Onboard Computer (OBC) and onboard radios to deliver / accept ACSES messages to be transported over the communications network.
Wireless Router	Provides alternative wireless bearer methods over WiFi and cellular frequencies.
RF Filters	Protect each of the wireless bearer methods from undesired out-of-band signals.
220 MHz Radio (PDR)	The primary communications method for transmission of data between the base and mobile objects.
900 MHz Radio	Provides alternative wireless bearer method.
160 MHz Filter	A new filter will be installed in the existing voice radio system to prevent interference between the voice radios and the PTC radio system.

2.4 Office Equipment

The following table lists the major (level 1) components of the Communications Subsystem that are located in the office (and backup office), and provides a brief description of each. Further details on the hardware can be found in the Comms Subsystem Hardware Design description [40] document.

Table 3: Office Equipment

Device	Description
Wayside Communication Controller (WCC)	Manages ACSES communication flow between the office and the wayside BCMs.
Railroad Gateway Server (RGS)	Manages ACSES communication flow between the office and the office of a tenant railroad.
HMAC Key Server	Added to the office architecture to support data authentication in the communication system.
Radio Frequency Manager (RFM)	Functions as a parallel and independent monitoring system to observe, record, configure, display and trend the key performance parameters of the network.
Layer 3 Switch	Provides network connectivity for office devices.
Firewall	Provides security between different zone like-Office, RWPS, Wayside interlocking, Remote office, etc.
External Network Router	Provides network connection between Amtrak and office.

2.5 Compliance Matrix

Table 4: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part I	12.10.12.A	Final Safety Report	Final Safety Report shall provide a summary of the results on the overall safety analysis, safety verification, and system safety demonstration	All

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part I	12.10.12.B		Final Safety Report shall contain evidence of safety analysis	3
Vol 2 Part I	12.10.12.C	MTTHE	Document the calculation and methodology to show the MTTHE requirements in 9.1 have been achieved	See System FTA
Vol 2 Part I	12.10.12.D	Risk Reduction Actions	Address all risk reduction actions taken during design, test, operation and maintenance to mitigate faults caused by Operating Scenarios, Failures, Latent Design Errors, Installation errors, Human Reaction, Post implementation changes to SW or HW, or Interoperability and compatibility issues.	4.1
Vol 2 Part I	12.10.12.E	Information in Report	Describes the Safety Certification process and issues encountered during certification. Describes certification status Describes remaining restrictions / open issues and actions / work arounds to ensure acceptable level of safety is maintained.	4

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
			Provides a schedule for eliminating restrictions / workarounds. As appropriate. Includes Certificate of Compliance	
Vol 2 Part 1	12.10.12.F	Resolution of all Hazards	Report shall contain evidence of the resolution of all hazards. Evidence of resolution shall consist of satisfactory closure of the items as listed in the Project Hazard Log and achievement of the items listed in the Certified Item List	4.1
	12.10.12.G	Approved by Engineer	Report format will be approved by the Engineer and submitted in draft form at FDR. Report will stay draft until final system certification is achieved.	4

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.12.H	Approval of Final Safety Report	Report is to be submitted to SSCB prior to Completion of Pilot Phase commissioning and testing. Once approved by SSCB then submitted to the FRA and revised to address comments with a disposition per FRA comment. The report will be revised when characteristics of any territory, TP interface or the TP is modified in a way that impacts the safety of the system.	4

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part I	9.1.E	MTTHE	The SI shall provide a quantifiable analysis of the safety of each of the ACSES II Subsystems and the ACSES II System as a whole. The minimum level of safety that the SI shall demonstrate through calculated Mean-Time-To-Hazardous-Event (MTTHE) is 10^{-9} hours. The MTTHE and the complete safety analysis and calculations for each ACSES II Subsystem and the ACSES II system shall be provided as part of the Final Safety Report, CDRL 2-136.	See System FTA
Vol 2 Part I	9.5.F	MTTHE	Final Safety Report shall document the complete safety analysis and calculations to support the MTTHE of the Comms Subsystem	See System FTA

2.6 Reference Documents

Table 5: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624

Reference Number	Document Name	Identification Number
[2]	LIRR Project Hazard Log (CDRL 2-126-20)	3035819
[3]	Certifiable Item List (CDRL 2-125-20)	3035818
[4]	Comms System Safety Concept Document (CDRL 2-124-03)	3036421
[5]	Comms Subsystem Design Description (CDRL 7-001)	3035965
[6]	Comms Subsystem Hazard Analysis (CDRL 2-128-06)	3037392
[7]	Comms Operating Hazard Analysis (CDRL 2-130-03)	3037418
[8]	Comms Interface Hazard Analysis (CDRL 2-131-03)	3037430
[9]	PVI for ACSES II LIRR MCP Configuration	3051839
[10]	PVI for ACSES II LIRR MCP Firmware	3051842
[11]	PVI for ACSES II LIRR BCP Firmware	3051873
[12]	PVI for ACSES II LIRR BCP Pilot Line 1 Configuration	3051848
[13]	PVI for ACSES II LIRR BCP Pilot Line 2 Configuration	3051849
[14]	Coms Preliminary Hazard Analysis (CDRL 2-127-03	3036420
[15]	LIRR SRAC	3045431
[16]	L2 Wood C-Case Site Installation Test Report (CDRL 2-085-201 Addend 1)	4009190
[17]	L2 Harold 2 Comms Hut Site Installation Test Report (CDRL 2-085-201 Addend 2)	4009292
[18]	L2 Wood 2 Comms Hut Site Installation Test Report (CDRL 2-085-201 Addend 3)	4009293
[19]	L2 SHEA C Case Site Installation Test Report (CDRL 2-085-201 Addend 4)	4009294
[20]	L2 Bay C-Case Site Installation Test Report (CDRL 2-085-201 Addend 5)	4009295
[21]	L2 Neck 1 C-Case Site Installation Test Report (CDRL 2-085-201 Addend 6)	4009296

Reference Number	Document Name	Identification Number
[22]	L2 Plandome C-Case Site Installation Test Report (CDRL 2-085-201 Addend 7)	4009297
[23]	L2 Port Washington C Case Site Installation Test Report (CDRL 2-085-201 Addend 8)	4009298
[24]	L1 Babylon C-Case Site Installation Test Report (CDRL 2-085-201 Addend 9)	4009300
[25]	L1 Babylon 2 C-Case Site Installation Test Report (CDRL 2-085-201 Addend 10)	4009301
[26]	L1 Babylon Yard C-Case Site Installation Test Report (CDRL 2-085-201 Added 11)	4009302
[27]	L1 Bayshore C-Case Site Installation Test Report (CDRL 2-085-201 Addend 12)	4009303
[28]	L1 Great River C-Case Site Installation Test Report (CDRL 2-085-201 Addend 13)	4009304
[29]	L1 Sayville C-Case Site Installation Test Report (CDRL 2-085-201 Addend 14)	4009305
[30]	L1 Patchogue C Case Site Installation Test Report (CDRL 2-085-201 Addend 15)	4009306
[31]	L2 CIL Comms Site Installation Test Report (CDRL 2-085-202 Addend 1)	4009056
[32]	L1 CIL Comms Site Installation Test Report (CDRL 2-085-202 Addend 2)	4009191
[33]	C-Case First Article Inspection (CDRL 2-086-20)	3046649
[34]	Communications Manager Units (MCM and BCM) First Article Inspection (CDRL 2-086 Addend)	3043426
[35]	LIRR CIL Communications Site Installation Test Procedure (CDRL 2-084-202)	3051506
[36]	LIRR Communication C-Case / Comms Hut Site Installation Test Procedure (CDRL 2-084-201)	3035779
[37]	MCM and BCM Functional Test Procedure (CDRL 2-080-001)	3044573
[38]	BCM and MCM FAT Test Report	4007534
[39]	Comms SRTM	3153125

Reference Number	Document Name	Identification Number
[40]	Comms Subsystem Hardware Design (CDRL 7-002)	3035966
[41]	Onboard Interface Control Document (CDRL 5-002)	3035903
[42]	BCM and MCM Pre-FAT Certification Phase 2, Release 1.4 Report	4008558

2.7 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in Table 6 respectively.

Table 6: Acronyms Specific to this Document

Acronym	Definition
FAT	Factory Acceptance Test
IHA	Interface Hazard Analysis
OHA	Operational Hazard Analysis
SSHA	Subsystem Hazard Analysis

3 Summary of Safety Analysis and Evidences

Safety analysis of the Comms subsystem was performed by analyzing the functions performed by the communication subsystem within the overall system. The analysis performed for the comms subsystem were the Subsystem Hazard Analysis, IHA, and OHA. If the status is noted as Approved, this indicates the Safety Working Group review has been completed and the document has been formally submitted to the Railroad.

Table 7 Safety Analysis

Name of Document	CDRL Number	PDM Number and Revision	Status



Hazard Status:

The Comms SSHA contained 55 hazards. All of the hazards are mitigated by identified safety Requirements. Please refer to the SRTM section for closure status of the hazards.

3.1 Comms FAT Tests

3.1.1 Comms Phase 2A FAT Test Results

As described in the Comms Baseline 2.3 FAT Test Report [38], the Comms Baseline 2.3 baseline is a regression of prior rounds of Pre-FAT testing.

As part of this round of Comms baseline 2.3 FAT, a total of 36 test cases were executed, 33 Passed and 3 Failed. 3 “New” Variance were opened, at least four variances were confirmed to be not verified. It should also be noted that 21 test cases were not performed by this test.

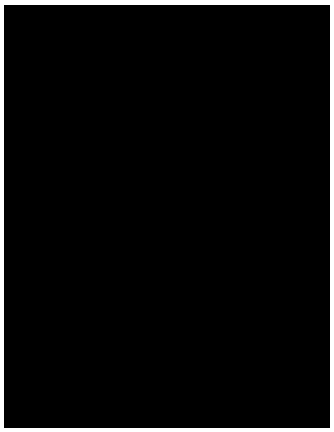
Table 8: Test Tools for Comms

Test Environment on Comms		
PTC - LIRR		
Software Configuration/ Version Control		
Pittsburgh FAT Lab		
Description	**PVI Version**	**S/W Version**

MCM		1_48_585_2453
BCM		1_48_585_2453
Radio		1.2.7

The SW used for this test is not part of the System Baseline Revision for Baseline 2.3 (PVI 3044660_Rev_B). This is the version prior to this revision. The Safety engineer cannot find conclusive evidence other than this in the project files and so these results are used. The project is encouraged to generate evidence of FAT testing for the current version that shows all test cases completed and variances resolved. Three test cases show failures, 33 out of 63 show pass, and 6 test cases are marked NA as they are indicated in the existing evidence as covered by other test cases. A total of 21 are blank with no comments or evidence.





3.1.2 Comms Pre-FAT Certification Phase 2 Release 1.4 Test Report

The Phase 2 Release 1.4 FAT Test Report [42], the test report does not reference the formal PVI defining the software version for this Test. Safety Engineer has reviewed 3044660 Rev_B and Rev_C do not match this version of software. 3044660_Rev_C is close (xcm_1_60_3030-master and xcm_py_1_60_3031_Master).

Table 9 Pre-FAT Certification Phase 2 Relase 1.4

Test Environment on Comms		
PTC - LIRR		
Software Configuration/ Version Control		
Pittsburgh FAT Lab		
Description	**PVI Version**	**S/W Version**
MCM		1_60_4238 1_60_3031_Master
BCM		1_60_4238 1_60_3031_Master
Radio		1.2.8

All 12 assigned test cases to this test report indicate pass. The test report does not mention nor does it record any regression testing for the failed test cases in the prior report. The test case ID's in this report do not match the failed test cases from the prior report. There are no recorded variances from this report.

3.1.3 Phase 2 Release 1.6 FAT Results

The Phase 2 Release 1.6 FAT Test Report see Attachment_C the test report does not reference the formal PVI defining the software version for this Test. Safety Engineer has reviewed 3044660 Rev_H and matches this version of software.

Table 10 Phase 2 Release 1.6 FAT

Test Environment on Comms		
PTC - LIRR		
Software Configuration/ Version Control		
Pittsburgh FAT Lab		
Description	**PVI Version**	**S/W Version**
MCM		1_60_5016 1_60_4541_Master
BCM		1_60_5016 1_60_4541_Master
Radio		Not reported

This report indicates that all 69 Test cases pass with no failures.

3.2 Comms Site installation Tests

3.2.1 Comms Baseline Site Installation Test Report

Comms Line 2 CIL Site Installation Test Report 4009056[31] was generated to cover all CIL on Line 2. The report is on the network equipment in the CIL. Only one Variance is reported in this report 262855 for no label on ethernet wiring from WIU to L2 switch for Wood, Bay, Neck 1, Neck 2, Neck 3 and PW CIL. All other tests passed. The PVI assigned for this test aligned with the System Baseline 3.2 PVI's for communication equipment.



3.2.2 L2 Wood C-Case SIT Test Report

Comms Line 2 CIL Site Installation Test Report 4009190[16] was generated to cover Wood C-Case on Line 2. The report is on the communication equipment in Wood C-Case. One of 24 test cases failed and two are marked pending and another two are marked N/A. The remaining 19 test cases are passed The PVI assigned for this test aligned with the System Baseline 3.2 PVI's for communication equipment



[redacted]

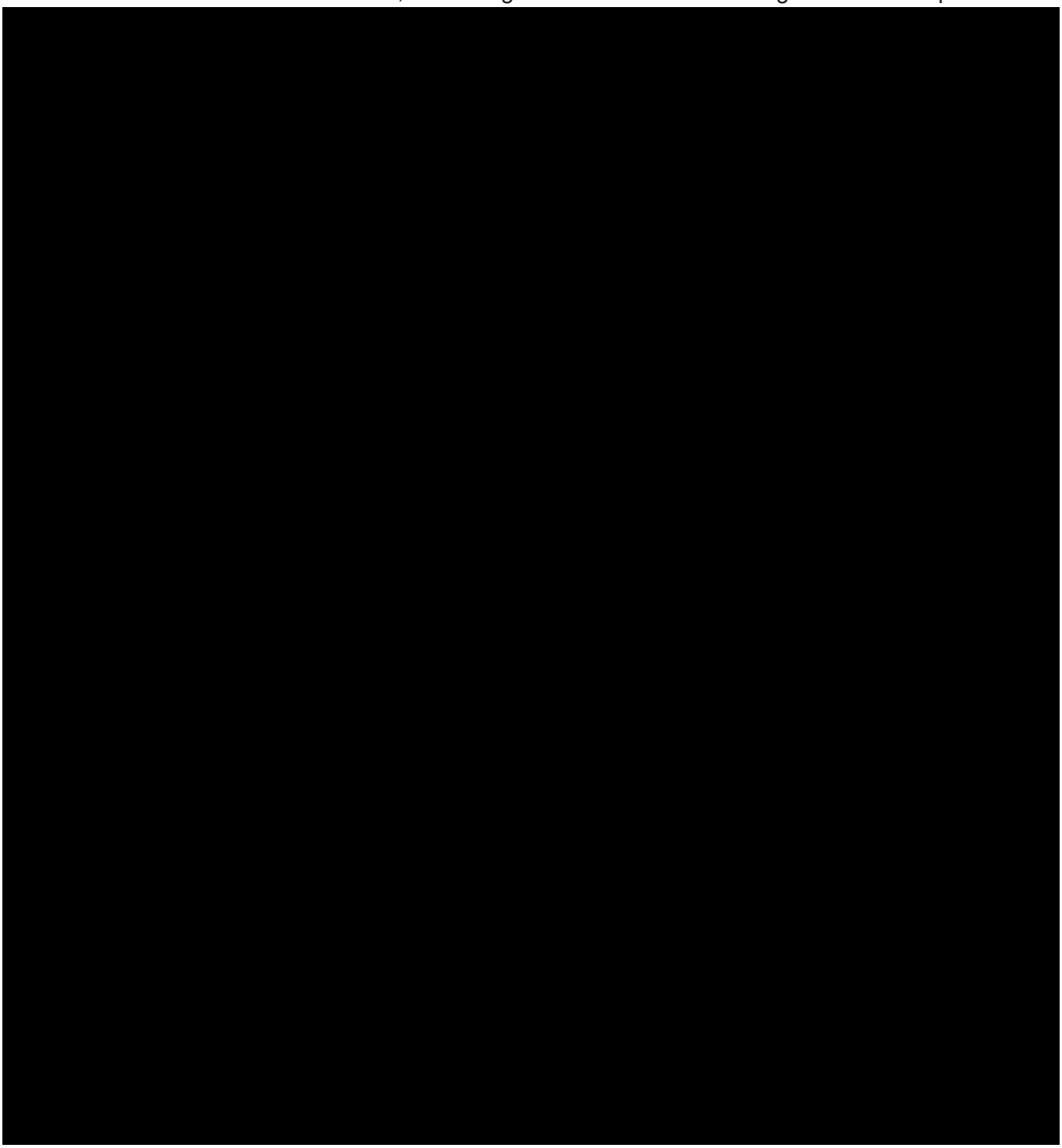
3.2.3 L1 Network CIL Comms Site Test Report

Comms Line 1 CIL Site Installation Test Report 4009191[32] was generated to cover all CIL on Line 1. The report is on the network equipment in the CIL. Only one Variance is reported in this report 262841 for no label on ethernet wiring from WIU to L2 switch for S20/5W, 60/9W, S384/13E, S398, S434, S435, S447 / S 448, S461 / S462, S484 / S485, and Y Sayville All tests passed for Patchogue and S409 / S410. For Bablyon the component test failed with Variance 214117. The PVI assigned for this test aligned with the System Baseline 3.2 PVI's for communication equipment.

[redacted]

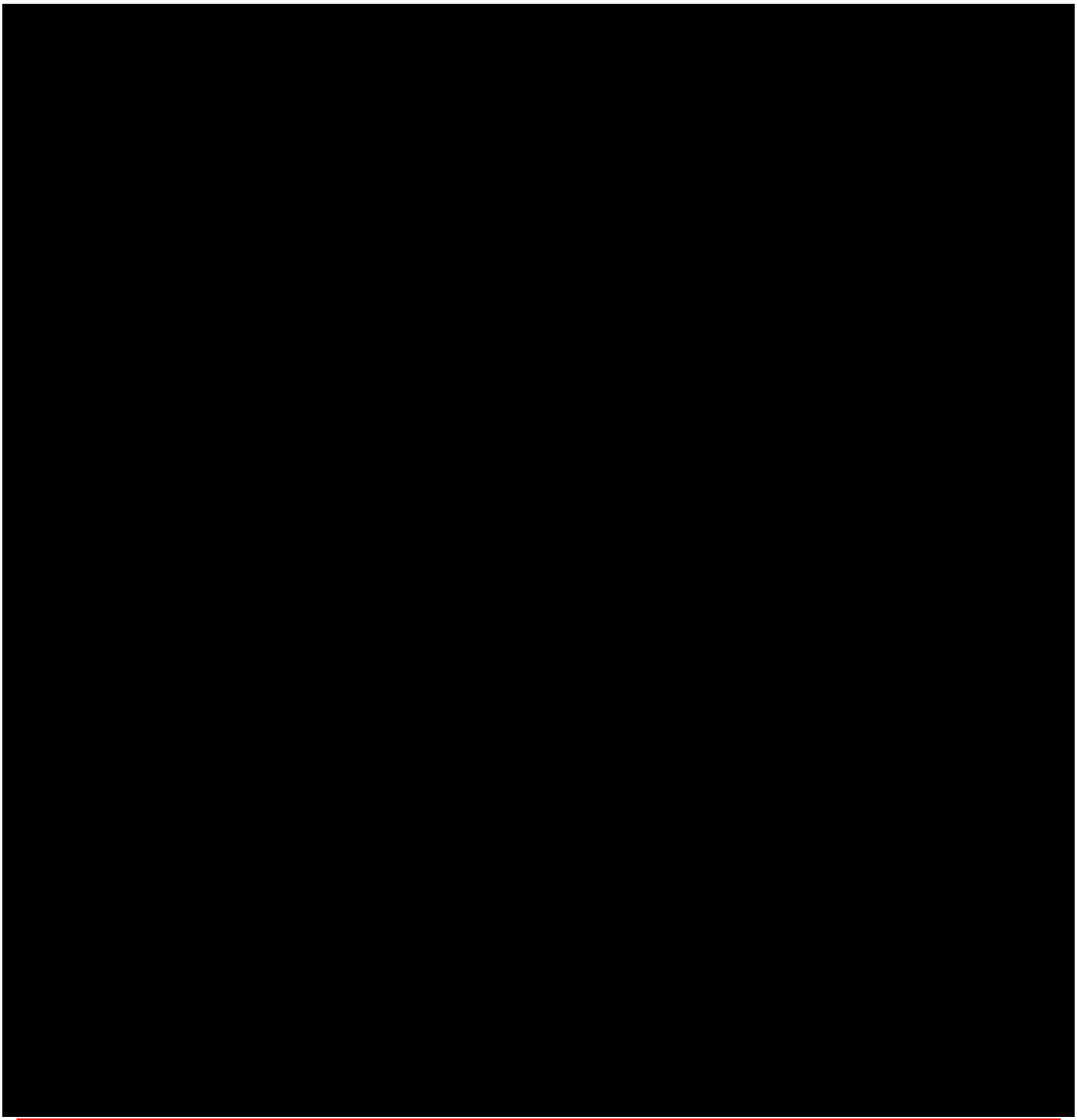
3.2.4 Line 2 Harold 2 Comms Site Installation Test Report

Comms Line 2 Harold 2 CIL Site Installation Test Report 4009292[17][18] was generated to cover Harold 2 C-Case on Line 2. The report is on the communication equipment in Harold 2 C-Case. Of the 24 test cases 1 failed, 2 Pending and 2 N/A. The remaining 19 test cases passed.



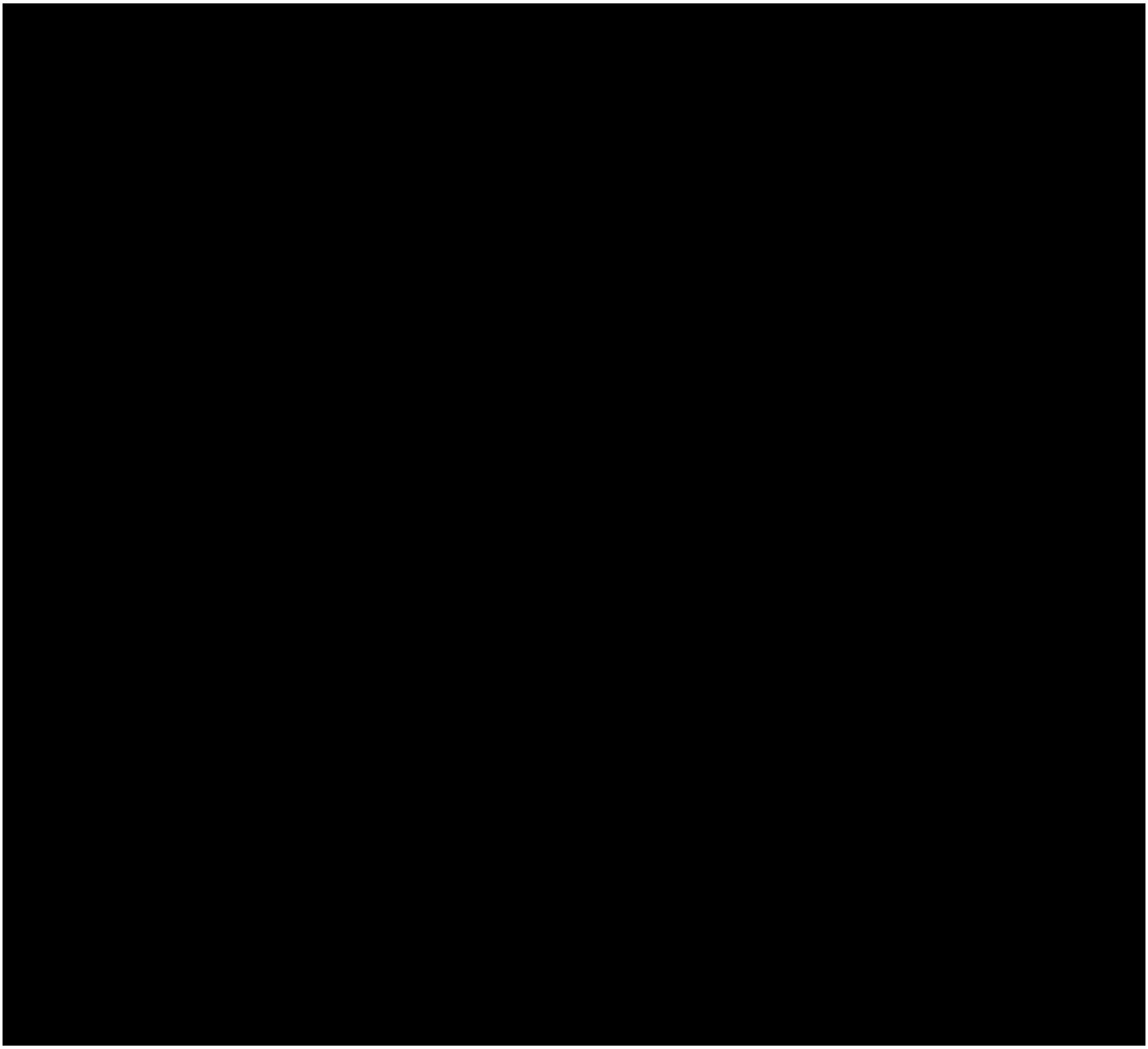
3.2.5 L2 Wood 2 Comms Site Installation Test Report

Comms Line 2 Wood 2 CIL Site Installation Test Report 4009293[18] [18] was generated to cover Wood 2 C-Case on Line 2. The report is on the communication equipment in Wood 2 C-Case. Of the 24 test cases 1 failed, 2 Pending and 1 N/A. The remaining 20 test cases passed.



3.2.6 L2 Shea C Case Site Installation Test Report

Comms Line 2 Shea CIL Site Installation Test Report 4009294[18][19] was generated to cover Shea C-Case on Line 2. The report is on the communication equipment in Shea C-Case. Of the 24 test cases 2 failed, 1 Pending and 2 N/A. The remaining 19 test cases passed.





3.2.7 L2 Bay C Case Site Installation Test Report

Comms Line 2 Bay CIL Site Installation Test Report 4009295[18][20] was generated to cover Bay C-Case on Line 2. The report is on the communication equipment in Bay C-Case. Of the 24 test cases 1 failed, 1 Pending and 1 N/A. The remaining 22 test cases passed. The report incorrectly references NCR 214109. This should be 214119.



[redacted]

3.2.8 L2 Neck 1 C Case Site Installation Test Report

Comms Line 2 Neck 1 CIL Site Installation Test Report 4009296[21][18][20] was generated to cover Neck 1 C-Case on Line 2. The report is on the communication equipment in Neck 1 C-Case. Of the 24 test cases 1 failed, 1 Pending and 1 N/A. The remaining 22 test cases passed.

[redacted]

[redacted]

3.2.9 L2 Plandome C Case Site Installation Test Report

Comms Line 2 Plandome CIL Site Installation Test Report 4009297[22][18][20] was generated to cover Plandome C-Case on Line 2. The report is on the communication equipment in Plandome C-Case. Of the 24 test cases 1 failed, 2 Pending and 1 N/A. The remaining 20 test cases passed.

[redacted]

[redacted]

3.2.10 L2 Port Washington C Case Site Installation Test Report

Comms Line 2 Port Washington CIL Site Installation Test Report 4009298[23][18][20] was generated to cover Port Washington C-Case on Line 2. The report is on the communication equipment in Port Washington C-Case. Of the 24 test cases 3 failed, 2 Pending and 1 N/A. The remaining 18 test cases passed.

[redacted]



3.2.11 L1 Bablyon C Case Site Test Installation Report

Comms Line 1 Babylon CIL Site Installation Test Report 4009300[24][18][20] was generated to cover Babylon C-Case on Line 1. The report is on the communication equipment in Babylon C-Case. Of the 24 test cases 3 failed. The remaining 21 test cases passed.

Rev_B Test Case was reviewed by Safety.

Table 21 4009300 Babylon SIT NCR / Variances



3.2.12 L1 Babylon 2 C Case Site Installation Test report

Comms Line 1 Babylon 2 CIL Site Installation Test Report 4009301[25] as generated to cover Babylon 2 C-Case on Line 1. The report is on the communication equipment in Babylon 2 C-Case. Of the 24 test cases 3 failed, 1 NA and 1 Pending. The remaining 19 test cases passed.

Table 22 4009301 Babylon 2 SIT NCR / Variances

NCR ID	Status	Safety	Summary	Justification



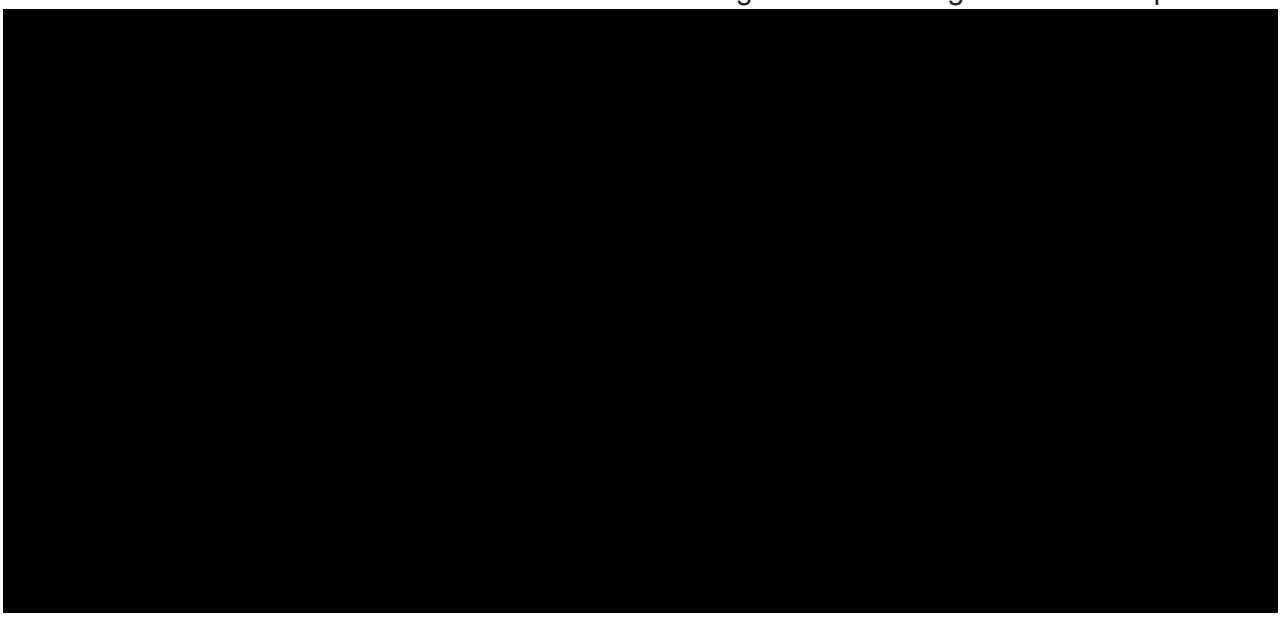
3.2.13 L1 Babylon Yard C-Case Site Installation Test Report

Comms Line 1 Babylon Yard CIL Site Installation Test Report 4009302[26] as generated to cover Babylon Yard C-Case on Line 1. The report is on the communication equipment in Babylon Yard C-Case. Of the 24 test cases 1 failed, 2 NA and 1 Pending. The remaining 20 test cases passed.



3.2.14 L1 Bayshore C-Case Site Installation Test Report

Comms Line 1 Bayshore CIL Site Installation Test Report 4009303[27] as generated to cover Bayshore C-Case on Line 1. The report is on the communication equipment in Bayshore C-Case. Of the 24 test cases 1 failed and 1 Pending. The remaining 22 test cases passed.



3.2.15 L1 Great River C-Case Site Installation Test Report

Comms Line 1 Great River CIL Site Installation Test Report 4009304[28] as generated to cover Great River C-Case on Line 1. The report is on the communication equipment in Great River C-Case. Of the 24 test cases 1 Pending. The remaining 23 test cases passed



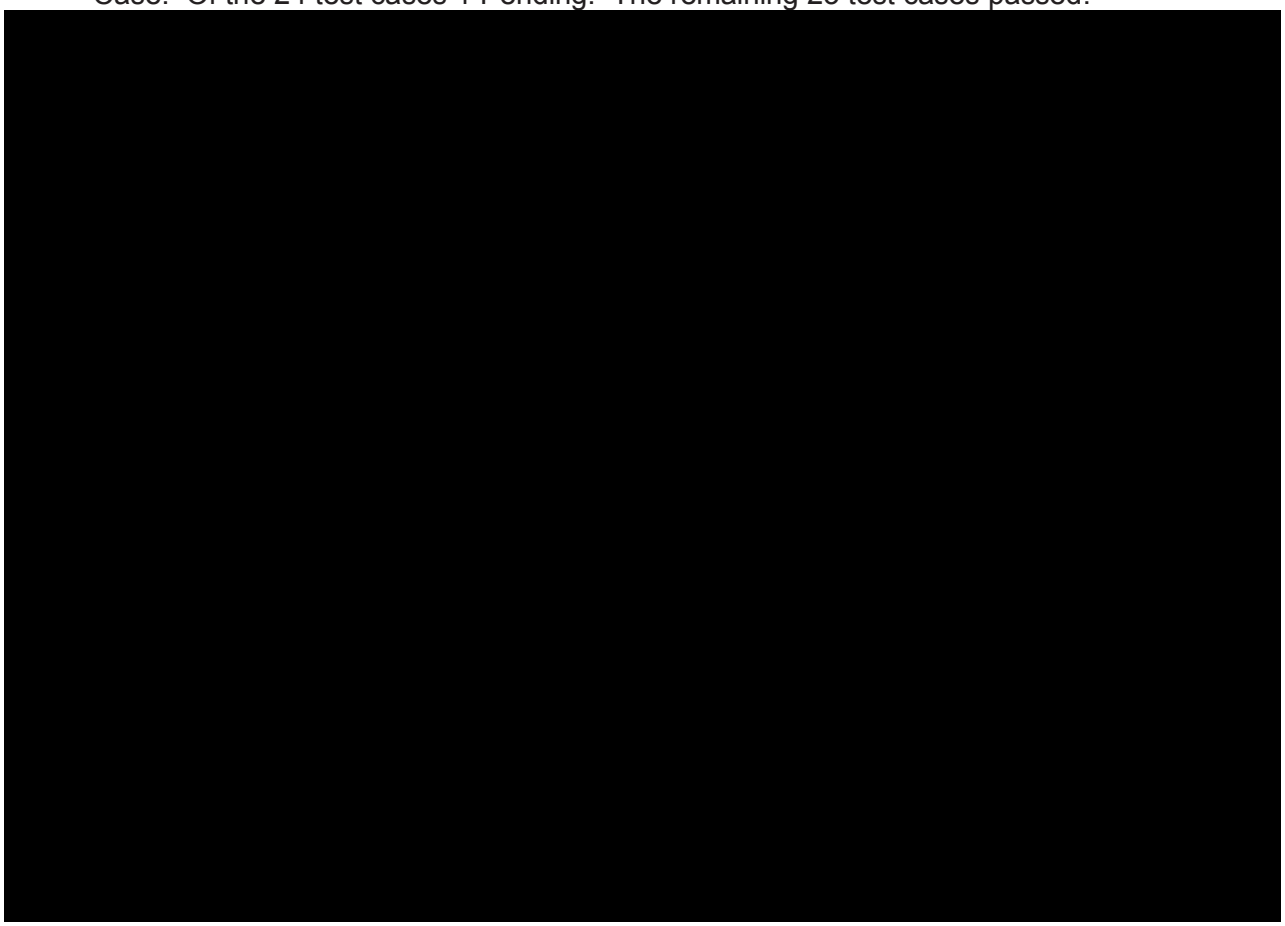
3.2.16 L1 Sayville C-Case Site Installation Test Report

Comms Line 1 Sayville CIL Site Installation Test Report 4009305[29]as generated to cover Sayville C-Case on Line 1. The report is on the communication equipment in Sayville C-Case. Of the 24 test cases 1 is marked fail and 1 Pending. The remaining 22 test cases passed.



3.2.17 L1 Patchogue C-Case Site Installation Test Report

Comms Line 1 Patchogue CIL Site Installation Test Report 4009306[30] as generated to cover Patchogue C-Case on Line 1. The report is on the communication equipment in Patchogue C-Case. Of the 24 test cases 1 Pending. The remaining 23 test cases passed.



4 Safety Certification Process

4.1 SRTM

Safety has completed the linking of the hazards to the subsystem requirements that define the mitigations that are relevant for communication functionality. Safety has reviewed that the factory testing in the rules based testing confirms that these requirements have been tested by the test cases defined in the test procedures.

All Comms Functional Safety Requirements are linked to the Comms SSLR or linked to appropriate System Safety Requirements.

The SRTM [39] has been released showing the analysis of the test case links between the Comms Safety Requirements and the requirements to be verified by testing. Safety Analysis indicates that linking must be completed. [redacted]

4.2 [redacted]

[redacted]

4.3 Remaining Open Variances

There are no Open safety critical variances related to the communication subsystem. The list of all open variances at the time of this report is included in Section 7.

5 Conclusion

All the testing has been completed for this release that is applicable per the limitations in the system integration. The lack of alternative radio communication was planned and the operation of the alternative radios is prevented by SRAC. The Open NCR's do require that a configuration management audit of the communication equipment be performed and reported prior to the start of revenue service testing. Once the configuration management audit is completed Revenue Service can begin with the identified releases.

The analysis of RGS and WCC is left to the Office Safety Report where those subsystem are integrated and tested.

6 Validation Conditions

[redacted]

7 Attachment A – Open Variance List

3037454_Rev__Attachment_A.pdf

8 Attachment B – Open Safety Critical NCR's

3037454_Rev__Attachment_B.pdf

9 Attachment C Phase 2 Release 1.6 FAT Test Report

3037454_Rev__Attachment_C.pdf

Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

RWPS Final Safety Report
CDRL 2-136-26

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Aaron Graham Safety Engineer	Aaron Graham	Aaron Graham 2019.06.05 14:43:33 -04'00'
Verified:	Jason Weighley Safety Engineer	Jason W Weighley	Jason W Weighley 2019.06.05 18:12:11 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.06.06 09:38:47 -04'00'
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group	Phil Magloire	Phil Magloire 2019.06.06 08:07:45 -04'00'
BT/SRA Review:	N/A Title		
BT/SRA Review:	N/A Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3037460

Effective Date:	Revision:	Language:
2019.07.05	_A	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2019-03-07	First Release
_A	2019-06-05	Updated for RWPS Baseline 2.4.1 Release

Table of Contents

Section	Subject	Page
1	**Executive Summary**	5
2	**Introduction**	5
2.1	**Compliance Matrix**	7
2.2	**Reference Documents**	10
2.3	**Glossary**	12
3	**Summary of Safety Analysis and Evidences**	12
3.1	**RWPS FAT Tests**	13
3.1.1	RWPS Baseline 2.1.0 FAT Test Results	13
3.1.1.1	Verified NCRs/Variances	14
3.1.1.2	New NCRs/Variances	15
3.1.2	RWPS Baseline 2.2.0 FAT Test Results	15
3.1.2.1	Verified NCRs/Variances	16
3.1.2.2	New NCRs/Variances	16
3.1.3	RWPS Baseline 2.3.0 FAT Test Results	16
3.1.3.1	Verified NCRs/Variances	17
3.1.3.2	New NCRs/Variances	17
3.1.4	RWPS Baseline 2.4.1 FAT Test Results	19
3.1.4.1	Verified NCRs/Variances	19
3.1.4.2	New NCRs/Variances	20
3.2	**RWPS Site installation Tests**	21
3.2.1	RWPS Baseline 2.1.0 Site Installation Test Report	21
3.2.1.1	Variance/NCR Summary for RWPS Baseline 2.1.0 Site Installation Test Report	21
3.2.1	RWPS Baseline 2.2.0 Site installation Test Report	22
3.2.2	RWPS Baseline 2.3.0 Site installation Test Report	22
3.2.3	RWPS Baseline 2.4.1 Site installation Test Report	22
3.3	**System Integration Testing**	22
3.3.1	SUP System Baseline 3.2 (RWPS Baseline 2.2.0)	22
3.3.1.1	FT2090 Establishing and Removing TSR from RWPS	22
3.3.1.2	FT 2091 Primary/Secondary RWIC transfers	23
3.3.2	SUP System Baseline 3.5 (RWPS Baseline 2.4.1)	24
3.3.2.1	FT2090 Establishing and Removing TSR from RWPS	25
3.3.2.1	FT 2091 Primary / Secondary RWIC Transfers	26
4	**Safety Certification Process**	27
4.1	**SRTM**	27
4.2	**Remaining Open NCR's**	27
4.3	**Remaining Open Variances**	29
4.3.1	Analysis of Open Variances	30

5 Conclusion. 31

6 Validation Conditions 31

List of Figures

Figure 1: RWPS to Office interfaces 6

List of Tables

Table 1: Compliance Matrix 7
Table 2: Reference Documents 10
Table 3: Terms Specific to this Document 12
Table 4: Acronyms Specific to this Document 12
Table 5: Test Tools for RWPS Baseline 2.1.0 13
Table 6: Verified NCR/Variance for RWPS Baseline 2.1.0 FAT Results 14
Table 7: New NCR/Variance for RWPS Baseline 2.1.0 FAT Results 15
Table 8: Test Tools for RWPS Baseline 2.2.0 15
Table 9: New NCR/Variance for RWPS Baseline 2.2.0 FAT Results 16
Table 10: Test Tools for RWPS Baseline 2.3.0 16
Table 11: Verified NCRs/Variances for RWPS 2.3.0 FAT Results 17
Table 12: New NCRs/Variances for RWPS 2.3.0 FAT Results 18
Table 13: Test Tools for RWPS Baseline 2.4.1 19
Table 14: Verified NCRs/Variances for RWPS 2.4.1 FAT Results 19
Table 14: New NCRs/Variances for RWPS 2.4.1 FAT Results 20
Table 13: Safety Related NCRs 28
Table 14: Safety Related Variances 30

1 Executive Summary

The RWPS Final Safety Report documents the closure of all hazards assigned to the RWPS subsystem and evidence of closure of all assigned safety requirements to the RWPS subsystem. Since the SI has designated the RWPS as a non-safety, the report does not detail the calculations of the MTTHE rates for the RWPS subsystem. The overall System FTA will generate rates that include the RWPS activities to show the system is protected without a specific safety target being achieved by the software/hardware of the RWPS.

This version of the report is focused on the requirements and hazards of the full ACSES functionality of the contract. The scope of this version of the RWPS Safety Report is only for RSD. The system documentation will determine the geographic area of operation.

2 Introduction

The Roadway Worker Protection System (RWPS) is a significant subsystem of the ACSES II system. The RWPS subsystem is comprised of the following components: EIC, RWPS Server, ADDC, SEC, NMS, and DMS. Its functions include

i. Allowing EIC to request TSR's for work zone protection.
ii. Checking input integrity of work zone protection TSRs.
iii. Maintaining copies of in progress work zone TSRs.
iv. Handling assignments of EIC's to work zone TSRs.

For more information on the messaging protocols used for all data exchanged between the RWPS and the User Interface Server (UIS), Data Maintenance Server(DMS), Network Management Server(NMS) and the Active Directory Domain Controller(ADDC) for the LIRR PTC Project, please refer to the RWPS Interface Control Document (ICD) [15].

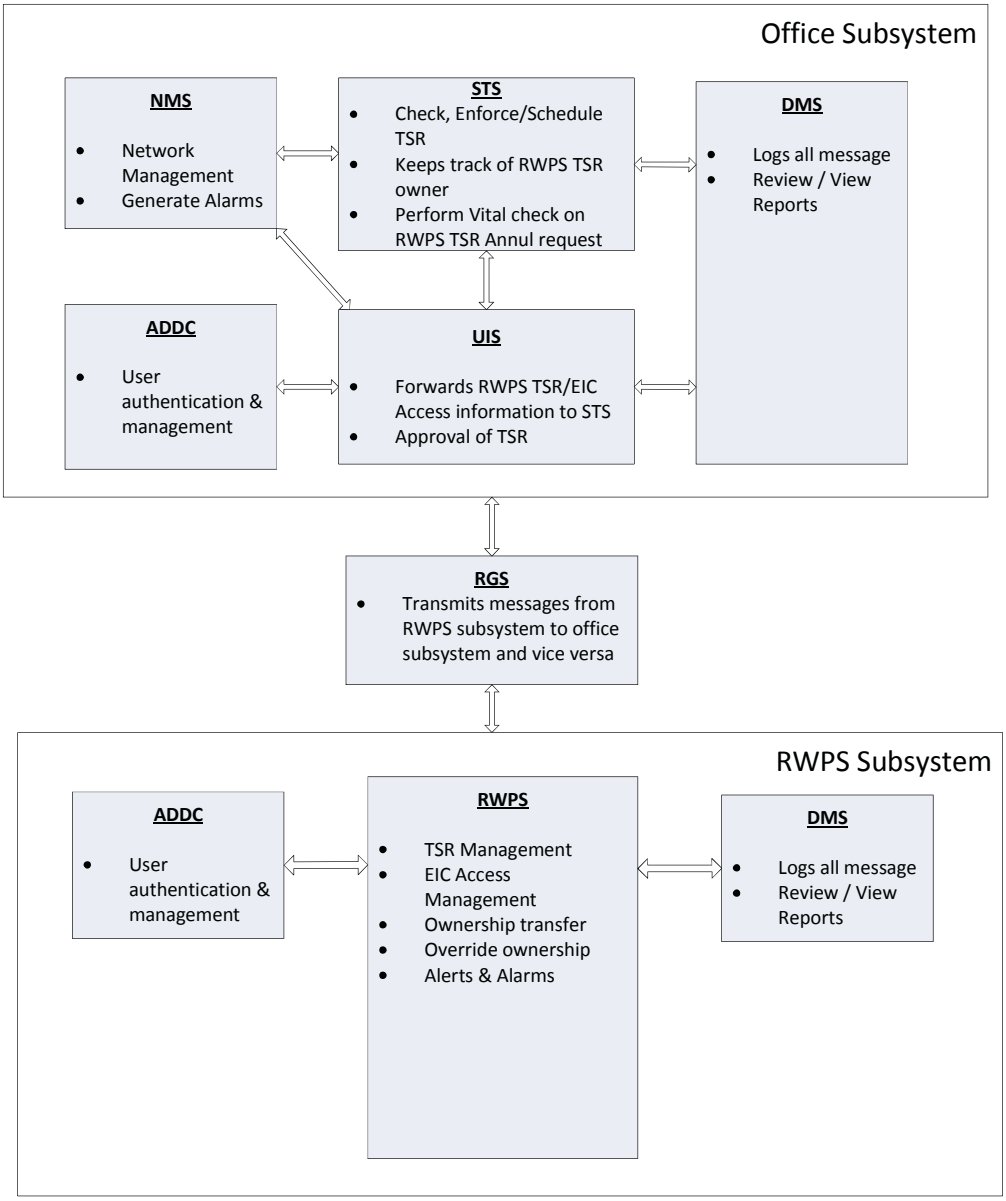


Figure 1: RWPS to Office interfaces

The above diagram explains the component specific features w.r.t RWPS functionalities and interaction with other components.

RWPS Subsystem

- RWPS Server: The RWPS server is responsible for TSR management, EIC Access assignment, alerts & Alarms and providing system admin functionalities.
- ADDC: The RWPS ADDC is responsible for user authentication and management. RWPS server communicates with RWPS ADDC to validate users.

- DMS: Redundant RWPS Data and Maintenance System (RWPS DMS) servers for logging data and managing the data logs for all RWPS subsystems, including messages from the EIC to the RWPS and feedback from the ACSES II Office system to EIC terminals

Office Subsystem

- UIS: The UIS is responsible for forwarding TSR/EIC access messages to STS. UIS Approver has the capability to approve RWPS TSR's, once TSR has been checked by STS.
- STS: The STS will check/enforce the RWPS TSR's. Also, STS will do a vital check on Annul TSR request by storing primary owner information.
- DMS: The office DMS is responsible for logging data and managing the data logs
- NMS: The office NMS is responsible for monitoring all networked Office and RWPS devices including office and RWPS subsystem servers.
    - Monitoring all networked Office and RWPS devices is through ping and SNMP polls. Office NMS will directly communicate to the devices for the monitoring
    - Monitoring Office server applications is through ACSES heartbeat messages. NMS will log the data to Office DMS
    - Monitoring RWPS server applications is through ACSES heartbeat messages and these messages are routed through RGS. NMS will log the data to Office DMS. Since the heartbeat messages should go through RGS from RWPS subsystem to Office subsystem, the delay in heartbeat is slightly higher (i.e. 1 or 2secs instead of 500ms). The heartbeat delay is configurable and by default the delay is 1sec.
    - NMS will write all the data to Office SQL server

The RWPS server communicates with the UIS server through the RGS. The detailed information about the interface description is presented in the RWPS Subsystem Description Document [6].

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part I	12.10.12.A	Final Safety Report	Final Safety Report shall provide a summary of the results on the overall safety analysis, safety verification, and system safety demonstration	All

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part I	12.10.12.B		Final Safety Report shall contain evidence of safety analysis	3
Vol 2 Part I	12.10.12.C	MTTHE	Document the calculation and methodology to show the MTTHE requirements in 9.1 have been achieved	See System FTA
Vol 2 Part I	12.10.12.D	Risk Reduction Actions	Address all risk reduction actions taken during design, test, operation and maintenance to mitigate faults caused by Operating Scenarios, Failures, Latent Design Errors, Installation errors, Human Reaction, Post implementation changes to SW or HW, or Interoperability and compatibility issues.	4.1
Vol 2 Part I	12.10.12.E	Information in Report	Describes the Safety Certification process and issues encountered during certification. Describes certification status Describes remaining restrictions / open issues and actions / work arounds to ensure acceptable level of safety is maintained.	4

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
			Provides a schedule for eliminating restrictions / workarounds. As appropriate. Includes Certificate of Compliance	
Vol 2 Part 1	12.10.12.F	Resolution of all Hazards	Report shall contain evidence of the resolution of all hazards. Evidence of resolution shall consist of satisfactory closure of the items as listed in the Project Hazard Log and achievement of the items listed in the Certified Item List	4.1
	12.10.12.G	Approved by Engineer	Report format will be approved by the Engineer and submitted in draft form at FDR. Report will stay draft until final system certification is achieved.	4

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.12.H	Approval of Final Safety Report	Report is to be submitted to SSCB prior to Completion of Pilot Phase commissioning and testing. Once approved by SSCB then submitted to the FRA and revised to address comments with a disposition per FRA comment. The report will be revised when characteristics of any territory, TP interface or the TP is modified in a way that impacts the safety of the system.	4

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624
[2]	LIRR Project Hazard Log (CDRL 2-126-20)	3035819
[3]	Certifiable Item List (CDRL 2-125-20)	3035818
[4]	RWPS System Safety Concept Document (CDRL 2-124-06)	3036417
[5]	RWPS Product Safety Plan (CDRL 2-123-06)	3036415
[6]	RWPS Subsystem Design Description (CDRL 2-201)	3035851
[7]	RWPS Preliminary Hazard Analysis (CDRL 2-127-06)	3036416

Reference Number	Document Name	Identification Number
[8]	RWPS Subsystem Hazard Analysis (CDRL 2-128-06)	3037401
[9]	RWPS Operating Hazard Analysis (CDRL 2-130-06)	3037424
[10]	RWPS Interface Hazard Analysis (CDRL 2-131-06)	3037436
[11]	PVI for RWPS Subsystem - 2.4.1	3151297 Rev _F
[12]	PVI for RWPS Application	3052243 Rev _E
[13]	PVI for RWPS Data & Maintenance System (DMS)	3151122 Rev_C
[14]	PVI for RWPS ADDC	3151302 Rev_C
[15]	RWPS Interface Control Document (CDRL 2-225)	3035874
[16]	LIRR SRAC	3045431
[17]	RWPS Site Installation Test Procedure	3152543
[18]	RWPS Site installation Test Report (CDRL 2-075-202)	4009500 Rev__ 4009500 Rev_A
[19]	RWPS FAT Test Procedure	3151889
[20]	RWPS Baseline 2.1.0 FAT Test Report	4009341 Rev_B
[21]	RWPS Baseline 2.2.0 FAT Test Report	4009341 Rev_C
[22]	RWPS Baseline 2.3.0 FAT Test Report	4009341 Rev_D
[23]	RWPS Baseline 2.4.1 FAT Test Report	4009341 Rev_E
[24]	RWPS SRTM	3153124
[25]	SUP Baseline 3.2 Integrated System Test Report (CDRL 2-090-216)	4009572
[26]	System Database Safety Verification Report (CDRL 2-133-20)	3035832
[27]	SUP Baseline 3.5 Integrated System Test Report (CDRL 2-090-228)	4010033

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in Table 3 and Table 4 respectively.

Table 3: Terms Specific to this Document

Term	Definition
N/A	

Table 4: Acronyms Specific to this Document

Acronym	Definition
ADDC	Active Directory Domain Controller
DMS	Data & Maintenance System
EMC	Electromagnetic Compatibility
FAT	Factory Acceptance Test
IHA	Interface Hazard Analysis
MAS	Maximum Authorized Speed
OHA	Operational Hazard Analysis
RTC	Rational Team Concert
RWIC	Roadway Worker In Charge
SSHA	Subsystem Hazard Analysis

3 Summary of Safety Analysis and Evidences

Safety analysis of the RWPS was performed by analyzing the functions performed by the RWPS subsystem within the overall system. The analysis performed for the RWPS subsystem were the Preliminary Hazard Analysis, Subsystem Hazard Analysis, IHA, and OHA. If the status is noted as Approved, this indicates the Safety Working Group review has been completed and the document has been formally submitted to the Railroad.

Name of Document	CDRL Number	PDM Number and Revision	Status



Hazard Status:

The RWPS SSHA contained 68 hazards when this report was written. All of the hazards are mitigated by identified safety Requirements. Please refer to the SRTM section for closure status of the hazards. The SSHA updates to reflect this status will be updated in the next release of the CDRL.

3.1 RWPS FAT Tests

3.1.1 RWPS Baseline 2.1.0 FAT Test Results

As described in the RWPS Baseline 2.1.0 FAT Test Report [20], the RWPS 2.1.0 baseline is a regression of prior rounds of Pre-FAT and FAT testing. The Regression FAT execution was performed using RWPS Subsystem 2.1.0 Release.

As part of this round of RWPS 2.1.0 FAT, a total of 20 test cases were executed, 19 Passed and 1 Failed. 4 “New” Variance was opened, and 10 Variances were “Verified”.

Table 5: Test Tools for RWPS Baseline 2.1.0

Test Environment on RWPS
PTC - LIRR
Software Configuration/ Version Control
Pittsburgh FAT Lab

Description	PVI Version	S/W Version
RWPS	3052243 Rev _A	2.2.0
DMS	3151122 Rev_A	19.1.0/1.17
ADDC	3151302 Rev_B	3.0
SEC	N/A for this release	N/A for this release

3.1.1.1 Verified NCRs/Variances

The following Variances have been verified while performing Regression FAT (Witnessed by customer) for LIRR RWPS 2.1.0 Release.



3.1.1.2 New NCRs/Variances

The following new Variances have been found while performing Regression FAT (Witnessed by customer) for LIRR RWPS 2.1.0 Release.



3.1.2 RWPS Baseline 2.2.0 FAT Test Results

As described in the RWPS Baseline 2.2.0 FAT Test Report [21], the RWPS 2.2.0 baseline is a regression of prior rounds of Pre-FAT and FAT testing. The regression FAT execution was performed using RWPS Subsystem 2.2.0 release.

As part of this round of RWPS 2.2.0 regression FAT, a total of 6 test cases were executed, 6 Passed and 0 Failed. 1 “New” Variance was opened and 2 Variances were “Verified”.

Table 8: Test Tools for RWPS Baseline 2.2.0

Test Environment on RWPS		
PTC - LIRR		
Software Configuration/ Version Control		
Pittsburgh FAT Lab		
Description	**PVI Version**	**S/W Version**
RWPS	3052243 Rev _B	2.2.1
DMS	3151122 Rev_A	19.1.0/1.17
ADDC	3151302 Rev_B	3.0
SEC	N/A for this release	N/A for this release

3.1.2.1 Verified NCRs/Variances



3.1.2.2 New NCRs/Variances

The following new NCRs/Variances have been found while performing FAT (witnessed by customer) for LIRR RWPS 2.2.0 Release.



3.1.3 RWPS Baseline 2.3.0 FAT Test Results

As described in the RWPS Baseline 2.3.0 FAT Test Report [22], the RWPS 2.3.0 baseline is a regression of prior rounds of FAT testing. The Regression FAT execution was performed using RWPS Subsystem 2.3.0 Release.

As part of this round of RWPS 2.3.0 Regression, out of the Total 35 Test Cases; 28 Test Cases were executed, 17 Passed and 11 Failed. 7 Test Cases were “Deferred” because of existing PVI Limitations. 13 “New” Variances were opened, and 10 Variances were “Verified”. 1 “New” NCR was also opened during this regression testing.

Table 10: Test Tools for RWPS Baseline 2.3.0

Test Environment on RWPS		
PTC - LIRR		
Software Configuration/ Version Control		
Pittsburgh FAT Lab		
Description	**PVI Version**	**S/W Version**

RWPS	3052243 Rev _C	2.9.0
DMS	3151122 Rev_B	24.0.0/1.17.2
ADDC	3151302 Rev_B	3.0
SEC	N/A for this release	N/A for this release

3.1.3.1 Verified NCRs/Variances



3.1.3.2 New NCRs/Variances

The following new NCRs/Variances have been found while performing Regression FAT (Witnessed by customer) for LIRR RWPS 2.3.0 Release.

3.1.4 RWPS Baseline 2.4.1 FAT Test Results

As described in the RWPS Baseline 2.4.1 FAT Test Report [23], the RWPS 2.4.1 baseline is a regression of prior rounds of FAT testing. The Regression FAT execution was performed using RWPS Subsystem 2.4.1 Release.

As part of this round of RWPS 2.4.1 Regression, out of the Total 16 Test Cases; 15 Test Cases were executed, 13 Passed and 2 Failed. 1 Test Cases was “Deferred” because of existing Lab Limitations. 5 “New” Variances were opened, and 14 Variances were “Verified”. 3 “New” NCR were also opened during this regression testing.

Table 13: Test Tools for RWPS Baseline 2.4.1

Test Environment on RWPS		
PTC - LIRR		
Software Configuration/ Version Control		
Pittsburgh FAT Lab		
Description	**PVI Version**	**S/W Version**
RWPS (Application)	3052243 Rev _E	3.6.1
DMS	3151122 Rev_C	28.1.0/1.17.2
ADDC	3151302 Rev_C	5.0
SEC	N/A for this release	N/A for this release

3.1.4.1 Verified NCRs/Variances





3.1.4.2 New NCRs/Variances



[redacted]

3.2 RWPS Site installation Tests

3.2.1 RWPS Baseline 2.1.0 Site Installation Test Report

As described in the RWPS Baseline 2.1.0 Site installation Test Report [18], the RWPS application was installed on Workstation and iphone/ipad devices. Android devices were not included in this SIT, as a limitation of the android application not being available, See Validation Condition ~~VC_RWPS_01~~.

3.2.1.1 Variance/NCR Summary for RWPS Baseline 2.1.0 Site Installation Test Report

[redacted]

[redacted]

3.2.1 RWPS Baseline 2.2.0 Site installation Test Report

Site Installation tests for RWPS Baseline 2.2.0 have not been run. Please see Validation Conditions Section 6.

3.2.2 RWPS Baseline 2.3.0 Site installation Test Report

Site Installation tests for RWPS Baseline 2.3.0 have not been run. Please see Validation Conditions Section 6.

3.2.3 RWPS Baseline 2.4.1 Site installation Test Report

Site Installation tests for RWPS Baseline 2.4.1 has been installed and run with iphone/ipad and android devices and completed with no new Variances [18]. The android device limitation can be removed.

3.3 System Integration Testing

3.3.1 SUP System Baseline 3.2 (RWPS Baseline 2.2.0)

All test cases associated with RWPS passed for System Integrated SUP Tests, for RWPS Baseline 2.2.0. Results can be seen below as shown in the SUP System Integration Testing for System Baseline 3.2 [25].

3.3.1.1 FT2090 Establishing and Removing TSR from RWPS

	Step #	Offline analysis Pass / Fail	Event number	On Site Sign off evidence file name
Pre-Conditions Verification	-	-		20181012_7629_Pre-Conditions.pdf
Procedure Step	**1**	PASS	n/a	20181012_FT2090.pdf
	2	PASS	n/a	
	3	PASS	n/a	

	4	PASS	n/a	
	5	PASS	n/a	
	6	PASS	n/a	
	7	PASS	n/a	
	8	PASS	n/a	
	9	PASS	n/a	
	10	PASS	n/a	
	11	PASS	n/a	
Conclusion / Comments	N/A			

3.3.1.2 FT 2091 Primary/Secondary RWIC transfers

	Step #	**Offline analysis Pass / Fail**	**Event number**	**On Site Sign off evidence file name**
Pre-Conditions Verification	-	-		20181012_7629_Pre-Conditions.pdf
Procedure Step	**1**	PASS	n/a	20181012_FT2091.pdf
	2	PASS	n/a	

	3	PASS	n/a	
	4	PASS	n/a	
	5	PASS	n/a	
	6	PASS	n/a	
	7	PASS	n/a	
	8	PASS	n/a	
	9	PASS	n/a	
	10	PASS	n/a	
	11	PASS	n/a	
Conclusion / Comments	N/A			

3.3.2 SUP System Baseline 3.5 (RWPS Baseline 2.4.1)

All test cases associated with RWPS passed after retest due to not properly following procedure for System Integrated SUP Tests, for RWPS Baseline 2.4.1. Results can be seen below as shown in the SUP System Integration Testing for System Baseline 3.5 [27].

3.3.2.1 FT2090 Establishing and Removing TSR from RWPS

	Step #	Offline analysis Pass / Fail	Event number ACSES_7213_052919.dat ACSES_7383_052919.dat	On Site Sign off evidence file name
Pre-Conditions Verification	-	-		20190529_Pre-Condition.pdf
Procedure Step	**1**	PASS	# 16509 (7383)	20190529_FT2090.pdf
	2	PASS	N/A	
	3	PASS	N/A	
	4	PASS	# 16522 (7383)	
	5	PASS	N/A	
	6	PASS	N/A	
	7	PASS	N/A	
	8	PASS	N/A	
	9	PASS	# 4763 (7213)	
	10	PASS	N/A	
	11	PASS with comment	# 4909 (7213)	
Conclusion / Comments	Step 11: The new TSR list is received and displayed in the log at 22:14:15. The TSR input is correctly removed.			

3.3.2.1 FT 2091 Primary / Secondary RWIC Transfers

	Step #	Offline analysis Pass / Fail	Event number ACSES_7213_052919.dat	On Site Sign off evidence file name
Pre-Conditions Verification	-	-		20190529_Pre-Condition.pdf
Procedure Step	**1**	PASS	# 5684	20190529_FT2091.pdf
	2	PASS	N/A	
	3	PASS	N/A	
	4	PASS	# 5799	
	5	PASS with comment	N/A	
	6	PASS	N/A	
	7	PASS with comment	# 6599	
	8	PASS	N/A	
	9	PASS	# 7175	
	10	PASS with comment	N/A	
	11	PASS with comment	# 7486	
Conclusion / Comments	Step 7 and 11: The new TSR list is received and displayed in the log at 22:38:15 and 22:50:45. The TSR input is correctly removed. Step 5 and 10 : See section 6.2 comment #1 and section 6.1 comment #9. Procedure to be redline.			

4 Safety Certification Process

4.1 SRTM

Safety has completed the linking of the hazards to the subsystem requirements that define the mitigations that are relevant for RWPS functionality. Safety has reviewed that the factory testing in the rules based testing confirms that these requirements have been tested by the test cases defined in the test procedures.

There are currently two RWPS Functional Safety Requirements that are not linked to the RWPS SSLR, RWPS_SR-35 and RWPS_SR-41. The following mitigations are temporary until the design limitations for RWPS_SR-35 and RWPS_SR-41 are addressed. To justify the absence of RWPS_SR-35 being linked to the RWPS SSLR, the SRACs SRC_L61 and SRC_L53 have been put in place until the requirement is implemented:

SRC_L61: “EIC Personnel shall check with Dispatcher to confirm TSR is in place before entering railway”.

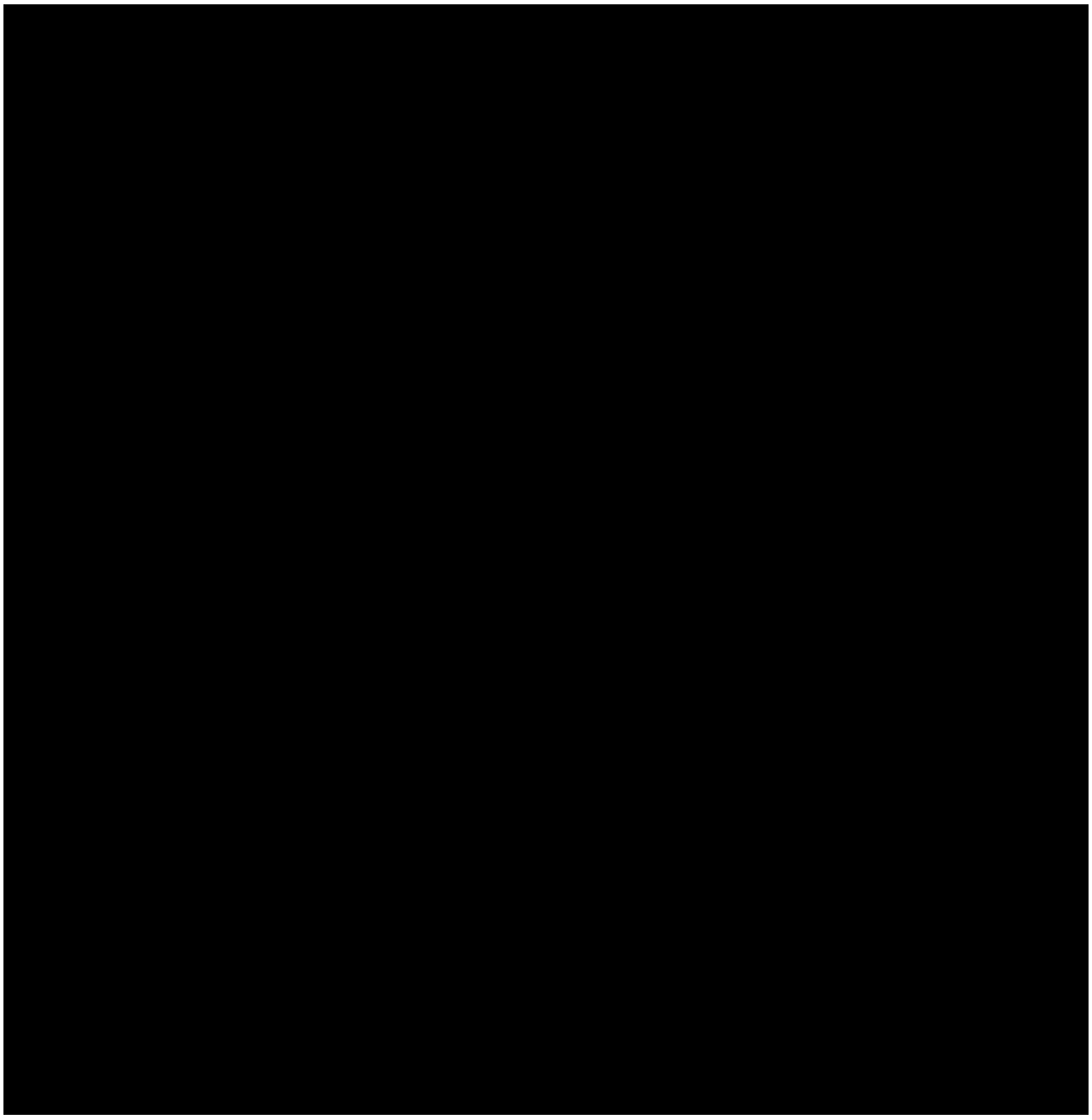
SRC_L53: “Primary EIC / Superuser shall confirm that all workers and work trains are out of work zone prior to removing TSR”.

NCR 262534 has been put in place for RWPS_SR-41. As well, SRAC SRC_L105 (From the LIRR SRAC Document [16]) is already in place to restrict BCC/PCC operation.

The SRTM [24] has been released showing the analysis of the test case links between the RWPS Safety Requirements and the requirements to be verified by testing. Safety Analysis indicates that linking must be completed. Two SSLR Safety Requirements are found to be testable but have no test links; these requirements are RWPS_SSLR-565 and RWPS_SSLR-658. Two requirements are not linked in DOORS SLR Baseline 3.0 and will be linked in the next release of the DOORS Baseline; these requirements are RWPS_SSLR-404 and RWPS_SSLR-658. There are currently 8 requirements that do not have a Verification Method; these requirements are RWPS_SSLR-433, RWPS_SSLR-157, RWPS_SSLR-502, RWPS_SSLR-581, RWPS_SSLR-579, RWPS_SSLR-569, RWPS_SSLR-583, and RWPS_SSLR-562. One Requirement is marked as safety “Yes” that safety believes should be safety “No”; this requirement is RWPS_SSLR-250. NCR 255037 tracks this issue until closure. One requirement is currently shown as safety “No” that safety believes should be safety “Yes”; this requirement is RWPS_SSLR-397. NCR 255037 also tracks this issue until closure. All remaining requirements are tested.

4.2 Remaining Open NCR’s

Listed below in Table 16 are all open Safety-Related NCR’s as of RWPS Subsystem Baseline 2.4.1.



4.3 Remaining Open Variances

Listed below in Table 17 are all open Safety-Related Variances as of RWPS Subsystem Baseline 2.4.1. All other Variances, such as those listed in Section 3 (Testing), that are not shown below in Table 17 do not impact safety.

[redacted]

4.3.1 Analysis of Open Variances

All open Variances are tracked in RTM CCM until closure. A list of Safety Critical Variances that are not closed are located above in Table 17. Of the Variances listed that are applicable, two are currently rated Category 2:

[redacted]

[redacted]

Mitigations for the Category 2 Variances are listed in Table 17.

5 Conclusion.

[redacted]

The Safety Engineer finds that sufficient evidence exists to allow RWPS Baseline 2.4.1 operation in Revenue Service Demonstration.

6 Validation Conditions

[redacted]

Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

System Database Safety Verification Report

CDRL 2-133-20

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Jason Weighley Safety Engineer	Jason W Weighley	2019.04.12 13:12:57 -04'00'
Verified:	Francis Tabi Safety Engineer	T. Tabi	2019.04.12 14:55:52 -04'00'
Approved:	Anthony DeFrancisco Project Director	Anthony DeFrancisco	2019.04.12 14:50:35 -04'00'
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group	Phil Magloire	2019.04.15 09:59:34 -04'00'
BT/SRA Review:	NA Title		
BT/SRA Review:	NA Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3035832

Effective Date:	Revision:	Language:
2019-04-12	_C	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2018-10-05	First Release
_A	2018-11-13	Updated for Baseline 3.2
_A1	2019-02-15	Updated for Baseline 3.4 – Draft for TRR
_B	2019-03-07	Updated for Baseline 3.4
_C	2019-04-12	Updated to Resolve RVW-0762 and comments from Verification Audit

Table of Contents

Section	Subject	Page
1	**Executive Summary**	6
2	**Introduction**	6
2.1	**Compliance Matrix**	6
2.2	**Reference Documents**	8
2.3	**Glossary**	10
3	**Database Safety Verification**	12
3.1	**Civil Database Verification**	12
3.1.1	Grade Verification	13
3.2	**Office Database Verification**	13
3.2.1	Data Correctness	13
3.2.2	Data Integrity	15
3.3	**Comms Database Verification**	15
3.4	**WIU Database Verification**	16
3.4.1	Data Correctness	16
3.5	**Transponder Database Verification and Validation**	16
3.5.1	Data Correctness	16
3.5.2	Data Integrity	17
3.6	**Database Safety Concepts Verification**	18
3.6.1	Office Database Safety Concepts Verification	18
3.6.1.1	ADDC	18
3.6.1.2	DMS	18
3.6.1.3	NMS	18
3.6.1.4	RGS	18
3.6.1.5	SDMF	18
3.6.1.5.1	SDMT	18
3.6.1.6	Security Server	18
3.6.1.7	STS	18
3.6.2	UIS Database Safety Concepts Verification	19
3.6.3	Transponder Database Safety Concepts Verification	19
3.6.4	Comms Database Safety Concepts Verification	20
3.6.5	RWPS Database Safety Concepts Verification	21
3.6.6	WIU Database Safety Concepts Verification	21
3.6.7	OBC	21
3.7	**Protection Methodology for Data Entry**	22
3.7.1	Transponder	22
3.7.1.1	Data Correctness	22
3.7.1.2	Data Integrity	23
3.7.2	WIU	23
3.7.3	Office	23
3.7.4	Comms	24

3.7.5 OBC 25

3.8 Protection Methodology for Data Storage 25
3.8.1 Transponder 25
3.8.2 Office 25
3.8.2.1 STS 25
3.8.2.2 UIS 25
3.8.2.3 All others (ADDC, NMS, SEC, RGS, WCC, and DMS) 26
3.8.3 WIU 26
3.8.4 RWPS 26
3.8.5 OBC 26
3.8.6 Communication 26

3.9 Protection Methodology for Data Usage 27
3.9.1 Office 27
3.9.1.1 ADDC 27
3.9.1.2 DMS 27
3.9.1.3 UIS 27
3.9.1.4 Security Server 27
3.9.1.5 SDMF 27
3.9.1.6 STS 27
3.9.2 WIU 27
3.9.3 Transponder 28
3.9.4 OBC 28
3.9.5 Communication Subsystem 28
3.9.6 RWPS 28

3.10 Data Verification Operation 28
3.10.1 Communications 28
3.10.2 Processing 29
3.10.2.1 SDMT (Office, RWPS, Transponder) 29
3.10.2.2 DT Tool 29
3.10.3 System Calculation 30

4 Testing and Controls 32

4.1 Testing 32

4.2 Controls 32
4.2.1 Staged Deployment 32
4.2.2 Application Updates 32
4.2.3 Database Updates 33

5 Conclusion 33

List of Figures

Figure 1 System Calculation 31

List of Tables

Table 1: Compliance Matrix 6
Table 2: Reference Documents 8
Table 3: Terms Specific to this Document 11
Table 4: Acronyms Specific to this Document 11
Table 5 Safety Evidence Cited from this Report 33
Table 6: NCRs from Verified Reports 37
Table 7: Variances from Verified Reports 39

1 Executive Summary

This document summarizes the safe delivery, protection and communication and availability of the data for the various subsystems to be used for operation in LIRR.

2 Introduction

This document describes the process and verification of the data for the application level of the ACSES II system. This document describes the process to verify the inputs of the data used by each subsystem. The integrity of the data for each subsystem is be defined through the data entry phase to the loading of the data into each subsystem. The configuration management and control of the data is be presented to ensure the data in each subsystem is compatible and correct. Finally, the planned system and subsystem test procedures to ensure the safety of the system with the final application data is presented and summarized.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part 1	12.10.9.A		Si shall submit a Database Safety Verification Report, on the handling of ACSES II databases to ensure their data integrity based on the database safety methods discussed in the System Safety Concept Document. Database Safety Verification report shall include input form subsystem suppliers, to include all verification methods employed by the subsystem suppliers	3.2 3.3 3.4 3.5 3.6

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.9.B		The verification shall discuss the methodology used for protection of the vital data during data entry, storage and use. The verification will also discuss operation including communications, processing, update and system calculations. The scope of protection will be quantified for use in the calculation of system fault probability, a component of the Mean Time To Hazardous Event (MTTHE)	3.7 3.8 3.9 3.10

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.9.C		The Database Safety Verification Report shall detail the methodology for ensuring that the databases are adequately controlled and tested to ensure that once a deployed in a multi-supplier environment the safety of the ACSES II System and ACSES II Subsystem is maintained. This shall include requirements for staged deployment as well as compatibility issues associated with updates to the database and application software where appropriate.	4.1 4.2

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624
[2]	Civil Data Verification Report Port Washington Branch (Pilot Line 2)	3050830
[3]	Civil Data Verification Report Montauk Line (Pilot Line 1)	3051385
[4]	Civil Data Verification & Validation Process	3051109
[5]	SDMF Test & Verification Plan	3035729
[6]	Onboard System Safety Concept Description CDRL 2-124-01	3036406

Reference Number	Document Name	Identification Number
[7]	LIRR – L2 Pilot Line SPT Database Verification Test Procedure Addendum 1 to CDRL 2-089-204	3052747
[8]	LIRR – L1 Pilot Line SPT Database Verification Test Procedure Addendum 2 to CDRL 2-089-204	3150849
[9]	LIRR SPT Database Verification Test Procedure CDRL 2-089-204	3052430
[10]	RWPS System Safety Concept Description CDRL 2-124-06	3036413
[11]	Office System Safety Concept Description CDRL 2-124-02	3036410
[12]	Communication System Safety Concept Description CDRL 2-124-03	3036421
[13]	WIU Subsystem Safety Concepts Document CDRL 2-124-04	3035817
[14]	LIRR - L1 Pilot Line Transponder FAT Test Report	4008795_Rev_G
[15]	LIRR - L2 Pilot Line Transponder FAT Test Report	4008751_Rev_D
[16]	LIRR Horizontal Alignment and Vertical Grade Data Verification Report	3052572_Rev_A
[17]	Montauk Transponder SIT Test Report	4009101_Rev_E
[18]	Port Washington Transponder SIT Test Report	4007924_Rev_E
[19]	Office Factory Test Report	4008709_Rev_K
[20]	Office Site Installation Test	4009178
[21]	SDMT Verification and Validation Report	4009864
[22]	Database Verification Report	3151611_Rev_B
[23]	SPT L1 Database Verification Test Report Addendum 2	4009314
[24]	SPT L2 Database Verification Test Report Addendum 1	4009316
[25]	SUP L1 Database Verification Test Report Addendum 2	4009467

Reference Number	Document Name	Identification Number
[26]	SUP L2 Database Verification Test Report Addendum 1	4009466
[27]	SUP Baseline 3.2 Pilot L1 Database Verification Test Report Addendum 2 to CDRL 2-090-214	4009570
[28]	SUP Baseline 3.2 Pilot L2 Database Verification Test Report Addendum 1 to CDRL 2-090-214	4009569
[29]	LIRR Map Office Specific Application Data Report	3151133_Rev_D
[30]	LIRR WIU Interlocking Configuration	3152795
[31]	LIRR PDS Report	3151549
[32]	WIU SVVR CDRL 2-12-24	3050366
[33]	WIU FAT Test Report Line 1	4009406
[34]	WIU FAT Test Report Line 2	4009407
[35]	WIU Site Acceptance Test Report Line 1	4009408
[36]	WIU Site Acceptance Test Report Line 2	4009409
[37]	RWPS Factory Test Report	4009341_Rev_C
[38]	Meeting Minutes from Office Block Review Oct 4 2018	
[39]	SUP Baseline 3.4 Pilot L1 Database Verification Test Report Addendum 2 to CDRL 2-090-214	4009778_Rev__
[40]	Comms SVVR	3036422
[41]	Port Washington Transponder Validation Report	3043407
[42]	Montauk Transponder Validation Report	3046231

Note: The PDS report is configuration controlled on Sharepoint at the following location:
https://sps.transportation.bombardier.com/sites/LIRRMNR/WABTEC/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2FLIRRMNR%2FWABTEC%2FShared%20Documents%2FBombardier_Wabtec%20Releases&FolderCTID=0x0120008692AF69B6EA0F41B3D9061879BC4D36&View={6F418254-EB2F-4969-B715-B6E4EBA81E8B}

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in Table 3 and Table 4 respectively.

Table 3: Terms Specific to this Document

Term	Definition
ARC GIS	Name of a GIS tool used in Civil database verification

Table 4: Acronyms Specific to this Document

Acronym	Definition
ADDC	Active Directory Domain Controller
CRC	Cyclic Redundancy Check
DMS	Data and Maintenance System
DS	Distant Signal
DT	Diagnostic Tool
GIS	Geographic Information System
GPS	Global Position System
HS	Home Signal
ICDD	Interface Control Design Description
LoMA	Limit of Movement Authority
MCM	Mobile Communication Manager
NMS	Network Management System
PDR	PTC Data Radio
PDS	Pre-Distant Signal
PTS	Positive Train Stop
PVI	Product Version Information
RCF	Radio Configuration File
RGS	Railroad Gateway Server
SCR	Software Change Request
SDMT	Software and Data Maintenance Tool
SEC	Security Server

Acronym	Definition
STS	Safety TSR Server
TSR	Temporary Speed Restriction
UCN	Universal Change Number
UIS	User Interface System
USB	Universal Serial Bus
VCD	Verified Civil Data
WIU	Wayside Interface Unit

3 Database Safety Verification

3.1 Civil Database Verification

To verify the civil database used to compile the application data for each ACSES subsystem the civil database developed by the Railroad was verified against a separate civil database generated by a GPS Camera system mounted to the trains. The Database Comparison tool is used to compare the two databases. This is done by assigning an identified number that matches in both the camera survey and GIS. IMAJING© assigns identified number as they process the data. Tolerances are entered in the Database Comparison tool when comparing the data. The tolerances entered is a difference in lat/long of over 7.2' and chainage greater than 15'ft.

Any delta's that fall out of tolerance are subject to a manual survey. When the manual survey is conducted, the data is entered into ARC GIS as well to compare to the GIS and Camera Survey Points. Another analysis is run to show the distance between the GIS, Manual Survey & Camera Survey.

Any GIS or Camera points that do not correspond to one another are also analyzed in ImajView® to see what the discrepancy is. In certain cases, the GIS may be missing data or new construction may supersede the data included in the GIS.

Any delta's that fall into the out of tolerance category are subject to a manual survey to confirm the finding of the discrepancy. When the manual survey is conducted, the data is entered into ARC GIS as well to compare to the GIS and Camera Survey Points. The findings of the manual survey is reflected in this report to show the distance between the GIS, Manual Survey & Camera Survey.

Any GIS or Camera points that do not correspond to one another (Unmatched 1 or Unmatched 2) are also analyzed in ImajView® to see what the discrepancy is. In certain cases, the GIS may be missing data or new construction may supersede the data included in the GIS. A manual survey may be necessary to find evidence of where the point actually is or reviewing the camera survey images in ImajView may provide conclusive evidence of where the point actually is.

The wayside elements that includes the office assets that are verified are

- Signals (SIG)
- Insulated Joints (IJ)
- Point of Switches (POS)

- Mileposts (MP)
- Bridges
- Platforms
- Grade Crossings

These are included in the data verification reports for Pilot Line L2 (Port Washington) [2] and Pilot Lines L1 (Montauk) [3].

Safety reviewed the above reports and audited the report findings by reviewing comparison tables attached to the report.

This section is only concerned with data correctness.

3.1.1 Grade Verification

A comparison of Track plans to survey data was completed by Systra. Two comparisons were performed one for the initial data and then a repeat for the regression analysis performed by Systra. BT then reviewed the regression alignment drawings to the track plans. Where necessary chainage on the regression alignment files was updated to match the track plan chainage. The alignments in the regression analysis were reviewed by Bombardier and any issues where corrected. A visual inspection was also performed by overlaying the final data into Google Earth to verify the alignment locations. This process has been defined by the Horizontal Alignment and Vertical Grade Data Verification Report [16]. The findings of this report are that other than several drafting errors the grade data in the track plan is sufficient to enter into SDMT.

This section is only concerned with data correctness.

Safety engineering has audited the findings of the Horizontal Alignment and Veridical Grade Data Verification Report. This audit consisted of checks of pilot line locations between Google Earth and the final comparison from the report above.

3.2 Office Database Verification

3.2.1 Data Correctness

The steps to verifying the data and design of the Office are detailed in the SDMF Test & Verification Plan [5]. Included in this verification is the verification of the TopoDB. The purpose of the TopoDB data verification is to ensure that the data provided in the input sources is complete. In TopoDB the various input sources are verified against each other. Office designs are based off of the civil data provided during population of data into the SDMT using the verified processed data. The office then utilizes the PDS radio coverage location data from the Comms designs in order to layout TSR Blocks, Shadow blocks, block track sections, and more. The PDS Coverage location is received through the PTS Report which is vitally generated by the SDMT. The initial PTS Report provides the civil locations of all ACSES signals within the system along with the following information:

- Railroad / Line Name
- Interlocking name
- Signal chainage
- PTS point chainage and distance
- PDS point chainage and distance
- Controlling grade
- LoMA Identifier (Yes/No)

With the above information, the Comms designs can begin. The PDS Coverage location designs must extend to at least the PDS point in the approach to both the UP and DOWN directions of an interlocking. Based on this, the designs can identify where there is actual radio coverage start and end points. These start and end points are used by the Office subsystem to align their TSR Blocks with the start and end BCP coverage points. The Office block design is manually modified from the comms design to adjust for LoMA and line boundaries. This along with designing of shadow blocks around line boundaries, allocation of block track sections and block zones which are all done within the SDMT.

The Database Verification Report [22] compares the data from the civil data verification reports agains the data entered into SDMT. Assets such as grade, switches, Mileposts, bridges, platforms and Grade Crossings is confirmed by this verification. This data confirms the correct location for physical assets is included into the final SDMT. For the office each transponder line SDMT is combined into an overall project file. Each Transponder Line SDMT is compared against its corresponding Civil Database verification report. The ICDD is then reviewed against the data generated from this verified SDMT database to make sure the WIU is aligned to the overall system data.

The STS Block zone design is compared to the PDS Coverage location design to ensure that the blocks align to the radio coverage of the system and the PTS Limits. The Office block design is manually modified from the comms design to adjust for LoMA and line boundaries, A meeting to review the office block design was held on Oct 4 2018 [38] after the Office Database Verification Report was found insufficient to cover this verification. The meeting found issues with the block overlap design for LIRR Line 2 – Port Washington Blocks 2, 4, 7 and 14. Pilot Line 1 Montauk block design was checked, and issues were found in block coverage between block 10 and 34. This gap in coverage is from 171217 to 171127, any TSR created in the gap area would not be accepted. For Line 1 overlap block issues were found in blocks 48. The issues with the overlap blocks could potentially keep TSR's from being sent to trains but should be mitigated by subsequent radio requests in adjoining blocks. (Overlap blocks are used for the final portion of the TSR List so additional requests in other blocks would ensure proper TSR communicated to the trains).

The independent verifier has reviewed theses records and found this evidence sufficient. The test records for the radio coverage and correct TSR blocks was used as verification evidence of correct block layout. The test records that document this are included in the SPT and SUP Database Verification Reports [23][24][25][26][27][28].

Verification of Office Design including; verification of the TSR blocks, block zones, etc. are designed in accordance with the system application rules. The Office Database verification report provides sufficient evidence of the Office design in accordance the system rules for the block designs.

Safety reviewed the LIRR Map Office Specific Application Data Report to ensure that each entry for the office data was properly entered and that all inputs were reviewed. Each change to the Map is done through an SCR. During this meeting the verification evidence for the change as well as justification for the change are presented. Safety reviews the evidence prior to the SCR review and if necessary, schedules additional review to ensure that all entries are correct and all errors are corrected. As per the above section it was noted in the SCR review that different overlaps were not correct. This covers OV1 reference from the SDMT Verification and Test Plan.

The SDMT Verification Report[21] ensures that the proper calculations are made by the independent calculations of the SDMT application and that the final data will be correct and accurate. This is to satisfy the OV2 verification identified in the SDMT Verification and Test Plan.

Safety does not review the network configuration files. These files are generated and reviewed by engineering and some verification is performed as indicated I the SDMT Verification and test plan, but safety does not review the verification of this data as it will not impact the safety of the system.

The RWPS uses the same data files as the UIS. This section covers the RWPS data correctness and integrity as well.

3.2.2 Data Integrity

Verification of Office binaries. The STS binary files are vitally export from the SDMT and are protected with a 64-bit CRC to ensure the data has not become corrupt. The XML script for UIS is compared to the STS Binary data through the Office Specific Application Data Report [29]. This report looks for consistency in the data exported to UIS and what is in the STS binary file. Comparisons are made between the UIS data and the STS database. This report also verifies the data matches rules contained in the report to align with STS and UIS designs. The report also indicates if the maximum TSR block count will potentially exceed the maximum TSRs for that block. Please note that RWPS uses the UIS files.

Verification of NMS IP configuration files. Configuration files of the NMS along with the IP allocation within the NMS have been peer reviewed. The review records are in configuration management. The test records for the radio coverage and correct TSR blocks was used as verification evidence of correct block layout. The test records that document this are included in the SPT and SUP Database Verification Reports [23][24][25][26][27][28].

3.3 Comms Database Verification

The steps to verifying the data and design of the Comms are detailed in the SDMF Test & Verification Plan [5]. The SDMT uses its data to generate a PTS Report. This report has the location of the signals, IJs, PTS point and chainage, PDS point and chainage. From this report a PDS Coverage location is coverage to the PDS point from the PTS points. The steps detailed in the SDMT Verification and Test Plan to verify the communication application data are as follows:

1. Verification of chaining from SDMT to Lat/Long conversion.
2. PDS Coverage location design verification; ensuring PDS Coverage is sufficient to meet needs of the system based on PTS information provided in PTS Report.
3. Verification of Lat/Long from comms design to chaining conversion for entry into SDMT.
4. IP address allocations and port assignments are verified for their uniqueness.

PDS Coverage location need to be verified of their frequency levels in the field after installations are complete.

The Database Verification Report [22] compares the data from the civil data verification reports against the data entered into SDMT. Assets such as grade, switches, IJs, Mileposts, bridges, platforms and Grade Crossings is confirmed by this verification. The changes from the civil data verification were not sufficient enough to warrant a review of the original comms design. Therefore, the PTS Report was not exported again after the initial version.

A meeting to review the office block design was held on Oct 4, 2018 [38] after the Office Database Verification Report was found insufficient to cover this verification. The meeting did check the radio communication PDS limits to the office block design. The test records for the radio coverage and correct TSR blocks was used as verification evidence of correct block layout. The test records that document this are included in the SPT and SUP Database Verification Reports [23][24][25][26][27][28]. This review by safety satisfies the intent of CV3 as referenced in the SDMT Verification and Test Plan. It should be noted that while the system must align to function properly small errors in RF coverage will not make the system unsafe as the vital subsystem have mitigations to enforce safe actions if no communication between the subsystems occurs.

3.4 WIU Database Verification

3.4.1 Data Correctness

The WIU SVVP provides the plan for the verification activities to be carried out on the project for each interlocking. The Verification evidence from this plan is reported in the WIU SVVR. The WIU Application data has been checked at certain stages in development including the design, FAT, and Field Testing phases. At each phase the vital configuration UCN of the configuration has been checked. The UCN is a unique number generated by the DT tool upon any change of any parameter within the vital configuration to track the unique configuration of each interlocking. This UCN must be entered into the WIU to enable the unit to run.

At the design phase, the design engineer generates the vital configuration based on the ICDD, Line Boundary Drawings, and IP address information. This configuration is then checked by an independent checker. The checker makes any comments and reviews with the developer until all comments are resolved. The final UCN for any changes are noted in the Checked copy of the design. The WIU SVVR references the F_EN_108 form for the engineering review.

The completed WIU design yields the full ATCS address, including the Signal ID and Encoder ID, switch ID and switch ATCS address which are filled into the ICDD tables and entered back into the SDMT for other subsystem designs.

The WIU FAT verifies the Application configuration data conforms to the information located in the BoP for the location under test. The test has been performed by an independent engineer according to procedures generated. The test results are recorded in CDRL 2-053 and noted in the WIU SVVR.

The WIU Site Acceptance test verifies the Application configuration data conforms to the area under test. The WIU Site acceptance Test reports have been documented in CDRL 2-057 and is reference by the WIU SVVR.

Details of the verification of the WIU data along with the inputs and outputs and actions taken by engineering to verify the transponder data are shown in the SDMF Verification & Test Plan.

3.5 Transponder Database Verification and Validation

3.5.1 Data Correctness

Details of the verification of the transponder data along with the inputs and outputs and actions taken by engineering to verify the transponder data are shown in the SDMF Verification & Test Plan [5]

Transponder designs and telegram generation are dependent on the SDMT. As such, the majority of the data is automated or structured in a way to assist in transponder layout designs. Transponder placement is automated within the SDMT; however, engineering manipulations are required post placement. This is to adhere to location specific designs including placing transponders at insulated joints for maintainability and optimization of transponder sets. For a full list of rules reference the System Application Rules (Transponder section) [1]

Transponder set locations can be determined once the VCD is available and entered in the SDMT. The population of transponder sets is automated, however still requires engineering to fine tune and optimize layouts. The detailed software telegrams however, cannot be completed until both the WIU and Comms designs are completed and appropriate information is filled out in the ICDD Tables and PTS Report. Initial designs are done by red-lining drawings to illustrate the proposed transponder locations and required package configurations.

The Database Verification Report [22] compares the data from the civil data verification reports against the data entered into SDMT. Assets such as grade, switches, IJs, Mileposts, bridges, platforms and Grade Crossings is confirmed by this verification report.

Verification of the Transponder design is enforced by rules programmed into the SDMT application. This tool verifies correct transponder placement according to the safe braking analysis for the worst grade and train type brake profile applicable for that area. The correct package selection is also determined by the tool according to rules verified by the tool application team. The package contents are also verified through factory and field testing to ensure correct package placement and proper brake enforcement. These rules will be verified through a SDMT SRTM document once the rules are fully entered into DOORS.

Safety has reviewed the errors and notices generated by the SDMT application to ensure these have been reviewed and that no missing data was detected.

The SDMT Verification Report[21] ensures that the proper calculations are made by the independent calculations of the SDMT application and that the final data will be correct and accurate. This is to satisfy the TV2 verification identified in the SDMT Verification and Test Plan. Safety reviews the Review records generated by Engineering for the installation table and telegram files. These review records are generated for each release and verify that each telegram has the proper CRC with no duplicate packages. The installation table review ensures that each transponder has correct name and the distances to the related signaling object is correct.

Safety reviews the redline markups to the drawings submitted with each review to ensure that all relevant package changes and transponder changes are properly recorded. The actual drawing release occurs from the redlines reviewed with safety.

3.5.2 Data Integrity

The SDMT tool application uses diverse coding to ensure no failures are present in the output of the tool calculations. In addition, the packages are protected by 64bit CRC to prevent corruption after the completion of calculations and during the storage and programming cycles.

Engineering documents the final design with signaling drawings detailing the packages and distances used in the packages. This data is verified by engineering against the SDMT package information to verify the drawing and package information is correctly implemented on the railroad.

3.6 Database Safety Concepts Verification

3.6.1 Office Database Safety Concepts Verification

3.6.1.1 ADDC

Only configuration files no database or tie to system database. Files are not relevant to safety.

3.6.1.2 DMS

Only configuration. Files are not relevant to safety.

3.6.1.3 NMS

Only configuration files. Files are not relevant to safety.

3.6.1.4 RGS

Only configuration files. Files are not relevant to safety.

3.6.1.5 SDMF

This section applies to Data Integrity.

Database files generated by SDMF tools and data files used for generating these database files are maintained and managed as part of configuration management using IBM Rational Team Concert. Software and data installation procedures have instructions to verify the data and software files on the final targets.

Data accuracy is ensured by confirming of the CRC identified in the PVI for the data release with the files stored in SDMF by the configuration manager. As each file is loaded it is confirmed with the file verification documented in the PVI. This same technique is also used to verify the file once it is loaded onto the media to transfer the file to the final hardware (USB stick or laptop) depending on the subsystem being programmed.

3.6.1.5.1 SDMT

This section applies to Data Integrity.

Data accuracy is ensured by confirming of the CRC identified in the PVI for the data release with the files stored in SDMF by the configuration manager. As each file is loaded it is confirmed with the file verification documented in the PVI. This same technique is also used to verify the file once it is loaded onto the media to transfer the file to the final hardware (USB stick or laptop) depending on the subsystem being programmed.

3.6.1.6 Security Server

Only configuration files no database or tie to system database. Files are not relevant to safety.

3.6.1.7 STS

This section applies to Data Integrity

The STS part of the office components is considered to be SIL 4 and safety critical. The process of protecting the vital database is shown below;

It has been analyzed that each record in the vital static database is protected by a 16 bit CRC. Additionally, every 2000 byte block of records is protected by a 64 bit CRC. The 64-bit CRC is the same algorithm included in the generic product. The binary file is stored on a solid-state disk on the C computer. Each vital process running in the RATP GP A and B computers initially sends a file read request to the C computer. The C computer reads the data and sends it back to the A and B computers. Each A and B computer then copies the file to the corresponding RAM memory and validates the file format and the CRC64 for each block of data. The STS performs this test every reboot and this feature is tested in Factory Testing[19].

The chainage of each milepost must be accurately recorded into the STS configuration file and verified with the actual chainage of the milepost identifiers on the railway to assure that TSR's are properly placed where requested. The Milepost chainage was verified in the Civil Data verification report.[1][2]. The data for the milepost entry into SDMT from the civil data verification report is found in the Database Verification Report [22]. The SPT and SUP Database verification reports [23][24][25][26][27][28] provide further evidence through testing that these points align to the physical marker locations.

Please refer to the Office Safety Concept Description[11] for more information.

3.6.2 UIS Database Safety Concepts Verification

This section applies to Data Integrity

The UIS compares the map version with the STS map version to ensure that data used by both subsystems is aligned. The Office Specific Application Data Report [29] also verifies the data elements used by the office subsystem and ensures that each element is based on the same physical location as that entered into the SDMF.

Data accuracy is ensured by confirming map release defined in the PVI for the data release with the files stored in SDMF by the configuration manager. As each file is loaded it is confirmed with the file verification documented in the PVI. This same technique is also used to verify the file once it is loaded onto the media to transfer the file to the final hardware (USB stick or laptop) depending on the subsystem being programmed.

3.6.3 Transponder Database Safety Concepts Verification

This section applies to Data Integrity.

Package accuracy is based on 10yd increments in packages. Therefore, installation errors greater than the above need to be corrected or modified data generated to remove the errors.

Movement of the Transponder by maintenance is verified for installation tolerance and recorded in Site Installation Test Reports[17][18] . The SDMF Test & Verification Plan [5] defines this activity

The transponder must accurately be placed within a specific tolerance of the location the transponder is programmed for. Below is how transponders are arranged.

1. A transponder set has a minimum of two transponders in order to provide direction to the passing train based upon the order in which the train reads the transponders.
2. When the number and size of the transponder message packages required at any location exceeds the capacity supported by four transponders, a new set is created to accommodate all of the data.
3. The minimum distance between transponders in the same set is ten feet. (Safety Description Sect Req 2)

4. The maximum distance between transponders in the same set is twelve feet. (Safety Description Sect Req 2)

   a. To maintain uniformity, the optimum separation between adjacent transponders in the same set is between eleven feet and eleven feet, six inches, depending on the tie spacing. (Safety Description Sect Req 2)

5. All transponder sets are located a minimum distance of one hundred linear feet from any other set. Where the maximum authorized speed of any train over a set exceeds eighty MPH, the minimum distance is two hundred feet. (Safety Description Sect Req 2)

6. Transponder sets are placed six feet adjacent to insulated joints unless the design requires a transponder set to be located at a non-insulated joint location.

7. Due to safety crosstalk considerations, the first transponder adjacent to an impedance bond is placed a minimum of 6.5 feet from the impedance bond. This extends the minimum distance from the insulated joint to 20.5 feet, as illustrated in (Safety Description Sect Req 2)

   a. The remaining transponders in the set are placed adjacent to the first transponder in the offset direction away from the insulated joints in accordance with optimum separation.

   b. By convention, transponders are placed a minimum distance of 20.5 feet from the insulated joint when possible to maintain consistency.

8. Transponder sets placed at interlocking HS and DS locations are normally placed on the approach side of the insulated joint that is closer to the signal.

9. Transponder sets placed at locations other than interlocking HS and DS locations are placed on the side of the insulated joint that best balances the linking distances between that set and the next set in each direction.

Transponders are linked to enable the OBC to detect any missing (or temporary, unlinked) transponders. The linking distances are used by the OBC to calibrate wheel wear and to reduce position error. The linking distance qualifier is used to identify situations in which the distance to the next transponder set may vary due to divergent routes. In these cases, an inexact linkage is indicated. The OBC uses the transition from an inexact linking distance to an exact linking distance to detect that it has exited an interlocking. The linking distance is verified in the SIT Test Report[17][18].

In addition to the lining the transponders include a header package define the number of transponders in the set, the track ID, Line ID, and direction of travel. The onboard can verify this information with the information in the other transponders within the set to verify correct installation of the set as well as the correct installation of other sets based on current data.

The vital data transmitted between the transponder and Onboard systems is protected by a 72 bit CRC. A BCH code is a multilevel cyclic variable-length digital error-correcting code used to correct multiple random error patterns. The telegram code format is a modified BCH block code. The code is a cyclic code and this property is exploited to avoid the need to wait for a start of a block and allowing decoding before synchronization. The block length is 255 bits with 180 information bits in the block. The basic BCH code is a (255,191,17) code with the Cyclic Redundancy Check (CRC) extended by 8 bits for synchronization purposes. The CRC is verified in the PICO section of the Transponder SIT Test Report[17][18].

3.6.4 Comms Database Safety Concepts Verification

This section applies to Data Integrity.

The safety of the data transmitted through radio frequency as stated in the Comms System Safety Concept Description [12] are as follows;

The MCM uses the HMAC keys stored in the RCF file. The MCM computes CRC's for the RCF files and compare the calculated CRC's with CRC's sent with the RCP Beacon. Two CRC's are used full set and working set. If the calculation fails for the full set, then a remote download of the RCF's is attempted by the MCM. If the full set CRC checks out, then the correct RCF defined by the working set CRC is selected. The Radio departure test functionality of the system has been analyzed to confirm the working set CRC of the RCF.

Safety Reviews the Comms SIT reports to ensure the correct executables and configuration files are loaded to the installed units. These reports are summarized in the Comms SVVR[40].

3.6.5 RWPS Database Safety Concepts Verification

This section applies to Data Integrity.

Also, the Database which is safety critical is verified by the following means; Common Track/MAP database for the safety critical data between the exchange to UIS and STS. The RWPS/EIC must compare its database version with the UIS database version to ensure they are the same. Note that the UIS compares its map with the STS and rejects TSR lists and TSR creation commands if the maps do not match.

It has been analyzed that the EIC Track/MAP database will be downloaded from the RWPS server at login. The maximum login time of an EIC will be 24 hours, forcing an update of checked download. In addition, the EIC Operating procedures will require EIC reboot when the RWPS is updated. Should a static check being performed by the RWPS fail, then the RWPS must ignore all future TSR requests to be sent to UIS and TSR List Responses to EIC Terminals. The map version check has been tested in RWPS Factory Testing [37].

3.6.6 WIU Database Safety Concepts Verification

This section applies to Data Integrity.

Steps are taken to verify and ensure the safety of the WIU subsystem. Below are the steps that are taken for this action from the WIU System Safety Concept Description [13]

The vital application generated by the DT Tool is confirmed by a UCN number that is also generated by the DT Tool for all parameters within that configuration. This UCN number must be entered by the user into the WIU prior to commissioning the WIU.

The unique check number guarantees that the vital configuration parameters are set by the user as intended.

The application designer also ensures that restrictive states for default values in the variable definition so that loss of communication with the executive does not result in unsafe states.

Factory and in-field integration testing confirm the correct UCN is loaded to the correct units.

3.6.7 OBC

This section applies to Data Integrity.

The onboard subsystem does not have any application data, but specific parameters are programmed when the OBC SW is loaded including Vehicle Type, Train ID, Wheel Diameter and scanner offset. These parameters are range limited and verified by the entering technician. The parameters are downloaded from the OBC and stored in the SDMF after verification by the installer. The parameters are protected by multiple software techniques identified in the OBC SSCD.

3.7 Protection Methodology for Data Entry

Safety engineering analyzed the engineering evidence to ensure that the verification required from the SDMT Verification and Test Plan for DB1 and DB2 were properly performed.. DB1 review consists of a review of the Civil Data Verification reports and Database Verification Report. This report also covers the requirements for DB2, and safety has audited the report and is findings.

The civil database survey confirms the correct data used as a baseline of the SDMT data for the line. The ICDD and PTS Report are generated from this base data to allow data to be generated by the Comms and Transponder teams. These documents are released with PVI's and submitted to the relevant development teams once the Civil Data verification has been performed and data entry of the civil data into SDMT has been verified. Once this data is generated and the SDMT updated for the Radio Block design and WIU ICDD updates, this data is entered into SDMT and the Transponder design is updated for the WIU and communication application data. The Database Verification Report [22] confirms the data entry of the civil verified data[2][3] matches the data entered into SDMT database. The ICDD and PTS Reports are then regenerated by SDMT from this verified data to ensure no changes to these documents occur from the corrected civil data.

3.7.1 Transponder

3.7.1.1 Data Correctness

For the Transponders, the designs and telegrams are generated on the SDMT. Some of the transponder data is automatically generated by the SDMT based on the civil data entered into the SDMT, but engineering is still required to verify this data in the final design and modify if necessary. Manual entry of the transponder data is also required and this data is specifically verified for correct entry into SDMT and correct output in the transponder telegram via textual reporting of the data by the SDMT tool.

The Transponder SCR provides details on the proper input of the PTS Report and ICDD changes from comms and WIU that impact the transponder application. The SCR and the review records for each Transponder release are recoded in the Transponder validation reports[41][42].

3.7.1.2 Data Integrity

The SDMT is considered a T3 tool. With assurance of correct data being entered into the tool, following all rules detailed in the SDMT User manual and the System Application Rules, the tool will populate correct outputs. Verification is required on all data inputs to the SDMT. As the tool handles both vital and non-vital data, the vital data is exported in an A/B configuration to ensure correctness of the data being generated. A/B configuration is when two independent engineers are given the same design/requirements to produce their code for export. At the export each of their outputs are compared to ensure the results match. Assuming the A/B match, export A is kept and available for use, while B is deleted. If there are any mismatches in the data export, the export fails and all data is deleted from export. The SDMT Verification Report[21] provides evidence of the two implementations performing the correct functions.

Note: A/B configuration is a comparison of two diversified sets of code.

Any data not matching the system application rules is reported by the tool in a report. Any errors in the output reports to the rules are documented and justified in the transponder SCR. A simulation test is performed on the TransponderSim and the results of this testing are in the Transponder Factory Acceptance testing. Factory testing can only confirm the transponder design to the inputs. Input verification has been performed during Site Testing.

The Track Plan is updated with the final Transponder layout and the transponder telegram details are added to this drawing and verified by engineering against the SDMT Tool Report that generates the readable format of the telegrams. Any errors in the drawing are reviewed against the SDMT tool report and corrections are made. The Track Plan verification is documented in the Transponder SCR. The Transponder Validation report[41][42] provides the evidence of the review of the SDMT Tool Report against the drawings. Safety audits the review records of engineering verification to ensure the verification is performed and all issues are resolved.

3.7.2 WIU

This section applies to Data Correctness.

For the WIU's, they are not generated till the civil data is updated in the ICDD which is an output from the SDMT diversified code and includes information on the switch and signal tables. The WIU team address the relevant switch and signal input data from the WIU configuration. The ICDD data is used to the WIU Application design documentation are used to generate the application design in the DT Tool. This input data is verified by a check engineer against the approved WIU design documentation from the WIU designer. The checker is independent of the designer. The WIU DT Tool is used to generate the application data files to be loaded onto the WIU. The evidence from this data being correctly entered into the design and application of the WIU being completed is the WIU Book of Plans being marked "As Checked" or greater ("As Tested, Factory Tested, As Installed, and As in Service are the greater levels. The WIU SVVR[32] provides evidence that the review records have been completed and all open issues resolved.

3.7.3 Office

This section applies to Data Correctness.

The office design is also generated based on the civil data populated into the SDMT, Radio configuration data entered into SDMT and IP addresses from the communication design. The PTS report entry into the SDMT is verified by the Map SCR's. System Line Boundaries are entered and verified by a peer review of the system line boundaries. The IP addresses are also allocated during the design and entered into the SDMT for proper generation of both Vital and Non-Vital data accordingly and verified through SCR changes. The SDMT has some validation constraints built in to assist in the development of the Office data listed above. The LIRR Map Office Specific Application Data Report[29] provides the evidence that all physical elements required for the office configuration or properly entered into SDMT from their inputs. This report is audited by Safety during SCR reviews to ensure all inputs are entered an any open issues resolved.

The SDMT is considered a T3 tool. With assurance of correct data being entered into the tool, following all rules detailed in the SDMT User manual and the System Application Rules, the tool will populate correct outputs. Verification is required on all data inputs to the SDMT. As the tool handles both vital and non-vital data, the vital data is exported in an A/B configuration to ensure correctness of the data being generated. A/B configuration is when two independent engineers are given the same design/requirements to produce their code for export. At the export each of their outputs are compared to ensure the results match. Assuming the A/B match, export A is kept and available for use, while B is deleted. If there are any mismatches in the data export, the export fails and all data is deleted from export. The SDMT Verification Report[21] provides evidence of the two implementations performing the correct functions.

Note: A/B configuration is a comparison of two diversified sets of code.

The SDMT has some validation constraints built in to assist in the development of the Office data listed above. These constraints are reported in the final SDMT output report. Any errors in the SDMT output reports are fully documented and justified in the Map SCRs.

The SPT and SUP Database test reports [23][24][25][26][27][28] confirm proper entry of PDS Coverage location, Infrastructure data and other inputs into the office database.

3.7.4 Comms

This section applies to Data Correctness.

Comms designs are based off of the civil data provided in the PTS Report using data populated into the SDMT using the verified processed data. External to the SDMT the chainage values of the PTS and PDS points are converted to Lat/Long coordinates using Civil 3D software. Since this process alters data to the report, it requires an additional verification effort outside of the SDMT. The coverage requirements are used to determine placement for each location. Once the PDS Coverage location are complete and the actual RF start and end locations are known they are entered back into the PTS Report in a Lat/Long coordinate and again converted back into a chaining using Civil 3D software. This chaining value that has been verified is then entered back into the SDMT for use by other subsystems. The SPT and SUP Database test reports [23][24][25][26][27][28] confirm proper entry of PDS Coverage location into the office data

The LIRR Map Office Specific Application Data Report[29] reviews the block design the RF Coverage entered into SDMT. It should be noted that errors in RF coverage will not cause a safety issue with the system.

3.7.5 OBC

This section applies to Data Integrity.

The onboard subsystem does not have any application data but specific parameters are programmed when the OBC SW is loaded including Vehicle Type, Train ID, Wheel Diameter and scanner offset. These parameters are range limited and verified by the entering technician. The parameters are downloaded from the OBC and stored in the SDMF after verification by the installer. The parameters are protected by multiple software techniques identified in the OBC System Safety Concept Description.

3.8 Protection Methodology for Data Storage

This section applies to Data Integrity.

Data accuracy is ensured by confirming of the CRC or other file verification technique identified in the PVI for the data release with the files stored in SDMF by the configuration manager. As each file is loaded it is confirmed with the file verification documented in the PVI. This same technique is also used to verify the file once it is loaded onto the media to transfer the file to the final hardware (USB stick or laptop) depending on the subsystem being programmed.

3.8.1 Transponder

This section applies to Data Integrity.

For transponder data as files are stored on the PTE, the CRC within the telegram file is used to confirm that no changes are made. The CRC is verified after the file is programmed into the transponder to confirm that no changes from the final released file occurred.

3.8.2 Office

3.8.2.1 STS

This section applies to Data Integrity.

File CRC is read within the assigned configuration files and checked by the server to ensure the files are not changed while residing on the server. This test is repeated upon reboot of each server.

The STS will check that map version used by the STS is the same version reported by the UIS. If the map versions do not match an error will be reported by the STS to the NMS and no TSR requests will be accepted from the UIS by the STS.

3.8.2.2 UIS

This section applies to Data Integrity.

Data accuracy is ensured by confirming file identified in the PVI for the data release with the files stored in SDMF by the configuration manager. As each file is loaded it is confirmed with the file verification documented in the PVI. This same technique is also used to verify the file once it is loaded onto the media to transfer the file to the final hardware (USB stick or laptop) depending on the subsystem being programmed

The UIS will check its map version with the Map version sent by the STS. If the map versions are not the same the UIS will not accept TSR lists from the STS and will send an alarm to the NMS.

3.8.2.3 All others (ADDC, NMS, SEC, RGS, WCC, and DMS)

No Application data is released to these servers only configuration files not related to the railroad infrastructure.

3.8.3 WIU

This section applies to Data Integrity.

The UCN number on specific values as specified by the designer is checked by the WIU for changes. Each WIU must be programmed with the UCN of the vital configuration file in order to accept the vital configuration for running. The maintainer DT tool has been modified from generating the UCN to prevent accidental changes to the vital configuration from the staff loading the database and software from the design application team intended designs.

3.8.4 RWPS

This section applies to Data Integrity.

Data accuracy is ensured by confirming file identified in the PVI for the data release with the files stored in SDMF by the configuration manager. As each file is loaded it is confirmed with the file verification documented in the PVI. This same technique is also used to verify the file once it is loaded onto the media to transfer the file to the final hardware (USB stick or laptop) depending on the subsystem being programmed

The map version used by the RWPS will be checked with the Map version sent from the UIS. If the map versions are not the same the RWSPS will not accept the TSR lists and indicate an alarm to the NMS.

3.8.5 OBC

This section applies to Data Integrity.

The onboard subsystem does not have any application data but specific parameters are programmed when the OBC SW is loaded including Vehicle Type, Train ID, Wheel Diameter and scanner offset. These parameters are range limited and verified by the entering technician. The parameters are downloaded from the OBC and stored in the SDMF after verification by the installer. The parameters are protected by multiple software techniques identified in the OBC System Safety Concept Description

3.8.6 Communication

This section applies to Data Integrity.

Data accuracy is ensured by confirming file identified in the PVI for the data release with the files stored in SDMF by the configuration manager. As each file is loaded it is confirmed with the file verification documented in the PVI. This same technique is also used to verify the file once it is loaded onto the media to transfer the file to the final hardware (USB stick or laptop) depending on the subsystem being programmed. An MD5 checksum for each communication application file is checked at installation.

3.9 Protection Methodology for Data Usage

3.9.1 Office

3.9.1.1 ADDC

Only configuration data no Application data is loaded on this server.

3.9.1.2 DMS

Only configuration data no Application data is loaded on this server.

3.9.1.3 UIS

This section applies to Data Integrity.

The following best practices are used to insure data integrity and protection for SQL databases.

1. Using Storage Area Network (SAN) storage with RAID 10 for disk redundancy to protect data from corruption.

2. Using SDMF system for managing any database of software update which will protect database from any unintended corruption.

3.9.1.4 Security Server

Only configuration data no Application data is loaded on this server.

3.9.1.5 SDMF

This section applies to Data Integrity.

Data accuracy is ensured by confirming of the CRC or other file verification technique identified in the PVI for the data release with the files stored in SDMF by the configuration manager. As each file is loaded it is confirmed with the file verification documented in the PVI. This same technique is also used to verify the file once it is loaded onto the media to transfer the file to the final hardware (USB stick or laptop) depending on the subsystem being programmed.

3.9.1.6 STS

This section applies to Data Integrity.

It has been analyzed that each record in the vital static database is be protected by a 16 bit CRC. Additionally, every 2000 byte block of records is protected by a 64 bit CRC. The 64-bit CRC is the same algorithm included in the generic product. The binary file is stored on a solid-state disk on the C computer. Each vital process running in the RATP GP A and B computers initially sends a file read request to the C computer. The C computer reads the data and sends it back to the A and B computers. Each A and B computer then copies the file to the corresponding RAM memory and validates the file format and the CRC64 for each block of data.

The above check is repeated periodically when the STS is rebooted. Please refer to the Office Safety Concept Description [11] for more information.

3.9.2 WIU

This section applies to Data Integrity.

The UCN number on specific values as specified by the designer is checked by the WIU for changes. Each WIU must be programmed with the UCN of the vital configuration file in order to accept the vital configuration for running. The maintainer DT tool has been modified from generating the UCN to prevent accidental changes to the vital configuration from the staff loading the database and software from the design application team intended designs

3.9.3 Transponder

This section applies to Data Integrity.

For transponder data as files are stored on the PTE, the CRC within the telegram file is used to confirm that no changes are made. The CRC is verified after the file is programmed into the transponder to confirm that no changes from the final released file occurred.

3.9.4 OBC

This section applies to Data Integrity.

The onboard subsystem does not have any application data, but specific parameters are programmed when the OBC SW is loaded including Vehicle Type, Train ID, Wheel Diameter and scanner offset. These parameters are range limited and verified by the entering technician. The parameters are downloaded from the OBC and stored in the SDMF after verification by the installer. The parameters are protected by multiple software techniques identified in the OBC System Safety Concept Description

3.9.5 Communication Subsystem

This section applies to Data Integrity.

Data accuracy is ensured by confirming file identified in the PVI for the data release with the files stored in SDMF by the configuration manager. As each file is loaded it is confirmed with the file verification documented in the PVI. This same technique is also used to verify the file once it is loaded onto the media to transfer the file to the final hardware (USB stick or laptop) depending on the subsystem being programmed. An MD5 checksum for each communication application file is checked at installation. The Comms SVVR[40] provides the evidence that the correct executable and configuration files are installed on the correct physical units.

3.9.6 RWPS

This section applies to Data Integrity.

The Database which is safety critical is verified by the following means; Common Track/MAP database for the safety critical data between the exchange to UIS and STS. The RWPS/EIC must compare its database version with the STS database version to ensure they are the same. It has been analyzed that the EIC Track/MAP database is downloaded from the RWPS server at login. The maximum login time of an EIC will be 24 hours, forcing an update of checked download. Should a static check being performed by the RWPS fail, then the RWPS must ignore all future TSR requests to be sent to UIS and TSR List Responses to EIC Terminals.

3.10 Data Verification Operation

3.10.1 Communications

This section applies to Data Integrity.

Data accuracy is ensured by confirming of the CRC or other file verification technique identified in the PVI for the data release with the files stored in SDMF by the configuration manager. As each file is loaded it is confirmed with the file verification documented in the PVI. This same technique is also used to verify the file once it is loaded onto the media to transfer the file to the final hardware (USB stick or laptop) depending on the subsystem being programmed.

For the application data development, the ICDD and PDS reports are configuration management and transferred between sites in PDF format only after being archived in the Document management system. Once the file is delivered between BT and Siemens any changes to that version are documented and the all parties notified of the changes to the file and relevant line sections.

3.10.2 Processing

3.10.2.1 SDMT (Office, RWPS, Transponder)

This section applies to Data Integrity.

The SDMT is considered a T3 tool. With assurance of correct data being entered into the tool, following all rules detailed in the SDMT User manual and the System Application Rules, the tool will populate correct outputs. Verification is required on all data inputs to the SDMT. As the tool handles both vital and non-vital data, the vital data is exported in an A/B configuration to ensure correctness of the data being generated. Assuming the A/B match, export A is kept and available for use, while B is deleted. If there are any mismatches in the data export, the export fails, and all data is deleted from export. The SDMT Verification Report[21] provides evidence of the two implementations performing the correct functions.

Note: A/B configuration is a comparison of two diversified sets of code.

The SDMT is verified by the developers of the tool. Please see the SDMT Verification Report[21].

For verification of the SDMT data, a Review Report is generated to document every asset within the tool and its civil properties as needed. This report is to be verified back to the VCD to ensure correctness of the data entered.

Any intermediate files, such as the ICDD Tables and PTS Report that get altered external to the SDMT with subsystem designs for the WIU and Comms, must be verified by their respective competent engineer prior to reentry into the SDMT. Once the data is reentered into the SDMT it can once again be re-verified against its source for correctness.

3.10.2.2 DT Tool

This section applies to Data Integrity.

The Diagnostic Terminal is a non-vital tool (since it is installed on a Windows-based platform) that is used to create the Vital Configurations for the WIU. The generated Program Report (a human readable file of the configurable parameters) is put under a thorough verification process where an independent checker reviews the design and only appends the master drawings to “as checked” once all the issues are resolved. If multiple versions are verified Beyond Compare is used to identify changes since the last check and only changes are verified. There is also a process for verifying the integrity of a binary file generated by the DT tool. To insure a file has not been corrupted the original Program Report is compared with a Program Report taken off a physical WIU unit with a separate laptop.

3.10.3 System Calculation

The system FTA includes modeling of Human errors of the Data Entry and Data Entry Verification. This model is shown below. The data for the failure rates in this model are standard human error failure rates shown in the model.

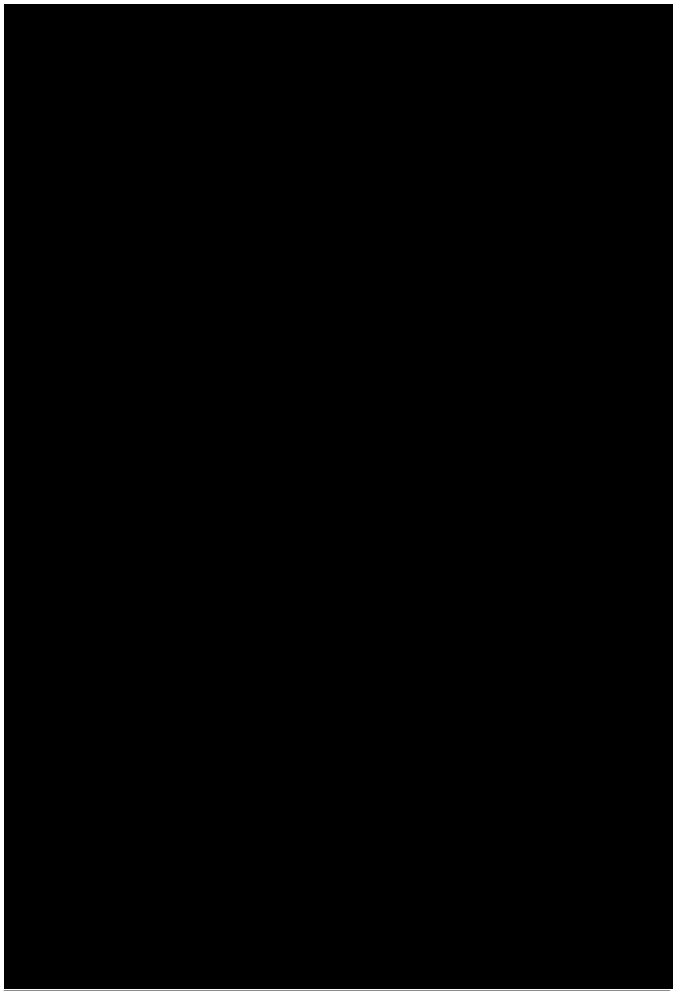


Figure 1 System Calculation

4 Testing and Controls

4.1 Testing

The database testing reports for both pilot lines for LIRR (L1 and L2) [23][24][25][26][27][28] [39] record that the physical infrastructure encoded into the ACSES database was successfully entered into the ACSES subsystems. These reports verify the accuracy of PTS Enforced stopped locations, MAS and PSR speed restrictions, Milepost markers, Grade crossings, and stations. The testing also verifies the interlocking speeds, routing and interface to the vital signaling logic. Testing with line boundary data will be performed outside the pilots once this functionality is completed and ready for testing on the pilots.

WIU Site Installation Testing was performed at each interlocking and verifies each switch and signal and all routes through each interlocking [35][36].

Transponder Site Installation[17][18] testing was completed to verify the proper installation of each transponder and that the correct telegrams are programmed into the correct transponders. PICO test results were also included in the Transponder Site Installation Reports.

4.2 Controls

4.2.1 Staged Deployment

The plan for data implementation is presented in the SDMF V&T Plan. This plans state that first the Civil Database is verified. After the civil database is verified for a line the PTS Report and ICDD are generated from the verified data and released to the Comms and WIU development teams. When the WIU and communication data design is completed and verified it is combined into SDMT and the Office Application design is developed to determine the TSR Blocks, and the Transponder application data is completed. Changes to the ICDD and PTS report must be carefully communicated to the different development teams and changes must be indicated to the WIU and communication teams to ensure no changes to the final system configuration occur from these changes. Each line is completed and then compiled into a formal Railroad database that used to generate the Office configuration files.

The line boundaries for this activity are carefully selected and controlled to limit changes to the previous set of data generated for the transponder, WIU and communication subsystems. The transponder line sections will include new shadow Transponders to allow linking distances between the line segments to be calculated. These shadow transponders must be verified with the database for the shadow line to ensure proper data entry and proper linking.

4.2.2 Application Updates

The application data for each subsystem is defined by ICD's so that the SW and application data are compatible. Any changes to the structure of the data within the database requires a change the ICD. The SDMT would then need to be modified to change for format of the data as well as the subsystem application that reads that data. For data between the STS and Onboard, WIU and Onboard as well as transponder and onboard these messages are controlled by the Project MDD ICD's. These changes would also have to approved by the NEC railroads to ensure interoperability between the different suppliers. This would include any additional messages to the system.

Application rules have been established for each subsystem on the data entry rules. For transponder these rules have been programmed into the SDMT. All subsystems have an application rule document and the data entered is checked against these documents.

4.2.3 Database Updates

The ICDD and PTS reports and releases control the data released between subsystems. The map data also has major and minor revision numbers. The major revision number is modified for any changes that would cause errors between the office components are between other subsystems. This major map version is checked between office components to make sure compatible data is being used.

When updates or changes are made in the field, this is coordinated to engineering through a Map SCR which is then implemented in the SDMT design and then documented in the database verification reports to account for the changes that were made in the SDMT ensuring that the ICDD and PTS reports are updated and other subsystems updated as necessary.

5 Conclusion

The following table shows the Evidence for each section of this report that was reviewed by Safety Engineering. The sections that do not reference external documents are noted and reference only to the section of this document.

Table 5 Safety Evidence Cited from this Report

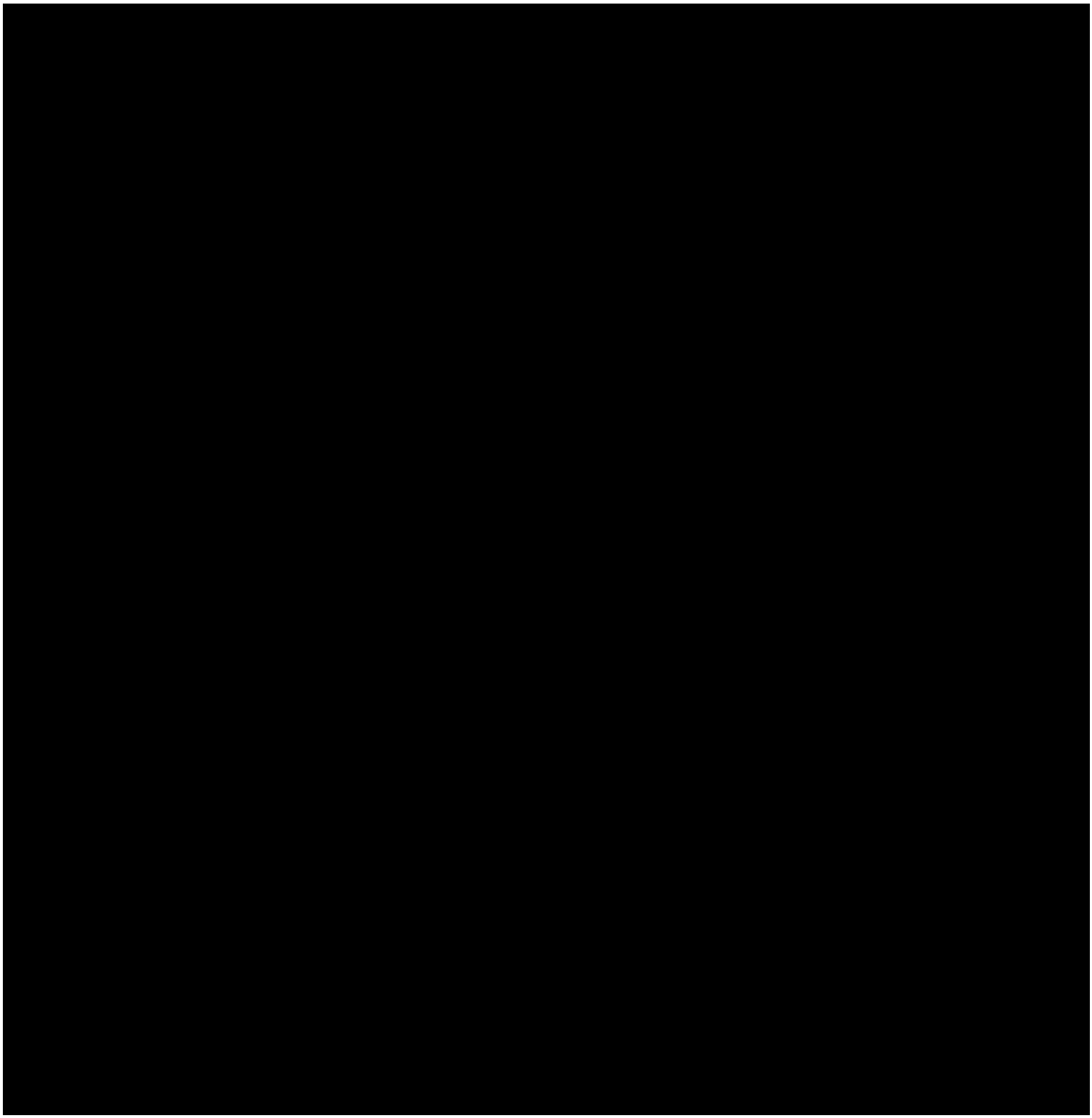
Section ID	Section Name	Evidence Supporting	PDM Number of Evidence
3	Civil Database Verification	PW Civil Database Verification Report Montauk Civil Database Verification report	3050830 3051385
3.1	Grade Verification	Horizontal Alignment and Veridical Grade Verification Report	3052572_Rev_A
3.2.1	Office Database Verification	Database Verification Report LIRR Map Office Specific Application Data Report	3151611 3151133
3.2.2	Office Database Integrity	LIRR Map Office Specific Application Data Report	3151133
3.3	Comms Database Verification	Database Verification report	3151611
3.4	WIU Database Verification	WIU SVVR WIU FAT Line 1 WIU FAT Line 2 WIU SIT Line 1 WIU SIT Line 2	3050366 4009406 4009407 4009408 4009408

3.5.1	Transponder Database Correctness	Database Verification report Port Washington TP Validation report Montauk TP Validation Report SDMT Verification Report	3151611 3043407 3046231 4009864
3.5.2	Transponder Data Integrity	SDMT Verification Report	
3.6.1	Office Database Safety Concepts	Office System Safety Concept Description Office SIT Report (versions installed)	3036410
3.6.2	UIS Database Safety Concepts	Office System Safety Concept Description Office SIT Report (versions installed)	3036410
3.6.3	Transponder Database Safety Concept	PW TP SIT Test Report Montauk TP SIT Test Report	4007924 4009101
3.6.4	Coms Database Safety Concept	Communication System Safety Concept Description Comms SVVR	3036421
3.6.5	RWPS Database Safety Concept	RWPS Factory Test Report	4009341
3.6.6	WIU Database Safety Concept	WIU Subsystem Safety Concepts Document WIU SIT Line 1 WIU SIT Line 2	3035817
3.6.7	OBC Database Safety Concept	Onboard System Safety Concept Description	3036406
3.7	Protection Methodology for Data Entry	Database Verification report	3151611
3.7.1	Transponder Protection Methodology for Data Entry	Port Washington TP Validation report Montauk TP Validation Report SDMT Verification Report	3043407 3046231 4009864
3.7.2	WIU Protection Methodology for Data Entry	WIU SVVR CDRL 2-12-24	3050336
3.7.3	Office Protection Methodology for Data Entry	LIRR Map Office Specific Application Data Report SDMT Verification Report	3151133 4009864
3.7.4	Comms Protection Methodology for Data Storage	LIRR Map Office Specific Application Data Report	3151133

3.7.5	OBC Protection Methodology for Data Storage	Onboard System Safety Concept Description	3036406
3.8.1	transponder Protection Methodology for Data Storage	No evidence See section for details	
3.8.2	Office Protection Methodology for Data Storage	No evidence See section for details	
3.8.3	WIU Protection Methodology for Data Storage	No evidence See section for details	
3.8.4	RWPS Protection Methodology for Data Storage	No evidence See section for details	
3.8.5	OBC Protection Methodology for Data Storage	No evidence See section for details	
3.8.6	Comms Protection Methodology for Data Storage	No evidence See section for details	
3.9.1	Office Protection Methodology for Data Usage	Office System Safety Concept Description	3036413
3.9.2	WIU Protection Methodology for Data Usage	WIU Subsystem Safety Concepts Document	3035817
3.9.3	TP Protection Methodology for Data Usage	No evidence See section for details	
3.9.4	OBC Protection Methodology for Data Usage	Onboard System Safety Concept Description	3036406
3.9.5	Comms Protection Methodology for Data Usage	Comms SVVR	3036422
3.9.6	RWPS Protection Methodology for Data Usage	No evidence See section for details	

3.10.1	Database Verification Operations Communications	No evidence See section for details	
3.10.2	Database Verification Operations Processing	SDMT Verification Report	4009864
3.10.3	Database Verification Operations System Calculations	No evidence See section for details	
4.1	Testing	SPT L1 Database Verification Test Report Addendum 2 SPT L2 Database Verification Test report Addendum 1 SUP L1 Database Verification Test Report Addendum 2 SUP L2 Database Verification Test Report Addendum 2 SUP Baseline 3.2 Pilot L1 Database Verification Test Report Addendum 2 to CDRL 2-090-214 SUP Baseline 3.2 Pilot L2 Database Verification Test Report Addendum 2 to CDRL 2-090-214 SUP Baseline 3.4 Pilot L1 Database Verification Test Report Addendum 2 to CDRL 2-090-214 WIU SIT Test Line 1 WIU SIT Test Report Line 2 TP SIT Test Report Line 1 TP SIT Test Report Line 2	4009314 4009316 4009467 4009466 4009570 4009569 4009778 4009408 4009409 4009101 4007924
4.2.1	Controls - Staged deployment	No evidence See section for details	
4.2.2	Controls Application Update	No evidence See section for details	

The Following Tables (Table 6 & Table 7) show open issues from the verified reports that have been referenced, as well as a Safety Justification for each issue. All safety NCRs and Variances in the below tables from referenced documents are justified. Look to the System Safety Report CDRL 2-136 for final justification.



Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

Project Hazard Log

CDRL 2-126-20

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Jason Weighley Safety Engineer		Jason W Weighley 2019.07.18 15:14:59 -04'00'
Verified:	Francis Tabi Safety Engineer		Francis Tabi 2019.07.18 15:18:35 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.07.19 10:57:51 -04'00'
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group		Phil Magloire 2019.07.19 10:52:26 -04'00'
BT/SRA Review:	NA Title		
BT/SRA Review:	NA Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3035819

Effective Date:	Revision:	Language:
2019-07-18	_N	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2014-07-18	First issue
_A	2014-08-27	Updated disclaimer on signature page
_B	2014-10-20	Updated Hazard Log for PDR
_C	2015-12-18	Submitted for PDR
_C.1	2016-11-14	Updated to Align with PHA
_C.2	2016-12-16	Revised table for improved alignment with the hazard sources. Updated to include hazards identified since last revision. Multiple updated to address review comments from SYSTRA/AECOM
_D	2016-12-21	Released for FDR – Review with RR complete
_E	2017-12-06	Updated for Nov 2017 Release of Hazard Log. Updated for internal review comments.
_F	2018_05-01	Updated to remove revision and SRAC from Hazard Logs. Attached subsystem hazard logs.
_G	2018-09-10	Updated System and Subsystem Hazard Log Entries
_H	2018-11-08	Updated System and Subsystem Hazard Log Entries for November
_J	2018-12-05	Updated System and Subsystem Hazard Log Entries for December
_K	2019-01-24	Updated to Address RR comments SI-RVW-0757, Added SRAC column to System Log, Updated OBC and RWPS HL
_K1	2019_04_08	Updated for Hazard Log Review
_L	2019_04_22	Releaed for System Baseline 3.4
_M	2019-06-25	Updated to Address RR comments SI-RVW-0757
_N	2019-07-17	Updated to Address PTCSP comments

Table of Contents

Section	Subject	Page
1	Executive Summary	4
2	Introduction	4
2.1	Compliance Matrix	4
2.2	Reference Documents	5
2.3	Glossary	5
3	Hazard Tracking Process	6
3.1	Sources of Hazards for the Hazard Log	6
3.2	Hazard Log Configuration Management and Format	7
3.3	Risk Assessment Classification	7
3.4	Hazard Tracking Log Attributes	10
4	Project Hazard Log	12
5	Attachment A - System Project Hazard Log	13
6	Attachment B – Comms Hazard Log	14
7	Attachment C – Office Hazard Log	15
8	Attachment D – Transponder Hazard Log	16
9	Attachment E – RWPS Hazard Log	17
10	Attachment F – WIU Hazard Log	18
11	Attachment G – OBC Hazard Log	19

List of Figures

No table of figures entries found.

List of Tables

Table 1: Compliance Matrix 4
Table 2: Reference Documents 5
Table 3: Hazard Sources 7
Table 4: Hazard Severity Classifications 8
Table 5: Hazard Probability Classifications 8
Table 6: Hazard Risk Assessment Matrix 9
Table 7: Hazard Risk Index (HRI) 9
Table 8: Hazard table column Definition/Description 10

1 Executive Summary

The Hazard Log provides a record of the System Level hazards associated with the development and implementation of the ACSES II system for LIRR. This record will be updated to accurately reflect the elements of the system safety analysis and current mitigations as implemented in the system design.

2 Introduction

This hazard log is exported from the Project Hazard Log module in the project DOORS database. DOORS is a tool that is used to perform configuration management on the Hazard Log and allow the log to be linked to mitigating system level requirements.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
2 – Part 1	12.10.7-A	Hazard management Process	Project Hazard Log should capture all hazards associated with implementation including the subsystem interfaces and interoperability issues	3
	12.10.7-B	Subsystem Hazards Monitoring	The SI shall monitor the subsystem Hazard Log and when appropriate transfer those hazards to the System Level	3
	12.10.7-C.1	Traceability to Source of Hazard		3
	12.10.7-C.2	Traceability to Mitigation Action	Each Hazard shall be linked to its Mitigation. For the System Hazard Log each Hazard will be linked to SLR Requirements that implement the Mitigation or require the implementation of mitigation.	3
	12.10.7-D	All Hazards entered into the Project Hazard Log	All hazards entered as they are identified. Follow-up Analysis shall be used to update the status of each Hazard and referenced from the Log.	3

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.7-E	EMC Hazards to be included	All EMC Hazards, caused by either internal or external sources, shall be entered into either the Subsystem or System Hazard Log.	3
	12.10.7-F	Hazard Log Format	The Hazard Log will be maintained in a database compatible with Microsoft Office.	3.2
	12.10.7-G	Hazard Identification Format	Defined Tables in line with Guidance from MIL-STD-822C shall be used to define Severity and Probability of each hazard.	3.3
	9.3.H.6	Safety Program	Project Hazard Logs (CDRL 2-126)	All
	9.4.D.4	Safety Program Responsibilities	The subsystem suppliers shall administer a hazard log for the applicable ACSES II Subsystems.	4
	12.10.4.B.5.	Failure Modes and Effects Criticality Analysis	Determination of the fail-safe acceptability of system reaction, or requirement for design modifications (to be transferred to the Hazard Log for tracking	4

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	LIRR System Product Safety Plan CDRL 2-123-20	PDM 3035815
[2]	MIL-STD-882C, *System Safety Program Requirements*	MIL–STD-882C
[3]	AREMA, *Communications and Signals Manual – 2009 Section* Parts 16, 17, 21, and 23.	Revision 2001
[4]	System Level Requirements SLR	DOORS/PDM 3052527

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms, document number 3035624.

3 Hazard Tracking Process

The Project Hazard Log identifies all the functional level hazards identified in the planned hazard analyses performed on the project (e.g. PHA, OHA, SHA, FTA, FMECA and IHA as well as EMC analysis.). Additional sources of hazards in the hazard log may include such things as recorded field incidents, observations during tests, or comments from independent review (by regulators, assessors, etc.). The Project Hazard Log identifies who is assigned to resolve each hazard entry, and provides information relative to the status of the hazard. The information provided in the hazard log will enable an audit from initial identification of the hazard to the point of its adequate resolution. The hazard will provide a reference from the originating analysis that defined the hazard to the final analysis that provides the verification evidence that the hazard can be closed. Each hazard will be linked to mitigating requirements.

The System Safety Engineer will maintain an overall Project Hazard Log for all hazards that originate from interfaces between the ACSES II subsystems, those hazards originating from systems external to the ACSES II system, hazards originating from system design, and hazards originating from Operations. Each hazard in the Project Hazard Log will be linked to at least a System Level Requirement (SLR) that provides mitigation to the hazard. The SLR will be linked to further requirements, designs and test cases that will provide the closure evidence.

In addition each subsystem will maintain a separate Subsystem Hazard Log. Each Subsystem Hazard Log will be linked to the appropriate SSLR to provide the traceability to the requirements, design and test cases that will be used to close the hazard. The System Safety Engineer will review and monitor the Subsystem Hazard Logs so that any hazards in these logs that should be transferred to the system level are transferred.

The Project Hazard Log serves as a single reference for the status and resolution of system safety-critical issues for the project. As safety issues are identified throughout the Safety Program [1], they are entered into the Project Hazard Log. The Project Hazard Log shall be updated by the associated owner and reviewed regularly by the safety working group. The purpose is to assess the progress of the design tasks in meeting the system safety requirements, and mitigating the identified hazards noted in the Project Hazard Log. Prior to safety acceptance, the Project Hazard Log shall provide the formal documented evidence that every identified hazard and related safety criteria have been covered by a set of appropriate mitigations

3.1 Sources of Hazards for the Hazard Log

The table below identifies sources of the hazards in the hazard log including the status of the source at the time of current hazard log revision. As a living document, the hazard log will be maintained for alignment as the sources evolve and its maturity if predicated on that of its sources.). The system vulnerability assessment will be tracked as a separate attachment to the Hazard Log to separate track security mitigations.

Table 3: Hazard Sources



3.2 Hazard Log Configuration Management and Format

The Project Hazard Log is stored in the project DOORS Database under the Safety directory. The Subsystem Hazard Logs are located in the Subsystem folder within this directory. The hazard log modules can be exported from the DOORS database to Microsoft Office Applications.

3.3 Risk Assessment Classification

Throughout the product development lifecycle, risk assessment practices are applied to guide the implementation of mitigating actions to control or eliminate each identified hazard such that the risk introduced by each is acceptable. Risk assessment and management is a decision-making process consisting of evaluation and control of the severity and probability of a potentially hazardous event. As hazard analyses are performed Bombardier will identify hazards that will require resolution through the risk assessment process as described below, and these hazard will be maintained in the hazard log.

The classification of severity for hazards will be based on the four categories from MIL-STD-882C [2] and AREMA section 17.3.5 [3] identified in Table 4 ranging from Category I (Catastrophic) to Category IV (Negligible). The number of lost work days in parenthesis are used to determine the severity of a hazard. The severity classification assigned to each hazard will provide a qualitative indication of the worst-case consequences that could occur if the hazard is not eliminated or controlled.

Probability classifications will be based on the five categories from MIL-STD-882C[2]and AREMA section 17.3.5 [3] as shown in Table 5. These range from Category A (Frequent) to Category E (Improbable). The assigned probability will be based on the likelihood that a particular hazard and effect would occur in the planned life expectancy of the product. To assist in assigning the specific categories of probabilityTable 5 shows definitions for both a specific individual item (i.e. a specific component of the system) as well as for the fleet or overall inventory of the system. The table also provides the Mean Time Between Events (MTBE) to guide the consistent application of the classifications. Note that since the probability categories are applied to hazards of all severities (even category IV), it is not appropriate to use Mean Time Between Hazardous Events (MTBHE) in Table 5 as all events may not be truly hazardous in nature and therefore MTBE is used.

Table 4: Hazard Severity Classifications

Description (duration of outage)	Category	Definition
Catastrophic (1 Yr-death)	**I**	Death, system loss, or severe environmental damage.
Critical (21-363 Days)	**II**	Severe injury, severe occupational illness, major system or environmental damage.
Marginal (8-20 Days)	**III**	Minor injury, minor occupational illness, or minor system or environmental damage.
Negligible (0-7 Days)	**IV**	Less than minor injury, occupational illness, or less than minor system or environmental damage.

Table 5: Hazard Probability Classifications

Description	Level	Specific Individual Item	Fleet or inventory
Frequent	**A**	Greater then 0.24 (number of accidents / number of employees / passengers). Likely to occur	Greater than 10^{-1} failures /hr. Continuously experienced.
Probable	**B**	(0.16 to 0.24 number of accidents / number of employees / passengers) Will occur several times in the life of an item.	(Greater than 1.39×10^{-3} to Less than 1.0×10^{-1}) Will occur frequently.
Occasional	**C**	(0.10 to 0.15 number of accidents / number of employees \ passengers) Likely to occur sometime in the life of an item.	Will occur several times. (>= 1.14×10^{-5} to <= 1.39×10^{-3})
Remote	**D**	Unlikely but possible to occur in the life of an item. . (0.02 – 0.09 - number of accidents / number of employees / passengers)	Less then 5.12×10^{-7} (>= (5.12×10^{-7} to < 1.14×10^{-5})

Description	Level	Specific Individual Item	Fleet or inventory
			Unlikely but can reasonably be expected to occur.
Unlikely	**E**	So unlikely, it can be assumed occurrence may not be experienced. (<0.01 number of accidents / number of employees / passengers)	Unlikely to occur, but possible. (5.12×10^{-7})

The combination of the hazard severity and hazard frequency forms a Hazard Risk Index (HRI). The resulting Hazard Risk Assessment Matrix is obtained from MIL-STD-882C [2] as shown in Table 6 and Table 7.

The HRI presents the hazard analysis results in a format useful to the decision maker in determining whether hazards should be eliminated, controlled, or accepted. This provides a logical basis for management decision-making, considering both the severity and probability of any individual hazard in a weighted fashion.

Table 6: Hazard Risk Assessment Matrix

	Catastrophic	Critical	Marginal	Negligible
Frequent	**IA**	**IIA**	**IIIA**	**IVA**
Probable	**IB**	**IIB**	**IIIB**	**IVB**
Occasional	**IC**	**IIC**	**IIIC**	**IVC**
Remote	**ID**	**IID**	**IIID**	**IVD**
Improbable	**IE**	**IIE**	**IIIE**	**IVE**

Table 7: Hazard Risk Index (HRI)

Hazard Risk Index	Acceptance Criteria
IA, IIA, IIIA, IB, IIB, IC	**Unacceptable**
ID, IIC, IID, IIIB, IIIC	**Undesirable** - Requires solution acceptable to Bombardier Project Manager and to the QSRW Safety Assessor.
IE, IIE, IIID, IIIE, IVA, IVB	**Acceptable with review -** Requires review by the QSRW Safety Assessor.
IVC, IVD, IVE	**Acceptable** - Review not required.

3.4 Hazard Tracking Log Attributes

The attributes of the project hazard log shown in section 4 are defined in this section.

The attributes of the Project Hazard Log ensure the tracking process is formally carried out and documented. The Safety Status attribute provides the current status of each hazard. The Mitigations / Controls / Safeguards indicates if a mitigation has been found for the hazard. The Verification method indicates what evidence verifies the mitigation has been put in place.

The hazards are analyzed and assessed to determine their associated risk. In general, the hazard assessment is performed according to Frequency and Severity of each hazard in the list. The hazard risk is derived according to best available data, problems reported from similar projects and other lessons learned from similar systems.

The analysis and assessment results are presented in table format which contains the following columns:

Table 8: Hazard table column Definition/Description

Column Title	Description
ID	A unique identification number automatically assigned and managed by DOORS is provided per line to simplify hazard location in the tables. All system level Project Hazard Log entries will be identified with PHL-xx where xx is a unique number.
Subsystem or Interfaces	Indicates which ACSES II subsystem or interfaces cause or are impacted by the Hazard.
Source of Hazard	Defines the analysis that defined the hazard and the numerical reference from that Analysis that provides the originating data for the hazard entry into the log. If not found during an analysis it is related to phase of the project where the hazard was found. See Table 3 for a list of hazard sources and their statuses at the time of this revision of the Hazard Log.
Hazard Description	Description of the hazard imported from the source
Primary Cause	Description of the initial System event that can cause the hazard. Imported from the source when available.
Initial Risk	Risk of the hazard occurring before any Mitigation Action. The risk was analysed based on the criteria set out in section 3.3.
Mitigations / Controls / Safeguards	Action, operating procedure, or functional requirement that will reduce or eliminate the cause of the hazard from occurring.

Column Title	Description
Safety Requirement ID	A unique identification assigned to a SLR Requirement that provides the mitigation. This column is generated based on the Links established in DOORS.
Safety Status	Open – Hazard Defined and not mitigated. Closed – Mitigation verified to be properly implemented Canceled – Hazard Closed without mitigation as it is not possible to occur. Mitigated – Requirements of design that can provide a mitigation to the hazard have been identified and linked to the hazard. Deleted – Hazard is no longer applicable or overcome by events as described in the Remarks column
Responsibility	Assignment of which Safety Group will be responsible for further analysis and mitigation of the hazard System Safety – Engineering Group responsible for analysis at System Level to ensure SLR and System Design and training verify mitigation. Transponder Safety - Engineering group responsible for analysis of Transponder subsystems to ensure SSLR and subsystems designs and training verify mitigation WIU Safety – Engineering group responsible for analysis of WIU subsystems to ensure SSLR and subsystems designs and training verify mitigation. Onboard Safety – Engineering group responsible for analysis of Onboard subsystem to ensure SSLR and subsystem designs and training verify mitigation. Office Safety - Engineering group responsible for analysis of Office subsystems to ensure SSLR and subsystem designs and training verify mitigation RWPS Safety - Engineering group responsible for analysis of RWPS subsystems to ensure SSLR and subsystem designs and training verify mitigation
Final Risk	Residual Risk of the hazard occurring after successful implementation the assigned mitigation actions. The risk was analysed based on the criteria set out in section 3.3.
Remarks	Additional information, if any, to support the respective hazard entry.

4 Project Hazard Log

Attachment A contains the tabular system hazard. The columns correspond with the attributes described in Table 8.

5 Attachment A - System Project Hazard Log

3035819 Rev_N Attachment A – Project Hazard Log – DOORS /LIRR_MNR PTC/3. Technical Analysis/Hazard/Project Hazard Log – Baseline 8.0JW1

ID	Subsystem or Interfaces	Source of Hazard	Risk - Before	[redacted]	afety equirement ID	SA_LIRR_Status	Responsibility	Risk Mitigation	Remarks
HL- 2						Canceled			Replaced with PHL- 476
HL- 38	Onboard	SHA-229	IC		R_41 R_125	Closed	System Safety	IE	MAS speed will not be displayed in MTEA or MBS areas with ASC cut-out. Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program. ABS/CMB
HL- 4	Onboard	PHA-02	IC		R_11	Closed	Onboard Safety	IE	N/A
HL- 3	Onboard	PHA-01	IC		R_1 R_2 R_500 R_505	Closed	Onboard Safety	IE	Intended to cover PTCIP Hazard 1C - No enforcement MAS
HL- 21	Transponder	PHA-39	IB		R_20 R_21 R_22	Closed	Transponder Safety	IE	Coverage of LIRR PTCIP Hazard 1D - PSR

HL- 16	Office Onboard Comms	SHA-285 PHA-22	IC	R_317	Closed	System Safety	IE	Coverage of LIRR PTCIP Hazard 1D and 1E - PSR and TSR enforcement
HL- 417	Office	SHA-218	IC	R_283	Closed	Office Safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 418	Office	SHA-219	IC	R_284	Closed	Office Safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 35	Onboard WIU	SHA-226	IC	R_22 R_429 R_511	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

HL- 198	Office / Onboard	SHA-281 PHA-59	IC	[redacted]	R_55 R_56 R_57 R_392 R_470	Closed	System Safety	ID	Point TSR will be at MAS
HL- 39	Onboard Transponder	SHA-230	IC		R_42 R_43 R_44 R_45 R_537 R_549 R_552	Closed	Wayside Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

HL- 202	Operations	PHA-63	IB	[redacted]	R_190	Closed	System Safety	ID	Updated Risk Assessment
HL- 216	Office to OBC	SHA-273 SYS_IHA_09	IB		R_69 R_75 R_76 R_77 R_80 R_84 R_421 R_422 R_423 R_458	Closed	System Safety	ID	

HL- 217	Office to OBC	SYS_IHA_10	IB	R_69 R_73 R_78 R_79 R_80 R_81 R_420 R_430 R_468	Closed	System Safety	IE	
HL- 419		SHA-251	IB	R_80 R_523	Closed	Onboard safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

HL- 420		SHA-233	IB	R_286 R_500 R_506 R_517 R_526	Closed	Office Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 218	Office to OBC	SYS_IHA_11	IC	R_69 R_75 R_83 R_84 R_85	Closed	System Safety	IE	

HL- 636	Interface between Onboard and STS	SYS_IHA_12	IC	R_80 R_83 R_84 R_85	Closed	System Safety	IE	
HL- 219	TP to OBC	SYS_IHA_18	IB	R_69 R_87 R_88 R_89 R_92 R_431 R_432 R_438	Closed	System Safety	IE	

HL- 640	TP to OBC	SYS_IHA_19	IB	R_64 R_69 R_89 R_438 R_478	Closed	System Safety	IE	
HL- 637	Itnteface between OBC and STS	SYS_IHA_13	IB	R_76 R_78 R_80 R_430	Closed	System Safety	IE	

HL- 638	Interface between OBC and STS	SYS_IHA_14	IB	R_74 R_75 R_76 R_80 R_83	Closed	System Safety	IE	
HL- 633	Interface between Onboard and STS	SYS_IHA_12	IC	R_75 R_83 R_84 R_85	Closed	System Safety	IE	
HL- 634	Office	SYS_IHA_13	IB	R_78 R_85 R_430	Closed	System Safety	IE	

HL- 220	TP to OBC	SHA-261 SYS_IHA_16	IB	[redacted]	R_64 R_69 R_73 R_89 R_90 R_91 R_92 R_389 R_432	Closed	System Safety	IE	

HL- 639	TP to OBC	SYS_IHA_17	IB	R_63 R_64 R_69 R_89 R_431 R_432 R_438 R_478	Closed	System Safety	IE	
HL- 635		SYS_IHA_14	IB	R_83 R_84 R_85	Closed	System Safety	IE	

HL- 221	TP to OBC	SHA-250 SYS_IHA_15	IB	R_63 R_64 R_69 R_90 R_93 R_140 R_431 R_473 R_478 R_525 R_555 R_570 R_571	Closed	System Safety	IE	
HL- 438	Onboard	SHA-260 PHA-11	IC	R_11 R_528	Closed	Onboard Safety	IE	N/A
HL- 439	Onboard	PHA-27	IC	R_11	Closed	Onboard Safety	IE	N/A
HL- 440	Onboard	PHA-35	IC	R_11	Closed	Onboard Safety	IE	N/A
HL- 441	Onboard	PHA-41	IC	R_11	Closed	Onboard Safety	IE	N/A
HL- 507	Onboard/ Onboard- Speed Sensor	SHA-64	IC	R_11	Closed	Onboard Safety	IE	

HL- 508	Onboard	SHA-65	IC	R_139 R_572	Mitigated	Onboard Safety	IE	
HL- 509	Onboard	SHA-66	IC	R_388	Closed	Onboard Safety	IE	
HL- 510	Onboard	SHA-67	IC	R_196	Closed	Onboard Safety	IE	
HL- 511	Onboard	SHA-68	IC	R_360	Mitigated	Onboard Safety	IE	Install Manual Link needed
HL- 512	Onboard - Train Mission Switch	SHA-69	IC	R_196 R_197	Closed	Onboard Safety	IE	
HL- 515	Onboard	SHA-72	IC	R_139 R_467 R_509 R_510	Closed	Onboard Safety	IE	Coverage of LIRR PTCIP Hazard 1E - TSR
HL- 516	Office	SHA-73	IB	R_22 R_468 R_469	Closed	System Safety	IE	

HL- 517	Office	SHA-74	IB	[redacted]	R_22 R_394 R_507	Closed	System Safety	IE	
HL- 518	Onboard/ Onboard- Speed Sensor	SHA-75	IC		R_11	Closed	Onboard Safety	IE	
HL- 242	Office to Adj RR	SYS_IHA_37	IB		R_55 R_108 R_110 R_392	Mitigated	System Safety	ID	Point TSR will be at MAS
HL- 442	Onboard Onboard Parameter Programming Tool	SHA-283 PHA-12	IC		R_3 R_65 R_66 R_432	Closed	Onboard Safety	IE	Linking to Op Procedure and Installation Procedure for insallation verification to be done.

[redacted] 3035819_Rev_N_Attachment_A System

HL- 443	Onboard Transponder	PHA-28	IC	[redacted]	R_3 R_63 R_64 R_65 R_66 R_432 R_478	Closed	Onboard Safety Transponder Safety	IE	Linking to Op Procedure and Installation Procedure for insallation verification to be done.

[redacted] 3035819_Rev_N_Attachment_A System

HL- 444	On-board Transponder Maintenance	PHA-36	IB	[redacted]	R_3 R_63 R_64 R_65 R_66 R_432 R_478 R_508	Closed	Onboard Safety Transponder Safety	IE	

HL- 445	Onboard Onboard Parameter Programming Tool	PHA-42	IC	R_3 R_63 R_64 R_65 R_66 R_432 R_478 R_508	Closed	Onboard Safety	IE	N/A
HL- 446	Onboard Onboard Parameter Programming Tool	SHA-259 PHA-13	IC	R_316	Closed	Onboard Safety	IE	N/A
HL- 447	Onboard Onboard Parameter Programming Tool	PHA-29	IC	R_316	Closed	Onboard Safety	IE	N/A
HL- 448	Onboard Onboard Parameter Programming Tool	PHA-37	IC	R_316	Closed	Onboard Safety	IE	N/A

HL- 449	Onboard Onboard Parameter Programming Tool	PHA-43	IC	R_316	Closed	Onboard Safety	IE	N/A
HL- 453	WIU Onboard	PHA-15 PHA-69	IC	R_429	Closed	System Safety	IE	N/A
HL- 454	WIU Onboard	PHA-32	IC	R_429	Closed	System Safety	IE	Duplicate of 453
HL- 668					Canceled			Heading Not Applicable
HL- 498	Onboard	SHA-18	IC	R_360	Closed	Onboard Safety	ID	Link to Instal and maintenance manua
HL- 302	Onboard	SHA-01	IC	R_139	Closed	Onboard Safety	IE	
HL- 303	Onboard	SHA-02	IC	R_139 R_505 R_506 R_572	Closed	Onboard Safety	IE	
HL- 304	Onboard	SHA-03	IC	R_11	Closed	System Safety	IE	
HL- 305	Onboard	SHA-04	IC	R_187 R_188	Closed	Onboard Safety	IE	No SLR Req.
HL- 306	Onboard	SHA-07	IC	R_189	Closed	Onboard Safety	IE	

HL- 307	Onboard	SHA-08	IC	[redacted]	R_190 R_191	Closed	System Safety	IE	
HL- 308	Onboard	SHA-09	IC		R_11	Closed	System Safety	IE	
HL- 309	Transponder	SHA-10	IB		R_22 R_468 R_469	Closed	System Safety	IE	
HL- 310	Transponder	SHA-11	IB		R_22 R_324 R_537 R_549	Closed	System Safety	IE	
HL- 311	Onboard	SHA-12	IC		R_388	Closed	System Safety	IE	

HL- 312	Transponder	SHA-13	IB	R_22 R_324	Closed	System Safety	IE	
HL- 313	Transponder	SHA-14	IB	R_193 R_194	Closed	System Safety	IE	
HL- 314	Railroad	SHA-15	IB	R_195 R_505 R_506	Closed	Railroad	IE	
HL- 315	Onboard	SHA-16	IC	R_11	Closed	System Safety	IE	
HL- 316	Onboard	SHA-17	IC	R_196	Closed	System Safety	IE	
HL- 317	Onboard	SHA-19	IC	R_196 R_197	Closed	Onboard Safety	IE	
HL- 318	Onboard	SHA-20	IC	R_196	Closed	Onboard Safety	IE	

HL- 319	Onboard	SHA-21	IC	R_330	Mitigated	System Safety	IE	
HL- 325	Onboard	SHA-27	IC	R_139 R_509 R_510 R_529	Closed	System Safety	IE	
HL- 326	Office	SHA-287 PHA-89	IC	R_200 R_201 R_202	Closed	Office Safety	IE	
HL- 327	Onboard - Office	SHA-29	IC	R_430	Canceled	System Safety	IE	Duplicate of PHL-251 Duplicate of PHL-252
HL- 328	Office				Canceled			Replaced by PHL- 458
HL- 329	Onboard	SHA-31	IC	R_11 R_506	Closed	Onboard Safety	IE	
HL- 496	Onboard	SHA-05	IC	R_359	Mitigated	Onboard Safety	ID	Link to Instal and maintenance manual

HL- 497	Onboard	SHA-06	IC	R_102 R_359	Closed	Onboard Safety	ID	Link to Instal and maintenance manua
HL- 530	Onboard	SHA-90	IC	R_351 R_390 R_570 R_571	Closed	Railroad	IE	
HL- 531	Railroad	SHA-91	IB	R_69	Mitigated	Railroad	IE	Coverage of LIRR PTCIP Hazard 1B - No Speed Control
HL- 532	Onboard/ Onboard- Speed Sensor	SHA-92	IC	R_11	Closed	Onboard Safety	IE	Coverage of LIRR PTCIP Hazard 1B - No Speed Control
HL- 533	Onboard	SHA-93	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	Coverage of LIRR PTCIP Hazard 1B - No Speed Control

HL- 534	Onboard	SHA-94	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	Coverage of LIRR PTCIP Hazard 1B - No Speed Control
HL- 535	Onboard	SHA-97	IC	R_509 R_510	Closed	Onboard Safety	IE	
HL- 536	Onboard	SHA-98	IC	R_544	Closed	Onboard Safety	IE	
HL- 537	Office	SHA-100	IB	R_32 R_472	Closed	Office Safety	IE	
HL- 538	Office	SHA-101	IB	R_217	Closed	Office Safety	IE	
HL- 562	Onboard	SHA-142	IC	R_360	Mitigated	Onboard Safety	ID	Manual Link Required
HL- 564	Onboard/ Onboard- Speed Sensor	SHA-146 SHA-147	IC	R_11	Closed	Onboard Safety	IE	
HL- 565	Onboard/ Onboard- Speed Sensor	SHA-147	IC	R_11	Canceled	Onboard Safety	IE	Duplcate of HL 564

HL- 566	Onboard	SHA-148	IC	[redacted]	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 567	Onboard	SHA-149	IC		R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 570	Railroad	SHA-152	IB		R_366 R_506	Closed	Railroad	IE	
HL- 370	Onboard	SHA-138	IC		R_11 R_506	Closed	System Safety	IE	

HL- 371	Onboard	SHA-139	IC	R_478 R_570 R_571	Closed	System Safety	IE	
HL- 372	Onboard	SHA-140	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 373	Onboard	SHA-141	IC	R_196	Closed	Onboard Safety	IE	
HL- 374	Onboard	SHA-143	ICB	R_199 R_357	Closed	Onboard Safety	IE	
HL- 375	Onboard	SHA-145	IC	R_139	Closed	Onboard Safety	IE	
HL- 542	Onboard	SHA-116	IC	R_478 R_570	Closed	Onboard Safety	IE	

HL- 543	Onboard	SHA-117	IC	[redacted]	R_388	Closed	Onboard Safety	IE	
HL- 544	Onboard	SHA-118	IC		R_196	Closed	Onboard Safety	IE	
HL- 545	Onboard	SHA-119	IC		R_360	Mitigated	Onboard Safety	ID	Manual Link Required
HL- 548	Office	SHA-123	IB		R_22 R_507	Closed	System Safety	IE	
HL- 549	Office	SHA-124	IB		R_22 R_394 R_507	Closed	Office Safety	IE	
HL- 550	Onboard/ Onboard- Speed Sensor	SHA-125 SHA-126	IC		R_11	Closed	Onboard Safety	IE	
HL- 551	Onboard/ Onboard- Speed Sensor	SHA-126	IC		R_11	Canceled	Onboard Safety	IE	duplicate of 550 canceled

HL- 552	Onboard	SHA-127	IC	R_478 R_570	Closed	Onboard Safety	IE	
HL- 553	Onboard	SHA-128	IC	R_478 R_570 R_571	Closed	System Safety	IE	
HL- 556	Onboard	SHA-131	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 557	Onboard	SHA-132	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	

HL- 558	Onboard	SHA-134	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 559	Onboard	SHA-135	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 560	Railroad	SHA-136	IB	R_364	Mitigated	Railroad	IE	
HL- 561	Railroad	SHA-137	IB	R_365	Mitigated	Railroad	ID	
HL- 29	Operations	SHA-220	IB	R_29 R_30	Mitigated	System Safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program Need to confirm that TSR is held after comm loss

HL- 32	Office	SHA-223	IB		R_32 R_33 R_218 R_462	Closed	Office Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program Left open for PCC/BCC connections Mitigated for only one control center
HL- 31	Operations	SHA-222	IB		R_31 R_318	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 30	Operations	SHA-221	IB		R_29 R_30	Closed	System Safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

HL- 36	Onboard	SHA-227	IC	R_38 R_39 R_568 R_569	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program ABS/CMB
HL- 243	Office to Adj RR	SYS_IHA_38	IB	R_73 R_433 R_434	Mitigated	System Safety	IE	
HL- 392	Interface WIU to Legacy ILK	SYS_IHA_45x	IB	R_34 R_233	Mitigated	System Safety	IE	

HL- 212	WIU to OBC	SYS_IHA_01 SYS_IHA_02	IB	[redacted]	R_68 R_69 R_71 R_72 R_177	Closed	System Safety	IE	
HL- 213	WIU to OBC	PHA-85	IC		R_68 R_71 R_72 R_395 R_411	Closed	System Safety	IE	

HL- 214	WIU to OBC	SYS_IHA_03	IB	R_68 R_69 R_71 R_423	Closed	System Safety	IE	
HL- 215	WIU to OBC	SYS_IHA_04	IC	R_78 R_410 R_424 R_429	Closed	System Safety	IE	
HL- 628	WIU to OBC	SYS_IHA_05	IC	R_78 R_410 R_429	Closed	System Safety	IE	

HL- 629	Interface between Onboad and WIU	SYS_IHA_06	IB	R_78 R_410 R_429	Closed	System Safety	IE	
HL- 630	Interface between Onboard and WIU	SYS_IHA_07	IC	R_78 R_410 R_429	Closed	System Safety	IE	
HL- 631	Interface between Onboard and WIU	SYS_IHA_08	IC	R_78 R_410 R_429	Closed	System Safety	IE	
HL- 384	WIU to ATC	SYS_IHA_51	IB	R_338	Closed	Railroad	IE	

HL- 199	Operations / Transponder	PHA-60	IB	R_58 R_136	Mitigated	System Safety	IE	
HL- 200	Onboard	PHA-61	IC	R_60	Closed	System Safety	IE	
HL- 6	Onboard Onboard Parameter Programming Tool	PHA-05	IC	R_316	Closed	Onboard Safety	IE	N/A
HL- 5	Onboard Onboard Parameter Programming Tool	PHA-04	IC	R_3	Closed	Onboard Safety	IE	N/A
HL- 8	WIU Onboard	PHA-07	IC	R_426 R_429	Closed	System Safety	IE	N/A
HL- 428	Onboard Wayside	PHA-09	IC	R_310	Closed	Onboard Safety	IE	
HL- 33	Operations	SHA-224	IB	R_34 R_35	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 672	Transponder	SHA-320	IB	R_557	Mitigated	System Safety	ID	

HL- 34	Transponder Operations	SHA-225	IB	R_36 R_37	Closed	Wayside Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 222	WIU to ATC	SYS_IHA_20	IB	R_337 R_338	Closed	Wayside Safety	IE	
HL- 223	WIU to ATC	SYS_IHA_21	IB	R_338 R_440	Closed	Wayside Safety	IE	
HL- 224	WIU to ATC	SYS_IHA_22	IB	R_441	Closed	Wayside Safety	IE	Req missing at system level.
HL- 37	Onboard WIU	SHA-228	IC	R_40	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program ASC Only
HL- 203	On-Board	PHA-64	IIIB	R_62	Closed	System Safety	IIIE	

HL- 204	On-board	PHA-65	IIIB	R_11	Closed	Onboard Safety	IIIE	
HL- 205	On-board	SHA-280 PHA-66	IIIB	R_3 R_63 R_64 R_65 R_66	Closed	System Safety	IIIE	
HL- 206	On-board	PHA-67	IIIB	R_67	Mitigated	Onboard Safety	IIIE	

HL- 208	Wayside/On-Board	PHA-31	IB	R_60 R_203 R_254 R_255 R_429 R_501 R_502 R_503	Closed	System Safety	IE	
HL- 209	Railroad personnel	PHA-70	IIIB	R_7	Mitigated	System Safety	IIIE	
HL- 210	Wayside	PHA-71	IIIB	R_310	Closed	System Safety	IIIE	Must change Safety requirement ot PTS at entry
HL- 571	Onboard/ Onboard-Speed Sensor	SHA-153 SHA-161 SHA-162	IC	R_11	Closed	Onboard Safety	IE	

HL- 572	Onboard	SHA-154 SHA-163	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 573	Onboard	SHA-155 SHA-164	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 574	Onboard	SHA-156 SHA-157	IC	R_196	Closed	Onboard Safety	IE	Manual Link Required
HL- 575	Onboard	SHA-157	IC	R_360	Mitigated	Onboard Safety	ID	Duplate of HL 574
HL- 578	Onboard	SHA-160	IC	R_139 R_509 R_510	Closed	Onboard Safety	IE	
HL- 579	Onboard/ Onboard- Speed Sensor	SHA-161	IC	R_11	Canceled	Onboard Safety	IE	Duplcate of HL 571

HL- 580	Onboard/ Onboard- Speed Sensor	SHA-162	IC	R_11	Canceled	Onboard Safety	IE	Duplcate of HL 571
HL- 581	Onboard	SHA-163	IC	R_139	Canceled	Onboard Safety	IE	Duplcate of HL 572
HL- 582	Onboard	SHA-164	IC	R_388	Canceled	Onboard Safety	IE	Duplcate of HL-573
HL- 258	Transponder	SHA-203	IB	R_89 R_432	Closed	System Safety	IE	
HL- 259	Transponder	SHA-204	IB	R_138	Closed	System Safety	IE	
HL- 260	Onboard	SHA-205	IC	R_139	Closed	Onboard Safety	IE	
HL- 261	Onboard	SHA-206	IC	R_140	Mitigated	System Safety	IE	
HL- 201	Transponder,	PHA-62	IB	R_61	Closed	System Safety	IE	
HL- 12	Operations Onboard	PHA-18	IIC	R_8 R_9 R_10 R_498	Mitigated	System Safety	IIE	Coverage of LIRR PTCIP Hazard 1B - No Speed Control SRAC to RR for Operations and yard Signaling MNR - Yard TP not installed at this time. SRAC Issued. LIRR TP Installed and tested. SRAC still applicable for Yard Signaling.
HL- 13	Onboard	PHA-19	IC	R_11 R_12	Closed	Onboard Safety	IE	Coverage of LIRR PTCIP Hazard 1A - No Signal system Yard mode speed is function of Cab signaling and not strictly ACSES.

HL- 14	Comms	PHA-20	IIIB		R_147	Mitigated	Comms Safety	IIID	Inspection of Comms Design Modified Severity as this would only cause train damage.
HL- 46	Transponder	SHA-232	IB		R_50 R_51 R_52 R_53 R_466	Mitigated	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 17	Onboard	PHA-23	IIID		R_15	Closed	System Safety	IIIE	Insepction of Design Mitigatin is via First Article Inspection Reports
HL- 18	WIU Comms Transponder	PHA-24	IIIB		R_16 R_17 R_556	Closed	System Safety	IIIE	Inspection of Equipment Design First Article Inspection and PICO reports

HL- 585	Onboard	SHA-167	IC	R_478	Closed	Onboard Safety	IE	
HL- 586	Office	SHA-168	IB	R_363	Closed	Office Safety	IE	
HL- 587	Office	SHA-169	IB	R_129	Mitigated	Office Safety	ID	
HL- 588	Onboard	SHA-170	IC	R_139	Closed	Onboard Safety	IE	
HL- 539	Onboard	SHA-112	IC	R_478 R_570 R_571	Closed	Office Safety	IE	Coverage of LIRR PTCIP Hazard 9B - Train to Road Vehicle Collilsion - H'way activiation failure
HL- 540	Office	SHA-113	IB	R_363	Closed	Office Safety	IE	Coverage of LIRR PTCIP Hazard 9B - Train to Road Vehicle Collilsion - H'way activiation failure
HL- 541	Office	SHA-114	IB	R_129	Mitigated	Office Safety	ID	Coverage of LIRR PTCIP Hazard 9B - Train to Road Vehicle Collilsion - H'way activiation failure

HL- 19	Onboard Office Operations	PHA-25	IC		R_18 R_19 R_155 R_521 R_545 R_546	Closed	System Safety	IE	MNR - Stop and Proceed with restriction limited use only stop and proceed to be used. Note: no crossings P2. LIRR Ok
HL- 625	Comms	RR DEDM Installation Risk Assessment	IIIC		R_418 R_419	Closed	Comms Safety	IIID	DE/DM train type only
HL- 626	Comms	SHA-252	IIIC		R_418 R_419	Closed	Comms Safety	IIID	DE/DM train type only
HL- 589	WIU	SHA-172	IIB		R_221 R_367 R_368	Closed	System Safety	IIE	

HL- 590	Office	SHA-173	IIB	R_369 R_370 R_490	Closed	Office Safety	IIE	
HL- 591	Transponder	SHA-175	IIB	R_371 R_372	Closed	Transponder Safety	IIE	
HL- 592	Office	SHA-176	IIB	R_221 R_227	Closed	Onboard Safety	IIE	
HL- 593	WIU	SHA-178	IIB	R_373	Closed	WIU Safety	IIE	
HL- 594	Office	SHA-179	IIB	R_374 R_375	Closed	Office Safety	IIE	Manual Link Required
HL- 595	Comms	SHA-180	IIB	R_376 R_377	Closed	Comms Safety	IIE	Manual Link Required
HL- 596	Transponder	SHA-181	IIB	R_412	Closed	Transpodner Safety	IIE	Manual Link Required
HL- 597	RWPS	SHA-182	IIB	R_378 R_379	Closed	RWPS Safety	IIE	Manual Link Required

HL- 598	Onboard	SHA-184	IC	R_380	Closed	OBC Safety	IE	
HL- 599	WIU	SHA-185	IB	R_381	Closed	WIU Safety	IE	
HL- 600	Office	SHA-186	IB	R_382	Closed	Office Safety	IE	
HL- 601	Comms	SHA-187	IB	R_383	Closed	Comms Safety	IE	
HL- 602	Transponder	SHA-188	IB	R_384	Closed	Transponder Safety	IE	
HL- 603	RWPS	SHA-189	IB	R_385 R_463	Closed	RWPS Safety	IE	
HL- 377	Comms	SHA-174	IIB	R_224 R_225	Closed	Comms Safety	IIE	
HL- 620	Transponder	TP IHA 04	IIIC	R_403	Closed	Transponder Safety	IIID	PTE manual to be reviewed for mitigation.

HL- 378	Onboard WIU Office RWPS Transponder Comms	SHA-177	IIC	R_226 R_377	Closed	System Safety	IIE	Manual Link Neede
HL- 379	Onboard WIU Office RWPS Transponder Comms	SHA-183	IC	R_227 R_228	Mitigated	System Safety	IE	Manual Link Neede
HL- 15	Comms	PHA-21	IIIB	R_13	Closed	Comms Safety	IIID	Mast / Antennae is Railroad scope need to discuss Inspection of Coms Design
HL- 24	System	PHA-47	IIB	R_23 R_24 R_25	Closed	System Safety	IIE	Radio has passed FCC Licensing. ACSES handheld units are COTS and are FCC compliant.
HL- 25	System	PHA-48	IIB	R_26 R_553	Closed	System Safety	IIE	N/A
HL- 26	System	PHA-49	IIB	R_27	Mitigated	System Safety	IIE	N/A
HL- 27	System	PHA-50	IIB	R_28 R_383	Closed	System Safety	IIE	Inspection of Design

HL- 28	System	PHA-51	IIB	R_383	Closed	System Safety	IIE	N/A
HL- 9					Canceled			Repalced with PHL- 10, 448, and 455
HL- 10	Operations	PHA-08	IB	R_7	Mitigated	System Safety	IE	N/A
HL- 40	Onboard	HFA-1	IC	R_46	Mitigated	Onboard Safety	IE	

HL- 47	Office	HFA-3	IB	R_54	Mitigated	Office Safety	IE	
HL- 41	Onboard Office Transponder WIU Communication RWPS	HFA-2	IC	R_34	Mitigated	System Safety	IE	
HL- 44	Onboard	SHA-231	IIIC	R_47 R_48 R_49	Mitigated	System Safety	IIIE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 407	WIU Onboard				Canceled			Combined with PHL- 20
HL- 22					Canceled			Replaced by PHL- 480

HL- 11					Canceled			Replaced with PHL- 428, 451, and 456
HL- 23					Canceled			Replaced by PHL- 472
HL- 43					Canceled			Deleted from PHA during review.
HL- 45					Canceled			Transfer to appropriate subsystem Hazard Log
HL- 211					Canceled			Replaced by PHL- 473
HL- 225					Canceled			Deleted as interface to Legacy interlocking is parrallel only.
HL- 226					Canceled			Deleted as Interface is Parrallel
HL- 227					Canceled			Deleted as interface is Parallel.
HL- 228	OBC to Train	SHA-276 SYS_IHA_23	IB	R_94 R_97 R_263	Closed	Onboard Safety	IE	
HL- 229	OBC to Train	SHA-276 SYS_IHA_24	IB	R_97 R_189 R_263	Closed	Onboard Safety	IE	
HL- 230	OBC to Train	SHA-276 SYS_IHA_25	IB	R_95 R_97 R_263	Closed	Onboard Safety	IE	

HL- 231	OBC to Train	SHA-276 SYS_IHA_26	IB	R_95 R_97 R_263	Closed	Onboard Safety	IE	
HL- 232	OBC to Train	SHA-276 SYS_IHA_27	IB	R_96 R_97 R_263	Closed	Onboard Safety	IE	
HL- 669	OBC	SHA-265	IB	R_11 R_106 R_139 R_188 R_479 R_528	Closed	Onboard Safety	IE	

HL- 233	OBC to Train	SHA-264 SYS_IHA_28	IB	R_96 R_97 R_263	Closed	Onboard Safety	IE	
HL- 234	OBC to Train	SYS_IHA_29	IB	R_97 R_98 R_263	Closed	Onboard Safety	IE	
HL- 235	OBC to Train	SYS_IHA_30	IB	R_97 R_98 R_263	Closed	Onboard Safety	IE	
HL- 236	OBC to Train	SYS_IHA_31	IB	R_97 R_99 R_263 R_415	Closed	Onboard Safety	IE	

HL- 237	OBC to Train	SYS_IHA_32	IB	R_97 R_99 R_263 R_415	Closed	Onboard Safety	IE	
HL- 238	OBC to Train	SHA-266 SYS_IHA_33	IB	R_97 R_100 R_101 R_263	Closed	Onboard Safety	IE	
HL- 239	OBC to Train	SYS_IHA_34	IB	R_97 R_100 R_101 R_263	Closed	Onboard Safety	IE	
HL- 240	OBC to Train	SYS_IHA_35	IB	R_102	Closed	Onboard Safety	IE	

HL- 241	OBC to Train	SYS_IHA_36	IB	[redacted]	R_103 R_104 R_105 R_106	Closed	Onboard Safety	IE	

HL- 244	RWPS to Office	SYS_IHA_39	IB	[redacted]	R_111 R_112 R_113 R_117 R_118 R_435 R_443 R_444 R_461	Closed	System Safety	IE	

HL- 245	RWPS to Office	SYS_IHA_40	IB	[redacted]	R_73 R_115 R_116 R_129 R_227 R_436 R_444 R_449 R_450 R_465	Closed	System Safety	IE	
HL- 246	EIC to RWPS	PHA-77 SYS_IHA_41	IC		R_112 R_117 R_118 R_119	Closed	System Safety	ID	

HL- 247	EIC to RWPS	PHA-78 SYS_IHA_42	IC	[redacted]	R_129 R_436 R_437 R_444 R_452 R_453 R_462	Closed	System Safety	ID	

HL- 248	Train Engineer to OBC	SHA-270 SYS_IHA_43	IB	[redacted]	R_121 R_122 R_123 R_125 R_126 R_496	Closed	System Safety	IE	
HL- 249	Train Engineer to OBC	SHA-268 SYS_IHA_44	IB		R_121 R_122 R_123 R_125 R_126 R_496	Closed	System Safety	IE	

HL- 250	Train Engineer to OBC	SYS_IHA_45	IVB	R_121 R_125 R_126 R_496	Closed	System Safety	IVE	
HL- 251	Dispatcher to Office	SYS_IHA_46	IB	R_107 R_128 R_129 R_130 R_131 R_435 R_443	Closed	System Safety	ID	

HL- 641	OBC and Transponder Scanner	SYS_IHA_58	IB	R_63 R_69 R_446	Closed	Onboard Safety	IE	
HL- 252	Dispatcher to Office	SYS_IHA_47	IB	R_107 R_129 R_130 R_132	Closed	System Safety	ID	
HL- 253	Comms	SHA-198	IB	R_133 R_134	Mitigated	System Safety	IE	
HL- 437	Office				Canceled			Replaced by PHL- 481
HL- 455	Operations	PHA-16	IB	R_7	Mitigated	System Safety	IE	N/A

HL- 456	Onboard Wayside	PHA-17	IC		R_310 R_499 R_508 R_512 R_522 R_547	Closed	Onboard Safety	IE	Open for MNR until Yard TP installed
HL- 457	Dispatcher to Office Office (STS)	Sys-OHA-10	IB		R_317 R_454	Closed	System Safety	ID	

HL- 458	Dispatcher to Office Office	SHA-30	IB	R_318 R_519 R_520	Closed	System Safety	IE	
HL- 459	Onboard	PHA-10	IC	R_1 R_2 R_5 R_505 R_506	Closed	Onboard Safety	IE	MNR only

HL- 670	Onboard	SHA-277	IC	[redacted]	R_2 R_531 R_532 R_535	Closed	Onboard Safety	IE	

HL- 460	Onboard	PHA-34 PHA-26	IC	[redacted]	R_1 R_2 R_500 R_505 R_506	Closed	Onboard Safety	IE	N/A

HL- 461	Onboard	PHA-40	IC	[redacted]	R_1 R_2 R_500 R_505 R_506	Closed	Onboard Safety	IE	N/A
HL- 462	Onboard	SHA-272 PHA-81	IC		R_319 R_320 R_500 R_539	Closed	Onboard Safety	IE	N/A

HL- 464	Wayside/On-Board	PHA-69	IIIB	R_429	Canceled	System Safety	IIIE	Duplicate of HL-453
HL- 465	Onboard and STS	SYS_IHA_59	IC	R_69 R_74 R_75 R_76 R_78 R_81 R_430 R_437	Closed	System Safety	IE	EIC and RWPS designs and requiremetns not finalized
HL- 466	OBC to Decelerometer	SHA-262 SYS_IHA_60	IB	R_447 R_448	Closed	System Safety	IE	

HL- 467	Wayside	Sys-OHA-13	IB	R_34 R_157 R_321 R_322	Mitigated	System Safety	ID	
HL- 468	Office	SHA-28	IB	R_22 R_323 R_324	Closed	Office Safety	IE	
HL- 469	WIU	SHA-48	IB	R_22 R_512 R_522	Closed	Wayside Safety	IE	
HL- 470	WIU Onboard Operations	SHA-56	IC	R_325	Closed	Wayside safety	IE	

HL- 471	On-Board	PHA-26	IB	R_1 R_2 R_500 R_505 R_506	Closed	Onboard Safety	IE	Duplcate of HL-460
HL- 472	Office/On-Board Operations	PHA-46	IC	R_387 R_430	Closed	Office Safety	IE	

HL- 473	Operations	PHA-72 SYS_OHA_13	IC		R_34 R_157 R_159 R_321 R_322	Mitigated	Railroad	ID	
HL- 474	Transponder Office Onboard	SHA-286 PHA-73	IC		R_63 R_64 R_328 R_329 R_330 R_331 R_332 R_333 R_334 R_335 R_409 R_478 R_506	Closed	Onboard Safety Transpodner Safety	IE	Removed Transponder Message dulication. Current OBC does not enforce Speed restrictions after a missed TP so not needed.

HL- 475	Onboard Wayside ATC Interlocking	PHA-74	IC	R_204 R_313 R_336 R_337 R_338 R_501 R_502 R_503	Closed	Wayside Safety Onboard Safety	IE	
HL- 476	Operations	PHA-75	IB	R_263	Closed	Railroad	ID	
HL- 477	Operations Office	SHA_288 PHA-76	IC	R_339 R_340	Mitigated	Railroad	IE	
HL- 478	Onboard	PHA-82	IC	R_99	Closed	Onboard Safety	IE	

HL- 479	Onboard	PHA-86	IC	[redacted]	R_97 R_100 R_101	Closed	Onboard Safety	IE	No such requirment.
HL- 480	Transponder	PHA-92	IC		R_42 R_43	Closed	Transponder Safety	ID	
HL- 481	Onboard Office WIU RWPS	SHA-271 PHA-93	IC		R_63 R_64 R_82 R_101 R_328 R_330 R_331 R_336 R_341 R_342 R_343 R_344 R_345	Closed	Wayside Safety Onboard Safety	IE	

HL- 482	Training	Sys-OHA-52	IC	R_346	Mitigated	Wayside Safety	ID	Need Link to Maint Manual
HL- 483	Railroad	Sys-OHA-53	IIC	R_368	Mitigated	Wayside Safety	IID	
HL- 484	Training	Sys-OHA-54	IIIC	R_347	Mitigated	Wayside Safety	IIID	Need Link to Maint Manual
HL- 485	Training	Sys-OHA-55	IIIC	R_348	Mitigated	Wayside Safety	IIID	Need Link to Maint Manual
HL- 486	Railroad	Sys-OHA-56	IC	R_349	Mitigated	Railroad	ID	
HL- 487	Railroad	Sys-OHA-57	IC	R_47 R_350 R_551	Mitigated	Railroad	ID	Need Link to Maint Manual

HL- 488	Railroad	Sys-OHA-58	IC	R_351 R_478 R_570 R_571	Closed	Railroad	ID	
HL- 489	Railroad	SHA-274 Sys-OHA-59 Sys-OHA-62	IC	R_128 R_352 R_530	Closed	Railroad	ID	Coverage of LIRR PTCIP Hazard 1E -TSR

HL- 490	Railroad	Sys-OHA-60	IC	R_353	Mitigated	Railraod	ID	
HL- 491	Railroad	Sys-OHA-61	IC	R_354 R_500	Mitigated	Railraod	ID	
HL- 492	Office to Dispatcher	SYS_IHA_48	IB	R_129 R_355 R_356 R_435	Closed	System Safety	ID	

HL- 493	Interface Onboard to Transponder	SYS_IHA_49	IC	R_63 R_64 R_438 R_478 R_570 R_571	Closed	System Safety	IE	
HL- 495	OBC to PTS PB	SYS_IHA_57	IB	R_358	Closed	Onboard Safety	IE	
HL- 499	Onboard/ Onboard- Speed Sensor	SHA-40	IC	R_11	Closed	Onboard Safety	IE	
HL- 500	Onboard	SHA-41	IC	R_478 R_570	Closed	Onboard Safety	IE	

HL- 501	Onboard	SHA-42	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 502	Railroad	SHA-59	IB	R_69	Mitigated	System Safety	ID	
HL- 503	Onboard	SHA-60	IC	R_139	Closed	Onboard Safety	IE	
HL- 504	Onboard	SHA-61	IC	R_388	Closed	Onboard Safety	IE	
HL- 505	Onboard	SHA-62	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 506	Onboard	SHA-63	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 519	Onboard/ Onboard- Speed Sensor	SHA-76	IC	R_11	Closed	Onboard Safety	IE	

HL- 520	Onboard	SHA-77	IC	R_478 R_570	Closed	Onboard Safety	IE	
HL- 521	Onboard	SHA-78	IC	R_478 R_570	Closed	Onboard Safety	IE	
HL- 524	Onboard	SHA-81	IC	R_139	Closed	Onboard Safety	IE	
HL- 525	Onboard	SHA-82	IC	R_388 R_478 R_570	Closed	Onboard Safety	IE	
HL- 526	Onboard	SHA-83	IC	R_139 R_478 R_570	Closed	Onboard Safety	IE	

HL- 527	Onboard	SHA-84	IC	R_478 R_570	Closed	Onboard Safety	IE	
HL- 528	Onboard	SHA-85	IC	R_478 R_570	Closed	Onboard Safety	IE	
HL- 529	Onboard	SHA-86	IC	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 604	Onboard	SHA-190	IC	R_386 R_387	Closed	Onboard Safety	IE	
HL- 605	Onboard	SHA-191	IC	R_388	Closed	Onboard Safety	IE	
HL- 606	Onboard	SHA-192	IC	R_388	Closed	Onboard Safety	IE	

HL- 607	Onboard	SHA-193	IC	[redacted]	R_389 R_427	Closed	Transponder Safety	IE	
HL- 608	Transponder	SHA-194	IB		R_90 R_390 R_391	Closed	Onboard Safety	IE	
HL- 619	Onboard	TP IHA 02	IC		R_401 R_402	Closed	Onboard Safety	IE	Scanner installation design must account for wheel diameter range.
HL- 609	Office	SHA-197	IB		R_392 R_393	Closed	Railroad	IE	
HL- 610	Onboard	SHA-207	IC		R_11	Closed	Onboard Safety	ID	ABS / CMB
HL- 611	Onboard	SHA-208	IC		R_388 R_478	Closed	Onboard Safety	ID	ABS / CMB

HL- 613	Onboard	SHA-213	IC	R_139 R_509 R_510	Closed	Onboard Safety	ID	ABS / CMB
HL- 614	Onboard	SHA-214	IC	R_388	Closed	Onboard Safety	ID	ABS / CMB
HL- 615	Onboard	SHA-215	IC	R_203 R_394	Closed	Onboard Safety	ID	ABS / CMB
HL- 616	WIU to OBC	SYS_IHA_02	IB	R_68 R_69 R_71 R_72 R_395	Closed	System Safety	IE	

HL- 617	Onboard	SHA-235	IC		R_69 R_396 R_397	Closed	Onboard Safety	ID	Addresses S9 from Safety Integrated Issues List Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 254	Transponder	SHA-199	IB		R_135 R_136	Closed	System Safety	ID	
HL- 393	WIU - Legacy ILK	SYS_IHA_51	IC		R_234	Closed	System Safety	IE	
HL- 394	WIU - Interface to Points and Signals	SHA-278 SYS_IHA_50	IB		R_34 R_235 R_236 R_237 R_238 R_239 R_516	Closed	Wayside Safety System Safety	IE	

HL- 395	WIU - Interface to Points or Signals	SYS_IHA_52	IB	R_34 R_235 R_236 R_237 R_238 R_239 R_516	Mitigated	System Safety	IE	
HL- 396	WIU - WIU Interface	SYS_IHA_54	IB	R_238 R_242	Closed	Wayside Safety System Safety	IE	
HL- 397	OBC to ADU Interface	SYS_IHA_55	IB	R_243 R_244	Closed	Onboard Safety	IE	
HL- 643	WIU - Legacy Interlocking	SYS_IHA_53	IB	R_235 R_236 R_237 R_238 R_239 R_516	Mitigated	Wayside Safety	IE	

HL- 644	OBC - WIU	SHA-279 SYS_IHA_56	IB	R_78 R_410 R_429 R_476	Closed	OBC	IE	Exported from WIU need to link
HL- 255	Transponder	SHA-200	IB	R_36	Closed	System Safety	IE	
HL- 256	Transponder	SHA-201	IB	R_89 R_432	Closed	System Safety	IE	
HL- 262	Railroad	SHA-216	IB	R_141	Mitigated	System Safety	ID	
HL- 263	Transponder	SHA-217	IB	R_22 R_142	Mitigated	System Safety	IE	
HL- 264					Canceled			Deleted – No train on LIRR with Selector Switch
HL- 265	Railroad	Sys-OHA-02	IB	R_330	Mitigated	System Safety	ID	

HL- 266	On-board (Yard area)	Sys-OHA-03	IIB	R_143 R_144 R_145 R_498	Canceled	System Safety	IID	Removed from System OHA in Rev _A. Yard Excluded from Analysis Coverage of LIRR PTCIP Hazard 1A - Overspeed - No signal ssystem
HL- 267	Wayside	Sys-OHA-04	IB	R_146 R_147 R_148	Mitigated	System Safety	ID	No SLR
HL- 268	Comms	Sys-OHA-05	IIB	R_149 R_150	Mitigated	System Safety	IID	No SLR
HL- 269	Comms	Sys-OHA-06	IIIB	R_151 R_152 R_153	Mitigated	System Safety	IIID	Manual Link Required

HL- 270	Wayside/Train	Sys-OHA-07	IB	R_154	Mitigated	System Safety	ID	Installation Req
HL- 271	Wayside	Sys-OHA-08	IB	R_155	Mitigated	System Safety	ID	
HL- 272	wayside/office	Sys-OHA-09	IB	R_156	Mitigated	System Safety	ID	
HL- 273					Canceled			Duplicate of PHL-251
HL- 274	Wayside/office /Onboard	Sys-OHA-11	IC	R_34	Mitigated	System Safety	ID	Training Req
HL- 275	Office Wayside Transpponer Onboard	Sys-OHA-12	IC	R_190	Mitigated	System Safety	ID	
HL- 423		SHA-236	IB	R_291	Closed	Onboard Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 276	Wayside	PHA-79	IC	R_157 R_158 R_159 R_340	Mitigated	System Safety	IE	
HL- 277	On-Board	Sys-OHA-14	IB	R_160	Mitigated	System Safety	ID	

HL- 278	Office Onboard	Sys-OHA-15	IIC	R_162	Mitigated	System Safety	IID	
HL- 279	Office	Sys-OHA-16	IIB	R_163	Mitigated	System Safety	IID	
HL- 280	Office Onboard	Sys-OHA-17	IIC	R_162	Mitigated	System Safety	IID	
HL- 281	On-Board	SHA-263 Sys-OHA-18	IIB	R_165 R_475	Canceled	System Safety	IID	Removed from System OHA Rev _A.
HL- 282	On-Board	Sys-OHA-19	IIB	R_165	Mitigated	System Safety	IID	
HL- 283	Office	Sys-OHA-20	IIB	R_166	Mitigated	System Safety	IID	
HL- 284	Office	Sys-OHA-21	IIB	R_166	Mitigated	System Safety	IID	
HL- 285	Onboard	Sys-OHA-22	IIC	R_162	Mitigated	System Safety	IID	
HL- 286	Office Onboard	Sys-OHA-23	IIC	R_167 R_168	Mitigated	System Safety	IID	Covers shoving moves I.E. train operatored from cab not in the direction of travel.
HL- 287	Onboard	Sys-OHA-24	IIC	R_169 R_554	Mitigated	System Safety	IID	

HL- 288					Canceled			Combined to ACSES Exit – No specific Track End in ACSES territory
HL- 289	Onboard	Sys-OHA-26	IIC	R_170 R_171	Mitigated	System Safety	IID	Installation Training
HL- 290	Comms	Sys-OHA-27	IIB	R_34 R_172	Mitigated	System Safety	IID	Installation Training
HL- 291	Onboard	Sys-OHA-28	IIC	R_173	Mitigated	System Safety	IID	
HL- 292	Onboard	Sys-OHA-29	IIC	R_176 R_387	Canceled	System Safety	IID	Manual Link Needed Removed From System _HA Rev _A.
HL- 293	Onboard	Sys-OHA-30	IIC	R_330	Mitigated	System Safety	IID	
HL- 294					Canceled			Hazard deleted from Sys OHA
HL- 295	Onboard	Sys-OHA-32	IC	R_136 R_177	Mitigated	System Safety	ID	

HL- 296	Office	Sys-OHA-33	IIB	R_179 R_180	Canceled	System Safety	IID	Removed from System _OHA Rev _A.
HL- 297	Office	Sys-OHA-34	IIB	R_181	Mitigated	System Safety	IID	
HL- 298	Onboard	Sys-OHA-35	IC	R_182	Mitigated	System Safety	ID	
HL- 299	Onboard	Sys-OHA-36	IB	R_183	Mitigated	System Safety	ID	
HL- 300	Onboard WIU Transponder Office RWPS Comms	Sys-OHA-37	IC	R_34 R_184 R_185 R_464	Mitigated	System Safety	ID	
HL- 301	Onboard	Sys-OHA-38	IIC	R_186	Mitigated	System Safety	IID	Removed from System OHA Rev _A - No Door OPeration. Opened again due to concerns raised by LIRR on Accurate stop
HL- 398	Onboard	Sys-OHA-39	IIIC	R_245 R_246	Mitigated	System Safety	IIIE	Maunaul Link Needed

HL- 399	Onboard	Sys-OHA-40	IC	R_247	Mitigated	Onboard Safety	IE	Manual Link Needed
HL- 400	Onboard	Sys-OHA-41	IIIIC	R_248	Mitigated	Onboard Safety	IIIIE	Manual Link Neede
HL- 401	Onboard	Sys-OHA-42	IC	R_249 R_250	Mitigated	Onboard Safety	ID	Manual Link Neede
HL- 402	Onboard	Sys-OHA-43	IC	R_249	Mitigated	Onboard Safety	ID	Manual Link Neede
HL- 403	Onboard	Sys-OHA-44	IC	R_249	Mitigated	Onboard Safety	ID	Manual Link Neede
HL- 404	Onboard	Sys-OHA-45	IC	R_251	Closed	Onboard Safety	ID	Manual Reference Needed
HL- 405	Onboard	Sys-OHA-46	IC	R_34 R_252	Mitigated	Onboard Safety	ID	Manual Link Neede
HL- 406	Onboard	Sys-OHA-47	IC	R_249	Mitigated	Onboard Safety	ID	Manual Link Neede
HL- 671	Transponder	SHA_301	IIIC	R_558	Mitigated	Transponder Safety	IIID	
HL- 408	Onboard	Sys-OHA-48	IC	R_34 R_253	Mitigated	Onboard Safety	ID	Manual Link Neede

HL- 410	Onboard	Sys-OHA-49	IC	R_258 R_259 R_260 R_261	Mitigated	Onboard Safety	ID	Link to Cm Process
HL- 409	Onboard	SHA-258 Sys-OHA-50	IC	R_254 R_255 R_256 R_257	Mitigated	Onboard Safety	ID	
HL- 411	Onboard	SHA-275 Sys-OHA-51	IC	R_262 R_263	Mitigated	Onboard Safety	ID	RR to address departure test requirements.
HL- 330	Onboard	SHA-32	IC	R_139 R_474 R_548	Closed	Onboard Safety	IE	
HL- 331	Onboard	SHA-33	IC	R_11	Closed	Onboard Safety	IE	

HL- 332	Onboard	SHA-34	IC	R_478 R_570 R_571	Closed	System Safety	IE	
HL- 333	Onboard	SHA-35	IC	R_478 R_570 R_571	Closed	System Safety	IE	
HL- 334	Transponder	SHA-36	IB	R_22 R_142 R_324 R_514	Closed	Transponder Safety	IE	
HL- 335	Transponder	SHA-38	IB	R_194	Closed	Transponder Safety	IE	Manual Link Neede

HL- 336	Onboard	SHA-39	IC	R_203 R_324	Mitigated	Onboard Safety	IE	Manual Link Neede
HL- 337	Onboard	SHA-43	IC	R_139	Closed	Onboard Safety	IE	
HL- 338	Onboard	SHA-44	IC	R_203	Closed	Onboard Safety	IE	
HL- 341	WIU	SHA-47	IB	R_204 R_511 R_512 R_522	Closed	Wayside Safety	IE	
HL- 342	WIU	PHA-90	IC	R_205 R_206 R_207	Closed	Wayside Safety	IE	

HL- 343	WIU	SHA-49	IB	R_204 R_504 R_511	Closed	Wayside Safety	IE	
HL- 344	WIU	SHA-50	IB	R_208	Closed	System Safety	IE	
HL- 345	Onboard	SHA-51	IC	R_410 R_511 R_523	Closed	Onboard Safety	IE	

HL- 346	Onboard	SHA-52	IC	R_478 R_570 R_571	Closed	System Safety	IE	
HL- 347	Transponder	SHA-53	IB	R_22 R_324	Closed	Transponder Safety	IE	
HL- 348	Onboard	SHA-54	IC	R_388	Closed	System Safety	IE	
HL- 349	Railroad	SHA-55	IB	R_209 R_534	Closed	Railroad	IE	

HL- 350	WIU Onboard Operations	SHA-269 PHA-88	IC	[redacted]	R_210 R_211 R_212 R_325 R_477 R_497	Closed	Wayside safety	IE	ASC Only

HL- 351	Railroad	SHA-57	IB	R_86 R_540 R_541 R_542	Closed	Railroad	IE	ASB / CMB
HL- 352	Onboard	SHA-58	IC	R_214 R_215	Closed	System Safety	IE	
HL- 353	Railroad	SHA-87	IB	R_69	Mitigated	System Safety	ID	
HL- 354	Onboard	SHA-88	IC	R_11 R_506	Closed	Onboard Safety	IE	

HL- 355	Railroad	SHA-89	IB	R_478 R_570 R_571	Closed	Onboard Safety	IE	
HL- 356	Comms	SHA-95	IB	R_216	Mitigated	System Safety	IE	No SLR Req
HL- 357	Comms	SHA-96	IB	R_216	Mitigated	System Safety	IE	No SLR Req
HL- 358	Office	SHA-99	IB	R_217 R_518 R_521	Closed	Office Safety	IE	

HL- 359	Office	SHA-103	IB	[redacted]	R_128 R_129	Mitigated	Office Safety	ID	To reduce system Risk noted that Paper TSR process is not be abondanded and that this process can be used to check the TSRs within the system to detect manual entry errors as well as UIS errors.

HL- 360	Office	SHA-104	IB	[redacted]	R_128 R_129	Mitigated	Office Safety	ID	To reduce system Risk noted that Paper TSR process is not be abondanded and that this process can be used to check the TSRs within the system to detect manual entry errors as well as UIS errors.

HL- 361	Office	SHA-105	IB	[redacted]	R_128 R_129	Mitigated	Office Safety	ID	To reduce system Risk noted that Paper TSR process is not be abondanded and that this process can be used to check the TSRs within the system to detect manual entry errors as well as UIS errors.
HL- 362	Office	SHA-106	IB		R_118 R_119	Mitigated	Office Safety	IE	
HL- 422	Office	SHA-237	IB		R_289 R_290 R_533	Closed	Office Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

HL- 363	Onboard	SHA-107	IC	R_15	Closed	Onboard Safety	IE	
HL- 364	Transponder, Comms	SHA-108	IB	R_220	Closed	Transponder Safety	IE	
HL- 365	Onboard	SHA-109	IC	R_15	Closed	Onboard Safety	IE	
HL- 366	Transponder, Comms	SHA-110	IB	R_220	Closed	Transponder Safety	IE	
HL- 367	Railroad	SHA-111	IB	R_155	Mitigated	System Safety	ID	
HL- 368	Onboard	SHA-115	IC	R_11 R_506	Closed	System Safety	IE	
HL- 369	Onboard	SHA-122	IC	R_139	Closed	System Safety	IE	
HL- 376	Onboard	SHA-171	IIC	R_221 R_222 R_223	Closed	Onboard Safety	IIE	
HL- 380	Comms Office Railroad	SHA-195	IB	R_229 R_230 R_231	Mitigated	System Safety	IE	

HL- 618		SHA-238	IB	R_398 R_399	Closed	Office Safety	IE	
HL- 381	Office	SHA-196	IB	R_55 R_392	Closed	Railroad	ID	Point TSR will be at MAS Speed.
HL- 382	Office	SHA-239	IB	R_47 R_232 R_494 R_495 R_550	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 385	WIU				Canceled			Transfer to appropriate subsystem Hazard Log
HL- 386	WIU				Canceled			Transfer to appropriate subsystem Hazard Log
HL- 387	WIU				Canceled			Transfer to appropriate subsystem Hazard Log
HL- 388	WIU				Canceled			Transfer to appropriate subsystem Hazard Log
HL- 389	WIU				Canceled			Transfer to appropriate subsystem Hazard Log

HL- 390	WIU				Canceled			Transfer to appropriate subsystem Hazard Log
HL- 391	WIU				Canceled			Transfer to appropriate subsystem Hazard Log
HL- 412	RWPS	SHA-240	IC	R_264 R_265 R_266 R_267 R_451 R_455 R_456 R_457 R_460	Closed	RWPS Safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

HL- 413	Transponder	SHA-241	ID	[redacted]	R_268 R_269 R_298 R_335 R_396	Closed	Transponder Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 414	Comms	System Vulnerability Assessment	IC		R_270 R_271 R_272 R_273 R_274 R_275 R_276 R_277 R_278 R_437 R_471	Closed	System Safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

HL- 415	OBC	SHA-242	IC	R_279 R_513 R_538	Closed	Onboard Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 416	OBC	SHA-243	IC	R_280 R_281 R_282 R_517	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 421	Office	SHA-249	ID	R_287 R_288	Closed	Office Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program Mitigated for only one control center

HL- 425	System	SHA-248	IC	R_295 R_296 R_297	Mitigated	System Safety Onboard	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 424	Wayside	SHA-260	IC	R_292 R_293 R_294 R_543	Closed	Wayside Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program ABS / CMB
HL- 426	Wayside	SHA-247	IC	R_298 R_299	Closed	Transponder Safety Onboard Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program MBS
HL- 427	Comms	System Vulnerability Assessment	IC	R_429 R_430 R_485	Closed	Comms Safety	IE	

HL- 429	Onboard	SHA-246	IC	R_300 R_301 R_302	Closed	Transponder Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 430	Onboard	SHA-244	IC	R_304 R_305 R_524 R_538	Closed	Onboard Safety	IE	Modified from System Engineering Discussion.
HL- 431	ATC Operating Procedure	PHA-84	IC	R_330	Mitigated	Railroad	ID	RR prociedure is both conductor and Engineer view the DSI reducing risk
HL- 432	ATC	PHA-87	IC	R_306 R_307 R_308	Closed	Railraod	ID	

HL- 433	WIU ATC	SHA-289 PHA-80	IC	R_309 R_310 R_311	Closed	Railroad	IE	ABS / CMB
HL- 434	ATC	PHA-83	IE	R_312 R_313	Closed	Railroad	IE	ATC function must be analyzied by Railroad
HL- 436	Office	SHA-284 PHA-91	IC	R_116 R_314 R_315	Closed	Office Safety	IE	
HL- 621	Operations	Sys-OHA-63	IC	R_404 R_494	Closed	Railroad	ID	
HL- 622	Operations	Sys-OHA-64	IC	R_51	Mitigated	Railroad	ID	

HL- 623	Operations	Sys-OHA-65	IC	R_407	Mitigated	Railroad	ID	
HL- 649	Operations	SHA-253	IB	R_482	Mitigated	Railraod	ID	ACSES will command brake eforcement durring such events but the delay in rolling stock and OBC enforcement may cause the train to exceed PTS enforcement targets.
HL- 646	Operations	SHA-254	IB	R_479	Mitigated	Railroad	ID	ACSES will command braking to enforce PTS and TSR but delay in braking system may cause the tran to stop past start of enforcement espceciall if trian enginer accelerates near enforcement location. Also slow speed movement not protected by ACSES.
HL- 647	Operation	SHA-255	IIIB	R_480	Mitigated	Railroad	IIID	Rated a III - Very few trains reverese and then resume in same direction. Next TP read will reset TSR and PSR/MAS enforcement. Not appliable for turnback locations.
HL- 648	Onboard	SHA-256	IB	R_481	Closed	OBC	IE	Clear mitigation not yet decided. Back to Back ABS / CMB
HL- 645	Operations	SHA-257	IB	R_479	Mitigated	Railroad	ID	
HL- 632	Operations	SYS-OHA-66	IIB	R_186	Mitigated	Railroad	IID	

HL- 624	Operations	SHA-245	IB	R_396 R_407	Closed	Railroad	IE	Found in Transponder Design Reivew for Shey Stadium
HL- 679	Onboard	SHA-270	IC	R_565		Transponder	IE	Back to Back ABS / CMB
HL- 680	Onboard	SHA-271	IC	R_566		Transponder	IE	Back to Back ABS / CMB
HL- 650	STS - OBC	Interoperabilty Analysis	IIB	R_78 R_435 R_484	Closed	System	IID	All tenant trains must be updated or OPerating procedure for TSR enforcmeent by Paper TSR
HL- 673	Transponders	Back to Back Design Review	IB	R_42 R_43 R_559		Transponder	IE	Back to Back ASM/CMB

HL- 674	Onboard	Back to Back Design Review	IC	[redacted]	R_560		Onboard	IE	Back to Back ASM/CMB
HL- 675	System	Back to Back Design Reviews	IC		R_395		System	ID	Back to Back ASM/CMB SRAC
HL- 676	System	Announced Line Boundary Design	IC		R_128 R_561		System	IE	Line BOundary

HL- 677	WIU	WIU SSHL_16	IC	R_562 R_563		Railroad	ID	
HL- 681	Railroad	SHA_350	ID	R_47	Mitigated	Railraod	IE	
HL- 683	Onboard	SHA_352	IC	R_567	Mitigated	Onboard WIU	IE	Failure of mesage will enforce TSR on all tracks
HL- 684	STS - Adj STS	SHA_353	IC	R_133 R_575	Mitigated	Railroad	ID	

6 Attachment B – Comms Hazard Log

3035819 Rev_N Attachment B – Comms Hazard Log – DOORS /LIRR_MNR PTC/3. Technical Analysis/Hazard/Subsytem Hazard Log/Comms Hazard Log – Baseline 2.6 JW1

3035819_ [redacted]

ID	Subsystem or Interface	Source of Hazard	Hazard Description	Primary Cause	Initial Risk	Safety_Requirement_ID	Safety_Status	Responsibility	Final Risk	Remarks
CommsHL-1	All	COMMS-PHA-01	Material with electrical potential accessible to passengers in public area.	Design measures shall be taken to avoid contact of passengers with any COMS equipment with a different electrical potential.	IB	CM_SR_46 CM_SR_66	Closed	Comms Safety	ID	Not track power but only Internal Power to Comms equipment
CommsHL-2	All	COMMS-PHA-02	Inadequate maintenance procedures	Safe maintenance procedures and training to personnel coming in contact with high voltage COMS equipment.	IB	CM_SR_46	Mitigated	Comms Safety	ID	Not track power but only Internal Power to Comms equipment
CommsHL-3	Radio	COM_IHA_03	Incorrect Interlocking status recieved by Onboard	Message from the radio was corrupted or degraded and misinterpreted as correct due to network disturbance.	IB	CM_SR_50 CM_SR_54	Closed	System Safety	IE	Transfer to System IHA_69
CommsHL-4	BCM and WIU	COMM_IHA_4	Interlocking status request information not received..	Onboard fails to receive Interlocking status.	IB	CM_SR_52 CM_SR_53 CM_SR_74	Closed	System Safety	IE	System_IHA_01
CommsHL-5	WCC from STS	COMM_IHA_5	Incorrect TSR information received	Message from STS was corrupted or degraded over network	IB	CM_SR_76	Closed	System Safety	IE	Sys_IHA_13
CommsHL-6	BCM and WCC	COMM_IHA_6	Stale out of order information received	Message delayed sending a TSR response	IB	CM_SR_55	Closed	System Safety	IE	Sys_IHA_16

CommsHL-7	BCM and WCC	COMM_IHA_7	Stale out of order information received	Message delayed sending a TSR response	IB	[redacted]	CM_SR_56 CM_SR_75	Closed	System Safety	IE	Sys_IHA_01
CommsHL-10	MCM and OBC	COMM_IIHA-08	Stale out of order information received	Message delayed sending a TSR response	IB		CM_SR_55	Closed	System Safety	IE	Sys_IHA_16
CommsHL-11	MCM and OBC	COMM_IHA_09	Stale out of order information received	Message delayed sending a TSR response	IB		CM_SR_56 CM_SR_75	Mitigated	System Safety	IE	Sys-IHA-01
CommsHL-12	MCM and OBC	COM_IHA_10	Interlocking status request information not received.	Onboard fails to receive Interlocking status.	IB		CM_SR_74	Closed	System Safety	IE	Sys_IHA_01
CommsHL-13	MCM and OBC	COM_IHA_11	Incorrect TSR information received	Message from STS was corrupted or degraded over network	IB		CM_SR_76	Closed	System Safety	IE	Sys_IHA_13
CommsHL-14	MCM and RGS	COMM_IHA_12	Stale out of order information received	Message delayed sending a TSR response	IB		CM_SR_55	Closed	System Safety	IE	Sys_IHA_16
CommsHL-15	MCM and RGS	COMM_IHA_13	No response received to TSR Request	Loss of communication between WCC and STS	IB		CM_SR_56 CM_SR_64 CM_SR_75	Closed	System Safety	IE	Sys_IHA_01

CommsHL-16	MCM and RGs	COMM_IHA_14	Interlocking status request information not received.	Onboard fails to receive Interlocking status.	IB	[redacted]	CM_SR_64 CM_SR_74	Closed	Comms Safety	IE	Sys_IHA_01
CommsHL-17	MCM and RGS	COM_IHA_15	Incorrect TSR information received	Message from STS was corrupted or degraded over network	IB		CM_SR_76	Closed	System Safety	IE	Sys_IHA_13
CommsHL-18	MCM and BCM	COMM_IHA_16	Stale out of order information received	Message delayed sending a TSR response	IB		CM_SR_55	Closed	System Safety	IE	Sys_IHA_16
CommsHL-19	MCM and BCM	Comm_IHA_17	No response received to TSR Request	Loss of communication between WCC and STS	IB		CM_SR_55 CM_SR_63	Closed	System Safety	IE	To be transfered to Sytem IHA
CommsHL-20	MCM and BCM	COMM_IHA_18	Interlocking status request information not received.	Onboard fails to receive Interlocking status.	IB		CM_SR_64 CM_SR_74	Mitigated	Comms Safety	IE	Sys_IHA_01
CommsHL-21	MCM and BCM	COMM_IHA_19	Incorrect TSR information received	Message from STS was corrupted or degraded over network	IB		CM_SR_64 CM_SR_76	Mitigated	System Safety	IE	Sys_IHA_13
CommsHL-22	BCM and BCM	COMM_IHA_20	Incorrect interlocking status received by onboard	Message from the radio was corrupted or degraded and misinterpreted as correct due to network disturbance.	IB		CM_SR_54 CM_SR_65	Closed	System Safety	IE	Sys_IHA_96

CommsHL-23	BCM and BCM	COMM_IHA_21	Interlocking status request information not received.	Onboard fails to receive Interlocking status.	IB		CM_SR_50 CM_SR_74	Closed	System Safety	IE	Sys_IHA_01
CommsHL-24	BCM and BCM	COMM_IHA_22	No response received to TSR Request	Loss of communication between WCC and STS	IB		CM_SR_52 CM_SR_56 CM_SR_75	Mitigated	System Safety	IE	Sys_IHA_10
CommsHL-25	BCM and PDR	Comm_IHA_23	Interlocking status request information not received.	Onboard fails to receive Interlocking status.	IB		CM_SR_64 CM_SR_74	Mitigated	Comms Safety	IE	Sys_IHA_01
CommsHL-26	BCM to PDR	COMM_IHA_24	Incorrect TSR information received	Message from STS was corrupted or degraded over network	IB		CM_SR_64	Mitigated	Comms Safety	IE	Sys_IHA_13
CommsHL-27	BCM to PDR	COMM_IHA_25	Incorrect interlocking status received by onboard	Message from the radio was corrupted or degraded and misinterpreted as correct due to network disturbance.	IB		CM_SR_50 CM_SR_54	Closed	System Safety	IE	Sys_IHA_96

CommsHL-28	MCM to PDR	COM_IHA_26	No response received to TSR Request	Loss of communication between WCC and STS	IB	[redacted]	CM_SR_50 CM_SR_56 CM_SR_75	Mitigated	System Safety	IE	Sys_IHA_10
CommsHL-29	MCM to PDR	COMM_IHA_27	Interlocking status request information not received.	Onboard fails to receive Interlocking status.	IB		CM_SR_51 CM_SR_64	Mitigated	System Safety	IE	
CommsHL-30	MCM to PDR	COMM_IHA_28	Incorrect TSR information received	Message from STS was corrupted or degraded over network	IB		CM_SR_64	Mitigated	Comms Safety	IE	Sys_IHA_13
CommsHL-31	MCM to PDR	COMM_IHA_29	Incorrect interlocking status received by onboard	Message from the radio was corrupted or degraded and misinterpreted as correct due to network disturbance.	IB		CM_SR_50 CM_SR_80	Closed	System Safety	IE	Sys_IHA_96
CommsHL-32	BCM and WIU	COMM_IHA_30	Incorrect interlocking status received by onboard	Message was sent to the wrong WIU	IB		CM_SR_50 CM_SR_80	Closed	System Safety	IE	Sys_IHA_96

CommsHL-33	WCC and BCM	COMM_IHA_31	TSR information displayed to Dispatcher is incorrect	Loss of Communication	IB	[redacted]	CM_SR_58 CM_SR_64	Closed	System Safety	IE	
CommsHL-34	Programmer to WCC	COMM_IHA_33	WCC Programed with incorrect executable.	WCC Programed with incorrect executable.	IB		CM_SR_59 CM_SR_60 CM_SR_82	Mitigated	Comms Safety	IE	
CommsHL-35	BCM to WCC	COMM_IHA_34	Incorrect TSR information received	Message from OBC was corrupted or degraded over network	IB		CM_SR_54	Closed	System Safety	IE	
CommsHL-36	All	COMM_OHA_1	Maintenance personal works near active RF Transmission equipment.	Export to active RF Transmission Source	IIID		CM_SR_44	Mitigated	Comms Safety	IIIE	
CommsHL-37	All	COMM_OHA_2	Installation or maintenance personal comes into contact with live voltage while maintaining PTC equipment causing electrical shock	Exposure to High Voltage from track or other sources	IB		CM_SR_45 CM_SR_46	Mitigated	System Safety	ID	Track third rail voltage considered for maintenance activities involving access to tracks. Comms OHA needs to be amended.
CommsHL-38		Comm_OHA_03						Canceled		Severity of	Canceled
CommsHL-39		Comm_OHA_04						Canceled		Severity of	Canceled
CommsHL-40	Radio	Comm_OHA_05	Redundant Radio was manually operated.	Switchover is performed to failed radio.	IB		CM_SR_47	Closed	System Safety	ID	

CommsHL-41	Radio	Comm_OHA_06	Operator fails to Ack failure of radio test in departure test	Train operating in ACSES with a failed ACSES Radio	IB	[redacted]	CM_SR_47	Closed	System Safety	ID	
CommsHL-42	All	Comm_OHA_07	Maintenance personal access track to replace wayside radio equipment.	Protection for track worker not properly established.	IC		CM_SR_48 CM_SR_49	Closed	System Safety	ID	
CommsHL-43	All	Comm_PHA_01	Person in contact with or near an electrical power source	Material with electrical potential accessible to passengers in public area.	IID		CM_SR_66	Closed	Comms Safety	IIE	
CommsHL-44	All	Comm_PHA_02	Person in contact with high voltage field equipment.(i.e. Third Rail)	Inadequate maintenance procedures	IB		CM_SR_45	Open	System Safety	ID	
CommsHL-45	All	Comm_PHA_03	Burns to passengers, crew and third parties	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection etc.	IIC		CM_SR_68	Closed	Comms Safety	IIE	
CommsHL-46	All	Comm_PHA_04	Inhalation damage to passengers, crew, and third parties	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection, etc.	IB		CM_SR_69	Closed	Comms Safety	IE	
CommsHL-47	MCM, BCM and Radio	Comm_PHA_05	Comms failure causes error in system functionality	Hazard is from outside of system; duplication or hacking of messages.	IB		CM_SR_84 CM_SR_85	Closed	System Safety	IE	To be epxported to security log
CommsHL-48	MCM and Radio	Comm_PHA_06	Design of COMMS created components that injure maintenance or installation staff	Components have heavy weights.	IIIB		CM_SR_70	Closed	Comms Safety	IIID	
CommsHL-49	Radio	Comm_PHA_07	Comms failure causes error in system functionality	EMI causes loss of messaging or corruption of messaging	IB		CM_SR_71	Closed	Comms Safety	ID	

CommsHL-50	Radio	Comm_PHA_08	Person in the presence of a radiating ACSES II object	Equipment emitting harmful doses of radiation	IIIB	[redacted]	CM_SR_72 CM_SR_73	Closed	Comms Safety	IIID	
CommsHL-51	WCC	Comm_SSHA_01	Loss of communication between onboard and STS	WCC Failure	IB		CM_SR_62 CM_SR_81	Closed	System Safety	IE	
CommsHL-52	RGS	Comm_SSHA_02	Loss of Communication between STS and Adjacent Railroad STS	RGS Failure	IB		CM_SR_77	Mitigated	System Safety	IE	Sys_IHA_37
CommsHL-53	RGS	Comm_SSHA_03	loss of communcation between RWPS and Office	RGS Failure	IB		CM_SR_78 CM_SR_79	Mitigated	System Safety	IE	Sys_IHA_39
CommsHL-54	BCM and MCM	Comm_SSHA_04	Train performs turnback without interlocking status information and fails to enforce PTS.	Interlocking status resposne not received after turnback	IB		CM_SR_51	Closed	System Safety	IE	
CommsHL-55	BCM and MCM	Comm_SSHA_05	Train enters ACSES territory without interlocking status information from a yard or siding.	Interlocking status resposne not received	IB		CM_SR_51	Closed	System Safety	IE	
CommsHL-56	MCM	Comm_SSHA_06	Loss of communication to WIU and STS	Failure of the MCM	IB		CM_SR_51 CM_SR_61	Closed	System Safety	IE	
CommsHL-57	All	Comm_PHA_09	COMMS components or components track that injure maintenance or installation staff	Components or component shelves have sharp edges.	IIIB		CM_SR_83	Closed	Comms Safety	IIIE	

7 Attachment C – Office Hazard Log

3035819 Rev_N Attachment C – Office Hazard Log – DOORS /LIRR_MNR PTC/3. Technical Analysis/Hazard/Subsytem Hazard Log/Office Hazard Log – Baseline 2.7 JW1



3035819_[redacted]

ID	Source of Hazard	Subsystem or Interfaces	Hazard Description	Primary Cause	Risk - Before	[redacted]	ements	Safety Status	Responsibility	Risk Mitigation	Remarks
Office HL - 117	Office_PHA_01	STS / Fixed Database	TSR not placed at correct location	STS Database error	IB		7 8 157	Closed	Office	IE	
Office HL - 118	Office_PHA_02	STS	TSR not placed at correct location	STS processing error	IB		9 11 12	Closed	Office	IE	
Office HL - 119	Office_PHA_03	STS / Communication Path	TSR not placed at correct location	TSR corrupted undetectably before reaching Onboard	IB		4 10 14	Closed	Office	IE	
Office HL - 4	Office_PHA_04	STS	TSR not received by correct train	STS processing error	IB		3 4	Closed	Office	IE	test passed analysis is Office SSCD and IHA

Office HL - 5	Office_PHA_05	STS / Communication Path	TSR scheduled incorrectly	TSR corrupted undetectably before reaching Onboard	IB		5 6	Closed	Office	IE	verification of OF_SR5 still partially open
Office HL - 363	Office_SSHA_TBD	STS, Time sever	TSR scheduled incorrectly	Time server for STS unavailable	IC		177	Closed		ID	test passed analysis is Office SSCD
Office HL - 6	Office_PHA_06	STS / Communication Path	TSR not enforced as intended	TSR corrupted undetectably before reaching Onboard.	IB		4 136	Closed	System	IE	test passed analysis is Office SSCD and IHA
Office HL - 7	Office_PHA_07	All s/systems	Electrocution - Person in contact with or near an electrical power source.	Material with electrical potential accessible to passengers in public area.	IB		137	Closed	Office	ID	allocated to system
Office HL - 8	Office_PHA_08	All s/systems	Electrocution - Person in contact with or near an electrical power source.	Inadequate maintenance procedures	IB		138	Open	Office	ID	
Office HL - 9	Office_PHA_09	All s/systems	Fire - Burns to Office personnel	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection, etc.	IB		125	Closed	Office	ID	allocated to system

Office HL - 10	Office_PHA_10	All s/systems	Fire - Inhalation damage to Office personnel.	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection, etc.	IB		125	Closed	Office	ID	allocated to system
Office HL - 11	Office_PHA_11	UIS - STS	Unauthorized Access - Personnel struck by train	Unauthorized access to UIS allows a user to request a removal or additional TSR without Authorization.	IB		139 140	Closed	Office	IE	test passed, need inspection or installation dwgs.
Office HL - 211	OFFICE-PHA-12	All s/systems	Installation / Maintenance Staff Injury - Design of Office created components that injure maintenance or installation staff	Components have heavy weights, sharp edges, toxic or explosive materials etc.	IIIB		141	Mitigated	Office	ID	
Office HL - 212	OFFICE-PHA-15	WCC / STS	TSR not received by correct train	WCC processing error sends TSR to wrong train	IB		4 20 136	Closed	System	IE	

3035819_[redacted]

Office HL - 213	OFFICE-PHA-17	UISS / STS	Incorrect TSR request generated	UISS failure or Dispatcher error	IB	[redacted]	4 5 136 143	Closed	System	IE	
Office HL - 214	OFFICE-PHA-18	UISS / STS	Incorrect TSR request approved	UISS failure or Supervisor error	IB	[redacted]	4 5 136 144	Closed	System	IE	
Office HL - 215	OFFICE-PHA-20	SEC / UISS / STS	TSR improperly removed or added	Unauthorized access to UIS allows a user to request a removal or additional TSR without Authorization	IB	[redacted]	139 140	Closed	Office	IE	OF_SR140 allocated to system

Office HL - 216	OFFICE-PHA-21	RGS / STS	Information from adjacent railroad server not received by STS	RGS mismanages connection to adjacent railroad	IB	[redacted]	17 144	Closed	Office	IE	
Office HL - 220	OFFICE-PHA-22	SEC / ADDC / UISS / STS	TSR improperly removed or added	Unauthorized access to UIS allows a user to request a removal or additional TSR without Authorization	IB		139 140	Closed	Office	IE	
Office HL - 217	OFFICE-PHA-23	STS	TSR not enforced as intended	TSR exceeds maximum capacity of STS system, not recorded or transmitted	IB		145 146 147	Closed	Office	IE	
Office HL - 218	OFFICE-PHA-24	STS	TSR not placed at correct location	SDMF Database Corrupted or incorrect	IB		12 148	Closed	Office	IE	
Office HL - 120	OFFICE-PHA-25	STS / RWPS	Office does not receive information from RWPS	Link to RWPS fails	IB		15 16 17	Mitigated	Office	IE	
Office HL - 219	OFFICE-PHA-26	STS / Fixed Database	TSR not placed at correct location	Lack of synchronization between redundant STSs	IB		160	Closed	Office	IE	remaining tests require PCC and BCC

3035819_[redacted]

Office HL - 141	Office_OHA_01	Office	Electrocution - Operation staff comes into contact with electrical power source.	Material with electrical potential accessible to operation staff. Equipment design; Prior maintenance not correctly completed.	ID	[redacted]	124 125 138	Mitigated	Office	IE	
Office HL - 121	Office_OHA_02	Office	Electrocution - The maintenance or testing operator mistakenly connects to high power sources. Shock/electrocution results.	Electrical power source not properly shielded. Equipment design; Maintenance Personnel oversight	IC		18 19 138	Mitigated	Office	ID	

Office HL - 144	Office_OHA_03	UIS/Office	On-board receives TSR with speed higher then intended to be enforced or incorrect location	TSR entered incorrectly by the dispatcher	IC	3035819_ [redacted] 126 127 128 129		Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs

3035819_[redacted]

Office HL - 145	Office_OHA_04	Office	STS in each control center become Controlling and only one gets request. Trains fails to receive TSR.	GBN Dual Network Failure	IC	[redacted]	127 128 130 131	Mitigated	Office	IE	
Office HL - 146	Office_OHA_05	Office	TSR Removed with EIC in area.	Office failure allows TSR Removal when EIC still in area.	IC		118 132	Mitigated	System	ID	
Office HL - 147	Office_OHA_06	Office	EIC Terminal shows TSR where no TSR is enforced	Office failure indicates TSR where none exists	ID		133	Mitigated	System	ID	

3035819_[redacted]

Office HL - 148	Office_OHA_07	Office	Unauthorized personnel removes TSRs	Unauthorized personnel accessing ACSES II technical room	IC	[redacted]	134 135	Mitigated	System	ID	
Office HL - 136	Office_OHA_10	Operations	Dispatcher gives unsafe authority to TE when Depot/Yard operator cannot set route into transition Zone-	Dispatcher Error	II C	[redacted]	77 78	Mitigated	Office	II D	

3035819_[redacted]

Office HL - 138	Office_OHA_12	Operations	The Dispatcher issues unsafe authority into Transition zone when occupancy sates is unknown	Dispatcher Error	IIC	[redacted]	79 80	Mitigated	Office	II D	
Office HL - 149	Office_OHA_13	Office	Dispatcher issues unsafe authority into Transition Zone when Depot/Yard interlocking system is non-functional	Dispatcher Error	IIC	[redacted]	79 80	Mitigated	System	IID	
Office HL - 150	Office_OHA_18	Office	Fire	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection etc.	IC	[redacted]	125	Closed	Office	ID	allocated to system

Office HL - 151	Office_OHA_19	Office	Fire / Smoke	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection, etc.	IC	[redacted]	81	Mitigated	Office	ID	
Office HL - 152	Office_OHA_20	Wayside/Office/Onboard	Office equipment not correctly installed	Installation Personnel oversight	IC	[redacted]	19 82	Mitigated	System	ID	
Office HL - 153	Office_OHA_21	Wayside/Office	Dispatcher fails to apply a TSR to a highway crossing for which a failure has been reported resulting in unprotected crossing.	Dispatcher oversight	IC	[redacted]	163	Mitigated	System	ID	

3035819_[redacted]

Office HL - 154	Office_OHA_22	Office/Wayside	Train collides with obstruction on track that should have been protected by TSR.	Railroad staff failure to establish Zero speed TSRs for track obstructions.	IC	[redacted]	19 83	Mitigated	System	ID	
Office HL - 155	Office_OHA_23	On-Board/Office/Wayside	Maintenance personnel fail to ensure software configuration management (SCM) records and retrieval are correct, leading to incorrect version of software/data being used.	Maintenance Personnel oversight	IC	[redacted]	84	Mitigated	System	ID	
Office HL - 156	Office_OHA_24	On-Board/Office/Wayside	Maintenance personnel incorrectly configures compiled applications and databases. Components updated with incorrect files.	Maintenance Personnel oversight	IC	[redacted]	165	Mitigated	Office	ID	
Office HL - 157	Office_OHA_25	On-Board/Office/Wayside	Maintenance personnel fail to check CRCs, compare review reports, and perform other verification activities. Components updated with incorrect files.	Maintenance Personnel oversight	IC	[redacted]	85	Mitigated	System	ID	

3035819_[redacted]

Office HL - 158	Office_OHA_26	On-Board/Office/Wayside	Maintenance personnel fail to perform regular maintenance database backup. Disaster requires recovery of system.	Maintenance Personnel oversight	IC	[redacted]	166	Mitigated	System	ID	
Office HL - 159	Office_OHA_28	Office	The railroad fails to maintain the existing practice of documenting and communicating TSRs. Radio failure occurs.	Operator complacency	IC	[redacted]	86	Mitigated	System	ID	Office SSCD on S S
Office HL - 160	Office_OHA_29	Office	Newly controlling STS doesn't have latest TSR list	Control Center's STS servers not in synch prior to switchover.	IC	[redacted]	127 128 130 131	Mitigated	System	IE	Office SSCD on S S

Office HL - 161	Office_OHA_31	Office	Dispatcher allowed train to enter MBS area when another train is Occupying that area	Dispatcher Error	IC	[redacted]	87 88	Mitigated	Office	ID	
Office HL - 162	Office_OHA_32	ALL	Personnel who perform all maintenance activities on PTC system is not fully trained.	Management Error	IA	[redacted]	19	Mitigated	System	ID	
Office HL - 163	Office_OHA_33	Wayside/Office	Dispatcher fails to apply a TSR to a work zone	Dispatcher oversight	IC	[redacted]	89	Mitigated	System	ID	
Office HL - 164	Office_OHA_34	Office	Installation / maintenance staff Injury during equipment installation	Design of Office created components that injure maintenance or installation staff Components have heavy weights, sharp edges etc	IIIC	[redacted]	90	Mitigated	Office	IVD	

Office HL - 165	Office_OHA_35	Office	Improper management of TSRs.	NMS – UIS link failure	IC	[redacted]	91 92	Closed	Office	ID	3046852, LIRR UIS Use Cases
Office HL - 166	Office_OHA_36	Office	Operator fails to confirm the data within the UIS matches the manual TSR lists kept by operations.	Not all TSRs are being maintained by ACSES .	IC		93	Closed	Office	ID	Office IHA
Office HL - 167	Office_OHA_37	Office	Chief Dispatcher approves incorrect TSR request.	Corrupt message causes UIS to display incorrect information	IC		94	Open	Office	ID	
Office HL - 168	Office_OHA_38	Office	Dispatcher approves incorrect TSR request from EIC.	Incorrect Transfer of Information between RWPS and Office.	ID		153	Closed	Office	IE	
Office HL - 169	Office_OHA_39	Office	Dispatcher approves incorrect TSR request form EIC.	Incorrect data transfer from RWPS to EIC Terminal, and Dispatcher oversight.	ID		96	Mitigated	Office	IE	

Office HL - 170	Office_OHA_40	Office	Chief Dispatcher approves incorrect TSR request from EIC.	EIC enters incorrect data into TSR Request, and Dispatcher oversight.	ID	[redacted]	126	Closed	Office	IE	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases.
Office HL - 171	Office_OHA_41	Office	Dispatcher approves TSR Removal with Secondary EIC in area	RWPS failure allows TSR Removal when Secondary EIC still in area, and Dispatcher oversight.	ID		118 167	Mitigated	Office	ID	
Office HL - 172	Office_OHA_42	Office	TSR Removed with EIC in area.	Supervisor performs TSR Override with EIC still in area.	ID		97 98	Mitigated	System	ID	
Office HL - 173	Office_OHA_43	Office	Incorrect software revision in ACSES equipment	SDMF configuration management failure	IC		84	Mitigated	System	ID	

Office HL - 174	Office_OHA_44	Office	Incorrect software revision in ACSES equipment. WIU Configuration error which results in WIU to send a ATCS message with a less restrictive movement authority than intended	SDMF configuration management failure	IC		84	Mitigated	System	ID	
Office HL - 175	Office_OHA_45	Office	Train violates a work zone in an Adjacent Railroad.	Communication failure between Local and Adjacent STS Server; Chief Dispatcher fails to communicate workzone in adjacent railroad.	IC		99	Mitigated	System	ID	
Office HL - 176	Office_OHA_46	Office	Train violates a work zone in an Adjacent Railroad.	Radio failure near Adjacent Railroad Boundary.	IC		100	Mitigated	System	ID	

Office HL - 177	Office_OHA_47	Office	Trains receive different TSR Data as the STS in each control center is sending TSR Data.	GBN Dual Network Failure	ID	3035819_ [redacted]	130	Mitigated	Office	ID	

Office HL - 178	Office_OHA_48	Office	Unauthorized personnel removes TSR	Office Network is vulnerable to hacking.	ID	[redacted]	101 127 128 129	Closed	Office	IIID	
Office HL - 179	Office_OHA_49	Office	Maximum number of TSRs has been reached.	Dispatcher cannot add another TSR.	IIIC		102	Closed	Office	IIID	
Office HL - 180	Office_OHA_57	Office	Maintainer fails to recognize signs of necessity for maintenance.	Poor/insufficient training.	IIIC		103	Mitigated	Office	IIID	
Office HL - 181	Office_OHA_58	Office	Maintainer fails to recognize signs of poor network performance on NMS workstation, or does not know how to respond.	Poor/insufficient training.	IIIC		104	Mitigated	Office	IIID	

3035819_[redacted]

Office HL - 182	Office_OHA_60	Office	UIS operator fails to properly respond to alarm related to STS function.	Poor/insufficient training.	ID	[redacted]	105	Mitigated	Office	ID	
Office HL - 183	Office_OHA_61	System, Office, OBC	Office fails to response to OBC issues. Train alarms, TSR list requests not transmitted to Office.	Lack of adequate operational procedures developed for Office in response to non Office component failures.	ID		106	Mitigated	Office	ID	
Office HL - 184	Office_OHA_65	Office	Authorized users of UIS, DMS and NMS have differing knowledge of currently configured alarms regarding TSR Management and prescribed responses.	Poor/insufficient training. Lack of policy on Rules Based Alarm management configuratoin management and communication.	ID		107	Closed	Office	ID	
Office HL - 186	Office_OHA_69	Office	NMS Operator forces reboot of active/controlling STS while standby/controlling is not HOT, due to different MAP files or code.	Poor/insufficient training.	IC		109 121	Closed	Office	ID	

Office HL - 187	Office_OHA_71	Office	NMS Operator forces COLD standby controlling STS to become active while other controlling STS is active.	Poor/insufficient training.	IC	[redacted]	110 122 123	Mitigated	Office	ID	
Office HL - 188	Office_OHA_72	Office	PCC and BCC are not communicating, one is controlling.	Poor/insufficient training.	IC		111	Closed	Office	ID	
Office HL - 189	Office_OHA_74	Office	NMS misses signs of system degradation or possible network intrusion.	Poor or inadequate training and/or manuals.	IIIC		112	Mitigated	Office	IID	
Office HL - 190	Office_OHA_75	Office	User controls territory beyond their qualification.	Inadequate qualification assessment/criteria			113	Mitigated	Office	ID	

3035819_[redacted]

Office HL - 191	Office_OHA_76	Office	User controls more than one territory to allow another user to go off duty.	Inadequate resource planning	ID		114	Closed	Office	ID	
Office HL - 192	Office_OHA_77	Office	Fire	Fan overheats due to accumulation of dust/debris on fan	IC		115	Mitigated	Office	ID	
Office HL - 193	Office_OHA_78	Office	Inability to add new TSRs to any STS server.	Hardware or software failure Failure of one STS server causes loss of synch between Prmary and Backup control centers.	ID		116 117 127 128	Mitigated	Office	IE	

3035819_[redacted]

Office HL - 194	Office_OHA_79	UIS/Office	On-board receives TSR with speed higher then intended to be enforced or incorrect location	Dispatcher enters wrong type, speed or location	IC	[redacted]	126 127 128 129	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs
Office HL - 195	Office_OHA_80	UIS/Office	Train enters workzone.	Dispatcher enters wrong type, speed or location	IC		126 127 128 129	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs

3035819_[redacted]

Office HL - 196	Office_OHA_81	UIS/Office	Train enters workzone at speed greater than 15mph.	Dispatcher enters wrong type, speed or location	IC	[redacted]	126 128 129	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs
Office HL - 197	Office_OHA_82	UIS/Office	Train enters workzone at speed greater than intended.	Dispatcher enters wrong type, speed or location	IC		126 128 129	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs

Office HL - 198	Office_OHA_83	UIS/Office	Train fails to stop where intended.	Dispatcher enters wrong type, speed or location	IC	[redacted]	126 127 128 129	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs
Office HL - 200	Office_OHA_85	UIS/Office	Train fails to reduce speed where intended and/or does not reduce speed down to the intended level.	Dispatcher enters wrong type, speed or location	IC		126 127 128 129	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs

3035819_[redacted]

Office HL - 201	Office_OHA_86	UIS/Office	Train fails to stop where intended.	Dispatcher enters wrong type, speed or location	IC	[redacted]	126 127 128 129	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs
Office HL - 202	Office_OHA_87	UIS/Office	Train crosses grade with gate failure at speed greater than 15mph.	Dispatcher enters wrong type, speed or location	IC	[redacted]	126 127 128 129	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs

Office HL - 203	Office_OHA_88	UIS/Office	Train fails to stop at grade crossing with activation failure	Dispatcher enters wrong type, speed or location	IC	[redacted]	126 127 128 129	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs
Office HL - 204	Office_OHA_89	UIS/Office	Train crosses grades requiring speed restriction at speed greater than 15mph.	Dispatcher enters wrong type, or location	IC		126 127 128 129	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs

Office HL - 205	Office_OHA_90	UIS/Office	Train fails to reduce speed where intended or does not reduce speed down to the 15mph.	Dispatcher enters wrong type, or location	IC	[redacted]	126 127 128 129	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs
Office HL - 206	Office_OHA_91	Office	Host RR Dispatcher incorrectly or fails to set the boundary line TSR as per adjacent RR dispatcher request	Host Railroad Dispatcher Error	IC	[redacted]	119	Open	Office	ID	

3035819_[redacted]

Office HL - 207	Office_OHA_92	Office	Adjacent RR Dispatcher incorrectly or fails to set the boundary line TSR as per Host RR dispatcher request	External RailroadDispatcher Error	IC	[redacted]	120 126	Closed	Office	ID	OF_SR126 closed with CDRL 6-001 Addendum: Office Use Cases. Remaining SRs are SRACs
Office HL - 123	Office_IHA_02	WCC from STS	OBC enforces TSR at wrong speed, location or grade.	Message Corruption	IB		20	Closed	Office	IE	Per SLR, Ver Method : Inspection. (for presence of CRC) see 3041417, Onboard MDD. Test. Per linked OBS SLR - tests passed.
Office HL - 124	Office_IHA_03.1	WCC from STS	OBC fails to enforce TSR.	Loss of communication	IC		21	Closed	Office	IE	OBC reqmt. Per SLR, Ver Method :Analysis of Subsystem". Per linked OBS SLR - tests passed.

3035819_[redacted]

Office HL - 223	Office_IHA_03.2	WCC from STS	OBC fails to enforce TSR.	Loss of communication	IC	[redacted]	23	Closed	Office	IE	
Office HL - 224	Office_IHA_03.3	WCC from STS	OBC fails to enforce TSR.	Loss of communication	IC	[redacted]	24	Mitigated	System	IE	this is an operational reqmt; need to inspect Op manual, training records
Office HL - 225	Office_IHA_03.4	WCC from STS	OBC fails to enforce TSR.	Loss of communication	IC	[redacted]	25	Closed	Office	IE	
Office HL - 226	Office_IHA_03.5	WCC from STS	OBC fails to enforce TSR.	Loss of communication	IC	[redacted]	26	Mitigated	Office	IE	LIRR testing deferred MNR test failed
Office HL - 125	Office_IHA_04.1	WCC to STS	OBC fails to enforce TSR.	Delayed Message	IC	[redacted]	21	Closed	Office	IE	OBC reqmt. Per SLR, Ver Method :Analysis of Subsystem". Per linked OBS SLR - tests passed.
Office HL - 227	Office_IHA_04.2	WCC to STS	OBC fails to enforce TSR.	Delayed Message	IC	[redacted]	23	Closed	Office	IE	
Office HL - 228	Office_IHA_05	WCC to STS	OBC fails to enforce TSR.	Resequence / Resend of a message	IC	[redacted]	27	Closed	Office	IE	

3035819_[redacted]

Office HL - 229	Office_IHA_06.1	WCC to STS	OBC receives an invalid TSR List	Message Insertion	IC	[redacted]	20	Closed	System	IE	Reqmt allocated to OBC
Office HL - 230	Office_IHA_06.2	WCC to STS	OBC receives an invalid TSR List	Message Insertion	IC		28	Closed	System	IE	Reqmt allocated to OBC
Office HL - 231	Office_IHA_06.3	WCC to STS	OBC receives an invalid TSR List	Message Insertion	IC		29	Closed	System	IE	
Office HL - 232	Office_IHA_06.4	WCC to STS	OBC receives an invalid TSR List	Message Insertion	IC		73	Closed	Office	IE	
Office HL - 126	Office_IHA_07.1	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Message Corruption	IC		30	Closed	Office	IE	allocated to system
Office HL - 289	Office_IHA_07.2	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Message Corruption	IC		149	Closed	Office	IE	
Office HL - 127	Office_IHA_08.1	STS from/to Adj RR STS	Local STS has stale / no information on TSR's in adjacent RR.	Loss of Communication	IC		31	Open	Office	IE	remaining test involves adjacent railroad
Office HL - 128	Office_IHA_08.2	STS from/to Adj RR STS	Local STS has stale / no information on TSR's in adjacent RR.	Loss of Communication	IC		32	Open	Office	IE	remaining test involves adjacent railroad
Office HL - 129	Office_IHA_08.3	STS from/to Adj RR STS	Local STS has stale / no information on TSR's in adjacent RR.	Loss of Communication	IC		33	Open	Office	IE	remaining test involves adjacent railroad

3035819_[redacted]

Office HL - 290	Office_IHA_08.4	STS from/to Adj RR STS	Local STS has stale / no information on TSR's in adjacent RR.	Loss of Communication	IC	[redacted]	149	Closed	Office	IE	
Office HL - 130	Office_IHA_09.1	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Delayed Message	IC	[redacted]	34 49	Open	Office	IE	remaining test involves PCC and BCC
Office HL - 291	Office_IHA_09.2	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Delayed Message	IC	[redacted]	149	Closed	Office	IE	
Office HL - 131	Office_IHA_10.1	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Message Sequence out of order	IC	[redacted]	35	Closed	Office	IE	
Office HL - 132	Office_IHA_10.2	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Message Sequence out of order	IC	[redacted]	36	Open	Office	IE	remaining test involves adjacent railroad
Office HL - 292	Office_IHA_10.3	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Message Sequence out of order	IC	[redacted]	149	Closed	Office	IE	
Office HL - 133	Office_IHA_11.1	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Message Insertion	IC	[redacted]	37	Open	Office	IE	remaining test involves adjacent railroad

3035819

Office HL - 143	Office_IHA_11.2	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Message Insertion	IC		30	Closed	Office	IE	Allocated to system
Office HL - 208	Office_IHA_11.3	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Message Insertion	IC		38	Closed	Office	IE	
Office HL - 209	Office_IHA_11.4	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Message Insertion	IC		67	Closed	Office	IE	
Office HL - 293	Office_IHA_11.5	STS from/to Adj RR STS	Local STS has incorrect information for TSRs in adj RR.	Message Insertion	IC		149	Closed	Office	IE	
Office HL - 210	Office_IHA_12.1	UISS to/from STS	UISS has incorrect TSR information.	Message Corruption	IC		39	Closed	Office	IE	
Office HL - 233	Office_IHA_12.2	UISS to/from STS	UISS has incorrect TSR information.	Message Corruption	IC		40	Mitigated	Office	IE	remaining test involves Adjacent STS
Office HL - 234	Office_IHA_12.3	UISS to/from STS	STS receives incorrect TSR request information.	Message Corruption	IC		40	Mitigated	Office	IE	remaining test involves Adjacent STS
Office HL - 236	Office_IHA_13.1	UISS to/from STS	UISS has stale / incorrect TSR list information	Loss of Communication	IC		41	Closed	Office	IE	
Office HL - 237	Office_IHA_13.2	UISS to/from STS	TSRs cannot be processed.	Loss of Communication	IC		42	Closed	Office	IE	
Office HL - 238	Office_IHA_13.3	UISS to/from STS	TSRs cannot be processed.	Loss of Communication	IC		43	Mitigated	Office	IE	remaining test involves PCC and BCC

Office HL - 239	Office_IHA_14.1	UISS to/from STS	UISS has stale / incorrect TSR list information	Delayed Message	IC	[redacted]	41	Closed	Office	IE	
Office HL - 240	Office_IHA_14.2	UISS to/from STS	UISS has stale / incorrect TSR list information	Delayed Message	IC		64	Closed	Office	IE	
Office HL - 241	Office_IHA_15	UISS to/from STS	UISS has stale / incorrect TSR list information	Message Sequence out of order	IC		45	Closed	Office	IE	
Office HL - 242	Office_IHA_16.1	UISS to/from STS	STS receives unauthorized TSR requests.	Message Insertion	IC		46	Mitigated	Office	IE	remaining test involves PCC and BCC , and Adjacent STS
Office HL - 243	Office_IHA_16.2	UISS to/from STS	STS receives unauthorized TSR requests.	Message Insertion	IC		47	Mitigated	Office	IE	remaining test involves PCC and BCC
Office HL - 244	Office_IHA_16.3	UISS to/from STS	STS receives unauthorized TSR requests.	Message Insertion	IC		39	Closed	Office	IE	
Office HL - 245	Office_IHA_17	STS to/from STS	Standby STS has incorrect TSR	Message Corruption	IIIB		75	Closed	Office	IIIE	
Office HL - 246	Office_IHA_18	STS to/from STS	Standby STS has incorrect TSR	Loss of Communication	IIIB		75	Closed	Office	IIIE	
Office HL - 247	Office_IHA_19.1	STS to/from STSSTS to/from STS	Standby STS has incorrect TSR	Message Sequence out of order	IIIB		49	Mitigated	Office	IIIE	remaining test involves PCC and BCC
Office HL - 248	Office_IHA_19.2	STS to/from STS	Standby STS has incorrect TSR	Message Sequence out of order	IIIB		75	Closed	Office	IIIE	

3035819_[redacted]

Office HL - 249	Office_IHA_20.1	STS to/from STS	Standby STS has incorrect TSR	Delayed Message	IIIB	[redacted]	48	Mitigated	Office	IIIE	remaining test involves PCC and BCC
Office HL - 250	Office_IHA_20.2	STS to/from STS	Standby STS has incorrect TSR	Delayed Message	IIIB		75	Closed	Office	IIIE	
Office HL - 251	Office_IHA_21.1	STS to/from STS	Standby STS has incorrect TSR	Message Insertion	IIIB		49	Mitigated	Office	IIIE	remaining test involves PCC and BCC
Office HL - 252	Office_IHA_21.2	STS to/from STS	Standby STS has incorrect TSR	Message Insertion	IIIB		48	Mitigated	Office	IIIE	remaining test involves PCC and BCC
Office HL - 253	Office_IHA_21.3	STS to/from STS	Standby STS has incorrect TSR	Message Insertion	IIIB		51	Mitigated	Office	IIIE	remaining test involves PCC and BCC
Office HL - 254	Office_IHA_21.4	STS to/from STS	Standby STS has incorrect TSR	Message Insertion	IIIB		74	Mitigated	Office	IIIE	remaining test involves PCC and BCC
Office HL - 255	Office_IHA_21.5	STS to/from STS	Standby STS has incorrect TSR	Message Insertion	IIIB		75	Closed	Office	IIIE	
Office HL - 256	Office_IHA_22	UIS to ADDC	TSR improperly removed or added.	Message Corruption	IB		52	Closed	Office	IE	
Office HL - 258	Office_IHA_23.2	UIS to ADDC	TSR List unable to be changed	Loss of Communication	IIIC		54	Closed	Office	IIID	
Office HL - 259	Office_IHA_23.3	UIS to ADDC	TSR List unable to be changed	Loss of Communication	IIIC		55	Mitigated	System	IIID	

Office HL - 260	Office_IHA_24	UIS to ADDC	TSR List unable to be changed	Message Sequence out of order	IIID	[redacted]	55	Mitigated	System	IIID	
Office HL - 261	Office_IHA_25	UIS to ADDC	TSR List unable to be changed	Delayed Message	IIID		55	Mitigated	System	IIID	
Office HL - 262	Office_IHA_26	UIS to ADDC	TSR improperly removed or added.	Message Insertion	IB		52	Closed	Office	IE	
Office HL - 263	Office_IHA_27.1	UISS to/from UIS Workstation	TSR Information incorrect on UISS Workstation	Message Corruption	IB		61	Mitigated	Office	ID	
Office HL - 264	Office_IHA_27.2	UISS to/from UIS Workstation	TSR Information incorrect on UISS Workstation	Message Corruption	IIIC		62	Mitigated	Office	IIID	remaining test involves PCC and BCC, and Adjacent STS
Office HL - 265	Office_IHA_28	UISS to/from UIS Workstation	TSR information displayed to Dispatcher is incorrect	Loss of Communication	IIIC		63	Closed	Office	IIID	
Office HL - 266	Office_IHA_29	UISS to/from UIS Workstation	Message Receipt order not guaranteed n TCP/IP data transmission.	Message Sequence out of order	IIIC		64	Closed	Office	IIID	
Office HL - 267	Office_IHA_30.1	UISS to/from UIS Workstation	Network congestion causing message transmission delays	Delayed Message	IIIC		46	Mitigated	Office	IIID	remaining test involves PCC and BCC, and Adjacent STS

Office HL - 268	Office_IHA_30.2	UISS to/from UIS Workstation	Network congestion causing message transmission delays	Delayed Message	IIIC		65	Mitigated	Office	IIID	remaining test involves PCC and BCC, and Adjacent STS
Office HL - 269	Office_IHA_31	UISS to/from UIS Workstation	TSR information displayed to Dispatcher is incorrect	Message Insertion	IIIC		46	Mitigated	Office	IIID	remaining test involves PCC and BCC, and Adjacent STS
Office HL - 270	Office_IHA_32.1	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Message Corruption	IB		20	Closed	System	IE	allocated to OBC
Office HL - 271	Office_IHA_32.2	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Message Corruption	IB		69	Closed	System	IE	allocated to OBC
Office HL - 272	Office_IHA_33.1	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Loss of Communication	IB		70	Closed	Office	IE	
Office HL - 273	Office_IHA_33.2	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Loss of Communication	IB		70	Closed	Office	IE	
Office HL - 274	Office_IHA_33.3	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Loss of Communication	IB		21	Closed	System	IE	OBC reqmt. Per SLR, Ver Method :Analysis of Subsystem". Per linked OBS SLR - tests passed.

Office HL - 275	Office_IHA_33.4	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Loss of Communication	IB		69 150	Closed	System	IE	allocated to OBC
Office HL - 276	Office_IHA_34.1	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Message Sequence out of order	IB		21	Closed	System	IE	OBC reqmt. Per SLR, Ver Method :Analysis of Subsystem". Per linked OBS SLR - tests passed.
Office HL - 277	Office_IHA_34.2	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Message Sequence out of order	IB		23	Closed	Office	IE	
Office HL - 278	Office_IHA_35	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Delayed Message	IB		27	Closed	Office	IE	
Office HL - 279	Office_IHA_36.1	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Message Insertion	IB		20	Closed	System	IE	allocated to OBC
Office HL - 280	Office_IHA_36.2	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Message Insertion	IB		28	Closed	System	IE	allocated to OBC
Office HL - 281	Office_IHA_36.3	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Message Insertion	IB		29	Closed	System	IE	
Office HL - 282	Office_IHA_36.4	WCC to/from BCP	Train fails to enforce TSR or PTS at the correct location.	Message Insertion	IB		73	Closed	Office	IE	

3035819_[redacted]

Office HL - 283	Office_IHA_37.1	NMS to STS	STS Rebooted without operator Request	Message Corruption	IIB	[redacted]	56	Closed	Office	IIE	
Office HL - 284	Office_IHA_37.2	NMS to STS	STS Rebooted without operator Request	Message Corruption	IIB		127 128	Mitigated	System	IIE	
Office HL - 285	Office_IHA_38	NMS to STS	STS Server unable to be remotely rebooted.	Loss of Communication	IVB		56	Closed	Office	IVE	
Office HL - 294	Office_IHA_39	NMS to STS	Both controlling STS active in control center.	NMS inadvertently forces standby STS to active.	IIB		76	Closed	Office	IIE	
Office HL - 286	Office_IHA_41	NMS to STS	STS Server rebooted without authorization - and standby STS not synced	Message Insertion	IB		46 128	Mitigated	Office	IE	SRAC required to fulfill OF_SR128; remaining test involves PCC and BCC, and Adjacent STS
Office HL - 287	Office_IHA_42.1	NMS from UIS	UISS loss of communication	Loss of Communication	IIC		57	Closed	Office	IID	
Office HL - 288	Office_IHA_42.2	NMS from UIS	UISS loss of communication	Loss of Communication	IIC		127 128	Mitigated	System	IID	

Office HL - 295	Office_IHA_43	DMS from WCC	Updated diagnostic information is not available to determine faults.	Loss of Communication	IIIC	[redacted]	57	Closed	Office	IIID	
Office HL - 296	Office_IHA_44	DMS from WCC	Updated diagnostic information is not available to determine faults.	Loss of Communication	IIIC	[redacted]	57	Closed	Office	IIID	
Office HL - 297	Office_IHA_46.1	ADDC to UIS	An Office workstation fails to provide updated information to the Dispatcher.	Message Corruption	IB	[redacted]	58	Mitigated	Office	IE	Demonstration required.
Office HL - 298	Office_IHA_46.2	ADDC to UIS	An Office workstation fails to provide updated information to the Dispatcher.	Message Corruption	IB	[redacted]	46	Mitigated	Office	IE	remaining test involves PCC and BCC, and Adjacent STS
Office HL - 299	Office_IHA_46.3	ADDC to UIS	An Office workstation fails to provide updated information to the Dispatcher.	Message Corruption	IB	[redacted]	151	Open	Office	IE	Updated Risk Assessment
Office HL - 300	Office_IHA_47	ADDC to NMS	An Office workstation fails to provide updated information to the Dispatcher.	Message Corruption	IIIC	[redacted]	152	Closed	Office	IIID	
Office HL - 301	Office_IHA_48	OSW to/from OFW	Loss of connection between OSW to and from OFW.	Hardware failure	IC	[redacted]	50	Mitigated	Office	ID	
Office HL - 302	Office_IHA_49	OFW to/from LSW	Loss of connection between OFW to and from LSW.	Hardware failure	IC	[redacted]	50	Mitigated	Office	ID	
Office HL - 303	Office_IHA_50	SDMF to USB	Component programmed with an incorrect or corrupt file.	Data Corruption	IIIC	[redacted]	59	Mitigated	Office	IIID	Demonstration required.

Office HL - 304	Office_IHA_51	USB to UIS	Component programmed with an incorrect or corrupt file	Data Corruption	IIIC	[redacted]	59	Mitigated	Office	IIID	Demonstration required.
Office HL - 305	Office_IHA_52	USB to ADDC	Component programmed with an incorrect or corrupt file	Data Corruption	IIIC	[redacted]	59	Mitigated	Office	IIID	Demonstration required.
Office HL - 306	Office_IHA_53	USB to NMS	Component programmed with an incorrect or corrupt file	Data Corruption	IIIC	[redacted]	59	Mitigated	Office	IIID	Demonstration required.
Office HL - 307	Office_IHA_54	USB to DMS	Component programmed with an incorrect or corrupt file	Data Corruption	IIIC	[redacted]	59	Mitigated	Office	IIID	Demonstration required.
Office HL - 308	Office_IHA_55.1	USB to STS	Component programmed with an incorrect or corrupt file	Data Corruption	IB	[redacted]	59	Mitigated	Office	IE	Demonstration required.
Office HL - 309	Office_IHA_55.2	USB to STS	Component programmed with an incorrect or corrupt file	Data Corruption	IB	[redacted]	60	Closed	Office	IE	
Office HL - 310	Office_IHA_56	USB to SEC	Component programmed with an incorrect or corrupt file	Data Corruption	IIIC	[redacted]	59	Mitigated	Office	IIID	Demonstration required.
Office HL - 311	Office_IHA_58	USB to RGS	Component programmed with an incorrect or corrupt file	Data Corruption	IIIC	[redacted]	59	Mitigated	Office	IIID	Demonstration required.
Office HL - 312	Office_IHA_59	SDMF from User	Component programmed with an incorrect or corrupt file	Operator Error	IIIC	[redacted]	72	Mitigated	Office	IIID	
Office HL - 313	Office_IHA_57	USB to WCC	Wrong file selected for transfer to the USB	Data Corruption	IIIC	[redacted]	59	Mitigated	Office	IIID	Demonstration required.
Office HL - 314	Office_IHA_60	SDMF from User	Wrong file selected for transfer to the USB	Unauthorized person loads SW	IIIB	[redacted]	66	Closed	Office	IIID	allocated to system

3035819

Office HL - 315	Office_IHA_61	UIS from/to RWPS	EIC receives stale / incorrect TSR list information	Delayed Message	IC	[redacted]	118	Closed	Office	ID	allocated to system
Office HL - 316	Office_IHA_62	UIS from/to RWPS	EIC receives stale / incorrect TSR list information	Loss of Communication	IC		118	Closed	Office	ID	allocated to system
Office HL - 317	Office_IHA_63.1	UIS from/to RWPS	EIC receives stale / incorrect TSR list information	Message corruption	IC		118	Closed	Office	ID	allocated to system
Office HL - 318	Office_IHA_63.2	UIS from/to RWPS	EIC receives stale / incorrect TSR list information	Message corruption	IC		153	Closed	Office	IE	
Office HL - 319	Office_IHA_64.1	UIS from/to RWPS	EIC receives stale / incorrect TSR list information	Message Insertion	IC		118	Closed	Office	ID	allocated to system
Office HL - 320	Office_IHA_64.2	UIS from/to RWPS	EIC receives stale / incorrect TSR list information	Message Insertion	IC		133	Closed	Office	ID	allocated to system

Office HL - 321	Office_IHA_65	UIS from/to RWPSUIS from/to RWPS	EIC receives stale / incorrect TSR list information	Message Sequence out of order	IC		118	Closed	Office	ID	allocated to system
Office HL - 332	Office_IHA_74.1	UIS from RGS	STS receives unauthorized TSR requests.	Message Insertion	IC		155	Closed	Office	IE	
Office HL - 335	Office_IHA_85	UIS from/to RWPS	EIC receives incorrect TSR data (after missing data or data failed CRC)	Message corruption, message insertion, message sequence out of order	IC		118	Closed	Office	ID	allocated to system
Office HL - 336	Office_IHA_86	UIS from/to RWPS	EIC receives TSR data with missing data	Delayed Message, Loss of Communication	IC		118	Closed	Office	ID	allocated to system
Office HL - 337	Office_IHA_87	STS to/from Adj RR STS	Maps between Local STS and Adjacent STS differ at boundary area	Inadequate cross verification of Host and Adjacent railroad map dat at Hostcboundary.	IC		158	Open	Office	IE	
Office HL - 338	Office_IHA_89.1	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Message Corruption	IIIB		159	Mitigated	Office	IIIE	
Office HL - 339	Office_IHA_89.2	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Message Corruption	IIIB		160	Mitigated	Office	IIIE	remaining tests involves PCC and BCC
Office HL - 340	Office_IHA_90.1	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Loss of Communication	IIIB		160	Mitigated	Office	IIIE	remaining tests involves PCC and BCC

3035819_[redacted]

Office HL - 341	Office_IHA_90.2	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Loss of Communication	IIIB	[redacted]	161	Mitigated	Office	IIIE	
Office HL - 342	Office_IHA_90.3	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Loss of Communication	IIIB		162	Mitigated	Office	IIIE	
Office HL - 343	Office_IHA_91.1	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Message Sequence out of order	IIIB		49	Mitigated	Office	IIIE	remaining test involves PCC and BCC
Office HL - 344	Office_IHA_91.2	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Message Sequence out of order	IIIB		160	Mitigated	Office	IIIE	remaining tests involves PCC and BCC
Office HL - 345	Office_IHA_92.1	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Delayed Message	IIIB		49	Mitigated	Office	IIIE	remaining test involves PCC and BCC
Office HL - 346	Office_IHA_92.2	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Delayed Message	IIIB		160	Mitigated	Office	IIIE	remaining tests involves PCC and BCC
Office HL - 347	Office_IHA_93.1	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Message Insertion	IIIB		46	Mitigated	Office	IIIE	remaining test involves PCC and BCC, and Adjacent STS
Office HL - 348	Office_IHA_93.2	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Message Insertion	IIIB		49	Mitigated	Office	IIIE	remaining test involves PCC and BCC

Office HL - 349	Office_IHA_93.3	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Message Insertion	IIIB		48	Mitigated	Office	IIIE	remaining test involves PCC and BCC
Office HL - 350	Office_IHA_93.4	Controlling STS to/from Noncontrolling STS	Standby STS has incorrect TSR	Message Insertion	IIIB		74	Mitigated	Office	IIIE	remaining test involves PCC and BCC
Office HL - 142	SSHA	STS	TSR enforced on the wrong track.	TSR Requested over a section of track with a track ID change. Operations intended to keep the TSR on the same physical track.(Same physical track changes from Track 4 to Track 6).	IB		2	Closed	Office	IE	
Office HL - 352	FMECA records 42.1 and 45	Safety reqmt Allocated to NMS and UIS	Train not receiving TSR	failure to switchover upon failure	NA		168	Closed	Office	IIE	
Office HL - 353	FMECA record 42.1	STS	Train not receiving TSR	insufficent software capacity	NA		175	Mitigated	Office	IIE	Testing of one associated Office SSLR reqmt not executed for LIRR.
Office HL - 354	FMECA record 47	STS NMS	Train not receiving TSR	Standby server erroneously goes active	NA		172 173	Mitigated	Office	ID	what evidence expected?
Office HL - 355	FMECA record 48	STS NMS	Train not receiving TSR	both control centers become controlling due to dual GBN failure	NA		174	Open	Office	IE	Test deferred

3035819_[redacted]

Office HL - 356	FMECA record 48	Allocated to NMS	Train not receiving TSR	both control centers become controlling due to dual GBN failure	NA	[redacted]	172	Open	Office	IE	what evidence expected?
Office HL - 357	FMECA record 48	GBN	Train not receiving TSR	both control centers become controlling due to dual GBN failure	NA	[redacted]	171	Open	Office	IE	this is an operational reqmt; need to inspect Op manual
Office HL - 358	FMECA record 51	STS	Trains not receiving TSRs.	failure to accept switchover upon failure of Active server	NA	[redacted]	75 170	Open	Office	IIE	this is an operational reqmt; need to inspect Op manual
Office HL - 359	FMECA record 328	UIS, Operator	Improper management of TSRs	Failure to detect UIS failure.	NA	[redacted]	91	Mitigated	Office	ID	3046852, LIRR UIS Use Cases
Office HL - 360	FMECA records 42.1, 4	STS	Train not receiving TSR	software failure - insufficient capacity failure to switchover upon failure	NA	[redacted]	21	Closed	Office	IIE	OBC reqmt. Per SLR, Ver Method :Analysis of Subsystem". Per linked OBS SLR - tests passed.
Office HL - 361	FMECA records 47, an	Office	Train not receiving TSR	both control centers become controlling	NA	[redacted]	169	Closed	Office	IE	

Office HL - 362	FMECA record 328	NMS/UIS interface	Improper management of TSRs	Failure to detect UIS failure.	NA	[redacted]	OF_SR5	Mitigated	Office	ID	OF_SR5 testing not complete
Office HL - 364	SSHA TSR Transformai	Static STSDB	Improper management of TSRs	Excessive Interpolation error due to missing milepost data	ID		OF_SR176	Closed		IE	allocated to the system
Office HL - 365	SSHA TSR Transformai	Static STSDB	Improper management of TSRs	Error in STS sw or map data	ID		OF_SR179	Mitigated		IE	
Office HL - 366	SSHA TSR Transformai	OBC	Train not receiving TSR	Overlapping TSRs sent to OBC	ID		OF_SR180	Closed		IE	allocated to system
Office HL - 367	Office FTA	RWPS	TSR removed with EIC in area.	RWPS superuser role assigned.	IC		OF_SR181	Mitigated		ID	SRAC this is an operational reqmt; need to inspect Op manual

8 Attachment D – Transponder Hazard Log

3035819 Rev_N Attachment D – Transponder Hazard Log – DOORS /LIRR_MNR PTC/3. Technical Analysis/Hazard/Subsytem Hazard Log/Transponder Hazard Log – Baseline 3.6 JW1

TP_SSHA_ID	Subsystem or Interface	Source of Hazard	Hazard Description	Primary Cause	RIsk Before	SA Status	Safety Requirements ID	Responsibility	FInal Risk	Remarks
TP HL - 3		TP_PHA_04	Maintenance personnel come into contact with electrical power source during programming/installation of transponder	Transponder test tools expose electrcial power source to operator	IB	Mitigated	TP_SR_7	Transponder Sfaety	IE	
TP HL - 5	On-Board Computer (OBC)	TP_PHA_07	Transponder provides Source for hazardous smoke	ACSES II speed limit on curve is incorrect	IB	Closed	TP_SR_8 TP_SR_9 TP_SR_10 TP_SR_11	Transponder Safety	IE	
TP HL - 83	Transponder	TP_PHA_09	Inhalation damage to passengers, crew, and third parties	incorrect materials selection, etc.(PHA_51)	IB	Closed	TP_SR_12		IE	From latest Transponder PHA document 3036413 Rev_C

TP HL - 12	On-Board Computer (OBC) Transponder	TP_PHA_01 SHA-10 SHA-14	Onboard Recieves incorrect transponder telegram	ACSES II wrongly locating train relative to Limit of Movement Authority .	IB	[redacted]	Closed	TP_SR_8 TP_SR_9 TP_SR_10 TP_SR_13	Transponder Safety	IE	Analysis demonstrated in the FTA.
TP HL - 88	Transponder	TP_PHA_14	TP Data Incorrect	Transponder data modified by external influence.	IC		Closed	TP_SR_8		ID	From latest Transponder PHA document 3036413 Rev_C

TP HL - 75	Transponder	TP_PHA_01	Train not correctly enforced by ACSES II (PHA_03)	ACSES II wrongly locating train relative to Limit of Movement Authority .	IB	[redacted]	Closed	TP_SR_8 TP_SR_9 TP_SR_10 TP_SR_13		IE	From latest Transponder PHA document 3036413 Rev_C PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction.
TP HL - 77	ACSES II wayside equipment	TP_PHA_02 TP_PHA_24 TP_OHA_06	Transponder installed such that it interferes with train movement.	Transponder not correctly installed	IB		Closed	TP_SR_14		IE	From latest Transponder PHA document 3036413 Rev_C

TP HL - 78	Trannsponder	TP_PHA_03	ACSES II train derails as train speed is higher then safe operating speed. (PHA_39)	ACSES II speed limit on curve is incorrect	IB	[redacted]	Closed	TP_SR_8 TP_SR_9 TP_SR_10 TP_SR_11		IE	From latest Transponder PHA document 3036413 Rev_C PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction

TP HL - 79	Transponder	TP_PHA_04	Train not correctly enforced by ACSES II (PHA_12)	ACSES II wrongly locating train relative to Limit of Movement Authority	IB	[redacted]	Closed	TP_SR_8 TP_SR_9 TP_SR_10		IE	From latest Transponder PHA document 3036413 Rev_C PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 84	Transponder	TP_PHA_10	Train violates Home Signal after turnback	If the train tail is not past the HS transponder when the turnback is performed the tail OBC will not be able to enforce a PTS. (PHA_60)	IB		Mitigated	TP_SR_16 TP_SR_17 TP_SR_86		IE	From latest Transponder PHA document 3036413 Rev_C

TP HL - 86	Transponder	TP_PHA_12 TP_OHA_05	Train Speeds not correctly enforced by ACSES II	ACSES II wrongly locating train relative to Limit of Movement Authority (PHA_66)	IIB	[redacted]	Closed	TP_SR_8 TP_SR_9 TP_SR_10 TP_SR_11 TP_SR_84		IIE	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 92	Transponder	PHA_66 TP_OHA_11	Train Speeds not correctly enforced by ACSES II	Transponder programmed with incorrect data or the incorrect packet programmed into the wrong transponder.	IB		Closed	TP_SR_9 TP_SR_58 TP_SR_59		IE	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction

TP HL - 80	ACSES II	TP_PHA_05 TP_PHA_28 TP_OHA_07	Train speeds not correctly enforced by ACSES II	Transponder programmed with incorrect data or the incorrect packet programmed into the wrong transponder	IB	[redacted]	Closed	TP_SR_8 TP_SR_9 TP_SR_10 TP_SR_11		ID	From latest Transponder PHA document 3036413 Rev_C PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction

				Transponder programmed with incorrect data or the incorrect packet programmed into the wrong transponder. (PHA_92)							
				Wrong file selected by Operator using HHC							
TP HL - 87	Transponder	TP_PHA_13 TP_PHA_15 TP_PHA_16 TP_SSHA_08	TP data incorrect	Wrong file selected by operator with PTE	IC	[redacted]	Closed	TP_SR_10 TP_SR_11 TP_SR_18		IE	From latest Transponder PHA document 3036413 Rev_C

TP HL - 81	ACSES II Transponder	TP_PHA_06 TP_OHA_08 TP_SSHA_06 TP_SSHA_07	Train speeds not correctly enforced by ACSES II (PHA_36)	Transponder programmed with incorrect data or the incorrect packet programmed into the wrong transponder.	IB	[redacted]	Closed	TP_SR_8 TP_SR_9 TP_SR_10 TP_SR_11 TP_SR_19		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 93	Transponder	PHA_92 TP_OHA_12	TP data incorrect	Transponder programmed with incorrect data or the incorrect packet programmed into the wrong transponder.	IB		Closed	TP_SR_10 TP_SR_11		IE	

TP HL - 82	ACSES II Transponder	TP_PHA_07 TP_OHA_09 PHA_39	ACSES II train derails as train overspeeds	Transponder programmed with incorrect data or the incorrect packet programmed into the wrong transponder.	IB	[redacted]	Closed	TP_SR_8 TP_SR_9 TP_SR_10 TP_SR_11		IE	From latest Transponder PHA document 3036413 Rev_C PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 13	Transponder	TP_PHA-02	One or more trains not correctly enforced by ACSESII - wrong locatoon of train	Wayside equipment not correctly installed	IB		Closed	TP_SR_14	Transponder Safety	IE	

TP HL - 14	On-Board Computer (OBC) Transponder	TP_PHA-03	Train or wayside envelope not respected	ACSES II speed limit on curve is incorrect	IB	[redacted]	Closed	TP_SR_8 TP_SR_9 TP_SR_10 TP_SR_11	Transponder Safety	IE	Analysis demonstrated in the FTA. PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 17	Transponder	PHA-23 PHA-24	Transponder not correctly enforced by ACSES II - wrong location of train.	Transponder or its equipment was installed such that it fouls train movement.	IB		Closed	TP_SR_21 TP_SR_22	Transponder Safety	IE	Review the installation procedure.

TP HL - 18	On-Board Computer Transponder	SSCD 3.3 1	Transponder provides incorrect location or speed	Transponder message modified without authorization or moved without authorization.	IB	[redacted]	Closed	TP_SR_8 TP_SR_9 TP_SR_10 TP_SR_85		IE	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 19	Transponder	SSCD 3.3 -2	Transponder data was not verified during installation	Transponder data corrupted and OBC unable to detect data corrruption.	IB		Closed	TP_SR_26		IE	
TP HL - 20	Transponder	SSCD 3.3. -3 SSCD 3.3 - 4 SSCD 3.3 - 5	Transponder or its equipment was installed such that it fouls train movement	Transponder spaced to close will not be read.	IB		Closed	TP_SR_29		IE	

TP HL - 59	Transponder		Transponder fails to respond to scanner and provide data to train.	Transponder installation causes the air gap between the train and transponder to be less than 9 or more than 13 inches	IB	[redacted]	Closed	TP_SR_27 TP_SR_28 TP_SR_29 TP_SR_30 TP_SR_31		IE	

TP HL - 60	Transponder	TP_IHA-02	Transponder fails to respond to scanner and provide data to train.	Scanner installation causes the air gap between the scanner and transponder to be less than 9 in. or more than 13 in.	IIB	[redacted]	Closed	TP_SR_30 TP_SR_31 TP_SR_32		IID	
TP HL - 61	PTE	TP_IHA-04	Repeated exposure to radiation.	The PTE transmits 27 MHz radio signals within acceptable transmission power ranges for human safety. Frequent exposure to RF transmissions at a close range should be avoided.	IIIC		Mitigated	TP_SR_33		IIID	

TP HL - 64	On-Board Computer	TP_IHA_05	Onboard receives incorrect transponder telegram	Failure in transponder memory prior to transmission of transponder telegram to onboard	IB	[redacted]	Closed	TP_SR_8		IE	
TP HL - 65	On-Board Computer	TP_IHA_06	Onboard receives incorrect transponder telegram	Interference in transmission of transponder telegram to onboard	IB		Closed	TP_SR_8		IE	
TP HL - 66	HHC to PTE	TP_IHA_07	Transponder is programed with incorrect telegram	Transmission error in HHC.	IB		Closed	TP_SR_10 TP_SR_37 TP_SR_38		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 67	HHC to PTE	TP_IHA_08	Transponder is programed with incorrect telegram.	The incorrect file is selected by the user to be programmed on to the transponder	IB		Closed	TP_SR_10 TP_SR_37 TP_SR_38		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction

TP HL - 68	HHC to PTE	TP_IHA_09	Transponder is programed with incorrect telegram.	Failure in PTE	IB	[redacted]	Closed	TP_SR_10 TP_SR_37 TP_SR_38		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 69	SDMF to HHC	TP_IHA_10	Transponder is programmed with a telegram with incorrect data	Old File on HHC is used instead of file from SDMF	IB		Closed	TP_SR_10 TP_SR_39 TP_SR_50		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 70	SDMF to HHC	TP_IHA_11	Transponder is programmed with a telegram with incorrect data	Failure in SDMF transmission to HHC	IB		Closed	TP_SR_10 TP_SR_37 TP_SR_38 TP_SR_40		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction

TP HL - 71	Transponder to On-board COmputer	TP_IHA_12	Onboard receives incorrect transponder telegram	Metal within a defined area of the transponder installation causes cross talk.	IB	[redacted]	Closed	TP_SR_10		ID	
TP HL - 72	Transponder to On-board Computer	TP_IHA_13	Train fails to receive or looses a transponder packet.	Too many messages sent from Transponder to Onboard as train is parked over transponder.	IB		Mitigated	TP_SR_42 TP_SR_43 TP_SR_44		ID	
TP HL - 73	Transponder to On-board Computer	TP_IHA_14	Cross talk between sets	Transponder set on another line provides data for a train on a different track	IB		Closed	TP_SR_45		ID	
TP HL - 74	Transponder to On-board Computer	TP_IHA_15	Transponder Missed	Transponder with NULL programming installed in tracks.	IB		Mitigated	TP_SR_46		ID	

TP HL - 21		SSCD 3.3 - 6 SSCD 3.3 - 7 SSCD 3.3 8 SSCD 3.3 -9	Transponder Location	Transponder signal distorted by mteal near track..	IB		Closed	TP_SR_45 TP_SR_47 TP_SR_48 TP_SR_49		ID	
TP HL - 25	HHC to PTE	TP-IHA-07	Transponder is programed with incorrect telegram.	Transmission error in HHC.	IB		Closed	TP_SR_10 TP_SR_37 TP_SR_38		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction

TP HL - 26	HHC to PTE	TP_IHA_08	Transponder installation causes air gap between the train and transponder to be less than 9 inches or more than 13 inches.	The incorrect file is selected by the user to be programmed onto the transponder	IB	[redacted]	Closed	TP_SR_10 TP_SR_37 TP_SR_38		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 27	HHC to PTE	TP_IHA_09	Train violates home signal after turnback.	Failure in PTE	IB		Closed	TP_SR_10 TP_SR_37 TP_SR_38		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 28	SDMF to HHC	TP_IHA_10	Transponder is programmed with a telegram with incorrect data	Old File on HHC is used instead of file from SDMF	IB		Closed	TP_SR_10 TP_SR_37 TP_SR_39 TP_SR_50		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction

TP HL - 29	SDMF to HHC	TP_IHA_11	Transponder is programmed with a telegram with incorrect data	Failure in SDMF transmission to HHC.	IB	[redacted]	Closed	TP_SR_10 TP_SR_37 TP_SR_38 TP_SR_40		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction
TP HL - 30	TP to Onboard	TP_IHA_12	Onboard receives incorrect transponder telegram	Metal within a defined area of the transponder installation causes cross talk.	IB		Closed	TP_SR_41		ID	
TP HL - 31	TP to Onboard	TP_IHA_13	Train fails to receive or looses a transponder packet.	Too many messages sent from Transponder to Onboard as train is parked over transponder.	IB		Mitigated	TP_SR_42 TP_SR_44		ID	
TP HL - 32	TP to Onboard	TP_IHA_14	Cross talk between sets	Transponder set on another line provides data for a train on a different track.	IB		Closed	TP_SR_45		ID	
TP HL - 33	TP to Onboard	TP_IHA_15	Transponder Missed by Onboard	Transponder programmed with NULLs causes delay in onboard processing of transponder data.	IB		Mitigated	TP_SR_52		ID	

TP HL - 89	Operations	TP_OHA_02	Trains being operated at full operating speeds prior to reading the first DS set are traveling to fast to enforce PTS in sidings / yards where space is limited.	Train Speed too fast to enforce stop in all conditions.	IC	[redacted]	Closed	TP_SR_55		ID	
TP HL - 90	Operations	TP_OHA_01	During transponder installation/maintenance activities, wayside crew hit by train.	Protective TSR not established prior to work being authorized	IB		Mitigated	TP_SR_56 TP_SR_57		ID	
TP HL - 91	Operations	TP_OHA_04	Train Overspeeds after missing transponder	ACSES indicates missed transponder to the train engineer but does not display and may not be able to enforce speed restrictions.	IC		Closed	TP_SR_58 TP_SR_59		ID	
TP HL - 94	Operations	TP_OHA_13	Transponder unintentionally or accidently Removed	Transponder Removed by snow plow	IC		Mitigated	TP_SR_60		ID	
TP HL - 95	Maintenance	TP_OHA_14	User subjected to repeated EMI/EMC	Transponder programming requires verification of programming through RF interface.	IC		Mitigated	TP_SR_33		ID	
TP HL - 96	Maintenance	TP_OHA_15	Maintaineer trips due to Transponder Installation.	Transponder are installed at a certain height above the track bed and can pose a tripping hazard	IC		Mitigated	TP_SR_62		ID	

TP HL - 97	System	TP_SSHA_01	Train overruns a PTS target	Train misses Transponder with PTS packet	IB	[redacted]	Closed	TP_SR_30 TP_SR_31 TP_SR_59 TP_SR_76		ID	

TP HL - 98	Installation Checks	TP_SSHA_02	Train overruns a PTS target	Transponder located in the wrong location or moved.	IB	[redacted]	Closed	TP_SR_9 TP_SR_10 TP_SR_18 TP_SR_68 TP_SR_69 TP_SR_70 TP_SR_81 TP_SR_82		ID	

TP HL - 99	Transponder	TP_SSHA_03	Train speed exceeds Maximum Authorized Speed	Train misses Transponder with MAS Packet	IB	[redacted]	Closed	TP_SR_30 TP_SR_31 TP_SR_59		ID	

TP HL - 100	Installation Checks	TP_SSHA_04	Train speed exceeds Maximum Authorized Speed	Transponder located in the wrong location or moved	IB	[redacted]	Closed	TP_SR_9 TP_SR_10 TP_SR_18 TP_SR_63		ID	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction

TP HL - 101	Transponder	TP_SSHA_05	Train speed exceeds Permanant Speed Restriction	Train misses Transponder with PSR Packet	IB	[redacted]	Closed	TP_SR_30 TP_SR_31 TP_SR_59 TP_SR_72		IE	PICO will test TP index, including order of TP index within the set, Set ID, and location of each TP in the set. Onboard can also verify linking distances between Up/Down sets to determine proper direction

TP HL - 102	Installation Checks	TP_SSHA_09	Train speed exceeds Permanant Speed Restriction	Transponder located in the wrong location or moved	IB	[redacted]	Closed	TP_SR_9 TP_SR_10 TP_SR_18 TP_SR_63		ID	
TP HL - 103	Database process	TP_SSHA_10	Train speed exceeds Route Dependent Speed Restricton	Transponder programmed with incorrect speed	IB		Mitigated	TP_SR_11 TP_SR_64		IE	
TP HL - 104	Database Process	TP_SSHA_11	Train speed exceeds Route Dependent Speed Restricton	RR provides incorrect speed information	IB		Mitigated	TP_SR_19 TP_SR_66 TP_SR_67		ID	

TP HL - 105	Installation Checks	TP_SSHA_12	Train speed exceeds Route Dependent Speed Restricton	Transponder programmed with wrong data	IB	[redacted]	Closed	TP_SR_10 TP_SR_83		ID	
TP HL - 106	Installation Checks	TP_SSHA_13	Train speed exceeds Route Dependent Speed Restricton	Transponder located in the wrong location or moved	IB		Mitigated	TP_SR_9 TP_SR_10 TP_SR_18 TP_SR_63 TP_SR_64 TP_SR_72 TP_SR_73		ID	

TP HL - 107	Transponder	TP_SSHA_14	Train speed exceeds Route Dependent Speed Restricton	Train misses Transponder with PSR Packet	IB	[redacted]	Closed	TP_SR_30 TP_SR_31 TP_SR_59		ID	
TP HL - 108	Transponder	TP_SSHA_15	Train exceeds PTS or PTS target points.	Transponder sapcing not designed to limit posotion error to 500'	IB		Closed	TP_SR_65		IE	
TP HL - 109	Transponder	TP_SSHA_16	Train exceeds PTS of a Forward PTS packet.	Transponder with forward PTS packet missed.	IB		Closed	TP_SR_30		IE	

TP HL - 110	WIU	TP_SSHA_17	Train fails to stop at a Signal in a LoMA	DS Packet in HS transponder set missed	IB	[redacted]	Mitigated	TP_SR_79		ID	WIU is to proivde the LoMA as redundant stop notification. Need to add System safety requirement
TP HL - 111	Transponder	TP_SSHA_18	Train exceeds PTS Point near a station.	Train from another RR incorrectly determines stoping distnace from Accurate stop package.	IB		Closed	TP_SR_80		IE	Tennant OBC may have different accurate stop functionality therefore clear speration of accurate stop between RR to be implemented to prevent PTS overrun.
TP HL - 112	Transponder	TP_SSHA_19	Train exceeds PTS point near a station.	Transponder installed incorrectly	IB		Closed	TP_SR_9 TP_SR_10		IE	
TP HL - 113	Transponder	TP_SSHA_20	Train fails to stop prior to highway Grade Crossing	Missed transponder causes the position error to exceed 250'	IB		Closed	TP_SR_65		IE	

TP HL - 114	Transponder	TP_SSHA_21	Train fails to read transponder when in ACSES Mode	Constructon zone exit transponder missed or not read by onboard	IB	[redacted]	Closed	TP_SR_10 TP_SR_58 TP_SR_77		IE	
TP HL - 116	Transponder	TP_SSHA_22	Train exceeds MTEA speed limit	Exit transponder missed.	IB		Closed	TP_SR_74 TP_SR_75 TP_SR_78		IE	

9 Attachment E – RWPS Hazard Log

3035819 Rev_N Attachment E – RWPS Hazard Log – DOORS /LIRR_MNR PTC/3. Technical Analysis/Hazard/Subsytem Hazard Log/RWPS Hazard Log – Baseline 3.7 JW1

[redacted]

ID	Subsystem or Interfaces	Source of Hazard	Hazard Description	Potential Cause	Initial Risk	Safety Reqruirement ID	Safety Status	Responsibility	FInal Risk	Remarks
RWPS HL - 47	EIC Terminal, RWPS Workstation	RWPS_PHA_01	RWPS indicate TSR where no TSR has been applied. Or RWPS receives an incorrect TSR report from STS.	Message Failure between STS and RWPS. RWPS Failure indicating a TSR where no TSR exists	IB	RWPS_SR-3 RWPS_SR-28 RWPS_SR-55	Mitigated	RWPS Safety	ID	
RWPS HL - 48	EIC Terminal, RWPS Workstation	RWPS_PHA_02	TSR Requested or removed from incorrect location.	RWPS Database provides incorrect location RWPS Equipment Fails sending request for wrong location. EIC enters wrong location	IB	RWPS_SR-4 RWPS_SR-12 RWPS_SR-26 RWPS_SR-28 RWPS_SR-30	Mitigated	RWPS Safety	ID	
RWPS HL - 114	EIC Terminal, RWPS Workstation	RWPS_PHA_03	TSR removed from incorrect location.	RWPS Databse provides incorrect location. RWPS Equipment sends request for wrong location. EIC enters wrong location.	IB	RWPS_SR-4 RWPS_SR-12 RWPS_SR-28	Closed	RWPS Safety	ID	
RWPS HL - 49	All s/systems	RWPS-PHA-05	Person in contact with or near an electrical power source.	Inadequate maintenance procedures.	IB	RWPS_SR-6	Mitigated	RWPS Safety	IE	

RWPS HL - 50	All s/systems	RWPS-PHA-06	Burns to passengers, crew and third parties.	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection etc.	IIIB	[redacted]	RWPS_SR-7 RWPS_SR-8	Mitigated	RWPS Safety	IIID	
RWPS HL - 51	All s/systems	RWPS-PHA-07	Inhalation damage to passengers, crew, and third parties.	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection etc.	IB		RWPS_SR-7 RWPS_SR-8	Mitigated	RWPS Safety	IE	
RWPS HL - 52	EIC Terminal, RWPS Workstation	RWPS-PHA-08	TSR improperly removed.	Unauthorized access to EIC Terminal allows a user to request to remove TSR without authorization.	IB		RWPS_SR-9 RWPS_SR-10	Closed	RWPS Safety	IE	
RWPS HL - 53	All s/systems	RWPS-PHA-09	Design of RWPS created components that injure maintenance or installation staff.	Components have heavy weights, sharp edges etc.	IIIB		RWPS_SR-11	Mitigated	RWPS Safety	IIIE	
RWPS HL - 54	SDMT	RWPS-PHA-10	TSR Requested for incorrect location.	Database Generation Error.	IB		RWPS_SR-13	Mitigated	RWPS Safety	IE	
RWPS HL - 55	RWPS	RWPS-PHA-11	TSR improperly removed.	Invalid user logged in from WiFi or Cellular System.	IB		RWPS_SR-14	Closed	RWPS Safety	ID	
RWPS HL - 56	EIC	RWPS-PHA-12	TSR Requested for incorrect location.	EIC Database Failure.	IB		RWPS_SR-15 RWPS_SR-28	Mitigated	RWPS Safety	ID	
RWPS HL - 57	Office	RWPS-PHA-13	TSR Requested for incorrect location.	RWPS Server Database Version Error.	IB		RWPS_SR-16 RWPS_SR-17	Mitigated	RWPS Safety	IE	

RWPS HL - 58	RWPS	RWPS-PHA-14	TSR Requested for incorrect location.	RWPS Server Database Version Error.	IB	[redacted]	RWPS_SR-18 RWPS_SR-28	Mitigated	RWPS Safety	ID	
RWPS HL - 59	EIC	RWPS-PHA-15	TSR Requested for incorrect location.	EIC Terminal has incorrect SW.	IB		RWPS_SR-19	Mitigated	RWPS Safety	ID	
RWPS HL - 60	Office	RWPS-PHA-16	TSR improperly removed.	Secondary EIC sends remove request for TSR.	IB		RWPS_SR-20 RWPS_SR-21	Mitigated	RWPS Safety	IE	
RWPS HL - 61	RWPS	RWPS-PHA-17	TSR Indicated on EIC but not enforced.	Loss of communication between EIC and RWPS or RWPS and office.	IB		RWPS_SR-22 RWPS_SR-23 RWPS_SR-24 RWPS_SR-28	Closed	RWPS Safety	ID	
RWPS HL - 62	RWPS	RWPS-PHA-18	Incorrect TSR Location.	Communication failure between STS and RWPS.	IB		RWPS_SR-18 RWPS_SR-25 RWPS_SR-27 RWPS_SR-28	Closed	RWPS Safety	ID	

RWPS HL - 63	EIC	RWPS-PHA-19	Incorrect TSR Location.	Loss of communication between RWPS and EIC.	IB	[redacted]	RWPS_SR-22 RWPS_SR-23	Closed	RWPS Safety	ID	
RWPS HL - 64	Office	RWPS-PHA-20	Incorrect TSR Location.	Communication Error between RWPS and EIC.	IB		RWPS_SR-4 RWPS_SR-22	Closed	RWPS Safety	IE	
RWPS HL - 65	EIC	RWPS-PHA-21	Incorrect TSR Location.	Loss of communication between RWPS and UIS.	IB		RWPS_SR-24	Closed	RWPS Safety	ID	
RWPS HL - 66	Office	RWPS-PHA-22	Incorrect TSR Location.	Communication Error between RWPS and UIS.	IB		RWPS_SR-4 RWPS_SR-22	Closed	RWPS Safety	IE	
RWPS HL - 67	Office	RWPS-PHA-23	Incorrect TSR Location.	EIC Request work zone entry error.	IB		RWPS_SR-4	Closed	RWPS Safety	IE	
RWPS HL - 68	Office	RWPS-PHA-24	Incorrect TSR Location.	EIC Remove work zone entry error.	IB		RWPS_SR-4	Closed	RWPS Safety	IE	
RWPS HL - 69	Office	RWPS-PHA-25	Incorrect TSR Location.	Primary EIC change request error.	IB		RWPS_SR-20	Mitigated	RWPS Safety	IE	

RWPS HL - 70	RWPS	RWPS-PHA-26	TSR removed too early.	Primary EIC change request error.	IB	[redacted]	RWPS_SR-18 RWPS_SR-24 RWPS_SR-28 RWPS_SR-29	Mitigated	RWPS Safety	IE	
RWPS HL - 71	RWPS	RWPS-PHA-27	TSR requested too late.	Primary EIC change request error.	IB		RWPS_SR-18 RWPS_SR-24 RWPS_SR-28 RWPS_SR-29	Mitigated	RWPS Safety	IE	
RWPS HL - 72	RWPS	RWPS-PHA-28	Incorrect TSR Location.	EIC determines work zone location incorrectly.	IB		RWPS_SR-4	Closed	RWPS Safety	IE	
RWPS HL - 73	RWPS	RWPS-PHA-29	TSR removed too early.	EIC detemines that track is available for operations without all workers or work trains removed.	IB		RWPS_SR-29	Mitigated	Railroad	ID	

RWPS HL - 74	RWPS / Office	RWPS_IHA_01	TSR Request from RWPS fails to be set in the Office Subsystem.	Loss of Interface between RWPS and Office.	IB	[redacted]	RWPS_SR-31 RWPS_SR-32 RWPS_SR-33 RWPS_SR-43 RWPS_SR-44 RWPS_SR-89	Closed	RWPS Safety	ID	
RWPS HL - 75	RWPS / Office	RWPS_IHA_02	TSR request message from RWPS is corrupted before Office receives.	Incorrect Transfer of Information between RWPS and Office.	IB		RWPS_SR-34 RWPS_SR-45 RWPS_SR-87	Closed	RWPS Safety	ID	

RWPS HL - 76	RWPS / EIC Handheld	RWPS_IHA_03	TSR Request from EIC fails to be set in RWPS and in Office.	Loss of RWPS Interface to EIC Handheld.	IB	[redacted]	RWPS_SR-33 RWPS_SR-35 RWPS_SR-36 RWPS_SR-39 RWPS_SR-81 RWPS_SR-94	Mitigated	RWPS Safety	ID	
RWPS HL - 77	RWPS / EIC Handheld	RWPS_IHA_04	TSR request from EIC Handheld is incorrect.	Deliberate attack causes incorrect transfer of information.	IB		RWPS_SR-36 RWPS_SR-37 RWPS_SR-38 RWPS_SR-95	Closed	RWPS Safety	ID	
RWPS HL - 78	RWPS / RWPS	RWPS_IHA_06 RWPS_OHA_03	Both RWPS servers become controlling. TSR Request not sent to Office.	Dual failure of GBN network prevents health check messages.	IB		RWPS_SR-41 RWPS_SR-55 RWPS_SR-81	Mitigated	RWPS Safety	IE	

RWPS HL - 79	RWPS / EIC Handheld	RWPS_IHA_07	EIC Terminal receives a corrupted message from RWPS and displays the data to the EIC.	Deliberate attack causes incorrect data transfer from RWPS to EIC Handheld.	IB	[redacted]	RWPS_SR-36 RWPS_SR-38 RWPS_SR-47	Closed	RWPS Safety	ID	
RWPS HL - 80	RWPS / EIC Workstation	RWPS_IHA_08	EIC Terminal receives a corrupted message from RWPS and displays the data to the EIC.	Deliberate attack causes incorrect data transfer from RWPS to EIC Workstation.	IB		RWPS_SR-38 RWPS_SR-47 RWPS_SR-48	Closed	RWPS Safety	ID	
RWPS HL - 81	RWPS / EIC Handheld	RWPS_IHA_09	TSR request from EIC Handheld is incorrect.	Radio Interference causes incorrect transfer of information.	IB		RWPS_SR-36 RWPS_SR-37 RWPS_SR-38 RWPS_SR-49 RWPS_SR-95	Closed	RWPS Safety	ID	
RWPS HL - 82	RWPS / EIC Workstation	RWPS_IHA_13	EIC Terminal receives a corrupted message from RWPS and displays the data to the EIC.	Radio Interference causes incorrect transfer from RWPS to EIC Workstation..	IB		RWPS_SR-38 RWPS_SR-47	Closed	RWPS Safety	ID	

RWPS HL - 83	Superuser / Operation Superuser Workstation	RWPS_IHA_14	TSR removed while work crew on track.	EIC Handheld loss of communication not indicated to staff.	IB	[redacted]	RWPS_SR-29 RWPS_SR-63	Closed	Railroad	ID	
RWPS HL - 84	Display Interface for Superuser	RWPS_IHA_15	Single user removes TSR without proper checks.	Superuser logged in at UIS and RWPS.	IB		RWPS_SR-29 RWPS_SR-52	Mitigated	RWPS Safety	ID	
RWPS HL - 85	RWPS / NMS	RWPS_IHA_16	Wrong RWPS Server Active and Controlling.	Loss of communication - Remote reset of RWPS not possible.	IB		RWPS_SR-33	Mitigated	RWPS Safety	ID	
RWPS HL - 86	RWPS / EIC Workstation	RWPS_IHA_17	TSR request from EIC fails to be set in RWPS and in Office.	Loss of RWPS Interface to EIC Workstation.	IB		RWPS_SR-33 RWPS_SR-35 RWPS_SR-46 RWPS_SR-81 RWPS_SR-94	Closed	RWPS Safety	ID	

RWPS HL - 87	NMS / EIC Handheld	RWPS_IHA_18	Staff assumed clear when EIC is loss of comm.	Loss of EIC to NMS communication.	IB	[redacted]	RWPS_SR-29 RWPS_SR-35 RWPS_SR-81 RWPS_SR-94	Mitigated	Railroad	ID	
RWPS HL - 88	Installing Executables and Data Configuration Files for RWPS	RWPS_IHA_19 RWPS_OHA_21	Error in TSR Indication to EIC.	Executable Corruption.	IB		RWPS_SR-16 RWPS_SR-82 RWPS_SR-85	Open	RWPS Safety	ID	Still working on implemetnation of map check with RWPS
RWPS HL - 89	Installing Executables and Data Configuration files for EIC	RWPS_IHA_20 RWPS_OHA_22	Error in TSR Indication to EIC.	EIC Terminal executes incorrect executable.	IB		RWPS_SR-16 RWPS_SR-83	Open	RWPS Safety	ID	Still working on implementation of Map Chedk with RWPS
RWPS HL - 90	EIC / EIC Handheld	RWPS_IHA_21	Error in TSR Indication to EIC.	Screen changes TSR Start/Stop location or speed.	IB		RWPS_SR-33 RWPS_SR-38	Mitigated	RWPS Safety	ID	

RWPS HL - 91	EIC / EIC Workstation	RWPS_IHA_22	Error in TSR Indication to EIC.	Screen changes TSR Start/Stop location or speed.	IB	[redacted]	RWPS_SR-33 RWPS_SR-38	Mitigated	RWPS Safety	ID	
RWPS HL - 92	Office / RWPS	RWPS_IHA_23	TSR list from Office fails to be sent to the RWPS Subsystem.	Loss of Interface between Office and RWPS.	IB		RWPS_SR-18 RWPS_SR-31 RWPS_SR-32 RWPS_SR-33 RWPS_SR-43 RWPS_SR-44 RWPS_SR-84 RWPS_SR-89	Mitigated	RWPS Safety	ID	
RWPS HL - 93	Office / RWPS	RWPS_IHA_24	TSR list from Office is corrupted before RWPS receives.	Incorrect transfer of information between Office and RWPS.	IB		RWPS_SR-12 RWPS_SR-27 RWPS_SR-88	Closed	RWPS Safety	ID	

RWPS HL - 94	Wayside / Office / Onboard	RWPS_OHA_01	Maintenance of Electrical Equipment.	The maintenance or testing operator mistakenly connects to high power sources.	IC	[redacted]	RWPS_SR-54	Mitigated	Railroad	ID	
RWPS HL - 95	Office	RWPS_OHA_02	Train does not receive correct TSR and enters roadway worker protection area.	EIC Terminal User interface is not up to Human Factor Engineering Standard or best practice.	IC		RWPS_SR-55 RWPS_SR-72	Closed	RWPS Safety	ID	
RWPS HL - 97	RWPS	RWPS_OHA_04	TSR Removed with Secondary EIC in area.	RWPS failure allows TSR Removal when Secondary EIC still in area.	IC		RWPS_SR-57 RWPS_SR-63 RWPS_SR-74	Closed	RWPS Safety	ID	
RWPS HL - 98	RWPS	RWPS_OHA_05	EIC Terminal shows TSR where no TSR is enforced.	RWPS Failure indicates TSR where none exists.	IC		RWPS_SR-18 RWPS_SR-44 RWPS_SR-49 RWPS_SR-81	Closed	RWPS Safety	ID	
RWPS HL - 99	EIC Terminal	RWPS_OHA_06	EIC Terminal shows TSR where no TSR is enforced.	EIC Terminal Failure indicates TSR where none exists.	IC		RWPS_SR-49 RWPS_SR-81	Closed	RWPS Safety	ID	

RWPS HL - 100	RWPS	RWPS_OHA_07	TSR Removed with EIC in area.	Supervisor performs TSR Override with EIC still in area.	IC	[redacted]	RWPS_SR-52 RWPS_SR-60 RWPS_SR-61 RWPS_SR-62	Mitigated	RWPS Safety	ID	
RWPS HL - 101	RWPS	RWPS_OHA_08	TSR request not received by RWPS.	Loss of communication between EIC Terminal and RWPS.	IC		RWPS_SR-39 RWPS_SR-70 RWPS_SR-71 RWPS_SR-81	Mitigated	RWPS Safety	ID	
RWPS HL - 102	Office	RWPS_OHA_09	EIC Terminal shows TSR where no TSR is enforced.	STS Cold Start.	IC		RWPS_SR-67 RWPS_SR-78 RWPS_SR-79 RWPS_SR-80 RWPS_SR-81	Mitigated	Office Safety	ID	
RWPS HL - 103	RWPS	RWPS_OHA_10	Secondary EIC removed without authorization.	Unauthorized person requests removal of Secondary EIC.	IC		RWPS_SR-57 RWPS_SR-64 RWPS_SR-69	Closed	RWPS Safety	IE	

RWPS HL - 104	RWPS	RWPS_OHA_11	Primary EIC Removed from TSR without Acknowledgement.	Superuser override of Primary EIC Transfer.	IC	[redacted]	RWPS_SR-57 RWPS_SR-68	Mitigated	RWPS Safety	IE	
RWPS HL - 105	RWPS	RWPS_OHA_12	TSR Removed with Secondary EIC in area.	Primary EIC requests removal with Secondary EIC attached.	IC		RWPS_SR-55 RWPS_SR-57 RWPS_SR-63 RWPS_SR-64	Closed	RWPS Safety	IE	
RWPS HL - 106	RWPS	RWPS_OHA_13	TSR Request with incorrect data.	System Administrator loads incorrect data or Executable.	IC		RWPS_SR-55 RWPS_SR-65	Mitigated	RWPS Safety	IE	
RWPS HL - 107	EIC Handheld	RWPS_OHA_14	TSR Request with incorrect data.	Executable or data with incorrect data loaded.	IC		RWPS_SR-55 RWPS_SR-65 RWPS_SR-95	Closed	RWPS Safety	IE	
RWPS HL - 108	EIC Workstation	RWPS_OHA_15	TSR Request with incorrect data.	Executable or data with incorrect data loaded.	IC		RWPS_SR-55 RWPS_SR-65 RWPS_SR-95	Closed	RWPS Safety	IE	

RWPS HL - 109	RWPS	RWPS_OHA_16	Unauthorized users remove TSR.	System Administrator authorizes users for access who should not have access	IC	[redacted]	RWPS_SR-55 RWPS_SR-73	Mitigated	RWPS Safety	ID	
RWPS HL - 110	RWPS	RWPS_OHA_17	TSR request sent to UIS/STS at incorrect location or speed.	Incorrect static database prevents checks that RWPS could perform to reject requests.	IC		RWPS_SR-55 RWPS_SR-72 RWPS_SR-95	Closed	RWPS Safety	ID	
RWPS HL - 111	RWPS	RWPS_OHA_18	Parameters changed to unacceptable values.	Adjustment of default train speed set to high.	IB		RWPS_SR-73	Mitigated	RWPS Safety	ID	
RWPS HL - 112	EIC Terminal	RWPS_OHA_19	Work limits not extended for Secondary EIC.	Primary sets work limits too restrictive.	IC		RWPS_SR-75	Mitigated	RWPS Safety	ID	
RWPS HL - 113	EIC Terminal	RWPS_OHA_20	Work limits extend beyond beyond TSR.	Secondary sets work limits beyond TSR locations.	IC		RWPS_SR-76 RWPS_SR-77 RWPS_SR-93	Closed	RWPS Safety	IE	
RWPS HL - 115	Office	RWPS_OHA_23	TSR removed while Secondary EIC still in place.	UIS Cold Start.	IB		RWPS_SR-63 RWPS_SR-78 RWPS_SR-90 RWPS_SR-91	Closed	RWPS Safety	ID	

10 Attachment F – WIU Hazard Log

3035819 Rev_N Attachment F – WIU Hazard Log – DOORS /LIRR_MNR PTC/6. Siemens Data\Siemens_LIRR_MNR_PTC\48 SubVal\ WIU Subsytem Hazard Log – LIRR Baseline 1.0

WIU_SSHL_ID	Subsystem or Interface	Source of Hazard	Hazard Description	Primary Cause	Initial Risk	[redacted]	SR_ID	Safety Status	Responsibility	Final Risk	Remarks
WIU_SSHL_1	Maintenance	WIU-PHA-1	Unsafe Movement Authority Issued; Error in WIU vital input installation/ wiring results in less restrictive aspect than intended to WIU	Incorrect installation / wiring during maintenance due to improper installation instructions (manual; Book of Plans)	IC		WIU-SSHA-1	Mitigated Transferred Transferred	Wayside Safety Systems Safety Systems Safety	IE	
WIU_SSHL_2	Maintenance	WIU-PHA-2	Unsafe Movement Authority Issued; Error in WIU vital input installation/ wiring results in less restrictive aspect than intended to WIU	Incorrect installation / wiring during maintenance due to not following installation instructions correctly	IC		WIU-SSHA-2	Transferred Mitigated Transferred	Systems Safety Wayside Safety Systems Safety	IE	
WIU_SSHL_3	WIU WIU / OBC	WIU-PHA-3	Unsafe Movement Authority Issued; Vital input read incorrectly which results in WIU transmitting a less restrictive movement authority than intended to OBC	Hardware failure leading to a channel failure of the WIU	IC		WIU-SSHA-3	Mitigated	Wayside Safety	IE	
WIU_SSHL_4	WIU WIU / OBC	WIU-PHA-4	Unsafe Movement Authority Issued; Vital input read incorrectly which results in WIU transmitting a less restrictive movement authority than intended to OBC	Common-Mode hardware failure	IC		WIU-SSHA-4	Mitigated	Wayside Safety	IE	

WIU_SSHL_5	WIU / OBC WIU / OBC	WIU-PHA-5	Unsafe Movement Authority Issued; WIU transmits a less restrictive movement authority to OBC	Software execution error	IC	[redacted]	WIU-SSHA-5	Mitigated	Wayside Safety	IE	
WIU_SSHL_6	Maintenance	WIU-PHA-6	Unsafe Movement Authority Issued; WIU Configuration error which results in WIU sending an ATCS message with a less restrictive movement authority than intended	Configuration error during maintenance due to improper installation instructions (manual; Book of Plans)	IC		WIU-SSHA-6	Mitigated Transferred Transferred	Wayside Safety Systems Safety Systems Safety	IE	
WIU_SSHL_7	Maintenance	WIU-PHA-7	Unsafe Movement Authority Issued; WIU Configuration error which results in WIU sending an ATCS message with a less restrictive movement authority than intended	Configuration error during maintenance due to not following installation instructions correctly	IC		WIU-SSHA-7	Transferred Mitigated Mitigated Mitigated	Systems Safety Wayside Safety Wayside Safety Wayside Safety	IE	-
WIU_SSHL_8	WIU / OBC WIU / BCP	WIU-PHA-8	Unsafe Train Entry / Exit; OBC-ACSES fails to go to restrictive state in a timely manner when no ATCS messages are received	WIU fails to send the required ATCS messages	IC		WIU-SSHA-8	Transferred Mitigated	Systems Safety Wayside Safety	IE	-

WIU_SSHL_9	WIU / OBC WIU / BCP	WIU-PHA-9	Unsafe Train Entry / Exit; OBC-ACSES fails to go to restrictive state in a timely manner when no ATCS messages are received	Communication failure results in not receiving ATCS messages and OBC error	IC	[redacted]	WIU-SSHA-9	Transferred Mitigated	Systems Safety Wayside Safety	IE	-
WIU_SSHL_10	Operations WIU WIU	WIU-PHA-10	Unauthorized Access to PTC System (Malicious Attack or Damage by Trespasser); Malicious modifications of the VIU-20e software configuration leads to a hazardous event	Unauthorized personnel or action performed on the VIU-ACSES system	IC		WIU-SSHA-10	Transferred Mitigated Mitigated	Systems Safety Wayside Safety Wayside Safety	IE	-
WIU_SSHL_11	Maintenance	WIU-PHA-11	Unauthorized Access to PTC System (Maintainer Error); WIU issues an unsafe message due to being applied to an improper application	Unit is employed in an application for which the WIU was not designed	IC		WIU-SSHA-11	Transferred Mitigated Transferred	Systems Safety Wayside Safety Systems Safety	IE	-
WIU_SSHL_12	WIU WIU / OBC	WIU-PHA-12	Unsafe Movement Authority Issued; Non-vital function within WIU hardware & software leads to incorrect transmission of a movement authority	Non-vital subsystem used to send vital messages	IC		WIU-SSHA-12	Mitigated Transferred	Wayside Safety Systems Safety	IE	-

WIU_SSHL_13	Maintenance Maintenance WIU	WIU-PHA-13	Unauthorized Access to PTC System (Maintainer Error); Incorrect installation leads to a hazardous event	WIU with a verified site specific configuration is installed at the wrong site	IC	[redacted]	WIU-SSHA-13	Transferred Mitigated Mitigated	Systems Safety Wayside Safety Wayside Safety	IE	Consortium is collectively responsible for pre-revenue installation and testing of WIU.
WIU_SSHL_14	Wayside Wayside	WIU-PHA-14	Unsafe Movement Authority Issued; New software or relay logic for the legacy interlocking is not properly authorized, verified, tested which reports improper signal and switch status to WIU or authorized modifications to the legacy interlocking logic are not properly reflected in the WIU software configuration	Existing software or relay logic is not changed correctly or the WIU is not properly updated when legitimate modifications to the existing logic are made.	IC		WIU-SSHA-14	Transferred Mitigated	Systems Safety Wayside Safety	IE	-
WIU_SSHL_15	Maintenance	WIU-PHA-15	Unauthorized Access to PTC System; WIU application logic is improperly modified and creates a hazardous event	WIU application logic with respect to the default settings for configurable parameters and correct restrictive states is tampered with or changed	IC		WIU-SSHA-15	Transferred	Systems Safety	IE	-

WIU_SSHL_16	Maintenance	WIU-PHA-16	Unauthorized Access to PTC System; WIU Hardware is modified without authorization and creates a hazardous event	WIU internal hardware is modified [Boards/Chassis /etc.]	IC	[redacted]	WIU-SSHA-16	Transferred Mitigated	Systems Safety Wayside Safety	IE	-
WIU_SSHL_17	WIU / NMS Maintenance Maintenance	WIU-PHA-17	Unauthorized Access to PTC System; Failure is overlooked or improper corrective action is taken which creates a hazardous event	Improper corrective action is taken for a WIU failure	IC		WIU-SSHA-17	Mitigated Transferred Mitigated	Wayside Safety Systems Safety Wayside Safety	IE	-
WIU_SSHL_18	Maintenance	WIU-PHA-18	Unauthorized Access to PTC System; Periodic maintenance to prevent failure is not performed and leads to a hazardous event	Periodic preventative maintenance is not performed	IC		WIU-SSHA-18	Transferred	Systems Safety	IE	-
WIU_SSHL_19	WIU Wayside	WIU-PHA-19	Unsafe Movement Authority Issued; One or more trains; authority limit not correctly enforced by ACSES II	On-board enforces unsafe Limit of Movement Authority from wayside	IC		WIU-SSHA-19	Mitigated	Wayside Safety	IE	-

WIU_SSHL_20	Wayside	WIU-PHA-20	Unsafe Train Entry / Exit (Train Entering ASC from ABS); ATC fails to reduce the speed of a train after entering ASC from ABS territory	For LIRR ABS territory with ASC cut-out, a signal state could be "Stop and Proceed" which is considered permissive by ACSES II. If ATC fails to wake-up when entering the next ASC block the train could overspeed and cause a collision	IC	[redacted]	WIU-SSHA-20	Mitigated	Wayside Safety	IE	-
WIU_SSHL_21	WIU / OBC	WIU-PHA-21	Unsafe Movement Authority Issued; ATC cut-out	ACSES II does not detect that the ATC is cut-out and lets the train into the next block without safe train separation	IC		WIU-SSHA-21	Mitigated	Wayside Safety	IE	-
WIU_SSHL_22	WIU WIU Maintenance	WIU-PHA-22	Train Violates Movement Authority (Train Passes Signal at Red); WIU data incorrect	The vital application data / program has incorrect data	IC		WIU-SSHA-22	Mitigated Mitigated Transferred	Wayside Safety Wayside Safety Systems Safety	IE	-

WIU_SSHL_23	Wayside	WIU-PHA-23	Train Violates Movement Authority (Train Passes Signal at Red); Vital ACSES II data is not updated correctly because the WIU is reacting to invalid / stale data from the legacy system	Legacy system sends invalid / stale data to the WIU	IC	[redacted]	WIU-SSHA-23	Mitigated	Wayside Safety	IE	-
WIU_SSHL_24	WIU / OBC	WIU-PHA-24	Unsafe Movement Authority Issued; WIU configuration data incorrect (Signal ID, Track ID, Switch ID, Route ID, Entrance Signal ID, Exit Signal ID, Switch Positions, Entrance Track ID, Exit Track ID)	The vital configuration data / program has incorrect data	IC		WIU-SSHA-24	Mitigated	Wayside Safety	IE	-
WIU_SSHL_25	WIU / OBC	WIU-PHA-25	Overspeed; WIU configuration data incorrect (Speed, Distance to Speed Increase, Distance to Leave Current Track, Distance to Exit Track, Controlling Grade)	Train exceeds ACSES II target speed profile because the WIU configuration parameters are incorrect	IC		WIU-SSHA-25	Transferred Mitigated	Systems Safety Wayside Safety	IE	-
WIU_SSHL_26	WIU / OBC	WIU-PHA-26	Overspeed; Input data for configuration is incorrect (IJ Chainage, PTS Chainage, PS1 Chainage, PS2 Chainage, LOMA)	Train exceeds ACSES II target speed profile because input data (provided by the Systems Integrator) is incorrect for configuration calculations	IC		WIU-SSHA-26	Transferred	Systems Safety	IE	-

WIU_SSHL_27	WIU	WIU-PHA-27	EMI/EMC Disturbance Contributing to Signaling and Train Control Hazards; WIU messages corrupted due to EMI/EMC disturbance	Insufficient WIU immunity to EMI/EMC	ID	[redacted]	WIU-SSHA-27	Mitigated	Wayside Safety	IE	-
WIU_SSHL_28	Maintenance	WIU-PHA-28	Insufficient Protection for Personnel (Electrocution); Person in contact with or in close proximity to an electrical power source	Material with electrical potential due to the loss of proper grounding/bonding for the wayside PTC equipment/rack	IC		WIU-SSHA-28	Transferred	Systems Safety	IE	-
WIU_SSHL_29	WIU WIU / OBC Maintenance / Operations	WIU-PHA-29	Fire, Smoke; Damage or complete loss of WIU	Underrated cables, incorrect materials selection, insufficient protection against over voltage or shorted electric circuits	IC		WIU-SSHA-29	Mitigated Transferred Transferred	Wayside Safety Systems Safety Systems Safety	IE	-
WIU_SSHL_30	WIU / OBC Operations	WIU-PHA-30	Unsafe Train Entry / Exit; ACSES OBC fails to go to restrictive state in a timely manner when no ATCS messages are received	Communication failure due to a complete loss of power (e.g. Faulty Power Termination, DC-DC Converter Failure, Extended Mains Power Outage)	IC		WIU-SSHA-30	Transferred	Systems Safety	IE	-

WIU_SSHL_31	WIU WIU / NMS WIU / OBC	WIU-PHA-31	Unsafe Movement Authority Issued; WIU data incorrect or not complete	Communications lost between Main and Auxiliary WIUs	IC		WIU-SSHA-31	Mitigated Mitigated Transferred	Wayside Safety Wayside Safety Systems Safety	IE	-
WIU_SSHL_32	Wayside	WIU-PHA-32	Unsafe Train Entry / Exit; Battery signal improperly grounded which leads to a less restrictive aspect than intended reported to WIU	Improper wire terminations; loose wire, or poor separation / isolation causes an improper circuit ground	IC		WIU-SSHA-32	Mitigated Transferred	Wayside Safety Systems Safety	IE	-
WIU_SSHL_33	WIU Vital Executive Software	FMECA_1	Energized input interpreted as de-energized input; WIU will create WIU messages with more restrictive states	Corrupt processor data	IVC		WIU-SSHA-33	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_34	WIU Vital Executive Software	FMECA_2	De-energized input interpreted as a valid energized input; WIU reports incorrect and potentially less restrictive states	Corrupt processor data	IC		WIU-SSHA-34	Mitigated	Wayside Safety	IE	-
WIU_SSHL_35	WIU Vital Executive Software	FMECA_3	Logic execution error; WIU may display an incorrect and potentially less restrictive signal status and movement authority	Incorrect program	IC		WIU-SSHA-35	Mitigated	Wayside Safety	IE	-

WIU_SSHL_36	WIU Vital Executive Software	FMECA_4	Logic execution error; WIU may display an incorrect and potentially more restrictive signal status and movement authority	Incorrect program	IVC	[redacted]	WIU-SSHA-36	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_37	WIU Vital Executive Software	FMECA_5	Incorrect WIU message creation; WIU may display an incorrect and potentially less restrictive signal status and movement authority	Program error	IC		WIU-SSHA-37	Mitigated	Wayside Safety	IE	-
WIU_SSHL_38	WIU Vital Executive Software	FMECA_6	Incorrect WIU message creation; WIU may display an incorrect and potentially more restrictive signal status and movement authority	Program error	IVC		WIU-SSHA-38	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_39	WIU Vital Executive Software	FMECA_7	Incorrect ACSES encoder response message; WIU may display an incorrect and potentially less restrictive signal status and movement authority	Program error	IC		WIU-SSHA-39	Mitigated Transferred	Wayside Safety Systems Safety	IE	- Exported to OBC-
WIU_SSHL_40	WIU Vital Executive Software	FMECA_8	Incorrect ACSES encoder response message; WIU may display an incorrect and potentially more restrictive signal status and movement authority	Program error	IVC		WIU-SSHA-40	Mitigated Transferred	Wayside Safety Systems Safety	IVE	- Exported to OBC
WIU_SSHL_41	WIU Vital Executive Software	FMECA_9	MCF CRC Failure; WIU may report an incorrect and potentially less restrictive signal status	Data missing	IC		WIU-SSHA-41	Mitigated	Wayside Safety	IE	-

WIU_SSHL_42	WIU Vital Executive Software	FMECA_10	MCF CRC Failure; WIU may report an incorrect and potentially more restrictive signal status	Data missing	IVC		WIU-SSHA-42	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_43	WIU Vital Configuration	FMECA_11	Incorrect VIU-20e vital config. parameters; WIU may report an incorrect and potentially less restrictive signal status	Configuration error	IC		WIU-SSHA-43	Mitigated	Wayside Safety	IE	-
WIU_SSHL_44	WIU Vital Configuration	FMECA_12	Incorrect VIU-20e vital config. parameters; WIU may report an incorrect and potentially more restrictive signal status	Configuration error	IVC		WIU-SSHA-44	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_45	WIU Vital Configuration	FMECA_13	Signal status is mapped incorrectly; May result in reporting a less restrictive signal status, speed, and movement authority	User configuration error	IB		WIU-SSHA-45	Mitigated	Wayside Safety	IE	-
WIU_SSHL_46	WIU Vital Configuration	FMECA_14	Signal status is mapped incorrectly; May result in reporting a more restrictive signal status, speed, and movement authority	User configuration error	IVB		WIU-SSHA-46	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_47	WIU Vital Application Software (Generic Application)	FMECA_15	Application error; May result in reporting less restrictive signal status, and movement authority	Incorrect variable used; Data corrupted during internal handling	ID		WIU-SSHA-47	Mitigated	Wayside Safety	IE	-

WIU_SSHL_48	WIU Vital Application Software (Generic Application)	FMECA_16	Application error; May result in reporting more restrictive signal status, and movement authority	Incorrect variable used; Data corrupted during internal handling	IVD	[redacted]	WIU-SSHA-48	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_49	WIU Non-Vital Executive Software	FMECA_17	Incorrect messages; Messages are sent to the wrong location or are not sent; Incorrect event logging	Configuration server service error	IVB		WIU-SSHA-49	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_50	WIU Non-Vital Executive Software	FMECA_18	SIO messages - Corrupted - Incorrect sequence - Missing data -Stale message -Addressed improperly; Messages are sent to the wrong location or are not sent; Incorrect event logging	PCI message service error	IB		WIU-SSHA-50	Mitigated	Wayside Safety	IE	-
WIU_SSHL_51	WIU Non-Vital Executive Software	FMECA_19	SIO messages - Corrupted -Incorrect sequence - Missing data -Stale message -Addressed improperly; Messages are sent to the wrong location or are not sent; Incorrect event logging	PCI message service error	IVB		WIU-SSHA-51	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_52	WIU Non-Vital Executive Software	FMECA_20	Incorrect time management Messages are sent incorrectly or not sent; Incorrect event logging	Program error – time management	IVC		WIU-SSHA-52	Transferred	Systems Safety	IVE	Exported to OBC

WIU_SSHL_53	WIU Non-vital Executive Software	FMECA_21	Diagnostic failure; Maintenance tool messages incorrectly formatted or corrupt	Port failure	IVD		WIU-SSHA-53	Cancelled	Wayside Safety	IVD	Only impacts diagnostic function used for maintenance and troubleshooting. WIU will be replaced by authorized personnel during non-revenue maintenance
WIU_SSHL_54	WIU Non-vital Executive Software	FMECA_22	Interface to load configuration settings not functioning properly; Config. settings loaded via USB get corrupted	WIU USB hardware failure	IVD		WIU-SSHA-54	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_55	WIU Non-vital Configuration	FMECA_23	Incorrect VIU-20e non-vital config. Parameters; Possible module shut down	Configuration error	IVB		WIU-SSHA-55	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_56	VIU-20e Hardware (Configuration)	FMECA_24	USB communication failure; Failure or corruption of the USB protocol information	WIU Port failure	IC		WIU-SSHA-56	Mitigated	Wayside Safety	IE	-
WIU_SSHL_57	VIU-20e Hardware (Configuration)	FMECA_25	USB communication failure; Failure or corruption of the USB protocol information	WIU Port failure	IVC		WIU-SSHA-57	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_58	VIU-20e Vital Hardware	FMECA_26	Input hardware failure or damage during maintenance; WIU vital input read as energized when de-energized	Short between pins	IC		WIU-SSHA-58	Mitigated Transferred	Wayside Safety Systems Safety	IE	- Mitigation exported to RR for maintenance and inspection

WIU_SSHL_59	VIU-20e Vital Hardware	FMECA_27	Increased resistance; Input unable to be read correctly	Open circuit on any pin	IVC	[redacted]	WIU-SSHA-59	Mitigated Transferred	Wayside Safety Systems Safety	IVE	- Mitigation exported to RR for maintenance and inspection
WIU_SSHL_60	WIU ECD	FMECA_28	Failure or corruption of the ECD; May result in reporting less restrictive signal status, speed, and movement authority	Hardware failure	IC		WIU-SSHA-60	Mitigated	Wayside Safety	IE	-
WIU_SSHL_61	WIU ECD	FMECA_29	Failure or corruption of the ECD; May result in reporting more restrictive signal status, speed, and movement authority	Hardware failure	IVC		WIU-SSHA-61	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_62	Isolation Modules	FMECA_30	WIU becomes susceptible to high voltage; Risk of equipment damage	Loss of electrical isolation	IC		WIU-SSHA-62	Transferred Mitigated Transferred	Systems Safety Wayside Safety Systems Safety	IE	Exported to OBC - -
WIU_SSHL_63	Isolation Modules	FMECA_31	Input unable to be read correctly; Input read as de- energized	Connections to I/O open	IVC		WIU-SSHA-63	Transferred Mitigated	Systems Safety Wayside Safety	IVE	Mitigation exported to RR for maintenance and inspection -

WIU_SSHL_64	Relay (Vital)	FMECA_32	Incorrect input; Falsely permissive WIU status for functions communicated to OBC	False energization	ID		WIU-SSHA-64	Transferred	Systems Safety	IE	Mitigation exported to RR for addressing relay characteristics per FRA requirements for periodic inspection and test
WIU_SSHL_65	Relay (Vital)	FMECA_33	Incorrect input; Falsely restrictive WIU status for functions communicated to OBC	False de-energization	IVC		WIU-SSHA-65	Transferred	Systems Safety	IVE	Mitigation exported to RR for addressing relay characteristics per FRA requirements for periodic inspection and test
WIU_SSHL_66	AAR Terminals	FMECA_34	Faulty connection causes wire to back out; Loss of WIU power	Loose terminal fastener	ID		WIU-SSHA-66	Transferred	Systems Safety	IE	Exported to RR (Maintenance) Exported to OBC (Comm failure)
WIU_SSHL_67	AAR Terminals	FMECA_35	Faulty connection causes wire to back out; Loss of WIU power	Loose terminal fastener	IVD		WIU-SSHA-67	Transferred	Systems Safety	IVE	Exported to RR (Maintenance) Exported to OBC (Comm failure)
WIU_SSHL_68	Terminal Block	FMECA_36	Incorrect input; Input read as energized	Short between connections	IC		WIU-SSHA-68	Transferred Mitigated	Systems Safety Wayside Safety	IE	Mitigation exported to RR for periodic inspection of equipment and connections (Wall Placement Kits) -
WIU_SSHL_69	Terminal Block	FMECA_37	Incorrect input; Input read as de-energized	Open WIU connections	IVC		WIU-SSHA-69	Transferred Mitigated	Systems Safety Wayside Safety	IVE	Mitigation exported to RR for periodic inspection of equipment and connections (Wall Placement Kits) -

WIU_SSHL_70	Circuit Breaker	FMECA_38	Loss of protection for equipment; WIU components over current	Failure to clear circuit fault	IB	[redacted]	WIU-SSHA-70	Transferred	Systems Safety	IIID	- Exported to OBC
WIU_SSHL_71	Circuit Breaker	FMECA_39	Loss of protection for equipment; WIU components over current	Failure to clear circuit fault	IVB		WIU-SSHA-71	Transferred	Systems Safety	IVD	- Exported to OBC
WIU_SSHL_72	Surge Protector	FMECA_40	Loss of protection for equipment; WIU components overvoltage	Loss of protection	ID		WIU-SSHA-72	Transferred	Systems Safety	IE	- Exported to OBC
WIU_SSHL_73	Surge Protector	FMECA_41	Loss of protection for equipment; WIU components overvoltage	Loss of protection	IVD		WIU-SSHA-73	Transferred	Systems Safety	IVE	- Exported to OBC
WIU_SSHL_74	Surge Suppressor	FMECA_42	Loss of protection for equipment; WIU components overvoltage	Loss of protection	ID		WIU-SSHA-74	Transferred	Systems Safety	IE	See FMECA_52 for complementary failure Exported to OBC

WIU_SSHL_75	Diagnostic Tool	FMECA_43	N/A	All possible failure modes have no impact on system operation or safety	IVE	[redacted]	WIU-SSHA-75	Cancelled	Wayside Safety	IVE	This is performing an external diagnostic function used for maintenance and troubleshooting; No further analysis is required
WIU_SSHL_76	DC-DC Converter	FMECA_44	Loss of WIU power; Loss of WIU function	Reduction or loss of power; Failure of converter	IC		WIU-SSHA-76	Transferred	Systems Safety	IIID	See FMECA_53 for complementary failure Note: System is designed to be failsafe in that if the session is lost the connection states will not be set to less restrictive values. As a result hazard severity was decreased. Exported to OBC
WIU_SSHL_77	Rack	FMECA_45	Equipment improperly secured; Loss of WIU function	Structure failure	ID		WIU-SSHA-77	Transferred	Systems Safety	IE	Exported to RR (Maintenance) Exported to OBC (Comm failure)
WIU_SSHL_78	Rack	FMECA_46	Equipment improperly secured; Loss of WIU function	Structure failure	IVD		WIU-SSHA-78	Transferred	Systems Safety	IVE	Exported to RR (Maintenance) Exported to OBC (Comm failure)

WIU_SSHL_79	VIU-20e Mounting Cradle	FMECA_47	Equipment improperly secured; Loss of WIU function	Structure failure	ID	[redacted]	WIU-SSHA-79	Transferred	Systems Safety	IE	- Exported to OBC
WIU_SSHL_80	VIU-20e Mounting Cradle	FMECA_48	Equipment improperly secured; Loss of WIU function	Structure failure	IVD		WIU-SSHA-80	Transferred	Systems Safety	IVE	- Exported to OBC
WIU_SSHL_81	VIU-20e Plug Connector	FMECA_49	Incorrect input; WIU status becomes less restrictive	Short between connections	IC		WIU-SSHA-81	Transferred Mitigated	Systems Safety Wayside Safety	IE	Mitigation exported to RR for periodic inspection of equipment and connections -
WIU_SSHL_82	VIU-20e Plug Connector	FMECA_50	Loss of WIU functionality; WIU status becomes restricted worst case	Open WIU connections	IVC		WIU-SSHA-82	Transferred	Systems Safety	IVE	Mitigation exported to RR for periodic inspection of equipment and connections
WIU_SSHL_83	CDL File	FMECA_51	SNMP trap messages are not properly created and/or sent; Incorrect diagnostic messages received	Program error	IVD		WIU-SSHA-83	Mitigated	Wayside Safety	IVE	-
WIU_SSHL_84	Surge Suppressor	FMECA_52	Protection of equipment unchanged; No effect	Slight increase in series resistance	IVD		WIU-SSHA-84	Transferred	Systems Safety	IVE	See FMECA_42 for complementary failure
WIU_SSHL_85	DC-DC Converter	FMECA_53	Increased power supplied to WIU; WIU onboard voltage regulation prohibits overvoltage event	Improper voltage regulation	IVC		WIU-SSHA-85	Transferred	Systems Safety	IVD	See FMECA_44 for complementary failure

WIU_SSHL_86	Maintenance Maintenance	WIU-OHA-01	Maintenance personnel comes in contact with live voltage while maintaining WIU subsystem equipment, causing electrical shock because worker does not remove voltages or removes protective devices before working on equipment.	Maintenance Personnel oversight	IB	[redacted]	WIU-SSHA-86	Mitigated Transferred	Wayside Safety Systems Safety	ID	-
WIU_SSHL_87	Installation Installation	WIU-OHA-02	Installation personnel comes in contact with live voltage while maintaining WIU subsystem equipment, causing electrical shock because worker does not remove voltages or removes protective devices before working on equipment.	Installation Personnel oversight	IB		WIU-SSHA-87	Mitigated Transferred	Wayside Safety Systems Safety	ID	-
WIU_SSHL_88	Maintenance	WIU-OHA-03	Person in contact with or in close proximity to an electrical power source	Material with electrical potential due to the loss of proper grounding/bonding for the wayside PTC equipment/rack	IC		WIU-SSHA-88	Transferred	Systems Safety	IE	-
WIU_SSHL_89	Installation	WIU-OHA-04	WIU subsystem equipment not correctly installed	Installation Personnel oversight	IIC		WIU-SSHA-89	Transferred	Systems Safety	IID	-

WIU_SSHL_90	Installation	WIU-OHA-05	Error in WIU vital input installation/ wiring results in less restrictive aspect than intended to WIU	Incorrect installation / wiring during maintenance due to not following installation instructions correctly	IC	[redacted]	WIU-SSHA-90	Transferred	Systems Safety	IE	-
WIU_SSHL_91	Installation and Maintenance	WIU-OHA-06	WIU with a verified site specific configuration is installed at the wrong site	Installation or Maintenance Personnel oversight	IC		WIU-SSHA-91	Transferred Mitigated	Systems Safety Wayside Safety	IE	-
WIU_SSHL_92	Operations	WIU-OHA-07	Malicious modifications of the VIU-ACSES software configuration or wiring leads to a hazardous event	Unauthorized persons accessing WIU Subsystem housing	IB		WIU-SSHA-92	Transferred	Systems Safety	IE	-
WIU_SSHL_93	Operations	WIU-OHA-08	Poor Site Access Control	Unauthorized personnel accessing WIU Subsystem housing	IB		WIU-SSHA-93	Transferred	Systems Safety	IE	-
WIU_SSHL_94	Operations	WIU-OHA-09	WIU Hardware is modified without authorization and creates a hazardous event	Unauthorized personnel accessing WIU Subsystem housing	IB		WIU-SSHA-94	Transferred Mitigated	Systems Safety Wayside Safety	IE	-
WIU_SSHL_95	Maintenance	WIU-OHA-10	Personnel who perform operation, installation or maintenance on WIU Subsystem system is not fully trained	Management Error	IA		WIU-SSHA-95	Transferred	Systems Safety	ID	-

WIU_SSHL_96	Maintenance	WIU-OHA-11	Incorrect software revision in WIU equipment	Software updates not performed on spare equipment	IB	[redacted]	WIU-SSHA-96	Transferred Mitigated Mitigated Mitigated	Systems Safety Wayside Safety Wayside Safety Wayside Safety	IE	-
WIU_SSHL_97	Maintenance	WIU-OHA-12	WIU Configuration error which results in WIU to send an ATCS message with a less restrictive movement authority than intended	Installation Instructions are not properly followed	IC		WIU-SSHA-97	Transferred Mitigated Mitigated Mitigated	Systems Safety Wayside Safety Wayside Safety Wayside Safety	IE	-

WIU_SSHL_98	Wired Vital Input	WIU- IHA-1	Error in vital input installation/wiring results in the WIU detecting a signal with a less restrictive aspect than intended	Error in Installation Instructions	IC	[redacted]	WIU-SSHA-98	Transferred	Systems Safety		Siemens is responsible for providing the Training Manuals and the SAT Test Procedures for WIU, but not for ensuring that the training or the Site Acceptance Testing of each location is complete. Therefore this portion of mitigation is exported to SI and RR.
WIU_SSHL_99	Wired Vital Input	WIU- IHA-2	Error in vital input installation/wiring results in the WIU detecting a signal with less restrictive aspect than intended	Installation Instructions not followed	IC		WIU-SSHA-99	Transferred	Systems Safety		Siemens is responsible for providing the Training Manuals and the SAT Test Procedures for WIU, but not for ensuring that the training or the Site Acceptance Testing of each location is complete. Therefore this portion of mitigation is exported to SI and RR.
WIU_SSHL_100	Wired Vital Input	WIU- IHA-3	Vital input delivered in incorrect state by VSL which results in the WIU sending an ACSES message with a less restrictive movement authority than intended causing the ACSES OBC to show less restrictive movement authority than intended	External hardware or software failure	IC		WIU-SSHA-100	Transferred	Systems Safety		Failure in VSL or Wiring is external to WIU subsystem. Mitigation exported to Railroad.

WIU_SSHL_101	Ethernet Port 1	WIU- IHA-4	ACSES OBC fails to go to restrictive state in a timely manner when no ACSES WIU response messages are received	Communication failure resulting in WIU response messages not being delivered to OBC	IC	[redacted]	WIU-SSHA-101	Transferred	Systems Safety		Exported to OBC
WIU_SSHL_102	Ethernet Port 1	WIU- IHA-5	ACSES OBC fails to go to restrictive state in a timely manner when corrupt ACSES WIU response messages are received	Communication failure resulting in corrupt WIU response message to OBC	IC		WIU-SSHA-102	Mitigated	Wayside Safety	IE	-
WIU_SSHL_103	Ethernet Port 1	WIU- IHA-6	ACSES OBC fails to go to restrictive state in a timely manner when misaddressed ACSES WIU response messages are received	Communication failure resulting in WIU response message delivered to a wrong OBC	IC		WIU-SSHA-103	Mitigated	Wayside Safety	IE	-
WIU_SSHL_104	Ethernet Port 1	WIU- IHA-7	ACSES OBC fails to go to restrictive state in a timely manner when no ACSES WIU response messages are received	Communication failure resulting in OBC request messages not being delivered to WIU	IC		WIU-SSHA-104	Transferred	Systems Safety		Exported to OBC
WIU_SSHL_105	Ethernet Port 1	WIU- IHA-8	ACSES OBC fails to go to restrictive state in a timely manner when wrong ACSES WIU response messages are received	Communication failure resulting in corrupt OBC request message to WIU	IC		WIU-SSHA-105	Transferred	Systems Safety		Exported to OBC Request message 24 is sent Non-Vitally, without CRC. Mitigation for all conditions resulting from corruption of the request can only be implemented on OBC.

WIU_SSHL_106	Ethernet Port 1	WIU- IHA-9	ACSES OBC fails to go to restrictive state in a timely manner when misaddressed ACSES WIU response messages are received	Communication failure resulting in OBC request message delivered to a wrong WIU	IC	[redacted]	WIU-SSHA-106	Transferred	Systems Safety		Exported to OBC Request message 24 is sent Non-Vitally, without CRC. Mitigation for all conditions resulting from corruption of the request can only be implemented on OBC.
WIU_SSHL_107	Ethernet Port 1	WIU- IHA-11	Main WIU fails to go to restrictive state in a timely manner when no Auxiliary WIU response messages are received	Loss of Communication between Main and Auxiliary WIUs	IC		WIU-SSHA-107	Mitigated	Wayside Safety	IE	-
WIU_SSHL_108	Ethernet Port 1	WIU- IHA-12	Main WIU fails to go to restrictive state in a timely manner when wrong Auxiliary WIU messages are received	Corrupt communication between Main and Auxiliary WIUs	IC		WIU-SSHA-108	Mitigated	Wayside Safety	IE	-
WIU_SSHL_109	Ethernet Port 1	WIU- IHA-13	Main WIU fails to go to restrictive state in a timely manner when misaddressed Auxiliary WIU response messages are received	Communication failure resulting in Auxiliary WIU message being delivered to a wrong Main WIU	IC		WIU-SSHA-109	Mitigated	Wayside Safety	IE	-
WIU_SSHL_110	Ethernet Port 1	WIU- IHA-10	Auxiliary WIU communication to main WIU contains less restrictive value than intended due to configuration file error	Configuration file was not validated and/or tested properly	IC		WIU-SSHA-110	Mitigated	Wayside Safety	IE	-

11 Attachment G – OBC Hazard Log

3035819 Rev_N Attachment G – OBC Hazard Log – DOORS /LIRR_MNR PTC/6. Siemens Data\Siemens_LIRR_MNR_PTC\48 SubVal\ 48 OBC Hazard Log 2019-06 – Baseline 1.2

ID	Subsystem	Source Ref.	Hazard Description	Potential Cause	Initial Risk	[redacted]	SR ID	Safety Status	Responsibility	Final Risk	Remarks
OBC-HL-1	OBC	PHA	Train exceeds speed for a section of track.	Operator error, fails to respond to overspeed alarm.	IC		PHA: OB-SR-1	Mitigated	OBC	IE	
OBC-HL-2	OBC	PHA	Train exceeds speed for a section of track.	Operator error, fails to respond to overspeed alarm.	IC		PHA: OB-SR-2	Mitigated	OBC	IE	
OBC-HL-3	OBC	PHA	Train exceeds speed for a section of track.	Speed sensor fails to detect actual speed of train.	IC		PHA: OB-SR-3, OB-SR-04	Mitigated	OBC	IE	
OBC-HL-4	OBC	PHA	Train exceeds speed for a section of track.	OBC fails to receive the lowest speed limit that is in effect	IC		PHA: OB-SR-5	Mitigated	OBC	IE	
OBC-HL-5	OBC	PHA	Train exceeds speed for a section of track.	OBC fails to receive the lowest speed limit that is in effect	IC		PHA: OB-SR-6	Mitigated	OBC	IE	
OBC-HL-6	OBC	PHA	Train exceeds speed for a section of track.	OBC fails to receive the lowest speed limit that is in effect	IC		PHA: OB-SR-7	Mitigated	OBC	IE	
OBC-HL-7	OBC	PHA	Speed downgrade requires acknowledgement by operator	Missed transponder	IC		PHA: OB-SR-8	Mitigated	OBC	IE	
OBC-HL-8	OBC	PHA	Train does not accept valid messages since location used by OBC is incorrect	OBC wrongly located train	IC		PHA: OB-SR-9	Mitigated	OBC	IE	
OBC-HL-9	OBC	PHA	Train does not accept valid messages since location used by OBC is incorrect	OBC wrongly located train	IC		PHA: OB-SR-10	Mitigated	OBC	IE	

OBC-HL-10	OBC	PHA	Train does not accept valid messages since location used by OBC is incorrect	OBC wrongly located train	IC	[redacted]	PHA: OB-SR-48	Mitigated	OBC	IE	
OBC-HL-11	OBC	PHA	OBC speed and braking calculations incorrect if parameters from Configuration Memory Module are corrupted	Vehicle parameters (such as train type, scanner offset, wheel diameter) corrupted and used by the system during initialization (Daily Departure Test)	IIIC		PHA: OB-SR-11	Mitigated	OBC	IIIE	
OBC-HL-12	OBC	PHA	OBC speed and braking calculations incorrect if parameters from Configuration Memory Module are corrupted	Vehicle parameters (such as train type, scanner offset, wheel diameter) corrupted and used by the system during initialization (Daily Departure Test)	IIIC		PHA: OB-SR-12	Mitigated	System	IIIE	
OBC-HL-13	OBC	PHA	OBC speed and braking calculations incorrect if parameters from Configuration Memory Module are improperly entered at set-up.	Vehicle parameters (such as train type, scanner offset, wheel diameter) not correctly entered into CMM at installation or maintenance	IIIC		PHA: OB-SR-13	Mitigated	OBC	IIIE	
OBC-HL-14	OBC	PHA	OBC receives incorrect and unsafe Movement Authority from wayside	Message was corrupted	IC		PHA: OB-SR-14	Mitigated	OBC	IE	

OBC-HL-15	OBC	PHA	Train in yard exceeds speed limit	Train under operator control in a yard subject to restricted speed goes over speed limit	IC		PHA: OB-SR-15	Mitigated	OBC	IE	
OBC-HL-16	OBC	PHA	Incorrect TSR received by OBC.	OBC receives incorrect Mandatory Directive due to incorrect TSR	IC		PHA: OB-SR-16	Mitigated	OBC	IE	
OBC-HL-17	OBC	PHA	Collision with object on track due to incorrect Onboard ACSES installation	OBC equipment installed incorrectly on train	IIID		PHA: OB-SR-17	Mitigated	OBC	IIIE	3037841 (CDRL 2-036-201) - Sections 4.1 and 4.2
OBC-HL-18	OBC	PHA	Collision at failed grade crossing.	Highway crossing failure	IC		PHA: OB-SR-18	Mitigated	OBC	IE	
OBC-HL-19	OBC	PHA	Collision at failed grade crossing.	Highway crossing failure	IC		PHA: OB-SR-19	Mitigated	OBC	IE	
OBC-HL-20	OBC	PHA	Onboard ACSES allows unsafe operation	Hardware or software modified improperly due to vandalism	IC		PHA: OB-SR-20	Mitigated	System	IE	3043936 (CDRL 2-042-201) - Section 7 - Details the installation instructions for the OBC, Section 7.3 states that the equipment is to be installed in the existing crew locker (locked cabinet).

OBC-HL-21	OBC	PHA	EMI/EMC interference from nearby source causes incorrect and unsafe operation	Outside source of EMI /EMC corrupts messages or ACSES operation	IIIC		PHA: OB-SR-21, OB-SR-22, OB-SR-23	Mitigated	OBC	IIIE	4007785 - EMC/EMI Qualification Test Report for the M7 OBC and ADU - Section 6.2 - Shows that the equipment tested as described in the report complied with all of the tests in the program and met the requirements of the associated standard R-1498P - FCC Verification Test Report on PHW Inc. ACSES Transmitter - EMC Report for scanner antenna - section 6 states that the tests performed comply with the requirements imposed
OBC-HL-22	OBC	PHA	Electrical shock or electrocution	Electric shock due to Inadequate maintenance procedures	IC		PHA: OB-SR-24	Mitigated	OBC	IE	3037841 (CDRL 2-36-201)- Section 5 - Details corrective maintenance - first step of each subsection is to remove power at ACSES circuit breaker.
OBC-HL-23	OBC	PHA	Electrical shock or electrocution	Electric shock due to Inadequate maintenance procedures	IC		PHA: OB-SR-25	Mitigated	OBC	IE	TM-1051-05 - LIRR ACSES II Maintenance (Training Slideshow) - Slides 3-5 - These slides provide general safety guidelines and precautions to abide by during training.
OBC-HL-24	OBC	PHA	Electrical Shock or Electrocution	Material with electrical potential accessible to passengers	IC		PHA: OB-SR-26	Mitigated	System	IE	3043936 (CDRL 2-042-201) - Section 7 - Details the installation instructions for the OBC, Section 7.3 states that the equipment is to be installed in the existing crew locker (locked cabinet).

OBC-HL-25	OBC	PHA	Front of train encroaches into interlocking.	Incorrect vehicle parameters such as scanner offset is entered for that vehicle type	IC		PHA: OB-SR-28	Mitigated	OBC	IE	
OBC-HL-26	OBC	PHA	Failure of ACK button, allows improper acknowledgement	Acknowledge button hardware fails closed	IC		PHA: OB-SR-30	Mitigated	OBC	IE	
OBC-HL-27	OBC	PHA	Train passes PTS without confirmation that signals are clear.	Loss of communication between wayside and OBC	IC		PHA: OB-SR-31	Mitigated	OBC	IE	
OBC-HL-28	OBC	PHA	System reacts to old data when communication lost between ATC and OBC / AIU	OBC unsafely allows train to enter interlocking based on data not refreshed.	IC		PHA: OB-SR-32	Mitigated	OBC	IE	
OBC-HL-29	OBC	PHA	Train enters next block without safe train separation if ATC Cutout signal not received	ACSES does not detect that ATC is cut out and allows train into next block	IC		PHA: OB-SR-33	Mitigated	OBC	IE	
OBC-HL-30	OBC	PHA	Communications delay and OBC uses old data	ACSES data is not updated and OBC reacts to old data	IC		PHA: OB-SR-46	Mitigated	OBC	IE	Column I: Changed "specified distance" to "60 min"
OBC-HL-31	OBC	PHA	Communications delay and OBC uses old data	ACSES data is not updated and OBC reacts to old data	IC		PHA: OB-SR-35	Mitigated	OBC	IE	
OBC-HL-32	OBC	PHA	Communications delay and OBC uses old data	ACSES data is not updated and OBC reacts to old data	IC		PHA: OB-SR-36	Mitigated	OBC	IE	
OBC-HL-33	OBC	PHA	Vehicle encroaches into switch that has moved out of correspondence	By not changing the stale data timer from 120 to 42 during a message/radio failure as a vehicle was about to proceed, the permissions could be changed before the stale data timeout	IC		PHA: OB-SR-37	Mitigated	OBC	IE	

OBC-HL-34	OBC	PHA	Failed, safety-critical hardware item may exist on board and not detected.	Operator fails to run Daily Departure Test	IIIC		PHA: OB-SR-38	Mitigated	LIRR/MNR	IIIE	3037841 (CDRL 2-36-201) Section 4 states that the departure test is required to be performed every 24 hours.
OBC-HL-35	OBC	PHA	Brake Assurance function not available	Brake Assurance function does not protect from 42 mph to 16 mph	IC		PHA: OB-SR-39	Mitigated	OBC	IE	
OBC-HL-36	OBC	PHA	Unauthorized vehicle enters the mainline without permission.	Failure to follow operating rules when in the yard or a siding.	IC		PHA: OB-SR-40	Mitigated	OBC	IE	
OBC-HL-37	OBC	PHA	During turnback, the operator may creep the vehicle past the PTS point	Improper PTS location	IC		PHA: OB-SR-42	Mitigated	LIRR	IE	
OBC-HL-38	OBC	PHA	ADU displays an incorrect aspect	Aspect information incorrectly displayed on ADU. Operator uses speed codes higher than allowed.	IC		PHA: OB-SR-43	Mitigated	OBC	IE	
OBC-HL-39	OBC	PHA	Updated TSR not received	OBC does not receive lowest speed limit that is in effect	IC		PHA: OB-SR-45	Mitigated	OBC	IE	
OBC-HL-40	OBC	OHA	Noise exposure to person when brake vents	Personnel not aware that air will vent suddenly when power is removed	IIIC		OHA: OH-SR-1	Mitigated	Brakes / System	IIE	TM-1051-05 - LIRR ACSES II Maintenance (Training Slideshow) - Slides 3-5 - These slides provide general safety guidelines and precautions to abide by during training. Slide 4 states "Beware of unexpected equipment operation."

OBC-HL-41	OBC	OHA	Objects falls during removal or replacement	Equipment not secured during removal	IIIC		OHA: OH-SR-2	Mitigated	OBC	IIIE	TM-1051-05 - LIRR ACSES II Maintenance (Training Slideshow) - Slides 3-5 - These slides provide general safety guidelines and precautions to abide by during training. Precaution regarding handling of heavy components included on Slide 5.
OBC-HL-42	OBC	OHA	Train moves unexpectedly	Brakes not set	ID		OHA: OH-SR-3	Mitigated	System	IE	TM-1051-05 - LIRR ACSES II Maintenance (Training Slideshow) - Slides 3-5 - These slides provide general safety guidelines and precautions to abide by during training. Warning 3 of slide 6 states that all personnel involved must ensure that the handbrake is applied.
OBC-HL-43	OBC	OHA	Improper Installation (poor insertion or too far from gear) causes erratic speed measurement.	Improper installation depth of speed sensor	ID		OHA: OH-SR-4	Mitigated	OBC	IE	3043936 (CDRL 2-042-201) - Section 3.4 - Details installation of Speed Sensor
OBC-HL-44	OBC	OHA	Improper Installation (poor insertion or too far from gear) causes erratic speed measurement.	Improper installation depth of speed sensor	ID		OHA: OH-SR-5	Mitigated	OBC	IE	3037841 (CDRL 2-36-201) - Section 4.2 - 92 Day inspection includes steps to inspect and test the speed sensor assembly.

OBC-HL-45	OBC	OHA	The connectors on MTA are NOT coded. This leads to the possibility of mating the wrong mobile (cable) connector to its corresponding rack connector.	Connectors installed in wrong location	IIID	[redacted]	OHA: OH-SR-6	Mitigated	OBC	IIIE	3037841 (CDRL 2-36-201) - Section 5 details the corrective maintenance for removing/replacing OBC Locker equipment. Steps of instruction state to disconnect and reconnect the cables from their corresponding connectors.
OBC-HL-46	OBC	OHA	Board inserted wrong cardfile slot, causing erratic signals	Board inserted wrong cardfile slot	IIID		OHA: OH-SR-7	Mitigated	OBC	IIIE	D7710H0106-A01 - Sheet 1 of the drawing shows the complete assembly for the cardfile. The labels on the tabs of the PCBs in the cardfile correspond with the labels on the slots in the cardfile itself. D5574H22-A01 - Sheet 1 of the drawing shows a keying chart for the backplane of the cardfile. The PCB slots on the mother are keyed uniquely to match the uniquely keyed PCBS so that only the correct board will fit in the correct slot.

OBC-HL-47	OBC	OHA	Acel/Decel reading to OBC may be incorrect	Improper installation of decelerometer	IC	[redacted]	OHA: OH-SR-8	Mitigated	OBC	IE	3037841 (CDRL 2-36-201) - Section 5.1.9 outlines the corrective maintenance procedure for the decelerometer including installation and alignment. TM-1051-05 - LIRR ACSES II Maintenance (Training Slideshow) - Slides 211-212 provide detailed training on how to level the decelerometer.
OBC-HL-48	OBC	OHA	Acel/Decel reading to OBC may be incorrect	Improper installation of decelerometer	IC		OHA: OH-SR-9	Mitigated	OBC	IE	3037841 (CDRL 2-36-201) - Section 5.1.9 outlines the corrective maintenance procedure for the decelerometer including installation and alignment. The last step of the procedure is to perform departure test to ensure functionality.
OBC-HL-49	Train front end may encroach into interlocking	Incorrect offset data entered at installation	ID	Offset parameters are read back to the PTE before maintainer finalizes the values.	OHA: OH-SR-13		OHA: OH-SR-13	Mitigated	OBC	IE	TM-1051-05 - LIRR ACSES II Maintenance (Training Slideshow) - These slides detail the configuration setup for the ACSES onboard computer using ACSESView.
OBC-HL-50	Electrical shock or electrocution of LIRR personnel	Oversight by personnel	ID	Details in the Training/Manuals.	OHA: OH-SR-18		OHA: OH-SR-18	Mitigated	OBC	IE	3037841 (CDRL 2-36-201) - Section 5 - Details corrective maintenance - first step of each subsection is to remove power at ACSES circuit breaker.

OBC-HL-51	Electrical shock or electrocution of LIRR personnel	Oversight by personnel	ID	Details in the Training/Manuals.	OHA: OH-SR-20	[redacted]	OHA: OH-SR-20	Mitigated	OBC	IE	TM-1051-05 - LIRR ACSES II Maintenance (Training Slideshow) - Slides 3-5 - These slides provide general safety guidelines and precautions to abide by during training.
OBC-HL-52	Incorrect wheel diameter measurement or incorrect data entry of wheel size	Installation or Maintainer error	ID	OBC shall automatically compensate for wheel wear	OHA: OH-SR-30		OHA: OH-SR-30	Mitigated	OBC	IE	
OBC-HL-53	The connectors on MTA are NOT coded. This leads to the possibility of mating the wrong mobile (cable) connector to its corresponding rack connector.	Connectors installed in wrong location	IIID	Cables shall be identified with ID labels	OHA: OH-SR-34		OHA: OH-SR-34	Mitigated	OBC	IIIE	D7710H0201-A01 - LIRR M7 Main Level Assembly - As shown on the drawing, cables and connectors are uniquely labelled to reduce the risk of incorrect connector pairing
OBC-HL-54	The connectors on MTA are NOT coded. This leads to the possibility of mating the wrong mobile (cable) connector to its corresponding rack connector.	Connectors installed in wrong location	IIID	Cables shall be identified with ID labels	OHA: OH-SR-35		OHA: OH-SR-35	Mitigated	OBC	IIIE	D5600H120-A01 & D5600H121-A01 - These drawings show the design of the Power Supply PCB includes a diode (D1) which is used for Input reverse voltage protection.

OBC-HL-55	Newer message is sent before an older message	Communication failure/hardware failure between MCM/OBC Interface	IID	Successful radio link is required to pass the Departure Test and is monitored every 30 seconds during use when no other radio traffic is present.	IHA: IH-SR-03	[redacted]	IHA: IH-SR-03	Mitigated	OBC	IIE	
OBC-HL-56	Overspeed/collision/ derailment if message is corrupted	Corrupted message due to hardware failure	IC	Data radio messages are protected with 72-CRC	IHA: IH-SR-04		IHA: IH-SR-04	Mitigated	OBC	IE	
OBC-HL-57	Overspeed if Type 12 message, TSR List, is corrupted and does not contain the lowest / most restrictive speed.	Corrupted Type 12 message due to hardware failure	IC	Messages are protected with CRC-72 to protect data packets. If no speed limit is specified, OBC shall use the most restrictive speed for that part of the track. ADU will indicate NO TSR when no TSR Lists are available for enforcement.	IHA: IH-SR-09		IHA: IH-SR-09	Mitigated	ADU	IE	
OBC-HL-58	Newer message is sent before an older message	Messages are processed out of chronological order	IC	OBC Validated messages using pseudo-random time stamp	IHA: IH-SR-11		IHA: IH-SR-11	Mitigated	OBC	IE	
OBC-HL-59	Overspeed/Collision/ Derailment due to loss of interface - messages not received	Communication failure between MCM and OBC	IC	Radio link is verified every 30 seconds when no other radio traffic is present	IHA: IH-SR-12		IHA: IH-SR-12	Mitigated	ADU	IE	

OBC-HL-60	Out of chronological order. Newer message is processed before an older message	Hardware failure during processing or transmission.	IC	OBC continually check the health of PCBs	IHA: IH-SR-14	[redacted]	IHA: IH-SR-14	Mitigated	OBC	IE	
OBC-HL-61	Newer message is sent before an older message	Communication failure between MCM and OBC	ID	Every query request message sent by the same OBC will have the most up-to-date information, updated at every new processing cycle.	IHA: IH-SR-15		IHA: IH-SR-15	Mitigated	OBC	IE	
OBC-HL-62	Overspeed if a false, more permissive aspect is displayed on ADU	Hardware failure causes incorrect aspect display	IC	Aspects are monitored and the ADU display must match the ATC input	IHA: IH-SR-16		IHA: IH-SR-16	Mitigated	AIU	IE	
OBC-HL-63	ATC Cut-out switch functionality error	Hardware or wiring failure of ATC Cut-Out switch	IC	ADU will detect non-responsive ATC and notify OBC that ATC/AIU is cut-out.	IHA: IH-SR-17		IHA: IH-SR-17	Mitigated	OBC	IE	
OBC-HL-64	ATC Cut-out switch functionality error	Hardware or wiring failure of ATC Cut-Out switch	IC	OBC performs a cross-check of ATC status and signal level to determine when ATC is Cut Out	IHA: IH-SR-18		IHA: IH-SR-18	Mitigated	OBC	IE	
OBC-HL-65	Overspeed if brake relay not de-energized when requested by ATC	Failure of vital relay	ID	Brake are checked during Departure Test	IHA: IH-SR-19		IHA: IH-SR-19	Mitigated	Depart Test	IE	

OBC-HL-66	Incorrect transfer of data between ATC and ADU. ADU displaying a less restrictive speed aspect that commanded.	Corrupt serial message due to hardware failure	IC	ADU controls each individual aspect as a vital output. The aspects are tested during daily departure test	IHA: IH-SR-20	[redacted]	IHA: IH-SR-20	Mitigated	ADU, AIU	IE	
OBC-HL-67	Loss of interface. No message received.	Loss of communication link due to hardware failure.	IC	Errors are detected in the next processing cycle. Each cycle is 0.100 sec so the maximum time before detection is 0.200 sec. Processor will declare an error and shut down the processor.	IHA: IH-SR-21		IHA: IH-SR-21	Mitigated	ADU	IE	
OBC-HL-68	Loss of interface between OBC and ADU	Internal Onboard communications failure	IC	Vital techniques used to monitor OBC-ADU messages	IHA: IH-SR-24		IHA: IH-SR-24	Mitigated	OBC, ADU	IE	
OBC-HL-69	Loss of interface between ATC and ADU	Internal Onboard communications failure	IC	Vital techniques used to monitor AIU-ATC comms link	IHA: IH-SR-25		IHA: IH-SR-25	Mitigated	ADU	IE	
OBC-HL-70			Spare for Row 70 [Not Applicable]								
OBC-HL-71			Spare for Row 71 [Not Applicable]								
OBC-HL-72	OBC	IHA	Operator will not know why ATC indicators on ADU are darkened.	Hardware failure of ADU display board	IIC		IHA: IH-SR-28	Mitigated	ADU	IIE	
OBC-HL-73	OBC	IHA	Test LED on ADU fails to turn on when Departure Test is started	Hardware failure of ADU component	IIC		IHA: IH-SR-29	Mitigated	ADU	IIE	

OBC-HL-74	OBC	IHA	Overspeed LED on ADU fails to illuminate	Hardware failure of ADU component	IC		IHA: IH-SR-31	Mitigated	OBC	IE	3037841 (CDRL 2-036-201), Section 3.2.2
OBC-HL-75	OBC	IHA	No TSR LED on ADU fails to operate properly	Hardware failure of ADU component	IC		IHA: IH-SR-32	Mitigated	ADU	IE	
OBC-HL-76	OBC	IHA	Incorrect transfer of data between ATC and ADU	Corrupt data leads to incorrect or multiple aspects being displayed	IC		IHA: IH-SR-33	Mitigated	ADU	IE	
OBC-HL-77	OBC	IHA	Command message from Main PCB to Transponder Reader PCB is corrupted	Internal Onboard communications failure	IC		IHA: IH-SR-35	Mitigated	OBC	IE	
OBC-HL-78	OBC	IHA	Transponder messages are processed out of chronological order	Internal Onboard communications failure	ID		IHA: IH-SR-36	Mitigated	OBC	IE	
OBC-HL-79	OBC	IHA	Incorrect information in transponder message due to corruption	Failure to read transponder	ID		IHA: IH-SR-37	Mitigated	OBC	IE	
OBC-HL-80	OBC	IHA	Transponder not detected when Main PCB fails to communicate with Transponder Reader PCB	Missed transponder	IID		IHA: IH-SR-38	Mitigated	OBC	IIE	Column I: Changed NO TSR to NO XPDR
OBC-HL-81	OBC	IHA	Scanner activates transponder on adjacent track due to excessive power	Failure to read transponder	ID		IHA: IH-SR-39	Mitigated	Scanner	IE	CTV Amplifier PCB Drawing/Schematic Drawing - D2074H06/D2074H07
OBC-HL-82	OBC	IHA	Message from ATC to Decel is corrupted	Internal Onboard communications failure	IC		IHA: IH-SR-40	Mitigated	Decel	IE	

OBC-HL-83	OBC	IHA	Message from ATC to Decel is corrupted	Internal Onboard communications failure	IC	[redacted]	IHA: IH-SR-41	Mitigated	Decel	IE	
OBC-HL-84	OBC	IHA	Comms failure between ATC and Decel	Internal Onboard communications failure	IC		IHA: IH-SR-42	Mitigated	Decel	IE	
OBC-HL-85	OBC	IHA	Comms failure between ATC/AIU and Decel	Internal Onboard communications failure	IC		IHA: IH-SR-43	Mitigated	Decel	IE	
OBC-HL-86	OBC	IHA	Incorrect message between OBC and Decel due to latency or hardware failure	Internal Onboard communications failure	IC		IHA: IH-SR-44	Mitigated	OBC, Decel	IE	
OBC-HL-87	OBC	IHA	Incorrect Decel status received by OBC or ATC	Internal Onboard communications failure	IC		IHA: IH-SR-45	Mitigated	OBC	IE	
OBC-HL-88	OBC	IHA	Incorrect number of pulses reported to OBC (higher or lower)	Speed sensor hardware failure	IIC		IHA: IH-SR-46	Mitigated	Speed Sensor	IIE	
OBC-HL-89	OBC	IHA	Neither or Both FWD and REV directions are active at the same time	Hardware failure of vehicle wiring	IC		IHA: IH-SR-47	Mitigated	OBC	IE	
OBC-HL-90	OBC	SSHA	Cab Active signals are active from both A and B cabs	Hardware failure of vehicle wiring	IC		IHA: IH-SR-49	Mitigated	OBC	IE	
OBC-HL-91			Spare for Row 91 [Not Applicable]								
OBC-HL-92	OBC	IHA	Memory is cleared or corrupted. Train parameters are not available.	Hardware failure or EMC event that corrupts the stored data or data is corrupted when read by OBC.	IC		IHA: IH-SR-53	Mitigated	OBC, CMM	IE	
OBC-HL-93	OBC	IHA	CMM data cannot be read by OBC during initialization.	Loss of interface due to hardware failure	IC		IHA: IH-SR-59	Mitigated	OBC, CMM	IE	

OBC-HL-94	OBC	IHA	Overspeed is TSR List not requested by OBC due to loss of interface	Communication failure between MCM and OBC	IC		IHA: IH-SR-61	Mitigated	OBC Training	IE	TM-1051-05 - LIRR ACSES II Maintenance (Training Slideshow) -Slide 75, 122 - Slide 75 provides explanation of No TSR Data Indicator, Slide 122 states that engineer must make an acknowledgement when NO TSR is lit to avoid penalty brake.
OBC-HL-95	OBC	IHA	Incorrect transfer of data between ATC and ADU. ADU displaying a less restrictive speed aspect that commanded.	Corrupt serial message due to hardware failure	IC		IHA: IH-SR-62	Mitigated	ADU	IE	
OBC-HL-96	OBC	IHA	TSR List Request messages are processed out of chronological order	Communication failure between MCM and OBC	IC		IHA: IH-SR-63	Mitigated	OBC	IE	
OBC-HL-97	OBC	IHA	Newer message is sent before an older message. Messages are processed out of chronological order.	Hardware failure in OBC-MCM interface.	IID		IHA: IH-SR-64	Mitigated	OBC		
OBC-HL-98	OBC	IHA	Corrupt message sent in radio message by OBC	Communication failure between MCM and OBC	IC		IHA: IH-SR-65	Mitigated	OBC	IE	
OBC-HL-99	OBC	IHA	Type 22 Message is not received by OBC.	Hardware failure in OBC-MCM interface.	IC		IHA: IH-SR-66	Mitigated	OBC	IE	
OBC-HL-100	OBC	IHA	Message not received by OBC	Hardware failure in OBC-MCM interface.	IC		IHA: IH-SR-67	Mitigated	OBC	IE	
OBC-HL-101	OBC	IHA	Out of chronological order. Newer message is processed before an older message.	Hardware error during processing or transmission.	ID		IHA: IH-SR-68	Mitigated	OBC	IE	

OBC-HL-102	OBC	IHA	Overspeed when corrupt configuration data used by OBC	Internal Onboard communications failure	IIC		IHA: IH-SR-70	Mitigated	PTE	IIE	TM-1051-05 - LIRR ACSES II Maintenance (Training Slideshow) - Slide 143 includes training on how to configure parameters in ACSESView, specifically a step to confirm changes to complete configuration.
OBC-HL-103	OBC	IHA	No configuration data is transferred from PTE to CMM	Internal Onboard communications failure	IIC		IHA: IH-SR-71	Mitigated	PTE	IIE	
OBC-HL-104	OBC	IHA	Service brake signal is falsely de-energized	Failure of safety relay	IID		IHA: IH-SR-32	Mitigated	Depart Test	IIE	
OBC-HL-105	OBC	IHA	ACSES Cut-In signal remains high after switch is turned to cut out ACSES.	Hardware failure within switch or wiring	IIC		IHA: IH-SR-32	Mitigated	OBC	IE	D7710H0223-A01 - LIRR M7 Bypass Switch Assembly - Sheet 1 of this drawing shows the Assembly and Parts List. Item 10 on the parts list on sheet 1 shows that the switch used for ACSES bypass is an 8 Pole Rotary Switch (Siemens P/n 200025). These types of switches have been used across multiple platforms and projects and have a robust service history. They are service proven to be highly reliable.
OBC-HL-106	OBC	IHA	Collision or derailment if corrupted during transmission and train moves into IXL that is not cleared.	Corrupted message. Incorrect request sent or sent to wrong WIU.	IC		IHA: IH-SR-32	Mitigated	OBC	IE	
OBC-HL-107	OBC	IHA	Derailment if incorrect IXL status is received by OBC due to corrupt message	Communication failure between MCM and OBC	IC		IHA: IH-SR-77	Mitigated	OBC	IE	

OBC-HL-108	OBC	SSHA	Train encroaches into interlocking due to incorrect scanner antenna offset distance	Internal Onboard communications failure	IC	[redacted]	SSHA: SR-SH-01	Mitigated	OBC	IE	
OBC-HL-109	OBC	SSHA	Train encroaches into interlocking due to incorrect scanner antenna offset distance	Internal Onboard communications failure	IC		SSHA: SR-SH-02	Mitigated	OBC	IE	
OBC-HL-110	OBC	SSHA	Train encroaches into interlocking due to incorrect scanner antenna offset distance	Internal Onboard communications failure	IC		SSHA: SR-SH-03	Mitigated	OBC	IE	
OBC-HL-111	OBC	SSHA	Wrong offset data entered into CMM via PTE	Improper maintenance activity	IC		SSHA: SR-SH-04	Mitigated	OBC	IE	TM-1051-05 - LIRR ACSES II Maintenance (Training Slideshow) - Slides 139-145 - These slides detail the configuration of parameters using ACSESView (through a PTE) 3037853 (CDRL 2-49-201) - LIRR ACSESView User Manual - Multiple Sections - This manual provides detail on connecting to system with a PTE.
OBC-HL-112	OBC	SSHA	Incorrect ID number sent by OBC to MCM. ID number includes ATCS address for that OBC system	Internal Onboard communications failure	IC		SSHA: SR-SH-06	Mitigated	OBC	IE	
OBC-HL-113	OBC	SSHA	Timeout and loss of comms of the data radio link when no activity occurs.	Communication failure between MCM and OBC	IIC		SSHA: SR-SH-07	Mitigated	OBC	IIE	
OBC-HL-114	OBC	SSHA	OBC sends incorrect or fails to send the distance-to-signal message to BCM when approaching IXL.	Communication failure between MCM and OBC	IIC		SSHA: SR-SH-09	Mitigated	OBC	IIE	

OBC-HL-115	OBC	SSHA	MCM sends incorrect radio link health status to OBC	Communication failure between MCM and OBC	IIC	[redacted]	SSHA: SR-SH-10	Mitigated	OBC	IIE	
OBC-HL-116	OBC	SSHA	Train fails to stop before reaching SAR TSR target point	Communication failure between MCM and OBC	IC		SSHA: SR-SH-11	Mitigated	OBC	IE	
OBC-HL-117	OBC	SSHA	Brake Assurance travel distance calculation error by OBC allows vehicle to encroach into restricted zone.	Internal Onboard communications failure	IC		SSHA: SR-SH-12	Mitigated	OBC	IE	
OBC-HL-118	OBC	SSHA	OBC clears Zero Speed TSRs when TSR List is erased when direction is changed (such as during turnback)	Internal Onboard communications failure	IC		SSHA: SR-SH-15	Mitigated	OBC	IE	
OBC-HL-119	OBC	SSHA	Zero Speed TSR is removed when TSR List is removed after 60 minutes	Internal Onboard communications failure	IC		SSHA: SR-SH-16	Mitigated	OBC	IE	
OBC-HL-120	OBC	SSHA	Overspeed if default speed limits are incorrectly applied in ABS/CMB territory.	Internal Onboard communications failure	IC		SSHA: SR-SH-17	Mitigated	OBC	IE	
OBC-HL-121	OBC	SSHA	PTS targets are not enforced in ABS/CMB territory.	Internal Onboard communications failure	IC		SSHA: SR-SH-18	Mitigated	OBC	IE	
OBC-HL-122	OBC	SSHA	Overspeed if default speed limits are incorrectly applied in MBS territory.	Internal Onboard communications failure	IC		SSHA: SR-SH-19	Mitigated	OBC	IE	
OBC-HL-123	OBC	SSHA	Train fails to stop prior to running past target point when BA is applied.	Internal Onboard communications failure	IC		SSHA: SR-SH-21	Mitigated	OBC	IE	

OBC-HL-124	OBC	SSHA	OBC fails to send Type 11 message, TSR request.	Communication failure between MCM and OBC	IC	[redacted]	SSHA: SR-SH-22	Mitigated	OBC	IE	
OBC-HL-125	OBC	SSHA	OBC configuration data is changed due to unauthorized Remote access with read/write permission.	Internal Onboard communications failure	IC		SSHA: SR-SH-23	Mitigated	OBC	IE	
OBC-HL-126	OBC	SSHA	Loose sensor provides inaccurate readings	Speed sensor failure	IC		SSHA: SR-SH-25	Mitigated	OBC	IE	
OBC-HL-127	OBC	SSHA	Train cannot move into IXL since second IXL contains HS for the first IXL (back-to-back transponder installation)	Internal Onboard communications failure	IC		SSHA: SR-SH-26	Mitigated	OBC	IE	
OBC-HL-128	OBC	SSHA	Turnback actions do not allow full ACSES functionality.	Internal Onboard communications failure	IC		SSHA: SR-SH-29	Mitigated	OBC	IE	
OBC-HL-129	OBC	SSHA	ATC failure during turnback actions. OBC fails to directly enforce PTS during turnback.	Internal Onboard communications failure	IC		SSHA: SR-SH-30	Mitigated	OBC	IE	
OBC-HL-130	OBC	SSHA	IXL status change to stop during turnback. OBC fails to enforce immediate PTS during turnback and enters a restricted zone.	Internal Onboard communications failure	IC		SSHA: SR-SH-31	Mitigated	OBC	IE	
OBC-HL-131	OBC	SSHA	Incorrect PTS enforcement if train moves in opposite direction before stopping at station (overshoots and then reverses into station).	Internal Onboard communications failure	IIC		SSHA: SR-SH-32	Mitigated	OBC	IIE	

OBC-HL-132	OBC	SSHA	Fault if transponder is read incorrectly, OBC improperly removed enforcement. Unauthorized train type enters East Side tunnel.	Missed transponder	IIC	[redacted]	SSHA: SR-SH-33	Mitigated	OBC	IIE	
OBC-HL-133	OBC	SSHA	Radio failed and train has an unknown route through IXL	Communication failure between MCM and OBC	IC		SSHA: SR-SH-34	Mitigated	OBC	IE	
OBC-HL-134	OBC	SSHA	CMM data is incorrect due to corruption or incorrect entry by PTE	Internal Onboard communications failure	IIC		SSHA: SR-SH-35	Mitigated	OBC	IIE	
OBC-HL-135	OBC	SSHA	Tachometers fail to detect start/stop of slip and slide conditions	Speed sensor failure	IC		SSHA: SR-SH-36	Mitigated	OBC	IE	
OBC-HL-136	OBC	SSHA	OBC to MCM communication link for data radio fails and provides incorrect data.	Communication failure between MCM and OBC	IIC		SSHA: SR-SH-38	Mitigated	OBC	IIE	
OBC-HL-137	OBC	SSHA	OBC fails to request TSR List when entering zone	Communication failure between MCM and OBC	IC		SSHA: SR-SH-39	Mitigated	OBC	IE	
OBC-HL-138	OBC	SSHA	Operator does not detect that no TSRs are being enforced and does not take required procedural actions. TSR not enforced.	Internal Onboard communications failure	IIC		SSHA: SR-SH-42	Mitigated	OBC	IIE	
OBC-HL-139	OBC	SSHA	Tach I/O fails to receive correct Perm Supp input from discrete wiring	Internal Onboard communications failure	IIC		SSHA: SR-SH-43	Mitigated	OBC	IIE	
OBC-HL-140	OBC	SSHA	OBC calculates incorrect alert and braking curves when BA is applied	Internal Onboard communications failure	IC		SSHA: SR-SH-46	Mitigated	OBC	IE	

OBC-HL-141	OBC	SSHA	Brake Assurance offset distance is incorrectly calculated	Internal Onboard communications failure	IC	[redacted]	SSHA: SR-SH-47	Mitigated	OBC	IE	
OBC-HL-142	OBC	SSHA	Speed limit may exceed max speed limit in ACSES territory	Internal Onboard communications failure	IC		SSHA: SR-SH-48	Mitigated	OBC	IE	
OBC-HL-143	OBC	SSHA	OBC incorrectly calculates Alert and Braking Curves for PTS target points for PSR enforcement	Internal Onboard communications failure	IC		SSHA: SR-SH-49	Mitigated	OBC	IE	
OBC-HL-144	OBC	SSHA	OBC distance calculation error causes non-enforcement of TSR length	Internal Onboard communications failure	IC		SSHA: SR-SH-50	Mitigated	OBC	IE	
OBC-HL-145	OBC	SSHA	OBC calculated distance error allows train to run past Point TSR location.	Internal Onboard communications failure	IC		SSHA: SR-SH-52	Mitigated	OBC	IE	
OBC-HL-146	OBC	SSHA	OBC fails to enforce proper speed limit when ATC is cut-out	Internal Onboard communications failure	IC		SSHA: SR-SH-53	Mitigated	OBC	IE	
OBC-HL-147	OBC	SSHA	PTS Target removed before final berthing, allows doors to open when not at platform.	Internal Onboard communications failure	IC		SSHA: SR-SH-55	Mitigated	OBC	IE	
OBC-HL-148	OBC	SSHA	EB relay is not tested and train is unsafely allowed to continue	Failure of vital relay	IC		SSHA: SR-SH-56	Mitigated	OBC	IE	
OBC-HL-149	OBC	SSHA	Overspeed if incorrect speed limits applied when exiting ACSES territory.	Internal Onboard communications failure	IC		SSHA: SR-SH-57	Mitigated	OBC	IE	
OBC-HL-150	OBC	SSHA	Train fails to enforce VZ and runs through SAR TSR point	Internal Onboard communications failure	IC		SSHA: SR-SH-58	Mitigated	OBC	IE	

OBC-HL-151	OBC	SSHA	SAR TSR enforcement is released by Ack when further than 250 feet from actual location	Train position failure due to OBC errors.	IC	[redacted]	SSHA: SR-SH-59	Mitigated	OBC	IE	
OBC-HL-152	OBC	SSHA	Partial or corrupted TP data is accepted by OBC.	Failure to read transponder	IC		SSHA: SR-SH-60	Mitigated	OBC	IE	
OBC-HL-153	OBC	SSHA	TSR and PTS target points are erased when entering new segment or line.	Internal Onboard communications failure	IIC		SSHA: SR-SH-61	Mitigated	OBC	IIE	
OBC-HL-154	OBC	SSHA	Failed speed sensor is not detected	Speed sensor failure	IC		SSHA: SR-SH-62	Mitigated	OBC	IE	
OBC-HL-155	OBC	SSHA	Decelerometer provides incorrect brake rate to OBC, slip or slide distance not estimated	Hardware failure of decelerometer	IC		SSHA: SR-SH-63	Mitigated	OBC	IE	
OBC-HL-156	OBC	SSHA	Wrong RR grade factor used. Collision due to insufficient calculated braking distance	Internal Onboard communications failure	IC		SSHA: SR-SH-64	Mitigated	OBC	IE	
OBC-HL-157	OBC	SSHA	Wrong train type grade is applied, passenger or freight	Internal Onboard communications failure	IC		SSHA: SR-SH-65	Mitigated	OBC	IE	
OBC-HL-158	OBC	SSHA	Incorrect brake curve	Internal Onboard communications failure	IC		SSHA: SR-SH-66	Mitigated	OBC	IE	
OBC-HL-159	OBC	SSHA	TSRs erased due to limited storage capacity	Internal Onboard communications failure	IIC		SSHA: SR-SH-67	Mitigated	OBC	IIE	
OBC-HL-160	OBC	SSHA	Immediate PTS not enforced during turnback when first cab is keyed off, allowing train to move without authorization when second cab is keyed on.	Internal Onboard communications failure	IC		SSHA: SR-SH-68	Mitigated	OBC	IE	

OBC-HL-161	OBC	Testing	Train can move at speeds lower than VZ detectable level.	Hardware limitation of speed sensor	IC	[redacted]	SSHA: SR-SH-69	Mitigated	OBC	ID	
OBC-HL-162	OBC	New	Braking curves are incorrectly established with respect to enforcement point targets.	OBC software error	IC		SSHA: SR-SH-70	Mitigated	OBC	IE	
OBC-HL-163	OBC	New	Incomplete transponder sets are used by OBC.	OBC software error	IIIC		SSHA: SR-SH-71	Mitigated	OBC	IIIE	
OBC-HL-164	OBC	New	OBC sends IXL status requests when not needed	OBC software error	IIIC		SSHA: SR-SH-72	Mitigated	OBC	IIIE	
OBC-HL-165	OBC	New	Enforcement point changes during an enforcement action	OBC software error	IC		SSHA: SR-SH-73	Mitigated	OBC	IE	
OBC-HL-166	OBC	New	Brake speed limit is more than 6 mph above speed limit	OBC software error	IC		SSHA: SR-SH-74	Mitigated	OBC	IE	
OBC-HL-167	OBC	New	Overspeed at the start of a PSR	OBC software error	IC		SSHA: SR-SH-75	Mitigated	OBC	IE	
OBC-HL-168	OBC	New	Route Dependent PSR is not enforced in IXL by OBC	OBC software error	IC		SSHA: SR-SH-76	Mitigated	OBC	IE	
OBC-HL-169	OBC	New	OBC continues to enforce PSR beyond IXL.	OBC software error	IIIC		SSHA: SR-SH-77	Mitigated	OBC	IIIE	
OBC-HL-170	OBC	New	OBC enforces TSR in Construction Zone	Internal Onboard communications failure	IIIC		SSHA: SR-SH-78	Mitigated	OBC	IIIE	
OBC-HL-171	OBC	New	Forward PTS is not accepted by OBC	Internal Onboard communications failure	IIIC		SSHA: SR-SH-79	Mitigated	OBC	IIIE	
OBC-HL-172	OBC	New	Overspeed if speed limit is not known	Internal Onboard communications failure	IC		SSHA: SR-SH-80	Mitigated	OBC	IE	

OBC-HL-173	OBC	New	OBC calculated distance error allows train to release PSR too early.	Internal Onboard communications failure	IC	[redacted]	SSHA: SR-SH-81	Mitigated	OBC	IE	
OBC-HL-174	OBC	New	PTS starting point is unknown.	Internal Onboard communications failure	IC		SSHA: SR-SH-82	Mitigated	OBC	IE	
OBC-HL-175	OBC	New	Zero Speed or Stop and Release (SAR) TSR is not enforced by OBC	Internal Onboard communications failure	IIIC		SSHA: SR-SH-83	Mitigated	OBC	IIIE	
OBC-HL-176	OBC	New	TSR in IXL is not enforced by OBC	Internal Onboard communications failure	IC		SSHA: SR-SH-84	Mitigated	OBC	IE	
OBC-HL-177	OBC	New	TSR in IXL is not enforced by OBC	Internal Onboard communications failure	IC		SSHA: SR-SH-85	Mitigated	OBC	IE	
OBC-HL-178	OBC	New	TSR in IXL is not enforced by OBC	Internal Onboard communications failure	IC		SSHA: SR-SH-86	Mitigated	OBC	IE	
OBC-HL-179	OBC	New	Overspeed after Absolute Stop Bypass switch is used	Internal Onboard communications failure	IC		SSHA: SR-SH-87	Mitigated	OBC	IE	
OBC-HL-180	OBC	New	Overspeed after Absolute Stop Bypass switch is used	Internal Onboard communications failure	IC		`	Mitigated	OBC	IE	
OBC-HL-181	OBC	New	Overspeed if default speed limits are incorrectly applied.	Internal Onboard communications failure	IC		SSHA: SR-SH-89	Mitigated	OBC	IE	
OBC-HL-182	OBC	New	PTS not enforced by OBC	Internal Onboard communications failure	IC		SSHA: SR-SH-90	Mitigated	OBC	IE	

OBC-HL-183	OBC	New	PTS Stop is not requested by ATC or AIU	Internal Onboard communications failure	IC	[redacted]	SSHA: SR-SH-91	Mitigated	AIU	IE	
OBC-HL-184	OBC	New	Overspeed enforcement suppression incorrectly determined by OBC	Internal Onboard communications failure	IIIC		SSHA: SR-SH-92	Mitigated	OBC	IIIE	
OBC-HL-185	OBC	New	Home Signal PTS is enforced when TP is not present	Internal Onboard communications failure	IIIC		SSHA: SR-SH-93	Mitigated	OBC	IIIE	
OBC-HL-186	OBC	New	Absolute Stop Bypass button fails to release PTS	Internal Onboard communications failure	IIIC		SSHA: SR-SH-95	Mitigated	OBC	IIIE	
OBC-HL-187	OBC	New	ASB Speed Limit remains active after OBC reads TP	Internal Onboard communications failure	IIIC		SSHA: SR-SH-96	Mitigated	OBC	IIIE	
OBC-HL-188	OBC	New	ASB Speed Limit remains active if IXL exit transponder is missed	Internal Onboard communications failure	IIIC		SSHA: SR-SH-97	Mitigated	OBC	IIIE	
OBC-HL-189	OBC	New	PTS is not released by radio message	Internal Onboard communications failure	IIIC		SSHA: SR-SH-98	Mitigated	OBC	IIIE	
OBC-HL-190	OBC	New	Brakes not applied when ACSES is cut-out or failed	Internal Onboard communications failure	IC		SSHA: SR-SH-99	Mitigated	OBC	IE	
OBC-HL-191	OBC	New	Overspeed if most restrictive speed limit not enforced when in active mode	Internal Onboard communications failure	IC		SSHA: SR-SH-100	Mitigated	OBC	IE	
OBC-HL-192	OBC	New	MNR only, train type is changed when in non-ACSES territory and wrong line speed is used when returned to ACSES territory	Internal Onboard communications failure	IC		SSHA: SR-SH-101	Mitigated	OBC	IE	

OBC-HL-193	OBC	New	Zero Speed TSR is released when TSR List is erased	Internal Onboard communications failure	IC	[redacted]	SSHA: SR-SH-102	Mitigated	OBC	IE	
OBC-HL-194	OBC	New	ABS/CMB territory is not enforced	Internal Onboard communications failure	IIIC		SSHA: SR-SH-103	Mitigated	OBC	IIIE	
OBC-HL-195	OBC	New	Incorrect curves used by OBC when Forward PTS transponder is read	Internal Onboard communications failure	IC		SSHA: SR-SH-104	Mitigated	OBC	IE	
OBC-HL-196	OBC	New	Overspeed if ASB is used in ABS/CMB territory	Internal Onboard communications failure	IC		SSHA: SR-SH-106	Mitigated	OBC	IE	
OBC-HL-197	OBC	New	OBC releases enforcement of speed limits too early when in ABS/CMB zone	Internal Onboard communications failure	IC		SSHA: SR-SH-107	Mitigated	OBC	IE	
OBC-HL-198	OBC	New	OBC releases enforcement of speed limits too early when in ABS/CMB zone	Internal Onboard communications failure	IC		SSHA: SR-SH-108	Mitigated	OBC	IE	
OBC-HL-199	OBC	New	OBC releases enforcement of speed limits too early when in ABS/CMB or MBS zone	Internal Onboard communications failure	IC		SSHA: SR-SH-109	Mitigated	OBC	IE	
OBC-HL-200	OBC	New	Overspeed if MBS territory is not enforced by OBC	Internal Onboard communications failure	IC		SSHA: SR-SH-110	Mitigated	OBC	IE	
OBC-HL-201	OBC	New	Emergency brake released before train has stopped	Internal Onboard communications failure	IC		SSHA: SR-SH-111	Mitigated	OBC	IE	

OBC-HL-202	OBC	New	Emergency brake signal for M7 or M9 is held for too long	Internal Onboard communications failure	IIIC	[redacted]	SSHA: SR-SH-112	Mitigated	OBC	IIIE	
OBC-HL-203	OBC	New	Emergency brake released before M7 or M9 train has stopped	Internal Onboard communications failure	IC		SSHA: SR-SH-113	Mitigated	OBC	IE	
OBC-HL-204	OBC	New	Decelerometer functions are not verified during use.	Internal Onboard communications failure	IIIC		SSHA: SR-SH-114	Mitigated	OBC	IIIE	
OBC-HL-205	OBC	New	Decelerometer functions are not verified during use.	Internal Onboard communications failure	IIIC		SSHA: SR-SH-115	Mitigated	OBC	IIIE	
OBC-HL-206	OBC	New	Decelerometer functions are not verified during use.	Internal Onboard communications failure	IIIC		SSHA: SR-SH-116	Mitigated	OBC	IIIE	
OBC-HL-207	OBC	New	Decelerometer functions are not verified during use.	Internal Onboard communications failure	IIIC		SSHA: SR-SH-117	Mitigated	OBC	IIIE	
OBC-HL-208	OBC	New	PTS Hold is not applied by OBC in the correct location	Internal Onboard communications failure	IIIC		SSHA: SR-SH-118	Mitigated	OBC	IIIE	
OBC-HL-209	OBC	New	PTS Hold is not applied by OBC	Internal Onboard communications failure	IIIC		SSHA: SR-SH-119	Mitigated	OBC	IIIE	
OBC-HL-210	OBC	New	Turnback is not enabled	Internal Onboard communications failure	IIIC		SSHA: SR-SH-120	Mitigated	OBC	IIIE	

OBC-HL-211	OBC	New	Turnback PTS is not enforced	Internal Onboard communications failure	IIIC	[redacted]	SSHA: SR-SH-121	Mitigated	OBC	IIIE	
OBC-HL-212	OBC	New	TSR List not requested during Turnback	Internal Onboard communications failure	IIIC		SSHA: SR-SH-122	Mitigated	OBC	IIIE	
OBC-HL-213	OBC	New	Brakes not released during turnback due to PTS	Internal Onboard communications failure	IIIC		SSHA: SR-SH-123	Mitigated	AIU	IIE	
OBC-HL-214	OBC	New	Overspeed upon manual release of Turnback function	Internal Onboard communications failure	IIIC		SSHA: SR-SH-124	Mitigated	OBC	IIE	
OBC-HL-215	OBC	New	OBC fails to make radio contact after turnback	Internal Onboard communications failure	IIIC		SSHA: SR-SH-125	Mitigated	OBC	IIIE	
OBC-HL-216	OBC	New	Home signal changes to Stop or Unknown after Turnback Enforcement is Released	Internal Onboard communications failure	IC		SSHA: SR-SH-126	Mitigated	OBC	IE	
OBC-HL-217	OBC	New	Home signal changes to Stop or Unknown after Turnback Enforcement is Released	Internal Onboard communications failure	IC		SSHA: SR-SH-127	Mitigated	OBC	IE	
OBC-HL-218	OBC	New	Turnback fails to be initiated by Forward PTS package	Internal Onboard communications failure	IIIC		SSHA: SR-SH-128	Mitigated	OBC	IIIE	
OBC-HL-219	OBC	New	Incorrect alert and braking curves are used for Tunnel Avoidance	Internal Onboard communications failure	IC		SSHA: SR-SH-129	Mitigated	OBC	IE	

OBC-HL-220	OBC	New	Distance error compensation allows incorrect enforcement of tunnel stop target	Internal Onboard communications failure	IC		SSHA: SR-SH-130	Mitigated	OBC	IE	
OBC-HL-221	OBC	New	Distance error compensation allows incorrect enforcement of tunnel stop target	Internal Onboard communications failure	IC		SSHA: SR-SH-131	Mitigated	OBC	IE	
OBC-HL-222	OBC	New	Incorrect tunnel stop enforcement due to ATC status	Internal Onboard communications failure	IC		SSHA: SR-SH-132	Mitigated	OBC	IE	
OBC-HL-223	OBC	New	Overspeed enforcement suppression incorrectly determined by OBC	Internal Onboard communications failure	IC		SSHA: SR-SH-133	Mitigated	OBC	IE	
OBC-HL-224	OBC	New	Non-tunnel enabled train enters tunnel	Internal Onboard communications failure	IIIC		SSHA: SR-SH-134	Mitigated	OBC	IIIE	
OBC-HL-225	OBC	New	Incorrect Data Radio message releases tunnel enforcement	Internal Onboard communications failure	IIIC		SSHA: SR-SH-135	Mitigated	OBC	IIIE	
OBC-HL-226	OBC	New	Tunnel Enforcement is removed incorrectly by radio message	Internal Onboard communications failure	IIIC		SSHA: SR-SH-136	Mitigated	OBC	IIIE	
OBC-HL-227	OBC	New	Manual release of tunnel stop occurs in incorrect location	Internal Onboard communications failure	IIIC		SSHA: SR-SH-137	Mitigated	OBC	IIIE	
OBC-HL-228	OBC	New	Transponder fails to release tunnel stop enforcement	Internal Onboard communications failure	IIIC		SSHA: SR-SH-138	Mitigated	OBC	IIIE	
OBC-HL-229	OBC	New	OBC runs with a failed critical PCB	Internal Onboard communications failure	IC		SSHA: SR-SH-139	Mitigated	OBC	IE	

OBC-HL-230	OBC	New	OBC runs with a failed Decel	Internal Onboard communications failure	IC	[redacted]	SSHA: SR-SH-140	Mitigated	OBC	IE	
OBC-HL-231	OBC	New	OBC fails to self-monitor internal operations	Internal Onboard communications failure	IC		SSHA: SR-SH-141	Mitigated	OBC	IE	
OBC-HL-232	OBC	New	Permanent suppression rate is applied for wrong train type	Internal Onboard communications failure	IIIC		SSHA: SR-SH-142	Mitigated	OBC	IIIE	
OBC-HL-233	OBC	IHA	Corrupt message. Incorrect health status received by OBC	Internal Onboard communications failure	IIC		IHA: IH-SR-03	Closed	OBC	IIE	
OBC-HL-234	OBC	PHA	Fire and Smoke. Inhalation damage to passengers or staff.	Underrated cables or incorrect materials used.	IC		PHA: OB-SR-47	Closed	System	IE	
OBC-HL-235	OBC	New	OBC continues to request penalty brake after acknowledgement.	Internal Onboard communications failure	IIIC		None	Mitigated	OBC	IIE	
OBC-HL-236	OBC	New	OBC Fails to read transponder when train speed is greater than Vzero	Failure to read transponder	IC		None	Mitigated	OBC	IE	
OBC-HL-237	OBC	New	OBC Fails to read transponder when train speed is less than or equal to Vzero in PTS Zone	Failure to read transponder	IC		None	Mitigated	OBC	IE	
OBC-HL-238	OBC	New	OBC fails to update train data after reading transponder set	Internal Onboard communications failure	IC		None	Mitigated	OBC	IE	
OBC-HL-239	OBC	New	OBC Fails to determine trains direction of travel.	Failure to receive transponder message	IC		None	Mitigated	OBC	IE	

OBC-HL-240	OBC	New	OBC fails to update train location	OBC software error	IC	[redacted]	None	Mitigated	OBC	IE	
OBC-HL-241	OBC	New	Slip conditions not determined by the OBC	OBC software error	IC		None	Mitigated	OBC	IE	
OBC-HL-242	OBC	New	OBC fails to retain last measured speed and location upon entry into slip condition	OBC software error	IIC		None	Mitigated	OBC	IIE	
OBC-HL-243	OBC	New	Slide conditions not determined by the OBC	OBC software error	IC		None	Mitigated	OBC	IE	
OBC-HL-244	OBC	New	OBC fails to retain last measured speed and location upon entry into slide condition	OBC software error	IIC		None	Mitigated	OBC	IIE	
OBC-HL-245	OBC	New	OBC fails to adjust last measured speed while in slide condition	Internal Onboard communications failure	IIC		None	Mitigated	OBC	IIE	
OBC-HL-246	OBC	New	Incorrect brake curves used by OBC, OBC doesnít apply grade compensation	Internal Onboard communications failure	IC		None	Mitigated	OBC	IE	
OBC-HL-247	OBC	New	Incorrect brake curves used by OBC, OBC doesnít apply grade compensation	Internal Onboard communications failure	IC		None	Mitigated	OBC	IE	

OBC-HL-248	OBC	New	OBC fails to enter ACSES Territory mode when reading a transponder package	Missed transponder, Failure to read transponder, failure to receive transponder message	IIC	[redacted]	None	Mitigated	OBC	IIE	
OBC-HL-249	OBC	New	OBC fails to enter Non-ACSES Territory mode if end of construction zone is a misc. package	Missed transponder, Failure to read transponder, failure to receive transponder message	IIC		None	Mitigated	OBC	IIE	
OBC-HL-250	OBC	New	OBC fails to enter Construction Zone mode.	Missed transponder, Failure to read transponder, failure to receive transponder message	IIC		None	Mitigated	OBC	IIE	
OBC-HL-251	OBC	New	OBC fails to ignore transponder while in Construction Zone.	Incorrect reading of non valid transponder	IIC		None	Mitigated	OBC	IIE	
OBC-HL-252	OBC	New	OBC sets incorrect speed limit while in construction zone.	OBC software error	IIC		None	Mitigated	OBC	IIE	
OBC-HL-253	OBC	New	TSR list is corrupt, pseudo random timestamp does not match	Communication failure between MCM and OBC	IC		None	Mitigated	OBC	IE	

OBC-HL-254	OBC	New	OBC fails to request IXL status for train direction	OBC software error	IC	[redacted]	None	Mitigated	OBC	IE	
OBC-HL-255	OBC	New	OBC fails to request IXL status	OBC software error	IC		None	Mitigated	OBC	IE	
OBC-HL-256	OBC	New	OBC fails to request IXL status at the distance specified in TP	OBC software error	IC		None	Mitigated	OBC	IE	
OBC-HL-257	OBC	New	OBC fails to request IXL status of a nested IXL	OBC software error	IC		None	Mitigated	OBC	IE	
OBC-HL-258	OBC	New	OBC fails to purge TSR data that is not refreshed	OBC software error	IIC		None	Mitigated	OBC	IIE	
OBC-HL-259	OBC	New	Alert speed limit is more than 6 mph above speed limit	OBC software error	IC		None	Mitigated	OBC	IE	
OBC-HL-260	OBC	New	OBC stops enforcing standard TSR due to missed transponder set	Missed transponder	IIC		None	Mitigated	OBC	IIE	
OBC-HL-261	OBC	New	OBC continues to request penalty brake when not needed.	OBC software error	IIIC		None	Mitigated	OBC	IIIE	
OBC-HL-262	OBC	New	OBC continues to request penalty brake when not needed.	OBC software error	IIIC		None	Mitigated	OBC	IIIE	

OBC-HL-263	OBC	New	Incorrect ATCS railroad number used.	Incorrect maintenance activity	IIIC	[redacted]	None	Mitigated	OBC	IIIE	
OBC-HL-264	OBC	New	Default value set to tunnel enabled	Incorrect maintenance activity	IIC		None	Mitigated	OBC	IIE	
OBC-HL-265	OBC	New	Default value set to tunnel enabled	Incorrect maintenance activity	IIC		None	Mitigated	OBC	IIE	
OBC-HL-266	OBC	New	Default value set to tunnel enabled	Incorrect maintenance activity	IIC		None	Mitigated	OBC	IIE	
OBC-HL-267	OBC	New	OBC continues departure test when antenna/CTV fails	Internal onboard communications failure	IIIC		None	Mitigated	OBC	IIIE	
OBC-HL-268	OBC	New	OBC fails to lock in train type or changes train type after Departure test	OBC software error	IC		None	Mitigated	OBC	IE	
OBC-HL-269	OBC	New	Departure test failure when cab is no longer active	Departure test performed incorrectly	IIIC		None	Mitigated	OBC	IIIE	
OBC-HL-270	OBC	New	Departure test failure when train is no longer at Vzero	Departure test performed incorrectly	IC		None	Mitigated	OBC	IE	
OBC-HL-271	OBC	New	Departure test failure when ACSES is cut out	Departure test performed incorrectly	IIIC		None	Mitigated	OBC	IIIE	

OBC-HL-272	OBC	New	OBC fails to release penalty brake when departure test is restarted	OBC Software Error	IIIC	[redacted]	None	Mitigated	OBC	IIIE	
OBC-HL-273	OBC	New	Unintentional movement above Vzero when direction is unknown	OBC Software Error	IC		None	Mitigated	OBC	IE	
OBC-HL-274	OBC	New	OBC fails to set most restrictive speed when train moves in opposite direction of current travel	OBC software error	IC		None	Mitigated	OBC	IE	
OBC-HL-275	OBC	New	Overspeed if OBC enforces higher speed limit in SAR TSR	OBC software error	IC		None	Mitigated	OBC	IE	
OBC-HL-276	OBC	New	OBC starts enforcement of SAR TSR too early	OBC software error	IC		None	Mitigated	OBC	IE	
OBC-HL-277	OBC	New	OBC fails to request penalty brake when ATC is cut out	Internal Onboard Communications failure	IC		None	Mitigated	OBC	IE	
OBC-HL-278	OBC	New	Vital functions not properly performed	OBC hardware or software failure	IC		None	Mitigated	OBC	IE	

OBC-HL-279	OBC	B2B	OBC enforces incorrect speed when in Back-to-back IXL	OBC software error	IC	[redacted]	None	Open	OBC	IE	
OBC-HL-280	not used										
OBC-HL-281	not used										
OBC-HL-282	not used										
OBC-HL-283	OBC	New	Documentation error in safety reports	System failure	IC		None	Transfer	BT	IE	
OBC-HL-284	OBC	IHA	Departure Test not done	Operational failure	IC		IH-SR-01	Transfer	Operations	IE	
OBC-HL-285	OBC	IHA	Vehicle design is changed	Maintenance failure	IC		IH-SR-48	Transfer	Car builder	IE	
OBC-HL-286	OBC	IHA	Permanent Suppression switch is incorrectly read by OBC	Training not performed	IC		IH-SR-50	Transfer	Training	IE	
OBC-HL-287	OBC	IHA	Incompatible SW used in the same area	Training not performed	IC		IH-SR-52	Transfer	Training	IE	
OBC-HL-288	OBC	IHA	Duplicate train ID numbers assigned	Operational failure	IIIC		IH-SR-54	Transfer	Operations	IE	

OBC-HL-289	not used										
OBC-HL-290	OBC	IHA	ATC Departure Test not performed	Operational failure	IC		IH-SR-58	Transfer	ATC provider	IE	
OBC-HL-291	OBC	IHA	Operator fails to use manual TSR lists	Training not performed	IC		IH-SR-61	Transfer	Operations	IE	
OBC-HL-292	OBC	IHA	Transponder locations do not allow data to be read by OBC	Operational failure	IC		IH-SR-69	Transfer	Transponder Install	IE	
OBC-HL-293	OBC	IHA	Transponder locations do not allow data to be read by OBC	Operational failure	IIC		IH-SR-74	Transfer	Transponder Install	IIE	
OBC-HL-294	OBC	IHA	Operator fails to use manual TSR lists	Operational failure	IC		IH-SR-75	Transfer	Operations	IE	
OBC-HL-295	OBC	PHA	Electrocution of maintenance personnel	Training not performed	IIC		OB-SR-25	Transfer	Training	IIE	
OBC-HL-296	OBC	PHA	Departure Test not performed, train has undetected failed equipment	Operational failure	IC		OB-SR-38	Transfer	Training	IE	
OBC-HL-297	OBC	PHA	Transponder locations do not allow data to be read by OBC	Operational failure	IC		OB-SR-42	Transfer	Transponder Install	IE	
OBC-HL-298	OBC	PHA	Train Type switch incorrectly applied	Training not performed	IC		OB-SR-46	Transfer	Training	IE	
OBC-HL-299	OBC	PHA	Train Type switch incorrectly applied	Training not performed	IC		OB-SR-47	Transfer	Training	IE	

OBC-HL-300	OBC	OSHA	Incompatible SW used in the same area	Operational failure	IC	[redacted]	OH-SR-10	Transfer	Maintenance	IE	
OBC-HL-301	OBC	OSHA	Incompatible SW used in the same area	Training not performed	IC		OH-SR-11	Transfer	Maintenance	IE	
OBC-HL-302	OBC	OSHA	Incompatible SW used in the same area	Training not performed	IC		OH-SR-12	Transfer	Maintenance	IE	
OBC-HL-303	OBC	OSHA	Departure Test not performed, train has undetected failed equipment	Operational failure	IC		OH-SR-14	Transfer	Operating	IE	
OBC-HL-304	OBC	OSHA	Operator error causes unsafe condition	Operational failure	IIIC		OH-SR-15	Transfer	Operating	IIIE	
OBC-HL-305	OBC	OSHA	Operator error causes unsafe condition	Operational failure	IC		OH-SR-16	Transfer	Operating	IE	
OBC-HL-306	OBC	OSHA	Operator error causes unsafe condition	Operational failure	IC		OH-SR-21	Transfer	Operating	IE	
OBC-HL-307	OBC	OSHA	Operator error causes unsafe condition	Operational failure	IC		OH-SR-22	Transfer	Operating	IE	
OBC-HL-308	OBC	OSHA	Operator error causes unsafe condition	Operational failure	IC		OH-SR-23	Transfer	Operating	IE	
OBC-HL-309	OBC	OSHA	Operator error causes unsafe condition	Operational failure	IC		OH-SR-24	Transfer	Operating	IE	
OBC-HL-310	OBC	OSHA	Maintainer error causes unsafe condition	Operational failure	IC		OH-SR-25	Transfer	Maintenance	IE	
OBC-HL-311	OBC	OSHA	Operator error causes unsafe condition	Operational failure	IC		OH-SR-26	Transfer	Operating	IE	

OBC-HL-312	OBC	OSHA	Dispatch error causes unsafe condition	Operational failure	IC	[redacted]	OH-SR-27	Transfer	Operating	IE	
OBC-HL-313	OBC	OSHA	Dispatch error causes unsafe condition	Operational failure	IC		OH-SR-28	Transfer	Operating	IE	
OBC-HL-314	OBC	OSHA	Operator error causes unsafe condition	Operational failure	IC		OH-SR-29	Transfer	Operating	IE	
OBC-HL-315	OBC	OSHA	Maintainer error causes unsafe condition	Operational failure	IC		OH-SR-31	Transfer	Maintenance	IE	
OBC-HL-316	OBC	OSHA	Maintainer error causes unsafe condition	Operational failure	IC		OH-SR-32	Transfer	Maintenance	IE	
OBC-HL-317	OBC	OSHA	Maintainer error causes unsafe condition	Operational failure	IC		OH-SR-33	Transfer	Maintenance	IE	
OBC-HL-318	OBC	OSHA	Operator error causes unsafe condition	Operational failure	IC		OH-SR-21	Transfer	Operating	IE	
OBC-HL-319	OBC	SSHA	Maintainer error causes unsafe condition	Operational failure	IC		SR-SH-05	Transfer	Maintenance	IE	
OBC-HL-320	OBC	SSHA	Dispatch error causes unsafe condition	Operational failure	IC		SR-SH-69	Transfer	Office	IE	
OBC-HL-321	OBC	SSHA	Departure Test not performed, train has undetected failed equipment	Operational failure	IC		SR-SH-24	Transfer	Operations	IE	
OBC-HL-322	OBC	SSHA	Maintainer error causes unsafe condition	Operational failure	IC		SR-SH-13	Transfer	Transponder Progra	IE	
OBC-HL-323	OBC	SSHA	WIU error	Operational failure	IC		SR-SH-40	Transfer	WIU	IE	
OBC-HL-324	OBC	SSHA	Dispatch error causes unsafe condition	Operational failure	IC		SR-SH-41	Transfer	Operations	IE	
OBC-HL-325	OBC	SSHA	Vehicle design is changed	Operational failure	IC		SR-SH-20	Transfer	Carbuilder	IE	
OBC-HL-326	OBC	SSHA	Train Type switch incorrectly applied	Operational failure	IC		SR-SH-28	Transfer	Operations	IE	

OBC-HL-327	OBC	New	Transponder message missed due to new Type 7 being used	Operational failure	IC	[redacted]	Back-to-Back	Open	Transponder	IE	
OBC-HL-328	OBC	New	OBC polls incorrect WIU	Missed transponder after turnback package is received	IC		Back-to-Back	Open	OBC	IE	
OBC-HL-329	OBC	New	Incorrect PTS released by ASB	Internal Onboard communications failure	IC		Back-to-Back	Open	RR-Training	IE	
OBC-HL-330	OBC	New	Radio failure after first IXL will cause PTS to not be enforced for remaining switches in nested IXL	Internal Onboard communications failure	IC		Back-to-Back	Open	RR-Tenant Interope	IE	
OBC-HL-331	OBC	OHA	Acknowledge button is always closed	Operator Error	IIC		OHA: OH-SR-36	Mitigated	OBC	IIE	
OBC-HL-332	OBC	IHA	Emergency penalty relay contacts are not open for at least one second.	Emergency Brake pulse (configurable vehicle parameter) not set at 2 seconds	IC		IHA: IH-SR-78	Open	OBC/PTE	IE	

Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

System Risk Assessment

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	PM	Analysis	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Wilt Alston Safety Engineer		Wilton D. Alston 2019.07.24 14:46:42 -04'00'
Verified:	Jason Weighley Safety Engineer		Jason W Weighley 2019.07.24 14:41:28 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.07.24 17:10:34 -04'00'
SI Quality Process Review:	Phil Maglorie BT Quality Assurance Group		Phil Magloire 2019.07.25 07:10:26 -04'00'
BT/SRA Review:	N/A Title		
BT/SRA Review:	N/A Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3155231

Effective Date:	Revision:	Language:
2019-07-24	__	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
Draft1	2019-02-20	First Draft reviewed with LIRR
__	2019-07-24	First Release – Updated to address SNC Lavalin Comments

Table of Contents

Section	Subject	Page
1	**Executive Summary**	5
2	**Introduction**	5
2.1	**Compliance Matrix**	6
2.2	**Reference Documents**	10
2.3	**Glossary**	11
2.4	**Purpose, Scope, and Objective of This Risk Assessment**	12
2.4.1	Purpose	12
2.4.2	Scope	13
2.4.3	Objective	13
2.5	**Regulatory Guidance**	14
2.1	**System Overview**	17
3	**Risk Assessment Methodology**	18
3.1	**Assumptions and Exclusions**	20
3.1.1	Faults in a Vital or Non-Vital Subsystem Performing a Safety Function	20
3.1.2	Faults Associated with Human Error	20
3.1.3	Faults associated with Database Validation and System Access	20
3.2	**Fault Tree Process and Fault Categories**	21
3.2.1	Faults in a Vital Subsystem Performing a Safety Function	22
3.2.2	Faults Associated with Human Error in the Performance of the Function	22
3.2.3	Faults Outside the Risk Assessment Scope	22
3.3	**Risk Assessment Outcomes**	23
3.3.1	Cut-Set Analyses from System-Level FTA	24
3.3.2	Discussion of for Failure Rates for Human Error Terminal Events in CMB Territory	26
3.3.3	Appendix C Compliance Analysis	27
3.3.4	Residual Risk Assessment	27
3.4	**49 CFR Part 236 Safety Principle Compliance Conclusions**	30
3.5	**Residual Risk Impact Assessment Conclusions – Final MTTHE Calculations**	31

List of Figures

Figure 1 – System Architecture 17

Figure 2 – ACSES II System Safety Scope 18

List of Tables

Table 1: Compliance Matrix 6
Table 2: Reference Documents 10
Table 3: Terms Specific to this Document 11
Table 4: Acronyms Specific to this Document 12
Table 5: Cut-Set Analysis – ATC Territory – Fault(s) with **w** Higher Than e^{-9} 25
Table 6: Cut-Set Analysis – CMB Territory – Fault(s) with **w** Higher Than e^{-9} 25
Table 7: Human Error Fault(s) Characterization and Proposed Failure Rates 26
Table 8: ACSES Functions List 27
Table 9: Appendix C Compliance Assessment 30
Table 10: List of MTTHE Calculations 31

1 Executive Summary

Identification of the potential faults associated with the implementation of ACSES II on the LIRR system and defining their hierarchical relationships with one another is the fundamental step required before one can complete the system Risk Analysis.

The fault identification and relationship analysis was performed using a Fault Tree Analysis (FTA). The FTA provides a well-accepted structured method for ensuring comprehensive fault identification, and naturally embodies the relationship among faults and their associated functions. This FTA was the subject of an entirely separate document, and is cited and referenced in this Risk Assessment. As pertinent, sections of the System FTA will be included herein.

2 Introduction

The Risk Assessment of the Advanced Civil Speed Enforcement System (ACSES) Positive Train Control (PTC) system has the objective of assessing the residual risk associated with the implementation and operation of the Vital Overlay ACSES PTC system and determining whether the Risk Assessment has met the requirements of 49 CFR Part 236 Subpart I. This assessment is based on the designation of ACSES as meeting the requirements of a Vital Overlay PTC system as per the Type Approval, substantiated by the entirety of the PTCSP, including this Risk Assessment.

The goal of LIRR is to implement a PTC system that enhances the safety of LIRR operations. The general safety target for LIRR's PTC system is equal to or greater than the existing Type-Approved Amtrak ACSES II. Therefore, the result of the risk assessment illustrates that the computed MTTHE for operations under LIRR PTC are equal to or greater than the existing LIRR ASC system, and, equal to or greater than that of the existing Type-Approved Amtrak ACSES II, in order to meet the safety criteria set forth in FRA Subpart I Appendix B.

The intent of this Risk Assessment Report is to provide a representative, aggregate assessment of risk for the ACSES system deployed on the LIRR PTC territory, based on the system architecture and concept of operations described in the PTCSP document. This Risk Assessment is intended to cover the set of features, capabilities, and settings that will be available in the ACSES PTC as of its implementation on LIRR. The Risk Assessment forms a key component of the overall safety case for the ACSES system and is an integral part of the LIRR PTC Safety Plan.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
2	12.10.8	Fault Tree Analysis	Detailed description of required content of the System FTA, listed here.	
	12.10.8, Subsection A		A system-level Fault Tree Analysis (FTA), CDRL 2-132, shall be submitted by the SI. The system-level FTA shall be used to allocate quantified targets to the ACSES II Subsystems. The ACSES II Subsystem FTA shall be used as part of the evidence to support compliance with the quantified safety requirements allocated to the ACSES II Subsystems	

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.8, Subsection B		The FTA analysis shall furnish a structured means of identifying faults associated with the ACSES II System and ACSES II Subsystem, which must be mitigated, and shall identify the system functions requiring fail-safe implementation. The FTA shall identify the system and subsystem faults, starting with the top level ACSES II System design and the SHL-identified hazards, clearly identifying the logical combinations of faults which are contributors to the hazard, and subsequently developed to the subsystem and interface level.	

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.8, Subsection C		The system-level FTA terminal events shall be used as the top-level events of detailed Fault Tree Analyses (FTAs), which analyze the hardware, and software of each ACSES II Subsystem performing vital functions. System level FTA terminal faults shall be reviewed for possible transfer to the Project Hazard Log for action, tracking, and review	
	12.10.8, Subsection D		The Fault Tree Analysis deliverables shall contain, as a minimum, the following elements: 1. A discussion of the analytic techniques used to generate the fault tree.	

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
			2. Explanation of the types of faults considered part of the ACSES II and those, which are external to the ACSES II, if any. 3. A comprehensive FTA diagram, using a graphical tool, which is suitable for the presentation of the tree logic in a clear and understandable manner. The symbols used and their meaning shall be explained in the text. Each fault or hazard shall be uniquely identified by a reference number.	

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.8, Subsection E		Reference from the unique terminal faults to where their resolution is addressed (e.g., further safety analysis, specific design techniques, Safety V&V, test). Subsequent to the system-level FTA, the ACSES II Subsystem suppliers shall submit FTA(s) to identify the elements that can combine to result in Category I events. The ACSES II Subsystem suppliers shall submit FTA as an input to the overall system-level FTA to be produced by the SI.	

.

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	BT Document ID
[1]	Dictionary of Terms and Acronyms	3035624
[2]	Preliminary Hazard Analysis CDRL 2-127	3035821
[3]	Project Hazard Log CDRL 2-126-20	3035819
[4]	ISOGRAPH Reliability Workbench, Version 12.0	N/A
[5]	System Design Description CDRL 2-27	3035724
[6]	LIRR System Architecture	3038633
[7]	LIRR System PSP CDRL 2-123-20	3035815
[8]	LIRR System Fault Tree Analysis (FTA) CDRL 2-132-20	3035830
[9]	IEEE Standard 1483-2000	N/A
[10]	AREMA C&S Manual, Part 17.3.5	N/A
[11]	System Hazard Analysis CDRL 2-128-20	3035823
[12]	Safety Analysis of Work Zone Incursion Protection (Appendix to PTCSP)	N/A

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in Table 3 and Table 4 respectively.

Table 3: Terms Specific to this Document

Term	Definition
Fault Tree top event	Top event of a fault tree, corresponding to a top-level hazard or system mishap
Fault Tree basic events	Lower level event in fault tree, usually corresponding to a hazard from the list of hazards.

Table 4: Acronyms Specific to this Document

Acronym	Definition
MTTHE	Mean Time to Hazardous Event
N/A	Not Applicable
TBD	To Be Determined

2.4 Purpose, Scope, and Objective of This Risk Assessment

2.4.1 Purpose

The Risk Assessment has been developed to demonstrate that the ACSES II system installed on LIRR meets the risk criteria generally accepted, i.e., industry-standard, for a vital system. (An MTTHE ≥ 10^9 hours is generally accepted in the signaling industry as “a mishap is sufficiently unlikely.”) The Risk Assessment will demonstrate in the following analysis that although there are four (4) categories of faults associated with the system as a whole (see Section 2.6 below), the faults of concern which could lead to an unsafe system hazard or condition in the ACSES II system are limited to faults occurring in three (3) categories; 1) unsafe faults associated with functions performed by vital portions of the equipment, 2) unsafe faults associated with functions performed by non-vital portions of the equipment, and 3) unsafe faults associated with functions performed by maintenance and operational personnel, i.e. human error faults.

2.4.2 Scope

The scope of the Risk Assessment includes the following:

- Identification of all unsafe faults in all categories, i.e.
- all unsafe faults associated with functions performed by vital ACSES II equipment and subsystems, and
- all unsafe faults associated with human error in performing ACSES-related maintenance and operational activities;
- Verification that the MTTHE of all unsafe faults associated with functions performed by vital portions of the ACSES II equipment and subystems is greater than or equal to 10^9 hours.
- Analysis of the potential human errors identified in the Risk Analysis that contribute to any cases that preclude the system MTTHE from being better than or equal to 10^9 hours. By performing a *Cut-Set Analysis*on the Terminal Events from the System FTA, it is possible to directly identify the specific Terminal Events, or combinations thereof, in this category. A **cut-set analysis** determines a distinct path of failure leading to the top undesired event, referred to as the Fault Tree top event in this analysis. A minimal cut-set is the unique and most direct (least safe) path of failure to the Fault Tree top event.

The scope of the Risk Assessment itself does NOT include:

- A safety verification activity that would verify that the operational and maintenance requirements, as written, meet the intent of that procedure as defined in the OHA.
- A safety verification of the LIRR Training Program, over and above realizing that training—specifically as identified in the OHA—can and will be used as an additional mitigation in some cases, for the potential human error faults noted above.

2.4.3 Objective

The objective of this Risk Assessment is to identify all functional faults within the spectrum of safety-critical functions required of and implemented by the vital, and non-vital subsystems of the ACSES II system, and then demonstrate that the risk associated with the possible occurrence of any of those functional faults is low enough to be acceptable. Note that 'acceptable risk' for a catastrophic unsafe event is generally defined by having an MTTHE equal to or greater than 10^9 hours, i.e. commensurate with that of a vitally designed fail-safe system. In that regard, this Risk Assessment (RA) is to demonstrate that the following safety-related aspects of the LIRR ACSES II PTC system have been adequately addressed:

1. all safety-related risks have been identified, including those associated with human error and lack of system availability;

2. the system functions allocated to and performed by fail-safe elements of the system all have an acceptable level of risk commensurate with vital function implementation;
3. the system functions allocated to and performed by non-vital elements of the system all have an acceptable level of risk, as is possible;
4. identified risks associated with human error introduced while performing safety-critical procedures have been exported to the OHA, if necessary for further analysis, or already have existing procedures that mitigate them;
5. functions allocated to non-vital systems do not introduce any additional risk.

As the ACSES system is a Vital Overlay, the level of safety performance achieved is based on evaluation against 49 CFR Part 236, Appendix C criteria, and is independent of the existing level of safety of railroad operations before PTC deployment.

The Risk Assessment is primarily based on the safety documentation provided by the supplier of the ACSES system components/subsystems that implement safety-critical functions. This supplier is responsible for providing sufficient product documentation including implementation of the specific Safety Assurance Concepts (as defined in IEEE 1483-2000 [9]) that are employed in their product designs to allow a clear assessment of their expected safety performance. The final assessment conclusions are dependent on both the accuracy and comprehensiveness of the safety evidence provided by the PTC equipment supplier.

2.5 Regulatory Guidance

In terms of the regulatory guidance upon which this Risk Assessment is developed, there are four (4) primary references, each of which is shown below. CFR 49 §236.1015(d)(3) establishes the requirement for a risk assessment. CFR 49 §236.1015(e)(2)(ii) establishes the context for the category of PTC system being deployed for LIRR, which is in this case a Vital Overlay. CFR 49 Part 236 Appendix B establishes the minimum criteria for the risk assessment. CFR 49 Part 236 Appendix C establishes the safety assurance criteria and processes that the designer must use to develop and validate the product that meets safety requirements of CFR 49 Subpart I.

Reference §236.1015(d)(3): *A risk assessment of the as-built PTC system described.*

Reference §236.1015(e)(2)(ii): *Vital overlay. A PTC system proposed on a newly constructed track or as an overlay on the existing method of operation and built in accordance with the safety assurance principles set forth in Appendix C of this part must, to the satisfaction of the Associate Administrator, be shown to: (ii) Have sufficient documentation to demonstrate that the PTC system, as built, fulfills the safety assurance principles set forth in Appendix C of this part. The supporting risk assessment may be abbreviated as that term is used in subpart H of this part.*

Reference Appendix B: *The safety-critical performance of each product for which risk assessment is required under this part must be assessed in accordance with the following minimum criteria or other criteria if demonstrated to the Associate Administrator for Safety to be equally suitable:*

(a) How are risk metrics to be expressed? The risk metric for the proposed product must describe with a high degree of confidence the accumulated risk of a train control system that operates over the designated life-cycle of the product.

(b) How does the risk assessment handle interaction risks for interconnected subsystems/components? The risk assessment of each safety-critical system (product) must account not only for the risks associated with each subsystem or component, but also for the risks associated with interactions (interfaces) between such subsystems.

(c) What is the main principle in computing risk for the previous and current conditions? The risk for the previous condition must be computed using the same metrics as for the new system being proposed.

(d) What major system characteristics must be included when relevant to risk assessment? Each risk calculation must consider the total signaling and train control system and method of operation, as subjected to a list of hazards to be mitigated by the signaling and train control system.

(e) What other relevant parameters must be determined for the subsystems and components? In order to derive the frequency of hazardous events (or MTTHE) applicable for a product, subsystem or component included in the risk assessment, the railroad may use various techniques.

(f) How are processor-based subsystems/components assessed? An MTTHE value must be calculated for each processor-based subsystem or component.

(g) How are non-processor-based subsystems/components assessed? The safety-critical behavior of all non-processor-based components, which are part of a processor-based system or subsystem, must be quantified with an MTTHE metric.

(h) What assumptions must be documented for risk assessment? The railroad shall document any assumptions regarding the derivation of risk metrics used.

***Reference Appendix C:** Safety Assurance Criteria and Processes that the designer must use to develop and validate the product that meets safety requirements of this part.*

*(1) **System safety under normal operating conditions.** The system (all its elements including hardware and software) must be designed to assure safe operation with no hazardous events under normal anticipated operating conditions with proper inputs and within the expected range of environmental conditions.*

*(2) **System safety under failures.***
- *(i) eliminate or mitigate unsafe systematic failures.*
- *(ii) operate safely under conditions of random hardware failures.*
- *(iii) no single point failures*
- *(iv) no non-self-revealing failure combined with a second failure can cause a hazard..*
- *(v) no common mode failures.*

*(3) **Closed loop principle.** System design adhering to the closed loop principle requires that all conditions necessary for the existence of any permissive state or action be verified to be present before the permissive state or action can be initiated.*

*(4) **Safety assurance concepts.** The product design must include one or more of the following Safety Assurance Concepts as described in IEEE-1483 standard.*
- *(i) Design diversity and self-checking.*
- *(ii) Checked redundancy.*
- *(iii) N-version programming*

(iv) Numerical assurance.
(v) Intrinsic fail-safety.

*(5) **Human factor engineering principle.** The product design must sufficiently incorporate human factors engineering that is appropriate to the complexity of the product; the educational, mental, and physical capabilities of the intended operators and maintainers; the degree of required human interaction with the component; and the environment in which the product will be used.*

*(6) **System safety under external influences.** The product must be shown to operate safely when subjected to different external influences.*

*(7) **System safety after modifications.** Safety must be ensured following modifications to the hardware or software, or both.*

2.1 System Overview

A full detailed description of the system design is provided by the System Design Description [5] Additional details and system architecture is provided in the LIRR System Architecture Description[6].

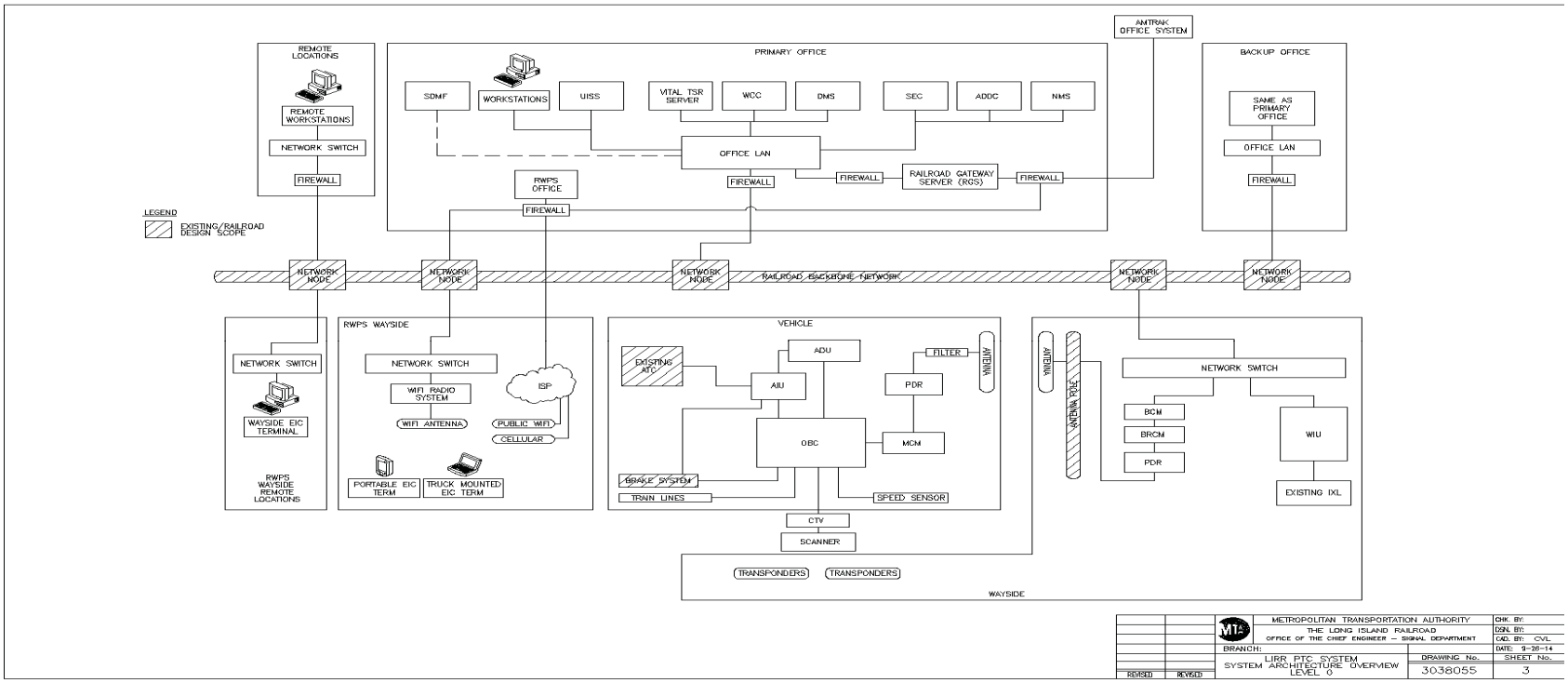


Figure 1 – System Architecture

Figure 2 depicts the ACSES II system safety scope as being within the dotted lines. As shown below, the LIRR ACSES II system complements the Cab Signaling System.

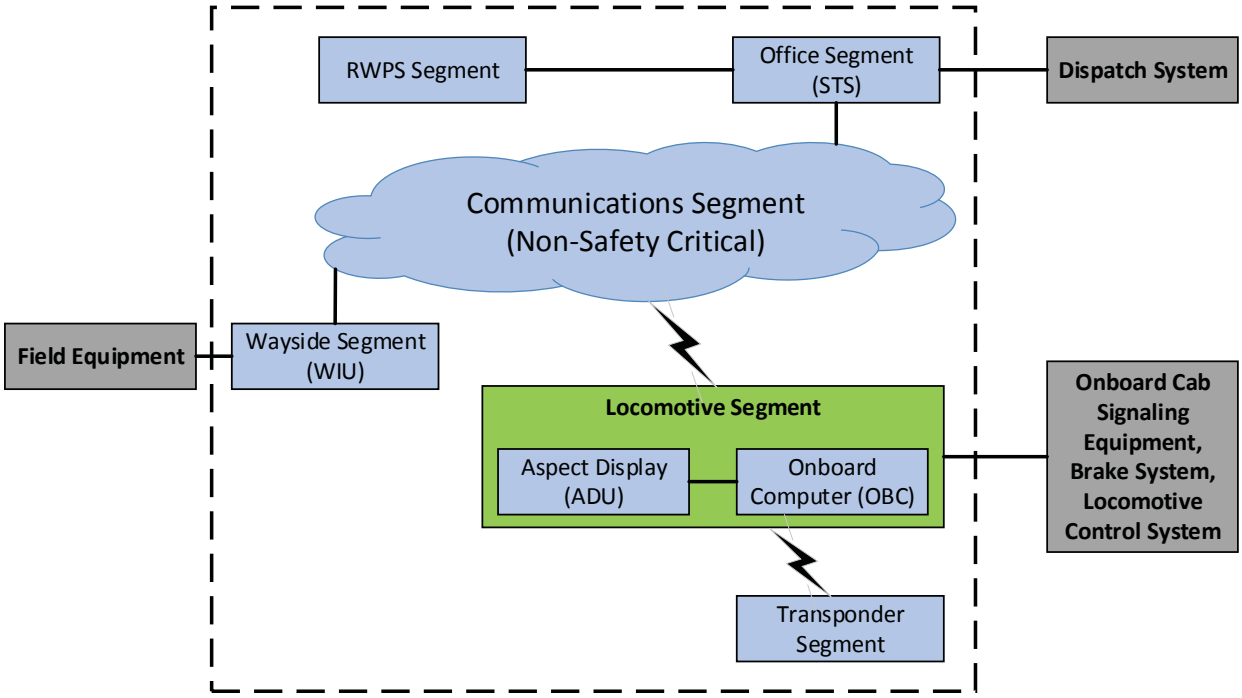


Figure 2 – ACSES II System Safety Scope

The ACSES II system consists of six (6) segments on LIRR, see above Figure 2: the Office Segment, which includes the Safety TSR Server (STS), the Locomotive Segment, which includes both the Aspect Display Unit (ADU) and the Onboard Computer (OBC), the Wayside Segment, which includes the Wayside Interface Unit (WIU), the Transponder Segment, the Roadway Worker Protection System (RWPS) Segment, and the Communications Segment, which is Non-Safety Critical. The architecture of the ACSES II system is shown in Figure 1. The Safety Scope for the ACSES II system, shown in Figure 2, divides the system into segments where the Locomotive, Office, and Wayside segments are allocated safety-critical requirements. Each of these segments has interfaces that are relevant to the risk assessment, as far as definition of the interface assumptions affecting the safety performance of the system.

3 Risk Assessment Methodology

In this analysis, the system concept of operations and other inputs are used to develop a detailed FTA. The FTA is intended to show that all PTC hazard mitigations and FRA-required PTC functions have been implemented. Moreover, it provides a means to quantitatively assess MTTHE at a system-level.

The System Fault Tree Analysis (FTA) was used as input to develop this RA. The FTA identifies all potential unsafe faults within the system and its operation at a functional level. (In fact, the FTA analyzes down to Terminal Events that are each further analyzed by the applicable ACSES II Subsystem or exported to the OHA. Each fault identified contributes to a potential top-level system

hazard. Each top-level hazard is traceable to a mishap which could potentially occur in the LIRR ACSES II system. The use of the structured FTA analysis—for not only the system level, but each subsystem—ensures that all defined potential faults are identified. Ultimately, the FTA shows which faults originate in the ACSES II system at the subsystem level, and also identifies faults external to the ACSES II subsystems, such as operator control or maintenance, that may contribute to system hazards. The FTA further decomposes those faults to the lowest-level terminal faults, which may then be quantitatively or qualitatively assessed to determine the risk.

The FTA is created with top level gates that match the high level categories of PTC preventable accidents. For this reason the HL organization has been designed to map directly into the FTA. By appropriately defining one of the top level gates, this organization of the FTA also facilitates the safety analysis required to meet FRA §236.1015(d)(13) unintended incursion, during system operation, into roadway work zone due to human error. The SI has included a safety analysis to determine whether, when the system operates in the areas of ASC, ABS, CMB, MBS, or MTEA, residual risk of an unintended incursion into work zone limits due to human error exists, if does, the level of this risk.

This PTCSP requires the SI to calculate the MTTHE using the FTA of the as-built system. While risk assessment is traditionally based on frequency and severity of mishaps, an MTTHE calculation addresses probability or frequency of hazards. This section addresses an abbreviated risk assessment in accordance with FRA §236.1015(e)(2)(ii). Fault tree-based MTTHE analysis meets further criteria in Appendix B of Part 236 requiring that the assessment methodology must consider failures caused by permanent, transient, and intermittent faults. The FTA also demonstrates that all hazards related to human error and system unavailability have been identified and mitigated.

Terminal fault events identified and associated with a vital subsystem functions will show an MTTHE value based upon the analysis completed by each subsystem and represented by the FTA for that subsystem. For terminal faults appearing only in the System-Level FTA—the totality of which are Human Error Faults—an MTTHE value will be assigned based upon applicable industry knowledge. Thereafter, the overall MTTHE for the system, as developed from this System FTA, will illustrate if the likelihood of occurrence of all faults meets the expected risk criteria (i.e. MTTHE $\geq 10^9$ hours) and therefore meets the intent of Subpart I.

Faults with an MTTHE of $\geq 10^9$ hours exemplify the lowest generally accepted frequency of occurrence of unsafe failures. As such, this MTTHE represents the lowest achievable risk in the current implementation. However, the System FTA identifies some Terminal Events with MTTHE worse than 10^9 hours . The aforementioned Cut-Set Analysis, completed on the System-Level FTA, identifies cases where there exist terminal events that directly impact the overall MTTHE, making it less than 10^9. This RA will analyze those cases and illustrate how they will be mitigated to a level commensurate with the goals and intent of 49 CFR Part 236 criteria. Those unsafe faults caused by human error associated with operational and/or maintenance procedures have been exported to the Operation Hazard Analysis (OHA) for verification that the procedures adequately mitigate the fault.

As long as all identified faults associated with the ASCES II system are shown to have a frequency of occurrence of $\leq 10^{-9}$ unsafe failures/hour or an MTTHE of $\geq 10^9$ hours, the system meets the intent of the FRA Rules regarding allowable risk.

The goal of LIRR is to implement a PTC system that enhances the safety of LIRR operations. The general safety target for LIRR's PTC system is to be equal to or greater than the existing Type approved Amtrak ACSES II. Therefore, the results of the risk assessment illustrate that the computed MTTHE for operations under LIRR ASC PTC is equal to or greater than that of the existing Type approved Amtrak ACSES II, therefore meeting the risk assessment safety criteria set forth in FRA Subpart I Appendix B.

3.1 Assumptions and Exclusions

3.1.1 Faults in a Vital or Non-Vital Subsystem Performing a Safety Function

It is the responsibility of the RA to demonstrate that the likelihood of any unsafe hazard and/or mishap being precipitated by an unsafe functional fault demonstrated by the system/subsystem MTTHE as relevant.

Assumptions made in the RA:

a. The MTTHE values of the ACSES II subsystems have been provided by the applicable subsystem teams and are assumed by the RA to be correct and were used in the System FTA.
b. All functional faults identified in the FTA have been successfully mitigated by actions taken in the subsystem design (as defined by the functional descriptions referenced in Section 2.3) with an MTTHE associated with the physical subsystems performing the functions.
c. Any functional faults identified in the FTA, but not mitigated by design have been mitigated by other means, as is noted in the System Hazard Log [3]

3.1.2 Faults Associated with Human Error

Generally, human error hazards identified in this Risk Assessment have been exported to the OHA and tracked through closure in that document. However, this RA uses the assumption that such faults fall into one of two categories. Either they represent human error hazards that existed before the implementation of ACSES II, or they are faults that are created because of the implementation of ACSES. A subset of this second category of faults is the case where a fault existed prior to ACSES, but has been partially mitigated by ACSES, even if not to the level of 10^9 hours. (An example of faults created by the implementation of ACSES are all cases of the use of the RWPS.) There are also faults that are unrelated to the addition of PTC to normal LIRR procedures or rules. These are unaffected by the FTA or Risk Assessment. In keeping with the overall goal of a vital overlay system, the overall MTTHE reflected for each territory tree in the System FTA illustrates if the system meets the requirements for a vital overlay, despite the identification and inclusion of terminal events with human error probabilities.

3.1.3 Faults associated with Database Validation and System Access

Other than their identification as external off-line but potentially unsafe faults, track equipment, database accuracy and integrity, and all other factors not directly associated with the ACSES II system components are excluded from this RA, and are the subject of other analyses that support the LIRR PTCSP.

3.2 Fault Tree Process and Fault Categories

In the System FTA document, fault trees were developed to illustrate the relationship between the primary hazards and their potential causative fault events. The complete set of graphical trees is shown in the Appendix of the System FTA **[8]**. Because LIRR has two (2) distinct territories with varying levels of equipment to vitally ensure safety—Automatic Train Control (ATC) versus Controlled Manual Block (CMB)—these territories were treated separately, with a tree being developed for each. As a result, there are analysis conclusions relevant to ATC and CMB territories separately. The development of the FTA was identical for each.

The FTA used a graphical tree structure to present the subsystem level faults which logically combine to precipitate each hazard. Top-Level Events were defined as per industry-standard categorization, including: Collision; Derailment; Personnel or Passenger Death or Injury; and, Fire. Fault Tree Analysis (FTA) was developed in a hierarchical fashion, from those defined top-level hazardous events, to decompose and identify the hazardous events that contribute to the top-level hazardous events at a level that correlates to the system segments/components being assessed.The system FTA ends at the identification of those Terminal Events.

The Terminal Events fall into several categories, each of which could be treated differently with regard to determining the overall system failure rate. These categories, and how they were treated in the System FTA **[8]**, are listed below:

- All Subsystems: These faults that are mitigated by functionality or requirements placed on all subsystems, such as fire retardancy.
- Comm: These faults are mitigated by the functionality in the Communications Subsystem.
- Human Error: These faults will have the standard failure rate for a trained person, which will be 10^{-3} failures/hour.
- Office: These faults are mitigated by functionality in the Office Subsystem;
- Onboard: These faults are mitigated by functionality in the Vehicle Subsystem;
- Railroad: These are faults that are mitigated by standard RR practice(s).
- RWPS: These are faults that are mitigated by the Railway Worker Protection System
- Transponder: These faults are mitigated primarily by the Transponder portion of the Wayside Subsystem;
- Wayside: These faults are mitigated primarily by the WIU portion of the Wayside Subsystem.

The completed subsystem analyses will contain failure probabilities for these events, which will be incorporated into the System FTA, to derive a system rate. In cases where analysis via Fault Tree Analysis has taken place, a reference to the event of interest on the corresponding subsystem tree is shown. The Human Error-Related Faults will be further analyzed in terms of the subcategories of “Existing” and “Enhanced” in this RA, and are also analyzed and mitigated as shown in the System Hazard Log [3][3]

3.2.1 Faults in a Vital Subsystem Performing a Safety Function

For vital functions, the Risk Assessment conclusions for ACSES will be based on computation of MTTHE and assessment as to whether the PTC system fulfills the safety assurance principles of Part 236, Appendix C. The MTTHE is primarily a quantitative analysis that is best represented though a Functional Fault Tree structure that decomposes system operation from a top-level hazardous event (or group of hazardous events) down to a sufficient level of detail where failure rates of lower-level components, subsystems, or procedures are available or may be reasonably inferred. Terminal fault events are associated with the MTTHE for the vital subsystem. Where available, all MTTHE values for the vital subsystem were provided by the applicable subsystem team, and incorporated in the System-Level FTA [8].

The risk of safety-related functions implemented by a vital subsystem function was evaluated quantitatively and if the resulting MTTHE was $\geq 10^9$, hours, they were analyzed no further.

3.2.2 Faults Associated with Human Error in the Performance of the Function

Faults that could be caused or influenced by human interaction were collected and will be analyzed separately as part of the OHA. Generally, these system faults that are mitigated via the OHA will also be exported to the System Hazard Log, where they will be tracked for closure via regular project means. However, if any such faults could directly effect the aggregate safety of the ACSES II system, as illustrated by the MTTHE shown in the System-Level [8], they are further analyzed by the use of a Cut-Set Analysis.

The objective is to illustrate that these faults fall into one of two (2) additional categories, over and above the categories established in Section 3.1.1. Category *Existing*, they existed before the implementation of ASCES, are therefore outside the intended safety scope of ACSES II and are mitigated by existing LIRR procedures. Category *Enhanced*, they exist as a direct result of the implementation of ASCES, and are therefore inside the intended safety scope of ACSES II, but are mitigated by ACSES II to a level that is an improvement over previous conditions. As previously mentioned, the use of RWPS is an example of one such case.

In the case of Human Error Faults in Category *Existing*, the specific OHA item that mitigates them will be identified. Human Error Faults in Category *Enhanced* are analyzed in this RA, and as applicable the specific OHA item that mitigates them is also identified.

3.2.3 Faults Outside the Risk Assessment Scope

This Risk Assessment excludes the validation of the system parameters such as those in the vital database, wherein the location of fixed track components is found. The RA also excludes items such as unauthorized access to the ACSES II System, which is the responsibility of LIRR, over and above the functionality of the System. In the case of database validations, while those locations, and the commensurate performance of the system with respect to those parameters, are safety-critical, those validations are outside the scope of this risk assessment. Such items have been considered and addressed in analyses such as the Operating (and Support) Hazard Analysis (OHA), and tracked for closure via the Project Hazard Log [3].

As part of the published test and commissioning phase of deployment, these parameters, and all other such data, will be verified according to the published procedures and validated as therein described. Correspondingly, this risk assessment is deemed complete without those items, and formally excludes them.

3.3 Risk Assessment Outcomes

This section will summarize the results or outcomes from the analysis completed in the RA. Given the specific assessment methodology applied, the outcomes are divided into its four (4) major components:

1. Cut-Set Analysis from System-Level FTAs
2. Top-Level System-Level FTA Results
3. Appendix C Compliance Analysis
4. Residual Risk Impact

Each of these components is described in additional detail under the dedicated subsections that follow.

3.3.1 Cut-Set Analyses from System-Level FTA

An examination of the System-Level FTAs shows that there exist Terminal Events that do not, by themselves, meet an MTTHE that is equal to or greater than 10^9 hours. In order to determine which of these Terminal Events directly affect the overall system MTTHE, a cut-set analysis was performed. This cut-set analysis illustrates only those Terminal Events, or combinations of Terminal Events, that directly affect the overall system MTTHE. Given that the goal of a vital overlay is to provide a vitally-designed fail-safe system, determining how these specific Terminal Events can be further mitigated is pertinent to completing an assessment of the system relative to the goals of Appendix C. Table below from the System FTA **[8]** is used as input to the RA.

Cut-Set Analysis Table Key

In the table below, which shows those Terminal Events, or combinations of Terminal Events, that directly effect the overall system MTTHE, the following columns are included here and in the FTA document [8]:

- **Gate Name** – The designation of the upper-most gate affected by the cut-set. The term, “FFT_TOP” means that the overall MTTHE is directly affected by the cut-set;
- **Count** – An ordinal count, showing the number of entries in the table;
- **Cut Set** – The identifier for either the specific Terminal Event, or the combination of Terminal Events of which the Cut Set is composed.;
- **Cut Set Description** – The description, as derived from the System FTA Terminal Event. In the case where multiple Terminal Events comprise the Cut Set, a “::” is shown to indicate the joining of two, or more, Terminal Events.
- **Set Failure Frequency** – The MTTHE for the Terminal Event, if a single Terminal Event accounts for the Cut Set, or the aggregate MTTHE, for a combination of Terminal Events comprising the Cut Set;
- **1st Subsystem** – The ACSES II subsystem to which the Terminal Event has been attributed. In the case where multiple Terminal Events comprise the Cut Set, the first one in the set.
- **Comments** – Relevant Comments about the Cut Set, if applicable.

Table 5: Cut-Set Analysis – ATC Territory – Fault(s) with **w**[1] Higher Than e^{-9}

Gate Name	Count	Cut Set	Cut Set Description	Set Failure Frequency	1st Subsystem	Comments
			None.			

Quoting directly from the System FTA:

The purpose of this ATC Territory Fault Tree Cut-Set Analysis is to illustrate and identify any Terminal Events that directly affect the MTTHE predicted by the full Fault Tree. In this case, all such Terminal Events, i.e., those that have a failure rate higher than e^{-9}, are mitigated either via vital systems or a combination of vital systems and other means. As such, no entries are applicable for this table. ATC Territory meets the requirement for vital overlay without further analysis.

Table 6: Cut-Set Analysis – CMB Territory – Fault(s) with **w**[2] Higher Than e^{-9}

Gate Name	Count	Cut Set	Cut Set Description	[redacted]	1st Subsystem	Comments
FFT_TOP	1	FFT2.2.3.1.2 ::FFT3.1.2.3	Dispatcher Commands Unsafe Switch Movement. [Human Error] ::Training is Ineffective in Assuring Procedural Compliance. [Railroad]		[Human Error]	Existing procedures and/or Operating Rules in place.

Quoting directly from the System FTA:

The purpose of this CMB Territory Fault Tree Cut-Set Analysis is to illustrate and identify any Terminal Events that directly affect the MTTHE predicted by the full Fault Tree. In this case, several such Terminal Events, i.e., those that have a failure rate higher than e^{-9}, exist. That means that these faults are not mitigated sufficiently by vital systems or a combination of vital systems and other means. As such, these Faults will be further analyzed in the Risk Assessment.

[1] The value "**w**" is defined as the Failure Frequency per Hour.
[2] The value "**w**" is defined as the Failure Frequency per Hour.

3.3.2 Discussion of for Failure Rates for Human Error Terminal Events in CMB Territory

For the purposes of the System-Level FTA [8] each of the Human Error Faults has been given a conservative failure rate expected, given industry-standard assumptions. This is true for both the ATC FTA and the CMB FTA. Thereafter, a cut-set analysis, the output of which is shown above, was used to identify any Terminal Events or combinations of Terminal Events that resulted in a top-level MTTHE that was lower than 10^9 hours. As shown, only one such combination of Terminal Events exists, and only for the CMB territory.

Table 7: Human Error Fault(s) Characterization and Proposed Failure Rates

Terminal Event ID	Terminal Event Description	[redacted]	Characterization	Proposed Action	Justification(s) – OHA Entries
FFT2.2.3.1.2	Dispatcher Commands Unsafe Switch Movement. [Human Error] ::Training is Ineffective in Assuring Procedural Compliance. [Railroad]		Existing	TBD	• Extensive Safety Training Required. • Terminal Event combination only applies to CMB Territory.

3.3.3 Appendix C Compliance Analysis

From an examination of the Appendix C—cited in the Introduction—It is understood that a vital overlay PTC system must fulfill the safety principles in Appendix C, with the preamble to the Final Rule stating "*FRA cannot overemphasize that vital overlay system designs must be fully designed to address the factors contained in Appendix C.*" As such, for each safety-critical function provided by the ACSES II PTC System, the following safety principles are addressed:

1. System safety under normal operating conditions;
2. System safety under failures;
3. Closed loop principle;
4. Safety assurance concepts;
5. Human factor engineering principle;
6. System safety under external influences; and,
7. System safety after modifications.

As part of substantiating the designation of vital overlay PTC system, evidence is reviewable for Appendix C compliance verification for non-vitally implemented safety-critical functions as well.

The safety evidence provided for each safety-critical component/subsystem was analyzed as part of this RA to determine whether the applicable Appendix C safety criteria were met at the component/subsystem level. Particular attention was given to all cases where the MTTHE target(s) for a component/subsystem are based on the dependent factors of a safety assurance concept to verify evidence of proper implementation.

3.3.4 Residual Risk Assessment

The system functions as defined in the PTCDP, as Table 5: ACSES Functions List in that document, are partitioned by safety criticality as shown in Table 8, shown below. The System Hazard Analysis (SHA) was reviewed to assess the System Functional Tree Analysis (FTA) representation of each safety critical function. Each function is identified by one of four classifications:

1. Type Approved ACSES II used unmodified – **TA A2**
2. Type Approved ACSES II Modified – **TM**
3. Type Approved LIRR PTCDP – **TA DP**
4. Enhanced Train Control Function – **EF** (Enhancement of ACSES capabilities particular to the high-density commuter railroad application.)

Table 8: ACSES Functions List

Function ID	ACSES II PTC Functionality	Approval Type
OBSx	**Onboard Specific functionality**	
OBS1	ACSES II Modes	TA A2
OBS2	Location Determination	TA A2
OBS3	Front of Train Offset by Direction	EF
OBS4	Distance Calculation	TA A2
OBS5	Wheel Diameters	TA A2

Table 8: ACSES Functions List

Function ID	ACSES II PTC Functionality	Approval Type
OBS6	Wheel Wear Compensation	TA A2
OBS7	Slip/Slide Compensation	TM
OBS8	Rollaway Protection	TA A2
OBS9	V-zero Determination	TA A2
OBS10	ATC Status	TA A2
OBS11	Cab Signal Failure Enforcement	TA A2
OBS13	Full Service Brake Application	TA A2
OBS14	Brake Curve Compensation	TM
OBS15	ACSES Brake Assurance	EF
TEIx	**Train Engineer Interface**	
TEI1	ACSES Display	TM
TEI3	Acknowledge	TA A2
TEI4	No TSR Data Status	TA A2
TEI5	No Transponder Status	TM
TEI6	ACSES Status	TM
TEI7	ATC Status	TM
TEI8	Absolute Stop Bypass Pushbutton	TA A2
DTx	**Departure Testing**	
DT1	Departure Test	TM
DT2	Radio Transmission Departure Test	EF
IPRx	**Interlocking Protection**	
IPR1	PTS Enforcement	TM
IPR2	LoMA	TM
IPR13	Line Boundaries	EF
IPR4	PTSO	TA A2
IPR6	C Signal Function	TA A2
IPR7	Interlocking Exit determination	TM
IPR8	ACSES II Terminate 15 MPH ASB enforcement when TP missed	EF
IPR11	Stopping Accurately at Stations Close to HS	EF
IPR12	ACSES II 8 Track Limit	TM
RCx	**Wireless Communications**	
RC1	220 MHz Data Radio Transmission	TM
RC3	220 MHz Data Radio	EF
RC5	TDMA Radio Messaging	EF
RC9	OBC Location Report to MCM	EF
RC10	Report Train Distance to Home Signal	EF
RC12	Data Radio Termination	TM

Table 8: ACSES Functions List

Function ID	ACSES II PTC Functionality	Approval Type
RC13	BCP Interlocking Configurations	EF
RC14	Nested ILKs with Different Radio Channels	EF
RC15	Cellular	EF
TSRMx	**Temporary Speed Restriction**	
TSRM1	User Input to Safety TSR Server	TM
TSRM4	TSR Select-Check-Execute	TM
TSRM5	TSR List Management	TM
TSRM6	Memorize A TSR in TSR List	TA A2
TSRM7	Delete A TSR from TSR List	TA A2
TSRM8	Approve TSR	TA A2
TSRM10	Output TSR List	TM
TSRM11	TSRs Through Junctions	EF
TSRM12	Shadow (Duplicate) TSRs	TM
TSRM13	Railroad Gateway Server	EF
TSRM15	Increase OBC TSR Storage	TM
TSRM18	Multi-STS Segment Control	EF
TSRM19	TSR Data Request (preload)	TM
TSRM20	Announced Line Boundary	EF
SENx	**Speed Enforcement**	
SEN1	Vitally Encoded Transponder data	TA A2
SEN2	Onboard Read of TP Data	TA A2
SEN3	Alert Curve	TA A2
SEN4	MAS Enforcement	TA A2
SEN5	PSR Enforcement	TA A2
SEN6	TSR Enforcement	TM
SEN8	“0” Speed TSR	TM
SEN9	Stop & Release TSR	TM
SEN10	Interlocking PSR	TA A2
SEN11	Route Dependent Speed Restriction	TA A2
SEN13	Route Dependent PTS	EF
TBNCx	**Territory Boundaries & Non-PTC territories**	
TBNC1	Yard & Siding Entry Protection	TM
TBNC2	PTS Enforcement at ABS/CMB Signals w/o cab signaling	TA DP
TBNC3	MTEA	EF
TBNC4	Protection of MTEA Boundaries	EF
TBNC5	Exiting ACSES Territory	TM
DIAGx	**Diagnostics**	

Table 8: ACSES Functions List

Function ID	ACSES II PTC Functionality	Approval Type
DIAG1	Maintenance and Error Messages	TM
DIAG2	OBC Event Logging	TM
DIAG3	DMS Event Logging	TM
DIAG4	Network Management System	TM
DIAG5	Event Recorder Memory Module	EF
DIAG9	OBC Remote Diagnostics	EF
MISCx	**Additional System**	
MISC1	Configuration Management	EF
MISC2	System Initialization	TM
MISC3	Security	EF
MISC4	ADDC and Single Sign-on	EF
RWPx	**Roadway Worker Protection System**	
RWP1	Roadway Worker Protection System	TA DP

3.4 49 CFR Part 236 Safety Principle Compliance Conclusions

The FTA was used to assess the accuracy of representation of the relationship between the unsafe failures associated with each function and the functional and safety requirements of the system. The terminal faults identified in the FTA are categorized into the following groups:

1. Faults associated with PTC subsystem functions that are implemented vitally and have a quantitative MTTHE derived from techniques in compliance with Part 236, Appendix C.
2. Faults associated with PTC subsystem functions that are implemented non-vitally and have a quantitative MTTHE derived from hardware FMEA calculations based on component MTBF and/or qualitative assignment based on expert judgment according to the failure probability categories of AREMA C&S Manual, Part 17.3.5 [10]
3. Faults associated with human errors associated with operations and maintenance of the PTC system. The subset of these faults that are unchanged from existing railroad operations are clearly identified to justify where these faults do not increase the safety risk over existing safe operations.

Table 9: Appendix C Compliance Assessment

Function ID	System Function	Assessment	Notes
OBSx	Onboard Specific Functionality	Compliant	None
OBS9	V-zero Determination	Compliant	None
TEIx	Train Engineer Interface (7 Functions)	Compliant	None
DTx	Departure Testing (2 Functions)	Compliant	None
IPRx	Interlocking Protection (9 Functions)	Compliant	None

Table 9: Appendix C Compliance Assessment

Function ID	System Function	Assessment	Notes
RCx	Wireless Communications	N/A	Non-Safety Critical
TSRMx	Temporary Speed Restriction (18 Functions)	Compliant	None
SENx	Speed Enforcement	Compliant	None
TBNCx	Territory Boundaries & Non-PTC Territories	Compliant	None
DIAGx	Diagnostics	N/A	Non-Safety Critical
MISCx	Additional System	N/A	Non-Safety Critical
RWPx	Roadway Worker Protection System	Compliant	None

3.5 Residual Risk Impact Assessment Conclusions – Final MTTHE Calculations

Of the full range of the ACSES II functionalities identified within the PTCDP (i.e., 68 safety-critical functions, divided among 11 functional groupings), 0 functions demonstrate unacceptable levels of safety risk (i.e., unsafe failure rates on the order of 1×10^{-5} or worse). These numbers are shown below.



It is appropriate to note that in the case of the RWPS, the non-vital nature of the device itself, which has an MTTHE of 10^6 hours, will be augmented with both procedural requirements for usage involving multiple people, including the RWIC interacting with the EIC and, in the specific case of the removal of a TSR, vital oversight by an ACSES II subsystem (STS). As such, this subsystem, as analyzed in the System FTA [8], and functionally described in Safety Analysis of Work Zone Incursion Protection [12] meets the requirements for a vital overlay, as is the case for all other listed system functions.

This Risk Assessment illustrates that the LIRR ACSES II System meets the requirements set for by 49 CFR Subpart I, in regard to system characteristics of a vital overlay for that portion of the system, i.e., excluding the performance of the Onboard.

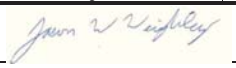
The design and practical performance of the LIRR ACSES II System complies with Appendix C Requirements that are pertinent to a vital overlay and implements a highly-reliable PTC System, that is substantially improved to the performance of the previous system. LIRR continues to work with its supplier to address any remaining areas of risk, through design updates and via continued training.

Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

System Operating Hazard Analysis

CDRL 2-130-20

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Report	Project	Released

Prepared:	Jason Weighley Safety Engineer		Jason W Weighley 2019.07.15 15:36:54 -04'00'
Verified:	Aaron Graham Safety Engineer		Aaron Graham 2019.07.16 09:54:50 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.07.16 10:49:15 -04'00'
SI Quality Process Review:	Phil Maglirie BT Quality Assurance Group		Phil Magloire 2019.07.16 10:42:20 -04'00'
BT/SRA Review:	NA		
BT/SRA Review:	NA		

Name / Title, Group	Signature	Date

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3035826

Effective Date:	Revision:	Language:
2019-07-15	_C	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2014-10-17	First issue
_A	2015-10-16	Submitted for PDR. Aligned with subsystem OHA's
_A1	2016_09_23	Updated for System FDR changes
_A2	2017-01-23	Updated to address review comments from SYSTRA/AECOM
_A3	2017-03-10	Updated to address review comments from SYSTRA/AECOM
_A4	2017-03-23	Corrected acronym for WIU. Deleted repeated occurance of OHA-34 from consoldiate requirements table. Made some correction to requirements allocation to subsystems in the OHA table. Made modification to hazard effects of Sys-OHA-02, 04, 07, and 08 for better alignment with their referenced PHA hazards.
_A5	2017-03-27	Added requirement OHA-79 to drive procedures for configuration of front end offset, wheel diameter, and train type. Removed requirement for restricted speed of unequipped trains and replaced with reference to regulatory requirements for the same. Corrected operating description for Sys-OHA-04. Corrected several hazards with erroenous reference to Office Hazard Analysis. Correct hazard descriptions for Sys-OHA-43, 44, and 45 for consistency with their respective operating descriptions.
_B	2017-03-27	Released for FDR
_C	2019-07-15	Updated for comments on PTCSP

Table of Contents

Section	Subject	Page
1	Executive Summary	4
2	Introduction	4
2.1	Objective	4
2.2	Scope	5
2.3	Compliance Matrix	5
2.4	Reference Documents	7
2.5	Glossary	8
2.6	Safety Targets	9
2.7	Document Overview	9
2.8	Document Updates	10
3	System Overview	10
4	OHA Methodology	10
4.1	Methodology	10
4.2	People who interact with the PTC system	10
4.3	The Hazard Risk Index	11
4.4	Hazard Tracking	11
5	OHA Result Table	12
6	Conclusion	37

List of Figures

No table of figures entries found.

List of Tables

Table 1: Compliance Matrix 5
Table 2: Reference Documents 7
Table 3: Acronyms Specific to this Document 8
Table 4: OHA Table Column Headings and Description 12
Table 5: Operating Scenarios Considered in OHA 13
Table 6: LIRR Operation Hazard Analysis 14
Table 7: Identified Operating Requirements 37

1 Executive Summary

This document records the Operational Hazard Analysis of the LIRR PTC system. This analysis covers the operation, installation, and maintenance including operation under degraded modes and failure conditions for the ACSES II implementation on LIRR. It defines procedures to develop the operational and\or maintenance manual documents to operate the PTC system.

The analysis evaluates the severity and frequency and identifies the causes of hazardous events in order to develop safety mitigation. These identified safety mitigations are translated into design requirements, safety operations and/or maintenance manual requirements. This OHA examines all human activities relating to ACSES II System to identify any hazard in the overall system design, procedure design, or resulting from human errors. And all identified hazards will be maintained in the System Hazard Log (or any planned hazard log) for tracking and proper closure

2 Introduction

As described in the LIRR System Product Safety Plan (SPSP) [4], the Operational Hazard Analysis (OHA) is an analysis of the potential hazards at human-machine interfaces involved in the operation, maintenance, and installation of the PTC System of the LIRR project. This OHA is focused on the system level operational, maintenance, and installation hazards. Once the OHA is finalized and approved, the OHA is incorporated into the system level master hazard log. This OHA is developed in accordance with guidance derived from MIL-STD-882C [3] for the execution of Operating and Support Hazard Analysis.

2.1 Objective

The purpose of the Operational Hazard Analysis (OHA) is to identify and analyze hazards associated with personnel and procedures during application, installation and testing, operation, and maintenance. The OHA is conducted on all tasks and human actions as summarized in § 4.2, including acts of omission and commission, by persons interacting with the system, and assembling of the system. The primary purpose of the OHA is to establish and document the fact that all hazards related to human interaction with the PTC system have been effectively mitigated.

Another outcome of the OHA is a set of recommendations for corrective or preventive measures to be taken to minimize the possibility that any human error or procedure will result in injury or system damage.

These measures include recommendations for:

- Hazards inherent in operating and support activities.
- Changes needed in functional or design requirements for system hardware/software, facilities, tooling, or support/test equipment to eliminate or control hazards or reduce associated risks.
- Warnings, cautions, and special emergency procedures, including those necessitated by failure of a computer software-controlled operation, to produce the expected and required safe result or indication.
- Requirements for storage, transportation, maintenance, and disposal of hazardous materials.

- Requirements for safety training and personnel certification.

Following completion of this OHA, the System Safety Engineer is responsible for ensuring that all identified hazards are included in the Hazard Log. Hazard tracking and control, including tracing through to the appropriate system level requirements is in accordance with the SPSP [4] section 6.2.4.

2.2 Scope

This System level OHA will identify and assess hazards associated with Human-Machine Interfaces of the overall all PTC system in compliance with the OHA requirements of the SPSP [4] section 6.4.3.7.

This system level OHA activity includes:

- Normal PTC operation.
- Dispatcher communication to operational and maintenance personnel (vice versa).
- Failure management and recovery of the system.
- Installation, preventative and corrective maintenances of the PTC system.

As cited in SPSP [4] section 6.4.3.7, each subsystem will produce its own Operation Hazard Analysis that will analyze human operation interfaces, rules, processes, installation procedures, maintenance procedures, and external data that are relied upon to mitigate certain subsystem hazards.

Failures due to outside influences that cannot be detected and/or controlled by the PTC system such as earthquake, fire, flood, evacuation, or terrorist acts are out of scope of this analysis, as stated in the PHA [5].

Operation in areas excluded by the applicable MTEA is out of scope of this analysis as is train-door operation.

2.3 Compliance Matrix

Table 1: Compliance Matrix

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Document Section Reference
1	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.5	An Operating Hazard Analysis (OHA), CDRL 2-130, shall be performed to analyze the interface between humans and the ACSES II System, including all systems and subsystems. The SI shall include operating rules and procedures applicable to the service delivery using the ACSES II System. Mitigation shall include identification of new or modified operating rules and procedures. The		§5 This document addresses system level OHA only.

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Document Section Reference
			writing of the actual rule modifications and/or new procedures is not required.		
2			Operations performed by the Train Engineer, maintenance staff, or other the Railroad personnel shall be considered, as well as system support and maintenance activities which have an impact on ACSES II safety assurance. The purpose of the OHA is to identify those specific procedural requirements that protect passengers and/or personnel from hazards.		§ 2.1
3			The Operating Hazard Analysis shall be performed and documented on all ACSES II System and Subsystems. The OHA identifies and evaluates hazards associated with operation and maintenance of the system. It shall consider the system configuration, the system state, phase of activity, environment, support equipment and all other factors that could affect operational and support safety. The OHA shall address, as applicable:	1.Facilities, support equipment, training and certification related to safety operations and maintenance;	§ 2.1
4				2. Activities, which occur under hazardous conditions, time periods, and the actions necessary to minimize risk;	§5 This document addresses system level OHA only.
5				3. Changes in functional or design requirements needed to eliminate or control hazards	§5 This document addresses system level OHA only.

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Document Section Reference
				or reduce associated risks;	
6				4. Requirements for safety devices and equipment;	§5 This document addresses system level OHA only.
7				5. Warnings, cautions, and special emergency procedures;	§5 This document addresses system level OHA only.
8				6. Requirements for packaging, handling, transportation, maintenance, and disposal of any hazardous materials;	§5 This document addresses system level OHA only.
9				7. Requirements for safety training and personnel certification;	§5 This document addresses system level OHA only.
10				8. Effects of commercial equipment, both hardware and software, across the interface with other components or subsystems;	§5 This document addresses system level OHA only.
11				9. Potentially hazardous system states under operator control (hardware/software).	§5 This document addresses system level OHA only.

2.4 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	PDM 3035624
[2]	System Description Document CDRL 2-27	PDM 3035724

Reference Number	Document Name	Identification Number
[3]	MIL-STD-882_C	
[4]	System Product Safety Plan CDRL 2-123-20	PDM 3035815
[5]	System Preliminary Hazard Analysis CDRL 2-127	PDM 3035821
[6]	Subsystem Operating Hazard Analysis CDRL's 2-130-21 – LIRR On-board Operation Hazard Analysis 2-130-22 – LIRR Office Operating Hazard Analysis 2-130-23 LIRR Comms Operating Hazard Analysis 2-130-24 LIRR WIU Operating Hazard Analysis 2-130-25 LIRR Transponder Operating Hazard Analysis 2-130-26 LIRR RWPS Operating Hazard Analysis	 PDM 3037414 PDM 3037416 PDM 3037418 PDM 3037420 PDM 3037422 PDM 3037424
[7]	System Level Requirements (as part of CDRL 2-004 RTM)	3036443
[8]	2-126 LIRR Project Hazard Log	3035819
[9]	2-128-21 Onboard SSHA 2-128-04 WIU SSHA 2-128-25 Transponder SSHA 2-128-22 Office SSHA 2-128-23 Comms SSHA 2-128-26 RWPS SSHA	3037390 3037399 3037394 3037391 3037392 3037395

2.5 Glossary

Please refer to the Dictionary of Terms and Acronyms, document number 3035624 [1]. Acronyms only related to this document are listed in the Table 3 below.

Table 3: Acronyms Specific to this Document

Acronym	Definition
DSP	Dispatcher
DSI	Distant Switch Indicator (Signal)
EIC	Employee In Charge
HZL	Project Hazard Log
LIRR	Long Island RailRoad
MBS	Manual Block System

Acronym	Definition
MTEA	Main Line Track Exclusion Addendum
OB	On-Board
OHA	Operational Hazard Analysis
PB	Penalty Brake
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PTC	Positive Train Control
RF	Radio Frequency
SLR	System Level Requirements
SPSP	System Product Safety Plan
SSHA	Subsystem Hazard Analysis
TBI	To Be Identified
TE	Train Engineer
TSR	Temporary Speed Restriction
WIU	Wayside Interface Unit

2.6 Safety Targets

The qualitative safety target for the operations and support activities are to demonstrate that all hazards have a documented safety requirement which mitigates the hazard to an acceptable safety level (a risk index value below the safety target identified in section 6.6 of the SPSP [4]).

2.7 Document Overview

Section 1 of this document presents the executive summary of this document.

Section 2 provides the objectives, scope of this analysis, along with references, abbreviations and definitions.

Section 3 provides an overview of the system, and the risk assessment from the hazard analysis and tracking descriptions.

Section 4 Methodology

Section 5 provides the operational hazard analysis result in a tabular format.

Section 6 provides the conclusion of this analysis.

2.8 Document Updates

This Operating Hazard Analysis is a living document and will be reviewed and updated as necessary throughout the LIRR project development lifecycle. For more information on the lifecycle please refer to the System Product Safety Plan[4]. Circumstances requiring an update to the OHA would include, for example, significant changes to the project functions, architecture, or design. Any update to this OHA will be produced, verified and approved by the System Safety Engineer.

3 System Overview

For an overview of the system architecture, please refer to CDRL 2-27 System Description Document [2]

4 OHA Methodology

4.1 Methodology

The identification of hazards extends the preliminary and system level hazard analysis to analyze interactions between the PTC system and people. Information from source documents is referenced for traceability, and is not duplicated to prevent inconsistencies in documentation as the project matures.

The methods used in this OHA to identify hazards are:

- Analysis of operations and support scenarios from the operators' perspective to identify hazards.
- Review of other documentation.
    - Review of System Level Requirement Specification [7] for requirements allocated to Safety Analysis for verification.
    - Review of hazards in the PHA [5] and Project Hazard Log[8] that are mitigated by operating and support activities.
    - Review of mitigations in the subsystem hazard analysis [6] of the On-Board, Office, WIU, Communication, Roadway Worker Protection and Transponder.
    - Review of System Description Document [2] to determine all functions that required operating procedures from the functional descriptions.

The hazards are assessed in accordance with the hazard risk assessment and acceptance criteria as defined in the SPSP [4].

The mitigations are recommended in accordance with the safety criteria as defined in the SPSP [4].

4.2 People who interact with the PTC system

The following people are identified as personnel who are involved in the operation of the PTC system:

- **Dispatcher (DSP):** The DSP manages and monitors the PTC system operation strictly following operating procedures. The PTC system will normally operate without the DSP's intervention in ACSES II Control Mode. During abnormal scenarios, which encompass failures or emergencies, the DSP may be required to intervene to ensure safety.
- **Train Engineer(TE):** The Train Engineer strictly follows operating procedures in coordination with the DSP to safely operate a train. The Train Engineer selects the train operating mode. In Manual Mode, the Train Engineer controls the train's speed and braking.
- **Employee In Charge (EIC):** Roadway worker that is responsible for requesting TSR's and providing status of TSR's for a specific section of the system that has Roadway workers present.
- **Staff:** The LIRR staff (staff) strictly follows operating procedures in coordination with the DSP to ensure safety. The staff monitors and controls points during failures.
- **Maintenance Staff:** The Maintenance staff performs planned preventive maintenance activities and corrective maintenance activities to restore the PTC system operation from a failure condition. The maintenance activities are governed by maintenance procedures which contain cautions and warnings to ensure safety.
    - Maintenance of Wayside (MoW): The MoW staff includes those groups responsible for planned preventive maintenance activities and corrective maintenance activities of track, signals and radios.
    - Maintenance of Equipment (MoE): The MoE staff includes those groups responsible for planned preventive maintenance activities and corrective maintenance activities of mechanical systems and radios.
- **Switching Group:** The Switching Group is the operations team responsible for coupling and moving trains in the yard.
- **Installation & Test:** Installation and Test staff are responsible for installation and test activities during commissioning of the LIRR PTC system.

4.3 The Hazard Risk Index

Please refer to the risk assessment process defined in CDRL 2-123-10 System Product Safety Plan [4] section 6.5.

4.4 Hazard Tracking

All hazards identified in the OHA for which mitigating risk reduction was required to achieve an acceptable safety level (risk index value below the safety target identified in section 6.6 of the SPSP [4]) will be entered into the Hazard Log [8], so that they can be tracked through resolution and regularly reviewed for appropriate action. Some OHA product level hazards may replace more general PHA [5] and subsystem OHA [6] resolutions, and the PHA [5] or subsystem OHA[6] item will be closed, with reference made to the OHA item in the Hazard Log[8].

5 OHA Result Table

Hazard-related information in the OHA worksheet is organized in a table format, consistent with those defined in the SPSP [4] for the PHA, and Project Hazard Log[8]. The detail of the OHA results table is presented in Table 6. A brief description of each column headings in the table is provided in the Table 4 below:

Table 4: OHA Table Column Headings and Description

Heading	Description
OHA ID	The unique ID reference number assigned to an individual hazard. This reference is provided for cross-referencing and traceability for the specific hazard, its cause, and potential resolutions. Format for OHA ID is Sys-OHA-xx, where xx corresponds to a unique and incremental number.
Reference ID	Where applicable, this ID provides reference to a system or subsystem hazard or analysis that may provide additional information of the hazard under assessment
Operating Scenario	A specific manual, procedure, or description which is utilized as part of the maintenance, operation, or installation step which could contribute to a hazard condition. (e.g. Train Entry from Depot/siding/Mainline Track Exception). The complete list of operating scenarios considered in this OHA are captured in Table 5. This list was built based on knowledge of the application of an ACSES II system, previous experience of PTC systems, and OHA review input.
Operating Description	The type of human interaction with the Product, such as transponder antenna usage, onboard system module maintenance, Train Engineer in control, etc.
Hazard Description	A hazard summary provides a description of the specific potential hazards that can be precipitated by the faults identified.
Potential Cause(s)	A potential cause of the hazard identified in the Hazard Description.
Hazard Effects	The potential effects on person(s) and/or system equipment should the hazard occur.
Initial Hazard Severity (I,II,III,IV)	The Severity of a hazard before the safety requirement has been implemented and mitigated the associated hazard.
Initial Hazard Probability (A-E)	The likelihood of a hazard occurring before the safety requirement has mitigated the associated hazard.
Type	The type of human interface analyzed, such as Operation, Maintenance, Installation.
Operating Requirements	This requirement is in the form of an operating or maintenance procedure that will eliminate or control the Hazard.
Operating Requirements ID	Each operating requirement is assigned a unique ID.
Residual Hazard Severity (I,II,III,IV)	The Severity of a hazard before and after the safety requirement has been implemented and mitigated the associated hazard severity will remain the same.
Residual Hazard Probability (A-E)	The likelihood of a hazard occurring after the safety requirement has mitigated the associated hazard.
Subsystem/Equipment	Subsystems or Equipment that are involved in that particular operating scenarios
Closure References	A reference to the document(s) where specific system/subsystem safety requirement(s) for the LIRR implementation are located. In some cases, these documents may not yet be published or available, and a new safety-critical requirement is generated in the OHA to be addressed in the document(s).
Comments	Any miscellaneous comments associated with the hazard's management.

Table 5: Operating Scenarios Considered in OHA

Operation of unequipped (i.e. without ACSES II) train	Normal Operation on Obstructed Track
Maintenance of Wayside Equipment	Maintenance of On Board
Maintenance of Data Communication Equipment	Configuration Management
Maintenance of communication equipment	Turn back Operation
Installation and Configuration of On-Board or Wayside equipment	Operation in Manual Block System territory
Protection of a Failed Highway Crossing	Operation in ABS/CMB Territory
Security Access	Installation and maintenance
TSR Entry by Dispatch	Updates to Software
Maintenance of Electrical Equipment	Departure Test
Traversal of TSR zone	Adj RR Database Alignment
Manual Switch Operation	Onboard failure to detect transponder
System Start-up Daily Departure test procedure	Entering Mainline
Train Exiting ACSES	Sidings with limited room for DS Transponder Placement
Train Entering ACSES	Execution of Stop & Release
Train Operation following an En route failure	East Side Access
Reverse Operation	Traversal of Interlocking authorized by Manual Bypass

Table 6: LIRR Operation Hazard Analysis

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
																Deleted – No train on LIRR with Selector Switch
Sys-OHA-02	PHA-08	Operation of unequipped (i.e. without ACSES II) train	Train Engineer drive unequipped (i.e. without ACSES II) Train	Unequipped (i.e. without ACSES II) train overruns a stop signal	Train Engineer fail to follow the operational rules	Collision, Derailment	I	B	Operation		OHA-02	I	D	System		
											OHA-66					
											OHA-03					

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-04	PHA-21	Maintenance of Wayside Equipment	Wayside Equipment Maintenance	Antenna masts fall from height	Incorrect Maintenance	Collision with Object on track or Infrastructure	I	B	Maintenance		OHA-07	I	D	Wayside		
						Staff Injury or Death			Warning		OHA-08					
									Maintenance		OHA-09					
									Maintenance		OHA-73					
Sys-OHA-05	Communication Hazard Analysis	Maintenance of Data Communication Equipment	Maintenance personnel perform maintenance work on communication equipment	Maintenance personnel works within unsafe distance from active RF antenna	Maintenance Personnel oversight	Staff Injury	II	B	Maintenance		OHA-10	II	D	Wayside communication		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-06	Wayside Hazard Analysis	Maintenance of communication equipment	Installation and maintenance adherence to Warnings, Cautions, and Notes	Installation or maintenance personnel comes in contact with live voltage while maintaining PTC equipment, causing electrical shock because worker does not remove voltages or removes protective devices before working on equipment.	Maintenance Personnel oversight	Staff Injury or Death	I	B	Maintenance		OHA-11	I	D	Wayside communication		
									Installation		OHA-12					
Sys-OHA-07	PHA-23	Installation and Configuration of On-Board or Wayside equipment	Installation and maintenance adherence to Warnings, Cautions, and Notes	On board or wayside equipment not correctly installed	Installation Personnel oversight	Collision with Object on track or Infrastructure	I	C	Installation		OHA-13	I	D	Wayside/Office/Onboard		
									Installation		OHA-46					

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-08	PHA-25	Protection of a Failed Highway Crossing	Dispatcher applying TSR to protect a failure highway crossing	Dispatcher fails to apply a TSR to a highway crossing for which a failure has been reported resulting in unprotected crossing.	Dispatcher oversight	Collision with Road vehicle or pedestrian	I	C	Maintenance		OHA-14	I	D	Wayside/Office		
Sys-OHA-43	OHA Review	TSR Entry by Dispatch	Dispatcher applying TSR to protect a work zone	Dispatcher fails to apply a TSR to a work zone	Dispatcher oversight	Collision	I	C	Maintenance		OHA-73	I	D	Wayside/Office		
Sys-OHA-09	PHA-33	Security Access	ACSES II should only operate by Authorized personnel only.	Vandalism	Unauthorized personnel accessing ACSES II technical room	Collision, Derailment	I	B	Operation		OHA-15	I	D	Wayside/Office		
Sys-OHA-10	Office Hazard Analysis	TSR Entry by Dispatch	TSR entering by the dispatcher	On-board receives TSR with speed higher then intended to be enforced or incorrect location	TSR entered incorrectly by the dispatcher	Collision, Derailment, Staff Injury or Death	I	B	Operation		OHA-16 OHA-67	I	D	Office (STS)		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-11	PHA-49	Maintenance of Electrical Equipment	Maintenance of Electrical Equipment	The maintenance or testing operator mistakenly connects to high power sources	Maintenance Personnel oversight	Staff Injury or Death	I	B	Maintenance		OHA-46	I	D	Wayside/office/Onboard		
Sys-OHA-12	PHA-63	Traversal of TSR zone	Train has traversed and is exiting the TSR zone.	ACSES reduces the train speed so that the front of the train enters the TSR at the correct speed, but the Train engineer accelerates past TSR restriction before rear of train is past TSR location.	Train Engineer fail to follow the operational rules	Derailment, Staff Injury or Death	I	B	Operation		OHA-18	I	D	On-board		Periodic audit of select runs on ACSES View may re-inforce the mitigating operation rules.
Sys-OHA-13	PHA-72	Manual Switch Operation	Switch maintenance	Operating staff fails to operate train in accordance to DSI indications in MBS territory.	Operation Staff oversight	Derailment, Staff Injury or Death	I	C	Operation		OHA-19	I	D	Wayside		
Sys-OHA-14	On Board Hazard Analysis	System Start-up Daily Departure test procedure	RR staff responsible for daily Departure Test verifies pre-requisite	RR staff responsible for daily Departure Test fails to sufficiently verify the train cannot	Maintenance Personnel oversight	Staff Injury/death	I	B	Maintenance		OHA-20	I	D	On-Board		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
			conditions exist before entering Departure Test mode.	move, and inadvertent train motion occurs during daily departure tests.					Maintenance		OHA-21					
Sys-OHA-15	On Board Hazard Analysis	Train Exiting ACSES	Train Entering into Depot/Yard area	Train Engineer does not follow directions of Yardmaster (or equivalent) when entering the Depot or Yard	Train Engineer Error	Collision, Derailment	I	C	Operation		OHA-22 OHA-23	I	D	On-Board		
Sys-OHA-16	On Board Hazard Analysis	Train Exiting ACSES	Train Entering into Depot/Yard area	External system operator gives unsafe authority to TE when Depot/Yard operator cannot set route into transition Zone	External operator Error	Collision	I	C	operation		OHA-24	I	D	On-Board		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-17	On Board Hazard Analysis	Train Exiting ACSES	Train Entering into Depot/Yard area	Train Engineer operates train unsafely in Transition zone	Train Engineer Error	Collision	I	C	Operation	OHA-22 OHA-23	I	D	On-Board		
Sys-OHA-19	On Board Hazard Analysis	Train Operation following an En route failure	Train On Board System	Train Engineer fails to detect and safely react to On-Board system or hardware failure leads to unexpected and severe enforcement braking	Train Engineer Error	Passenger Injury	III	C	Operation	OHA-26	III	D	On-Board		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-20	On Board Hazard Analysis	Train Entering ACSES	Train Exiting from Deport/Yard	The Dispatcher issues unsafe authority into Transition zone when occupancy state is unknown	Dispatcher Error	Collision, Derailment	I	C	Operation		OHA-27 OHA-68	I	D	On-Board		
Sys-OHA-21	On Board Hazard Analysis	Train Entering ACSES	Train Exiting from Deport/Yard	Dispatcher issues unsafe authority into Transition Zone when Depot/Yard interlocking system is non-functional	Dispatcher Error	Collision, Derailment	I	C	Operation		OHA-27 OHA-68	I	D	On-Board		
Sys-OHA-22	On Board Hazard Analysis	Train Entering ACSES	Train Exiting from Deport/Yard	Train Engineer disregards Dispatcher instructions/signal aspect and unsafely drive train into Transition Zone	Train Engineer Error	Collision, Derailment	I	C	Operation		OHA-69	I	D	On-Board		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
											OHA-23					
											OHA-68					
Sys-OHA-23	On Board Hazard Analysis	Reverse Operation	Reverse operation	Dispatcher fails to follow operating rules when authorizing train movement in reverse.	Dispatcher Error	Collision, Derailment	II	B	Operation		OHA-28	II	D	On-Board		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
											OHA-29					This is part of Sys_OHA_23
Sys-OHA-24	Office Hazard Analysis	Normal Operation on Obstructed Track	Some obstruction is in front of the train preventing Train to move	Train collides with obstruction on track that should have been protected by TSR.	Railroad staff failure to establish Zero speed TSRs for track obstructions.	Infrastructure or Vehicle Damage, Collision, or Derailment	I	B	Operation		OHA-30	I	D	Office/Wayside		Combined to ACSES Exit – No specific Track End in ACSES territory
									Operation		OHA-46					
Sys-OHA-26	On Board Hazard Analysis	Maintenance of On Board	Replacement with new OBC unit	Replacing OBC unit while power remains connected and maintainer is electrocuted.	Maintenance Error (non-compliance with procedures)	Staff Injury or Death, Equipment Damage	I	C	Maintenance		OHA-32	I	D	Wayside/On-Board		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
									Maintenanc		OHA-33					
									Maintenanc		OHA-34					
Sys-OHA-27	Communication Hazard Analysis	Maintenance of communication Equipment	Installation and maintenance adherence to Warnings, Cautions, and Notes.	Installation or maintenance personnel comes in contact with live voltage while maintaining ACSESS II equipment, causing electrical shock because worker does not remove voltages or removes protective devices before working on equipment.	Maintenance Personnel oversight	Staff Injury or Death	I	C	Installation		OHA-35	I	D	Communication/Wayside		
									Maintenanc		OHA-33					
									Maintenanc		OHA-34					

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-28	On Board and Office Hazard Analysis	Configuration Management	Configuration of OB/STS System	Maintenance personnel fail to ensure software configuration management (SCM) records and retrieval are correct, leading to incorrect version of software/data being used	Maintenance Personnel oversight	Collision; Derailment	I	C	Maintenance		OHA-36	I	D	On-Board/Office /Wayside		
Sys-OHA-30	Onboard Hazard Analysis	Train Operation following an En route failure	Train Engineer operating a train in which ACSES II has been cut out	Train Engineer cuts out ACSES II system and fails to stop at Stop Signal or violates TSR	Train Engineer Error	Collision; Derailment	I	C	Operation		OHA-39	I	D	On-Board		
									Operation		OHA-26					

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-32	Onboard Hazard Analysis	Turn back Operation	Train Engineer to ensure that train clears the last HS when performing a turnback. Onboard cannot release PTS without information from HS Set.	The entire train fails to pass the HS transponder completely when the turn back is performed in accordance with operating rules.	Train Engineer Error	Collision;	I	B	Operation		OHA-40 OHA-72	I	D	On-Board		
Sys-OHA-34	Onboard Hazard Analysis	Operation in Manual Block System territory	More than one train in MBS Territory	Dispatcher allowed train to enter MBS area when another train is Occupying that area	Dispatcher Error	Collision	I	B	Operation		OHA-43 OHA-42	I	D	Office		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-35	Onboard Hazard Analysis	Operation in Manual Block System territory	Train Engineer Speed Enforcement in MBS territory	Train Engineer fails to adhere to speed limit when operating in MBS territory.	Train Engineer Error	Collision	I	B	Operation	OHA-44	I	D	On-Board		
Sys-OHA-36	Onboard Hazard Analysis	Operation in ABS/CMB Territory	Train Engineer drives train in ABS/CMB territory.	Train Engineer fails to drive the train within the ABS/CMB maximum speed limit	Train Engineer Error	Passenger Injury	III	B	Operation	OHA-45	III	D	On-Board		
Sys-OHA-37	PTC System	Installation and maintenance	Personnel who perform operation, installation, maintenance are fully trained.	Personnel who perform all maintenance activities on PTC system is not fully trained.	Management Error	Collision; Derailment; Staffs Injury or Death	I	A	All	OHA-46	I	D	All		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-39	SIOHA-01 (Onboard OHA)	Maintenance of On Board	Performing periodic inspections	Secondary maintenance personnel could be exposed to a loud noise due to the sudden release of air from pneumatic brake vents as a result of the power being removed from the system.	Maintenance Error	Staff Injury	III	C	Maintenance		OHA-48	III	D	Maintenance Procedures		
Sys-OHA-40	SIOHA-02 (Onboard OHA)	Maintenance of On Board	Replacing onboard enclosure.	The system falls during removal causing a crush hazard.	Maintenance Error	Staff Injury / Death	I	C	Maintenance		OHA-49	I	D	Maintenance Procedures		
Sys-OHA-41	SIOHAIt Only - 03	Maintenance of On Board	Replacing the cardfile	During removal of the cardfile it could drop on an appendage.	Maintenance Error	Staff Injury	IV	C	Maintenance		OHA-50	IV	D	Maintenance Procedures		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-42	SIOHA-04	Maintenance of On Board	Replace Scanner Antenna	Vehicle brakes are not set when removing or inspecting the scanner antenna.	Maintenance Error	Staff Injury / Death	I	C	Maintenance		OHA-51	I	D	Maintenance Procedures		
Sys-OHA-43	SIOHA-05	Maintenance of On Board	Replace CTV Box	Vehicle brakes are not set when removing or inspecting the CTV Box.	Maintenance Error	Staff Injury / Death	I	C	Maintenance		OHA-51	I	D	Maintenance Procedures		
Sys-OHA-44	SISOHA-06	Maintenance of On Board	Replace Speed Sensor	Vehicle brakes are not set when removing or inspecting the Speed Sensor.	Maintenance Error	Staff Injury / Death	I	C	Maintenance		OHA-51	I	D	Maintenance Procedures		
Sys-OHA-45	SIOHA-07	Maintenance of On Board	Measuring the wheels for Wheel Wear Setting	Vehicle brakes are not set when measuring the wheels for Wheel Wear Setting.	Maintenance Error	Staff Injury / Death	I	C	Maintenance		OHA-51	I	D	Maintenance Procedures		
		Maintenance of On Board	Measuring the wheels for Wheel Wear Setting	Wheel measurement not within tolerance	Maintenance Error	Collision / Derailment	I	C	Operation		OHA-71					

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-46	SIOHAO-08	Maintenance of On Board	Speed Sensor Replacement	An improperly installed speed sensor (cocked or loose hardware) could vibrate in and out of its mounting hole resulting in erratic or absence of pulse detection. This may result in unexpected brake enforcements by ACSES.	Maintenance Error	Passenger Injury	II	C	Maintenance		OHA-46	II	D	Maintenance Procedures/ Wayside		
									Maintenance		OHA-70			Testing		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-47	SIOHA-13	Maintenance of On Board	Cable replacement	Vehicle brakes are not set when removing or inspecting the cables.	Vehicle brakes are not set when removing or inspecting the cables.	Staff Injury / Death	I	C	Maintenance		OHA-51	I	D	Maintenance Procedures		
Sys-OHA-48	SIOHA-14	Maintenance of On Board	Decelerometer installation or replacement	In one direction, the decelerometer will report higher than actual braking. This may result in an accident.	Maintenance error replacing decelerometer.	Collision	I	C	Maintenance		OHA-70	I	D	Maintenance Procedures		
Sys-OHA-49	SIOHA-15	Updates to Software	Updates to Software	Incorrect software revision in ACSES equipment.	Software updates not performed on spare equipment.	Unknown, errors during execution of software likely.	I	C	Maintenance		OHA-53	I	D	Maintenance Procedures/ Wayside		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-50	SIOHA-16	Installation and Configuration of On-Board or Wayside equipment	Configuration of Front End Offset, Wheel Diameter, and Train Type	Improper entry of offset distance antenna to front of vehicle, wheel diameter, or train type	Configuration update not performed on spare equipment.	Collision	I	C	Maintenance		OHA-54	I	D	Maintenance Procedures/ Wayside		
									Maintenance		OHA-79					
Sys-OHA-51	SIOHA-17	Departure Test	Railroad does not perform the departure test.	Failure to perform the departure test on the 24 hour cycle. Possible equipment failure not detected.	Equipment failure on onboard not detected.	Collision.	I	C	Operation		OHA-55	I	D	Operating Procedures		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-52	SSHA_7 SSHA_15 SSHA_16 SSHA_17	Installation and Configuration of On-Board or Wayside equipment	WIU Configuration Error	WIU Configuration error which results in WIU to send an ATCS message with a less restrictive movement authority than intended	Instruction in installation manual not followed	Train Collision, Derailment, or Serious Injury	I	C	Maintenance		OHA-46	I	D	Training/Wayside		
Sys-OHA-53	SSHA_10	Security Access	Unauthorized ACSES	Unauthorized personnel or action performed on the VIU-ACSES system	Unauthorized personnel or action performed on the VIU-ACSES system	Train Collision, Derailment, or Serious Injury	I	C			OHA-57	I	D	Railroad/Wayside		
Sys-OHA-54	SSHA_14 SSHA_18			Unit does not receive timely maintenance upon detection of failure.	Unit does not receive timely maintenance upon detection of failure.	Train Collision, Derailment, or Serious Injury	I	C	Maintenance		OHA-58	I	D	Training		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-55	SSHA_19	Maintenance of Electrical Equipment		Periodic maintenance to prevent failures is not performed.	Periodic maintenance to prevent failures is not performed.	Train Collision, Derailment, or Serious Injury	I	C	Maintenance		OHA-58	I	D	Training		
Sys-OHA-56		Adj RR Database Alignment		Train overruns a TSR due to changes in anticipation zone boundary	Adjacent Railroad updates the anticipation zone infrastructure but does not inform Railroad that updated database is required	Train Collision, Derailment, or Serious Injury	I	C	Operations		OHA-60	I	D	Railroad		
Sys-OHA-57		Maintenance of On Board	Tuning Onboard for new wheel diameter	Train fails to stop for PTS or overruns TSR	Maintainer fails to set new wheel diameter after replacement or cutting of wheel set.	Train Collision, Derailment, or Serious Injury	I	C	Maintenance		OHA-61	I	D	Railroad		
Sys-OHA-58		Onboard failure to detect transponder		Train Overspeeds after missing transponder	ACSES indicates missed transponder to the train engineer but does not display and may not be able to enforce speed restrictions.	Derailment	I	C	Operations		OHA-62	I	D	Railroad		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-59		Traversal of TSR zone	Failure to send TSR update to Train (60Min timeout or 3 BCP zone limit)	Train overspeeds through an established Temporary Speed Enforcement	ACSES indicates No TSR Data to the Train Engineer but the train Engineer does not have or does not enforce current speed Restriction	Derailment	I	C	Operations		OHA-63	I	D	Railroad		
Sys-OHA-60		Entering Mainline	Siding or Yard configured such that straight through manual switch remains in the yard / siding and turnout enters the mainline	Train exiting yard is not enforcing a PTS where the manual switch needs to be turnout to enter the mainline. Establishing this as a PTS would require an ABS to allow straight through moves.	PTS not enforced by ACSES prior to entry to Mainline	Train Collision, Derailment	I	C	Operations		OHA-64	I	D	Railroad		SDS section 5.8.1 Yard Scenario 4
Sys-OHA-61		Sidings with limited room for DS Transponder Placement	DS TP Set placed closer than Safe Braking Distance from PTS.	Trains being operated at full operating speeds prior to reading the first DS set are traveling to fast to enforce PTS in sidings / yards where space is limited.	Train Speed to fast to enforce stop in all conditions.	Train Collision, Derailment	I	C	Operations		OHA-65	I	D	Railroad		
Sys-OHA-62		Train Entering ACSES	Train leaving Amtrak territory	In presence of incorrect electronic TSR list due to transition between Amtrak STS and MNR/LIRR servers, the train operator fails to adhere to established TSR.	ACSES indicates No TSR Data to the Train Engineer but the train Engineer does not have or does not enforce current speed Restriction	Train Collision, Derailment	I	C	Operations		OHA-63	I	D	Railroad		

OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Causes	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	[redacted]	Operating Requirements ID	Residual Hazard Severity (I,II,III,IV)	Residual Hazard Prob. (A-E)	Subsystem/ Equipment	Closure References	Comments
Sys-OHA-63		Execution of Stop & Release	Train proceeding after a stop in accordance with a Stop & Release procedure	Train operator fails to follow operating procedures to ensure safe movement when executing a Stop & Release	Train Engineer Error	Train Collision, Derailment	I	C	Operations		OHA-76	I	D	Railroad		
Sys-OHA-64		East Side Access	Train proceeding passed a tunnel enforced stop	Train operator fails to follow operating procedures to ensure safe movement when proceeding passed a tunnel enforced stop	Train Engineer Error	Train Collision, Derailment	I	C	Operations		OHA-77	I	D			
Sys-OHA-65		Traversal of Interlocking authorized by Manual Bypass	Train traverses interlocking Speeds when cleared by manual bypass through an interlocking w/o WIU radio ISR and when ASC cutout.	Train operator fails to adhere to interlocking speed when cleared by manual bypass through an interlocking w/o WIU radio ISR and when ASC cutout.	Train Engineer Error	Train Collision, Derailment	I	C	Operation		OHA-78	I	D			

6 Conclusion

As a result of conducting the OHA, it has been shown that required LIRR operation and support activities involving a human interface have been effectively identified with operating requirements such that their successful execution results in risk levels which are acceptable to the LIRR customer. The specific list of identified operating requirements are captured in the table below.

Table 7: Identified Operating Requirements



Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Number: 1712

System Hazard Analysis (SHA)

CDRL 2-128-20

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Jason Weighley System Safety Engineer	Jason W Weighley	Jason W Weighley 2019.07.18 10:13:33 -04'00'
Verified:	Aaron Graham System Safety Engineer	Aaron Graham	Aaron Graham 2019.07.18 10:22:45 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.07.18 11:57:08 -04'00'
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group	Phil Magloire	Phil Magloire 2019.07.18 11:46:37 -04'00'
BT/SRA Review:	NA Title		
BT/SRA Review:	NA Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3035823

Effective Date:	Revision:	Language:
2019-07-18	_A	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
Draft1	2018-05-15	First draft for Safety Working Group Review
Draft2	2019-02-06	Updated to address comments from Working Group Review
__	2019-02-22	First Release
_A	2019-07-18	Update to address PTCSP comments

Table of Contents

Section	Subject	Page
1	**Executive Summary**	6
2	**Introduction**	6
2.1	**Compliance Matrix**	7
2.2	**Reference Documents**	10
2.3	**Glossary**	12
2.4	**Scope and Aim of the Analysis**	13
2.5	**Objective**	13
3	**ACSES II System Overview**	14
3.1	**System Level Physical Architecture**	14
3.2	**ACSES II Primary Functions**	14
3.2.1	Onboard Specific Functions	15
3.2.1.1	ACSES II Modes	15
3.2.1.2	Location Determination	15
3.2.1.3	Front of Train Offset	15
3.2.1.4	Distance Calculations	15
3.2.1.5	Wheel Wear	16
3.2.1.6	Slip/Slide Compensation	16
3.2.1.7	Rollaway Protection	16
3.2.1.8	V-Zero Determination	17
3.2.1.9	ATC Status	17
3.2.1.10	Cab Signal Failures	17
3.2.1.11	Train Types	17
3.2.1.12	Full-Service Brake Applications	17
3.2.1.13	Braking Curve Compensations	18
3.2.1.14	ACSES II Enforced Brake Assurance	18
3.2.2	Train Engineer Interfaces	18
3.2.2.1	ACSES Display	18
3.2.2.2	Acknowledge	19
3.2.2.3	No TSR Data	19
3.2.3	Departure Testing	19
3.2.3.1	Departure Test	19
3.2.3.2	Radio Transmission Departure Test	19
3.2.3.3	End of Train Departure Test	20
3.2.4	Interlocking Protection	20
3.2.4.1	PTS Enforcement	20
3.2.4.2	LoMA	20
3.2.4.3	Line Boundaries	21
3.2.4.4	PTSO	21
3.2.4.5	Absolute Stop Bypass	21
3.2.4.6	C Signal Function	22

3.2.4.7 Interlocking Exit Determination 22
3.2.4.8 ACSES II Terminate 15 MPH when Transponder Missed 22
3.2.4.9 Reduced Stale Data Timer 22
3.2.4.10 Turnback Function 23
3.2.4.11 Stopping Accurately at Stations Close to HS 23
3.2.4.12 ACSES II 8 Track Limit 23
3.2.5 Radio Communication 23
3.2.5.1 Data Radio Transmission 23
3.2.5.2 Eliminate 30 Second ISReq Cycles 24
3.2.5.3 220 MHz Data Radio 24
3.2.5.4 Redundant Base Radios 24
3.2.5.5 TDMA Radio Messaging 24
3.2.5.6 Mobile Radio Configuration 25
3.2.5.7 Continual Base Station Transmit 25
3.2.5.8 TSR Data Request 25
3.2.5.9 OBC Location to MCM 25
3.2.5.10 Report Train Distance to Home Signal 25
3.2.5.11 Data Radio Termination 26
3.2.5.12 BCP Interlocking Configurations 26
3.2.5.13 Nested Interlocking with Different Radio Channels 26
3.2.5.14 Wi-Fi and Cellular Communication 26
3.2.6 Temporary Speed Enforcement Management 26
3.2.6.1 User Input to Safety TSR Server 26
3.2.6.2 TSR Select-Check-Execute 27
3.2.6.3 TSR List Management 27
3.2.6.4 Memorize a TSR in TSR List 27
3.2.6.5 Delete A TSR from TSR List 27
3.2.6.6 Approve TSR 27
3.2.6.7 Vital TSR Scheduling 28
3.2.6.8 Output TSR List 28
3.2.6.9 Railroad Operation Forms 28
3.2.6.10 TSR Through Junctions 28
3.2.6.11 Shadowed TSR 29
3.2.6.12 Railroad Gateway Server 29
3.2.6.13 Respond To a Train Request 29
3.2.6.14 Increase OBC TSR Storage 29
3.2.6.15 Increased STS Capacity 30
3.2.6.16 Office Redundancy 30
3.2.6.17 Multi-STS Segment Control 30
3.2.7 Speed Enforcement 30
3.2.7.1 Vitally Encoded Transponder 30
3.2.7.2 Onboard Read of TP Data 30
3.2.7.3 Alert Curve 31
3.2.7.4 MAS Enforcement 31
3.2.7.5 PSR Enforcement 31
3.2.7.6 TSR Enforcement 32
3.2.7.7 “Point” TSR 32
3.2.7.8 Zero Speed TSR 32

3.2.7.9 Stop and Release TSR 33
3.2.7.10 Interlocking PSR 33
3.2.7.11 Route Dependent Speed Restriction 34
3.2.7.12 East Side Access Entry 34
3.2.8 ACSES Territory Boundaries and Non-Coded Areas 34
3.2.8.1 Yard & Siding Entry Protection 34
3.2.8.2 PTS Enforcement at ABS 35
3.2.8.3 Manual Block System Territory 35
3.2.8.4 MTEA 35
3.2.8.5 Exiting ACSES Territory 36
3.2.9 Events Diagnostics and Alarms 36
3.2.9.1 ACSES Run-time Diagnostic and Events 36
3.2.9.2 Offline Diagnostics 36
3.2.9.3 Onboard Offline Diagnostics 36
3.2.9.4 OBC Remote Diagnostics 37
3.2.9.5 ACSESView 37
3.2.9.6 SimACSES 37
3.2.10 Additional System Function 37
3.2.10.1 Configuration management 37
3.2.10.2 ACSES II System Data Maintenance 37
3.2.10.3 System Initialization 38
3.2.10.4 Security 38
3.2.10.5 ADDC and Single Sign On 38
3.2.11 Roadway Worker Protection 38
3.2.11.1 RWPS 38

4 Methodology 39

4.1 Analysis Process 39

5 System Hazard Analysis Results Table 39

5.1 System Hazard Analysis Table 40

5.2 New Hazards Introduced by SHA 41

6 Conclusion 41

7 Attachment – System Hazard Analysis Table 41

List of Tables

Table 1: Compliance Matrix 7
Table 2: Project-Specific Reference Documents 10
Table 3: External Reference Documents 12
Table 4: Terms Specific to this Document 12
Table 5: Acronyms Specific to this Document 12
Table 6: Hazard Table Column Definition / Description 40

1 Executive Summary

This document records the System Hazard Analysis (SHA) of the LIRR PTC system, as realized via ACSES II. This analysis forms the safety demonstration document for the System; its purpose is to verify safety compliance and identify hazards associated with the overall ACSES II System. The main focus of the SHA is on the faults recognized within the ACSES II System in conjunction with the identified hazards as maintained in the System Hazard Log [1].

The highest level hazards developed in the SHA are those mishaps which could result should a fault in the system occur, such as Trains Collide, Train Derails, and Personnel Injury. The functions and subsystems are as defined in the SDD documentation and hazards as originally identified in the PHA. The SHA identifies the faults and hazards in more detail than the PHA, providing information on hazard criticality that leads to the Hazard Risk Index. The SHA also specifies detailed implementation resolutions, which are expected to adequately mitigate the hazard risk.

The analysis evaluates the severity and verifies the methodology or actions in order to eliminate, minimized or control each hazard. The risk of any hazard before mitigation is defined as the Initial Risk Index. As well as recommend an approach for eliminating, controlling, or minimizing hazard identified during this analysis. In the SHA, the Final Hazard Risk Index is assigned based on the approaches for eliminating, controlling, or minimizing the identified hazards. The objective of the risk assessment is to assign a residual risk to the hazard that is both acceptable and achievable with regard to the proposed implementation. These mitigations will serve as part of the input to developing the Operation and Maintenance Procedures at the final phase of the project.

2 Introduction

This document consists of five (5) main sections:

Section 1. provides the Executive Summary of the document.

Section 2. defines the overall purpose, scope and provides general reference material for the System Hazard Analysis, including the Compliance Matrix Glossary, and References.

Section 3. provides a general overview of the ACSES II System, as analyzed in this document. (A detailed system overview for the ACSES II System may be found in Reference [4].)

Section 4. defines the analysis methodology and the Analysis Process.

Section 5. presents the results of the System Hazard Analysis in the form of a table.

Section 6 presents the conclusion derived from the analysis.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
II	12.10.3.A	SHA	A subsystem Hazard Analysis shall be documented to verify safety compliance and identify all hazards associated with each ACSEES II Subsystem. As an extension of the SHL, the main focus of the SSHA shall be the faults recognized within the ACSES II Subsystem	N/A
II	12.10.3.B		Methods or actions for eliminating, minimizing, or controlling each hazard, as well as the recommended approach for eliminating, controlling, or minimizing hazards identified during this analysis shall be documented in the SSHA including	4.1

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.3.B.1		Independent, dependent and simultaneous events or failures and system interactions that could create increased risk.	3.2
	12.10.3.B.2		Effects of reasonable human errors.	3.2
	12.10.3.B.3		Effects of system safety from functional, interoperable relationships between subsystems.	3.2
	12.10.3.B.4		Safety Design criteria has been satisfied.	3.2
	12.10.3.B.5		Analysis that implementation of safety recommendations and corrective actions will not impair or degrade safety performance of hardware or software and will not create additional hazards.	3.2

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.3.B.6		The SSHA is performed and documented to verify compliance with safety requirements and identify hazards associated with the design of subsystems. This includes hazards caused by component failure modes, critical human error inputs, and hazards resulting from functional relationships between equipment and compromising each subsystem.	3.2
	12.10.3.C		The following shall be considered the performance of a SSHA	3.2
	12.10.3.C.1		Modes of failure including reasonable human errors, signal point and common modes failures, and the effects of failures on subsystem elements.	3.2

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.3.C.2		Potential contribution of hardware and software controlled events, faults and occurrences.	3.2below
	12.10.3.C.3		Satisfaction of all safety design criteria.	3.2
	12.10.3.C.4		Integrating all safety design criteria.	3.2
	12.10.3.C.5		Integrating safety testing into hardware and software testing programs.	3.2
	12.10.3.C.6		Input information from other subsystems that is required to perform the functions of this ACSES II subsystem in a safe manner.	3.2

2.2 Reference Documents

Table 2: Project-Specific Reference Documents

Reference Number	Document Name	Identification Number
[1]	Project Hazard Log (PHL), CDRL 2-126-20	3035819
[2]	Preliminary Hazard Analysis (PHA), CDRL 2-127-03	3036420
[3]	Dictionary of Terms and Acronyms	3035624

Reference Number	Document Name	Identification Number
[4]	System Description Document (SDD), CDRL 2-27	3035724
[5]	System Product Safety Plan, CDRL 2-123-20	3035815
[6]	Onboard System Safety Concept Descriptions, CDRL 2-124 -01	3036406
[7]	Office System Safety Concept Descriptions, CDRL 2-124-02	3036410
[8]	Comms System Safety Concept Descriptions, CDRL 2-124-03	3036421
[9]	WIU System Safety Concept Descriptions, CDRL 2-124-04	3035817
[10]	Transponder Safety Concept Descriptions, CDRL 2-124-05	3036414
[11]	RWPS System Safety Concept Descriptions CDRL 2-124-06	3036413
[12]	System Interface Hazard Analysis (IHA), CDRL 2-131-20	3035828
[13]	System Fault Tree Analysis, CDRL 2-132	3035830
[14]	System Vulnerability Analysis CDRL 2-137	3035840
[15]	System OHA CDRL 2-130-23	3035826
[16]	System Level Requirements	3052527
[17]	Deleted	
[18]	System SHA Log – Filtered View of Project Hazard Log – Baseline 8.0JW1	NA
[19]	LIRR System Architecture Drawing Package	3038055
[20]	System Verification and Validation Plan	3035711

Table 3: External Reference Documents

Reference Number	Document Name
[21]	MIL-STD 882C, System Safety Program Requirements, 19 January 1993 with Notice 1, 19 January 1996.
[22]	IEEE Standard 1483-2000, “Standard for the Verification of Vital Functions in Processor-based Systems Used in Rail Transit Control.”
[23]	American Railway Engineering and Maintenance of Way Association (AREMA), Manual of Recommended Practices for Signals, current edition.
[24]	49 CFR 229, 231, 232, 236, Federal Railroad Administration, Rules, Standards, and Instructions for Railroad Systems.

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms [3]. Terms and acronyms only related to this document are listed below in Table 4 and Table 5.

Table 4: Terms Specific to this Document

Term	Definition
Preliminary Hazard Analysis (PHA)	An analysis performed on the potential hazards identified in the PHL, to provide an initial risk assessment of the hazards, and to identify requisite controls and follow-on actions.
System Hazard Analysis (SHA)	A (typically) To-Down analysis performed on the system, to both identify the hazards at a system level, and show that mitigation of them results in an acceptable Hazard Risk Index.
Project Hazard Log (PHL)	Also known as System Hazard Log (SHL) is the record of the system level hazards associated with the development and implementation of the ACSES II system for LIRR.

Table 5: Acronyms Specific to this Document

Acronym	Definition
PHA	Preliminary Hazard Analysis
HL	Project Hazard Log
SSHA	Subsystem Hazard Analysis

Acronym	Definition
SHA	System Hazard Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FFT	Functional Fault Tree
FTA	Fault Tree Analysis
HA	Hazard Analysis

2.4 Scope and Aim of the Analysis

The scope of this document is to define the functional-level safety hazards that impact or could be caused by a fault of the overall ACSES control system. The analysis is limited to ACSES II functionality and does not include other potential hazards that exist in the operating or maintenance processes or to operation external to the railroad system. The hazards associated with operating rules and procedures that were identified in the PHA are further analyzed in the Operational Hazard Analysis (OHA) [15] and then transferred to the Hazard Log [1] for tracking.

This SHA is undertaken in order to verify overall system compliance with safety requirements contained in both the system-level and subsystem-level specifications and prior hazard analysis which is related to the design and operation of the ACSES II System as the realization of the LIRR PTC system. The SHA shall also identify other hazards not previously identified from component failure modes, critical human error inputs, and from functional relationships between components and equipment. These hazards could come from any of the various subsystem analyses.

The document presents a hazard analysis for the ACSES II System. The starting point is the definition of all safety critical services for the various subsystems, including the Comms Subsystem; the Onboard subsystem, the Wayside subsystem, the Transponder subsystem, the Office subsystem, and the RWPS subsystem.

2.5 Objective

The following issues are considered during the performance of the SHA:

- Modes of failure including reasonable human errors, single point and common mode failures, and the effects of failure on subsystem elements.
- Potential contribution of hardware and software controlled events, faults and occurrences
- Satisfaction of all safety design criteria.
- Integrating safety testing into hardware and software testing programs.
- System level hazards attributed to subsystems are controlled.

- Input information from all subsystems that is required to perform the PTC functionality of the ACSES II System in a safe manner.

3 ACSES II System Overview

ACSES II is an overlay to the ASC System; ACSES II provides speed and stop enforcement utilizing Office, Wayside (which includes the Transponders and WIU), Onboard (which includes the Interface to the Train) and RWPS subsystems. ACSES II enforces positive stop at signals and enforces permanent and temporary speed restrictions. ACSES uses data obtained from passive track-mounted transponders and a data radio to impose permanent and temporary speed limits. The Onboard Subsystem responds to data acquired from transponders and through the data radios. The Onboard System calculates a speed profile for both warning and enforcement from the track profile and vehicle performance characteristics. The ACSES II System is fully described in CDRL 2-27, System Description Document (SDD) [4].

3.1 System Level Physical Architecture

The physical System Architecture is comprised by multiple levels providing details of the physical components and connections.

Five System Architecture levels have been defined with L0 as the highest level possible and L4 as the most detailed level. As L4 and part of L3 are meant to provide the information equivalent to the existing Book of Plans, these levels are generated and updated following the existing process for Book of Plans. A specific physical System Architecture is available for each of the Railroads.

The System Architecture Description [19] document (provide a comprehensive description of the different layers of the System Architecture for the Railroad. This document provides a summary description of each of the major components shown in the System Architecture drawings.

Four subsystems have been defined in the L0 and L1 System Architecture:

- **Office Subsystem** – Comprising the Office Servers, the Office LAN and the SDMF on both the Primary and the Backup control centers.
- **Wayside Subsystem** – Comprising the WIU, Wayside Network, RF equipment and Transponders.
- **Onboard Subsystem** – Including the OBC, Communications equipment and interface with the Train.
- **Roadway Worker Protection Subsystem** (RWPS) – Formed by the Office RWPS, Office RWPS LAN, Wayside communications equipment and EIC terminals.

3.2 ACSES II Primary Functions

This section provides a high level introduction to the primary functions provided with the ACSES II system. The System Design Description [4] was analyzed and the failures of each of the functions was reviewed. For each failure identified an entry was made into the SHA table and tracked through the hazard log.

3.2.1 Onboard Specific Functions

3.2.1.1 ACSES II Modes

ACSES II operation is defined by modes and conditions, being that these modes are the rules governing the operation of the system. There are three main "cut-in" operating modes:

- ACSES Territory Mode (OBC Mode 1)
- Non-ACSES Territory Mode (OBC Mode 2)
- ACSES Installation Territory Mode (OBC Mode 3)

Failure Modes:

ACSES stays in Installation Territory Mode after missing exit Installation Territory Message. SHA 250.

ACSES stays in ACSES after missing Entry to Installation Territory. SHA 250.

System stays in ACSES Territory mode after missing Exit Transponder SHA 250

System stays in Non-ACSES Territory Mode after missing Transponder SHA 250

OBC Reboot SHA 233

3.2.1.2 Location Determination

To implement the ACSES II functions, the Onboard Subsystem requires Train Location, Train Speed, and Train Direction of Travel. The Onboard Subsystem combines the information acquired from the Transponders with data received from its speed sensor. The ACSES II Onboard Subsystem calculates the current location of a train by tracking the distance traveled since the last transponder set was read.

Failures Modes:

Missed Transponder – Position Error to increase for PTS, TSR applications SHA 250

3.2.1.3 Front of Train Offset

The offset of the transponder scanner compensates for the distance between the transponder scanner and the absolute front of the train (i.e. coupler face). The offset is given for both directions of the train and taken into account by the OBC depending upon the direction of travel.

Failure Modes Considered:

Corruption of Front Offset Parameter SHA-258

3.2.1.4 Distance Calculations

The OBC measures the train’s distance travelled using a speed sensor. The distance travelled is proportional to the number of pulses received from the sensor within a sample time, the wheel diameter and the number of gear teeth for the axle mounted sensors.

Failure Modes Considered:

Wheel Diameter Parameter not correct SHA-259

Speed Sensor Failure SHA-260

Slip / Slide Compensation SHA 260

3.2.1.5 Wheel Wear

The allowable wheel diameter for each vehicle is defined within the Onboard Subsystem Description Document. This allowable wheel diameter is verified when wheel diameters are entered by the maintenance personnel to determine that the wheel diameter is within tolerance. For each vehicle type, the wheel diameter is bounded by the selected vehicle type within the ACSESview, meaning the maintainer can only enter values within the bounded range.

Failure Modes Considered:

Wheel Diameter Parameter not correct. SHA - 259

Transponder Data Errors SHA-261

Speed Sensor Failures SHA-260

3.2.1.6 Slip/Slide Compensation

The onboard provides for compensation of wheel slip and wheel slide conditions that impact the distance error accumulation.

The changes to the slip/slide compensation (from the type approved OBC) are related to the usage of decelerometers to determine the Slip/Slide situation. Based on a detected change in acceleration or deceleration from the speed sensor, a slip or slide condition is declared within the OBC. The decelerometer is then used to adjust for anticipated vehicle speed (and distance traveled) until the slip or slide condition is removed.

Failure Modes Considered:

Decelerometer Failure SHA 262

Speed Sensor Failure SHA-260

3.2.1.7 Rollaway Protection

The purpose of rollaway protection is to stop a train that rolls in either direction when no train movement is expected (Reverser is in neutral). When the reverser input is neutral, the cab is keyed (or active) and the OBC detects movement above V-zero, an immediate full-service brake application is commanded by the OBC and an audible alarm is generated

Failure Modes Considered:

Reverser Input Failure SHA-264

Speed Sensor Failure SHA-260

Train Movement Opposite Reverser Direction SHA -263

3.2.1.8 V-Zero Determination

The OBC determines that a train has achieved V-zero when it detects the speed below 0.5 MPH. There is not a specific amount of time (other than the sampling time of the speed sensing device) to determine the train has achieved V-zero.

Failure Modes Considered:

Speed Sensor Failure SHA-260

Decelerometer Failure SHA-262

SW Failures - VZero SHA-265

Speed intentionally kept below 0.5 MPH SHA-265

3.2.1.9 ATC Status

The ATC is responsible for enforcing the Train Stop in normal conditions (both ATC and ACSES II OBC active and healthy). When the ATC is healthy, the Stop aspect/indication information is displayed on the ADU. The ATC (or the AIU for non-Siemens ATC equipment) provides control of braking for PTS enforcement when the cab signal is Restricted (“0” cab code).

The ACSES II onboard directly controls the braking for PTS in systems when the ATC is indicating Cut-out. The ACSES II determines the status of the ATC from the Vital ATC Cut-out indication received from the ATC.

Failure Modes Considered:

ATC Status Failure SHA-266

3.2.1.10 Cab Signal Failures

The ACSES II monitors the status of the ATC/Cab Signal system

Failure Modes Considered:

ATC Status Failure SHA-266

3.2.1.11 Train Types

ACSES allows each train to be configured to match one of five programmed types (A to E). This configuration defines the braking rate to be used, the train type is also used by the system to determine if the train is a passenger or freight unit for application of speed enforcements (PSR and TSR). The train type is typically configured on each OBC. Some units allow the train type to be selected by the train engineer (MNR only).

Failure Modes Considered:

Train Type Parameter set incorrectly SHA-259

3.2.1.12 Full-Service Brake Applications

The Full-service brake is applied whenever the braking curve limits are exceeded for the worst case braking curve being monitored at the time.

Failure Modes Considered:

Brake Interface Failure SHA-07

3.2.1.13 Braking Curve Compensations

Calculation of stopping distances based on grade and speed to the speed reduction or stopping location. The grade utilized for the calculation is determined by recursive calculations to determine the worst case grade over the entire stopping distance.

Failure Modes Considered:

Incorrect Grade – SHA-230

Incorrect Speeds – SHA-11

Incorrect Civil Data SHA-10

3.2.1.14 ACSES II Enforced Brake Assurance

ACSES II OBC provides for a grade compensated vital brake assurance of the full service brake application. Brake assurance is implemented on all LIRR passenger train types utilizing a time-based monitoring of the brake application from the moment when the ACSES brake curve is reached or exceeded.

Failure Modes Considered:

Speed Sensor Failures SHA-260

Incorrect Grade data SHA-230

3.2.2 Train Engineer Interfaces

3.2.2.1 ACSES Display

ACSES will display the following data to the Train engineer Civil Speed enforcement, Cab signal aspect, ACSES Operational status, ATC Operational status, Brake Assurance (LIRR only)

Failures Modes Considered:

Incorrect display of Civil Speed enforcement SHA-268

Incorrect display of Cab Aspect SHA-15

Incorrect ACSES Operational Status Display SHA-20

Incorrect ATC Operational Status Display SHA-266

Incorrect Brake Assurance Status displayed. SHA-270

ATC Failure – SHA-269

ACSES Failure – SHA-270

3.2.2.2 Acknowledge

Indication to ACSES that train engineer has accepted the alert or enforcement being provided and therefore the event can be cleared. Events requiring Ack are downward change in track speed, missed transponder set, reading a transponder early, reading a partial transponder set, entering installation territory, entering MBS territory, exiting ACSES, expiry of a valid TSR list.

Failure considered:

Ack accepted from failed input SHA-271

Failure to activate the acknowledge after above event SHA-272, SHA-273

3.2.2.3 No TSR Data

Indication that the system is not currently enforcing TSR data because a valid list for the current direction of travel has not been received.

Failure Modes Considered:

Changes in direction SHA-27

Timeout of current list SHA-273

Train travelled past 3 interlockings since last list received. SHA-273

RR Line boundary SHA-238, SHA-196

3.2.3 Departure Testing

3.2.3.1 Departure Test

Test of onboard equipment performed outside of ACSES enforcement and enforced to be repeated every 24 hours. This test locks the status of the train type selector switch and changes the train type to the current selected train type if equipped. (MNR Only)

Failure Modes Considered:

No Departure test performed SHA-275

Departure test failure SHA-276

Train Type Selector Switch SHA-25, SHA-26

3.2.3.2 Radio Transmission Departure Test

Test on onboard radio equipment performed prior to start of service. This test includes a ping test and over the air test. The ping test is included I the departure test results but the over the air results are only logged.

Failures:

Radio Health Status Failure SHA-273

Radio RF Status Failure SHA-273

3.2.3.3 End of Train Departure Test

Departure test may be repeated on the non lead units while in a larger consist.

No additional analysis needed as this is the same functionally as departure test.

3.2.4 Interlocking Protection

3.2.4.1 PTS Enforcement

PTS enforcement function is applied to stop in approach to all signals displaying a Stop aspect with ACSES territory. Additionally, for non-interlocking intermediate signals at Stop and Proceed within ABS territory, where ASC is not installed, an ACSES PTS is enforced.

Function Failures:

Incorrect Grade SHA-230

Incorrect Brake Rate SHA-277

Incorrect Signal Status SHA-55

WIU Message corrupt SHA-279

WIU Message not received / Radio Failure SHA-58

Train Location Not correct. SHA-280

Incorrect civil location. SHA-10

Train following train receives ISRReq on clear route. SHA-58

Train on opposing route fails to stop. SHA-59

DS Transponder Missed SHA-250

PDS Transponder Missed SHA-250

3.2.4.2 LoMA

An ISResponse with LoMA information is sent to the Onboard ACSES II Subsystem when the train approaches two or more interlockings located less than safe braking distance to each other (nested interlockings).

Failure Modes Considered:

Incorrect Grade SHA-230

Incorrect Brake Rate SHA-277

Incorrect Signal Status SHA-55

WIU Message corrupt SHA-279

WIU Message not received / Radio Failure SHA-58

Train Location Not correct. SHA-280

Incorrect civil location. SHA-10

Train following train receives ISRReq on clear route. SHA-58

Train on opposing route fails to stop. SHA-59

DS Transponder Missed SHA-250

PDS Transponder Missed SHA-250

Nested DS transponder packages SHA-278

OBC Polls the wrong WIU for the wrong signal SHA-256

3.2.4.3 Line Boundaries

Changes within the current railroad line ID or line boundary between railroads. The line boundary may occur within a nested interlocking or non nested interlocking. This function describes the rules for application of the WIU, Transponder and Office at these different boundaries.

Failure Modes Considered:

Transponder Configuration SHA-53

WIU Configuration SHA-49

TSR Enforced on Adj RR but not owning RR. (ACSES boundary may not cover physical boundary) SHA-197

Network Failures SHA-281

3.2.4.4 PTSO

Override of PTS based on permissive signal from the interlocking or reception of a cab signal aspect more permissive than Restricted via the ATC.

Failure Modes Considered:

Failure of WIU Interlocking Status SHA-58

Stale interlocking status SHA-279

Failure of ATC SHA-55

Interlocking status sent to wrong train (Train trailing train approaching signal. SHA-58

3.2.4.5 Absolute Stop Bypass

A pushbutton installed in the train that allows the train engineer to resume operation after the enforcement of a PTS.

Failure Modes Considered:

Failure of ASB pushbutton SHA-271

Train not stopped near signal SHA-280

3.2.4.6 C Signal Function

The C Signal indicates to the train engineer that the train has authority to proceed to the next signal (the block is Clear). Within the LIRR system, there is no indication on the ADU for a C Signal, the train engineer is responsible to see the C Signal indication on the wayside and interpret this correctly.

Failure Modes Considered:

WIU Failure SHA-58

C Signal Territory Defined Correctly SHA-49

C Signal Status failure SHA-55

Train outside C Signal Territory SHA-269

ATC Failure SHA-55

3.2.4.7 Interlocking Exit Determination

HS transponder sets, which are placed just prior to the interlocking entrance signal, are always programmed with inexact linkage in the direction of the interlocking entrance.

Additionally, for LIRR, transponder sets are loaded with inexact linking for intermediate signals within ABS territory without cab signaling.

Failure Modes Considered:

Missed Transponder SHA-250

Interlockings less than 750’ apart (limitation in Exact linking distance targets) SHA-261

3.2.4.8 ACSES II Terminate 15 MPH when Transponder Missed

This change allows the OBC to release the 15 mph restriction when either the next exact linking transponder set is received OR a distance equivalent to the railroads longest interlocking distance is travelled.

Failure Modes Considered:

Missed Transponder SHA-250

ASB/CMB Territory (LIRR Only) 15 MPH enforced until next Interlocking SHA-227

3.2.4.9 Reduced Stale Data Timer

Reduce Stale Data timer from 120 seconds to 42 seconds.

Failure Modes Considered:

Train Following another train . SHA-58

Interoperability – tenant trains must enforce 42 Second timer SHA-231

3.2.4.10 Turnback Function

This function enables the OBC in controlling cab from the trailing condition to establish communication with an opposing HS signal following a turnback move without having to pass over a DS transponder set.

Failure Modes Considered:

Missed Transponder SHA-250

Turnback train doesn't clear Interlocking exit SHA-47

3.2.4.11 Stopping Accurately at Stations Close to HS

In situations where a train must close-up to a signal near a station, within a siding, or otherwise as operationally necessary, there may arise a problem with the train's ability to berth fully at the respective location. In these scenarios, the transponder layout is designed to reduce the error accumulation since the last DS transponder set and as needed additional transponder sets with an accurate stop transponder package are placed to allow the train to pass the first home signal within an HS transponder set.

Failure Modes Considered:

Interoperable train incorrectly process Accurate Stop Package (Reads Yards not Feet) SHA-246

Missed Transponder SHA-250

3.2.4.12 ACSES II 8 Track Limit

ACSES transponder and WIU messages limit the number of tracks to eight. The LIRR design utilizes these same messages but he system application has been modified to spit physical lines into virtual lines with line boundaries to accommodate areas with more than eight tracks.

Failure Modes Considered:

Line boundary change not occurring in an interlocking SHA-243

ACSES configuration between subsystems doesn't match SHA-11, SHA-13, SHA-73, SHA-49

Translation of TSR errors SHA-73,

3.2.5 Radio Communication

3.2.5.1 Data Radio Transmission

Data Radio transmission is initiated by the onboard following reception of a complete PDS or DS transponder set. The transponder PDS or DS transponder package provides the onboard with the signal address for the approaching HS signal. The Onboard sends a request for the interlocking status to the associated signal in the transponder; this prompts the mobile communications manager to initiate data radio transmissions. Alternatively, the reception of a TSR request package (outside of the PDS and DS transponder sets) prompts the onboard to send a TSR request to the mobile communications manager to initiate data radio transmission.

Failure Modes Considered:

Missed Transponder SHA-250

Loss of WIU Data SHA-58

Loss of TSR Data SHA-284

3.2.5.2 Eliminate 30 Second ISReq Cycles

The OBC was changed to perform the ISReq every 6 seconds regardless of train movement as long as the train is in approach to a home signal and the PDS/DS transponder information has been received.

Failure Modes Considered

Loss of WIU Data SHA-58

Loss of TSR Data SHA-284

3.2.5.3 220 MHz Data Radio

The ACSES II 220 MHz Data radio, 216.750 MHz to 222 MHz frequency band, is used as the primary radio for ACSES II train to wayside communications.

Failure Modes Considered

Loss of WIU Data SHA-58

Loss of TSR Data SHA-284

3.2.5.4 Redundant Base Radios

Each Data Radio within the base stations is implemented as a redundant pair controlled from a single BCM. Switching between active radios within a radio case is done by either automatic fail-over, commanded switchover from the NMS, or commanded switch-over using a local login at the radio case

Failure Modes Considered

Loss of WIU Data SHA-58

Loss of TSR Data SHA-284

3.2.5.5 TDMA Radio Messaging

The PTC Data Radio utilizes a Time Division Multiplexed Access (TDMA radio messaging scheme to manage the radio traffic of the system). The time slot management is handled through the Base Communication Manager (BCM) to provide time slots for up to 18 trains on the same BCM within a 6-second time window, known as an epoch.

Failure Modes Considered

Loss of WIU Data SHA-58

Loss of TSR Data SHA-284

3.2.5.6 Mobile Radio Configuration

The train utilizes an onboard lookup table to configure the radio to the appropriate frequency and power level. The identification of the Home Signal is used by the MCM to determine the radio channel required

Failure Modes Considered

Loss of WIU Data SHA-58

Loss of TSR Data SHA-284

3.2.5.7 Continual Base Station Transmit

The BCP continuously transmits a beacon once per second for trains entering the radio range. Radios are continuously transmitting at top of each second for synchronizing with the MCM.

Failure Modes Considered

Loss of WIU Data SHA-58

Loss of TSR Data SHA-284

3.2.5.8 TSR Data Request

This function was modified to allow for continuous communication on LIRR. Continuous communication is required for LIRR in order to protect for the grade crossings that occur between interlocking locations. Usage of the TSR Data Request package keeps the TSR list updated in between interlocking locations to further mitigate stale data.

Failure Modes Considered:

Loss of TSR Data SHA-284

3.2.5.9 OBC Location to MCM

The OBC provides the MCM with the ATCS address as determined from the transponder or a LoMA in order to allow the MCM to initiate communication to the appropriate radio channel and power level

Failure Modes Considered:

Loss of WIU Data SHA-58

Loss of TSR Data SHA-284

3.2.5.10 Report Train Distance to Home Signal

The MCM receives the distance to the PTS target from the OBC on a periodic basis (500 ms). This information is passed to the wayside communication manager (Base Radio Communication Manager (BCM)) in order to allow prioritization of time slots when more than one train in approach of the same signal is requesting information. The BCM utilizes the distance to the PTS target in order to only allocate TDMA time-slots to the closest two trains per approach track

Failure Modes Considered

Loss of WIU Data SHA-58

3.2.5.11 Data Radio Termination

Conditions to determine when the OBC can release time slot and allow other trains to poll.

Failure Modes Considered:

Loss of WIU Data SHA-58

Loss of TSR Data SHA-284

3.2.5.12 BCP Interlocking Configurations

Three high level configurations of BCP application that allow proper RF coverage to be provided with the capacity needed for that specific location. (Allows for more than one radio and radios on different frequencies at the same location)

Failure Modes Considered:

Loss of WIU Data SHA-58

Loss of TSR Data SHA-284

3.2.5.13 Nested Interlocking with Different Radio Channels

ACSES II provides the ability for trains to maintain their LoMA through nested interlockings regardless of changing radio channels.

Failure Modes Considered:

Loss of WIU Data SHA-58

3.2.5.14 Wi-Fi and Cellular Communication

Wi-Fi and cellular communication paths are provided as an alternate means of communication in the event that 220MHz spectrum is unavailable.

Failure Modes Considered:

Loss of WIU Data SHA-58

Loss of TSR Data SHA-284

3.2.6 Temporary Speed Enforcement Management

3.2.6.1 User Input to Safety TSR Server

Authorized users of the UIS Workstations provide input to the STS through the UIS Server for activation and deletion of TSRs

Failure Modes Considered:

Incorrect Data Entered SHA-285

UIS Modification of TSR Request SHA-284

Database mismatch between UIS and STS

TSR Count Exceeded SHA-237

BCP TSR Count Exceeded SHA-237

TSR near RR Boundary SHA-243

3.2.6.2 TSR Select-Check-Execute

Path of verification of TSR Request through UIS/STS. Both STS and UIS perform data checks of the TSR and the supervisor is to verify correct data prior to the TSR being enforced or removed.

Failure Modes Considered:

Incorrect Data Entered SHA-285

UIS Modification of TSR Request SHA-284

Database mismatch between UIS and STS SHA-28

3.2.6.3 TSR List Management

The TSRs on the Safety TSR Server are maintained in a single list within a Runtime Database. The ACSES II system manages TSRs within the system through a set of states. The state of the TSR changes as it progresses through various stages of entry, approval, execution and deletion.

Failure Modes Considered:

To many TSRs SHA-237

3.2.6.4 Memorize a TSR in TSR List

UIS and STS processing of TSR Add requests.

Failure Modes Considered:

To many TSRs SHA-237

Incorrect TSR Request SHA-285

Out of order messages

3.2.6.5 Delete A TSR from TSR List

UIS and STS processing of TSR Removal requests

Failure Modes Considered:

Incorrect TSR Request SHA-285

Out of order messages

3.2.6.6 Approve TSR

The Supervisor (Chief RTC/Dispatcher) or any other authorized user has the ability to approve TSRs that have gone through the Select and Check process between UISS and STS

Failure Modes Considered:

Incorrect TSR Request SHA-285

UIS Failures SHA-284

Out of order messages

3.2.6.7 Vital TSR Scheduling

Schedule a TSR for future activation or deactivation at a set time.

Failure Modes Considered:

TSR Removed automatically. Restricted by FRA comment to notification to dispatcher to remove. SHA-219

STS incorrect time. SHA-284

Incorrect UIS timers. SHA-284

3.2.6.8 Output TSR List

UIS and STS List management and display to dispatchers.

Failure Modes Considered:

UIS Failure SHA-284

Corrupted messages.

Adjacent RR STS Failures. SHA-196

3.2.6.9 Railroad Operation Forms

The UIS provides for entry and management of Railroad Operation forms. Forms include the Form L, Speed Restriction Notice (SRN), General Notice (GN) on LIRR.

Failure Modes Considered:

UIS Failures SHA-284

3.2.6.10 TSR Through Junctions

ACSES II provides the TSR list for current, next two BCP zones and overlapping zone on the fourth BCP zone for all possible routes through junction points.

Failure Modes Considered:

Loss of TSR Communication SHA-284

Line Boundary SHA-243

STS Database Errors SHA-287, SHA-73

3.2.6.11 Shadowed TSR

Where a TSR falls near a boundary between two lines, it is necessary to shadow TSRs of the other line onto the current line for the approaching train. The shadowing of a TSR is creating another TSR for the train that represents a “duplicate” of the TSR information but within the current lines chaining. The train receives both the actual TSR and the Shadow TSR for the approaching line as part of its TSR list from the STS.

Failure Modes Considered:

Loss of TSR Communication SHA-284

Line Boundary SHA-243

Adj STS Failures SHA-196

STS Database Errors SHA-287, SHA-73

3.2.6.12 Railroad Gateway Server

The ACSES II Railroad Gateway Server (RGS) is used to provide communication between the outside world and the ACSES II Office subsystem.

Failure Modes Considered:

Adj STS Failures SHA-281

STS Database Errors SHA-287, SHA-73

3.2.6.13 Respond To a Train Request

The Onboard subsystem sends a TSR request to the STS whenever it receives a TSR Data Request, PDS, or DS transponder message. The request continues every 30 seconds until the conditions for the request expire. Within the TSR request, the Onboard includes its current train ID, BCP ID, direction of travel, and current TSR list ID.

Failure Modes Considered:

Loss of TSR Communication (OBC to STS) SHA-284

TSR List sent to Tenant Train (Tenant Train ID may be the same as host) SHA-251

Missed Transponder SHA-250

3.2.6.14 Increase OBC TSR Storage

The OBC TSR storage capacity handles up to 80 TSRs (Sum of Actual and Shadowed TSRs not to exceed a count of 80) in the direction of travel.

Failure Modes Considered:

Loss of TSR Communication (OBC to STS) SHA-284

TSR List exceeds Max SHA-237

Tennant Trains have lower Max SHA-237

Adj RR Adds TSRs SHA-281

3.2.6.15 Increased STS Capacity

The STS database is designed to store up to 1500 TSRs in total to support the Railroads operational need for TSR capacity.

Failure Modes Considered:

Loss of TSR Communication (OBC to STS) SHA-284

TSR List exceeds Max SHA-237

Adj RR Adds TSRs SHA-281

3.2.6.16 Office Redundancy

The ACSES II STS is provided as a hot-standby server within a control center as well as hot-standby between control centers. The STS is also designed to monitor the health of the RGS, UIS, DMS, NMS, and WCC in order to switch those over should there be a catastrophic failure within one of those paired units or the entire control center.

Failure Modes Considered:

Network Failure prevents PCC/BCC communication (Split Brain) SHA-249

Cold Start SHA-273

3.2.6.17 Multi-STS Segment Control

Not Applicable.

3.2.7 Speed Enforcement

3.2.7.1 Vitally Encoded Transponder

The ACSES II Type approve transponders are strategically placed passive devices with vitally encoded data for MAS, PSR, vehicle to wayside communication and location information

Failure Modes Considered:

Transponder Programmed with Incorrect Data

Transponder Missed SHA-250

Transponder Data Corrupted SHA-11

Transponder Installed on Incorrect Line

3.2.7.2 Onboard Read of TP Data

The OBC transponder scanner energizes the transponder (transmitting a radio frequency of 27 MHz) as it passes over them at speed up to 160 MPH. The OBC transponder scanner receives the transponder message (receiving a radio frequency of 4.5 MHz). Once the transponder message is received, the read data is passed to the OBC for processing.

Failure Modes Considered:

Transponder Data Corrupted SHA-11

Transponder Installed on Incorrect Line SHA 280

Onboard Failure SHA-75

3.2.7.3 Alert Curve

The ACSES II alert curve varies in application depending on whether the Onboard is within a profile to a reduced speed target or the onboard is not currently profiling to a reduced speed. The alert curve is nominally an 8-second time offset from the penalty brake curve when profiling to a reduced speed target (including profiles to a stop or PTS target).

Failure Modes Considered:

Transponder Programmed with Incorrect Data SHA-283

Transponder Data Corrupted SHA-11

Transponder Installed on Incorrect Line SHA 280

Grade Error SHA-74

Onboard Failure SHA-75

3.2.7.4 MAS Enforcement

The MAS for the trains are stored within all transponder sets as a line speed package. The MAS information is included for all five train types within each of the transponder sets for both directions of travel

Failure Modes Considered:

Transponder Programmed with Incorrect Data SHA-283

Transponder Missed SHA-250

Transponder Data Corrupted SHA-283

Transponder Installed on Incorrect Line SHA 280

Onboard Failure SHA-75

Direction Changes SHA-27

3.2.7.5 PSR Enforcement

Permanent Speed Restriction Enforcement is a fundamental function of the ACSES II System to provide protection of permanent civil limitations of the track (including but not limited to curves and bridges). This function utilizes PSR information received from the transponders on the wayside to allow the OBC to enforce overspeed protection to this speed restriction value (if it is the most restrictive speed restriction active in the location) for the specific train type(s).

Failure Modes Considered:

Transponder Programmed with Incorrect Data SHA-283

Transponder Missed SHA-250

Transponder Data Corrupted SHA-283

Transponder Installed on Incorrect Line SHA 280

Onboard Failure SHA-75

Direction Changes SHA-27

3.2.7.6 TSR Enforcement

Temporary Speed Restrictions are placed by the Dispatcher/RTC within the Office to protect trains from various scenarios.

Failure Modes Considered:

Onboard Failure

UIS Failure SHA-284

TSR Request Error SHA-285

Train to Office communication failure SHA-273

TSR List Corrupt SHA-29

TSR List Invalid SHA-286, SHA-271

3.2.7.7 "Point" TSR

When a zero distance (10 yards) TSR, or "point" TSR, is received by the OBC, the train slows down in advance to the TSR starting location. Once the train reaches the starting location of the "point" TSR, the train is then released to the next highest permitted speed. There is no acknowledgement of this point TSR.

Failure Modes Considered:

Onboard Failure SHA-75

UIS Failure SHA-284

TSR Request Error SHA-285

Train to Office communication failure SHA-273

TSR List Corrupt SHA-29

TSR List Invalid SHA-286, SHA-271

3.2.7.8 Zero Speed TSR

When zero speed TSR is placed in the system, the OBC enforces the train (if applicable to the train type) to a stop before the TSR start location and does not release the train until a new TSR list is received in which the TSR is no longer present.

Failure Modes Considered:

Onboard Failure SHA-75

UIS Failure SHA-284

TSR Request Error SHA-285

Train to Office communication failure SHA-273

TSR List Corrupt SHA-29

TSR List Invalid SHA-286, SHA-271

Vital Zero Speed Error SHA-265

3.2.7.9 Stop and Release TSR

The Stop & Release (SAR) TSR is used to protect an area where the train is required to come to a stop prior to a specific location on the track. Once stopped, the train engineer is required to follow operational procedures (for example, contacting a roadway worker in charge, or sounding a warning horn at a crossing) then press the acknowledge button. Once the stop conditions for the stop and release have been satisfied (acknowledge button received), the train can proceed through the area at a speed defined within the Stop and Release TSR, or at line speed if no speed restriction was provided.

Failure Modes Considered:

Onboard Failure SHA-75

UIS Failure SHA-284

TSR Request Error SHA-285

Train to Office communication failure SHA-273

TSR List Corrupt SHA-29

TSR List Invalid SHA-286, SHA-271

Ack Failure SHA-271

3.2.7.10 Interlocking PSR

The Interlocking Permanent Speed Restriction (I-PSR) represents the lowest speed permitted along a route set for the train through the limits of the interlocking. The I-PSR changes depending on the route aligned through the interlocking (based on switch speeds and PSR within the route).

Failure Modes Considered:

Onboard Failure SHA-75

WIU Failure SHA-47

Train to Wayside communication failure SHA-58

ISR Response Incorrect – SHA-49

Incorrect Interlocking Speed in WIU Database SHA-278

ISRResponse from Wrong WIU – SHA-279

ATC Clears PTS SHA-55

3.2.7.11 Route Dependent Speed Restriction

Route Dependent Speed Restrictions are used when a specific Train Type requires a civil speed restriction on a particular track at the exit of the Interlocking.

Failure Modes Considered:

Onboard Failure SHA-75

Missed Transponder – RDSR held until OBC declares TP missed then Engineer responsible for speed enforcement SHA-241

ISR Response Incorrect SHA-226

Incorrect Interlocking Speed in WIU Database SHA-226

ATC Clears PTS SHA-55, SHA-241

3.2.7.12 East Side Access Entry

Due to size constraints of the East Side Access (ESA) Tunnels, it is necessary for ACSES to limit the movement of certain trains through the tunnels. ACSES provides a Transponder package identifying an exit track as a low clearance tunnel track with an ACSES track ID. Trains that can be routed into the low clearance tunnel tracks are configured by the OBC as tunnel enabled. Trains that cannot be routed into the low clearance tunnel tracks are configured by the OBC as NOT tunnel enabled.

Transponders configured with the Tunnel Package are placed at safe braking distance from the tunnel tracks and repeated in each transponder set in approach to the tunnel entrance. A minimum of two transponder sets with the Tunnel Package are required in approach to any interlocking with an exit to a tunnel requiring protection. An OBC with the tunnel enabled bit set will ignore the Transponder Tunnel Package and enforce its normal ACSES speed and routing functionality through the interlocking (including under a failed radio condition).

Failure Modes Considered:

Missed Transponder SHA-250, SHA-259, SHA-261

OBC not configured correctly. SHA-205

ISR Response not Received SHA-58, SHA-204, SHA-232

ASB Activation SHA-271, SHA-204

3.2.8 ACSES Territory Boundaries and Non-Coded Areas

3.2.8.1 Yard & Siding Entry Protection

The ACSES II system protects entry to the ACSES II territory by enforcing the Stop Signal aspects governing routes from the yards and sidings. For locations without physical signals a virtual signal is provided and the ASB pushbutton must be pressed to enter the mainline

Failure Modes Considered:

Missed Transponder SHA-250

OBC not configured correctly. SHA-39

ISR Response not Received SHA-58

ASB Activation SHA-271

Reboot of Trains in Sidings – (Is siding large enough for DS) SHA-233

3.2.8.2 PTS Enforcement at ABS

ACSES II enforces a PTS prior to intermediate automatic signals reporting a Stop and Proceed aspect in ABS territory without cab signaling. Transponder sets are installed on either side of the insulated joint in order provide a virtual interlocking entry and exit for the PTS stop.

Failure Modes Considered:

Missed Transponder SHA-250

Transponder Data Error SHA-283

ASB Activation SHA-271

Entry to ASC from ABS/CMB – Need for enforcing stop at any zero code rate. SHA-289

3.2.8.3 Manual Block System Territory

Within Manual Block System (MBS) Territory, ACSES II enforces civil speeds conveyed by the transponders, however the ADU displays a "- -" as ACSES does not know all speed enforcement information that may be governing the train engineer within MBS territory. Where a SAR TSR or Zero Speed TSR is enforcing 0, the ADU will display "0" in the track speed indicator.

Failure Modes Considered:

Missed Transponder SHA-250

Transponder Data Error SHA-283

Train to Office communication Failure SHA-273

OBC Reboot SHA-233

TSR not set for MBS Operation SHA-288

3.2.8.4 MTEA

Mainline Track Exclusion Areas (MTEA) are utilized in areas such as:

- Complex interlockings (such as LIRR Jamaica)
- Low speed terminals (such as Grand Central Terminal)
- Low traffic lines (Such as Ronkonkoma to Greenport on the LIRR)

ACSES provides speed enforcement only in these areas. A PTS is enforced on exit of the MTEA into the Mainline areas.

Failure Modes Considered:

Missed Transponder SHA-250

Transponder Data Error SHA-261

Train to Office communication Failure SHA-273

OBC Reboot SHA-233

3.2.8.5 Exiting ACSES Territory

A transponder set is used at the exit points to ACSES territory for the direction of travel. Within this transponder set, a line speed package is placed in order to have the ACSES II OBC enforce the MAS for the direction being exited, as long as ACSES remains cut-in. This line speed remains in effect until ACSES is cut-out, powered down, or the train returns to ACSES territory.

Failure Modes Considered:

Missed Transponder SHA-250

Transponder Data Error SHA-261

Train to Office communication Failure SHA-273

OBC Reboot SHA-233

3.2.9 Events Diagnostics and Alarms

3.2.9.1 ACSES Run-time Diagnostic and Events

In general, the event logs and alerts are continuously being sent for logging to the DMS and NMS. Alarms and alerts of the system are sent to the appropriate logged in user for display in an active appropriate window.

Failure Modes Considered:

N/A

3.2.9.2 Offline Diagnostics

Several subsystems of the ACSES II require additional utilities for local maintenance and diagnostic activities

Failure Modes Considered:

N/A

3.2.9.3 Onboard Offline Diagnostics

From a system level view, there is an event recorder provided in all onboard installations to capture the required ACSES II data for diagnostic and archiving of data logs

Failure Modes Considered:

N/A

3.2.9.4 OBC Remote Diagnostics

The remote diagnostic functionality allows users to access both the OBC event recorder and MCM log files from a remote workstation (PC). The remote terminal for LIRR is provided in a designated maintenance location utilizing a rack mounted Digi modem to provide cellular communication capabilities to any of the ACSES installed vehicles with an operational Digi modem.

Failure Modes Considered:

N/A

3.2.9.5 ACSESView

The OBC equipment provides internal capabilities for historical data logging and real-time data reporting. The OBC equipment supports a connection with a PC-based PTE application program, referred to as ACSESView

Failure Modes Considered:

N/A

3.2.9.6 SimACSES

SimACSES is graphic tool for use by the Design group to simulate the OBC reactions for an entire ACSES territory on RR's territory in response to the transponder packages as lay out on RR's territory and also in response to the data radio messages in the lab environment to ensure the OBC behaves as designed.

Failure Modes Considered:

N/A

3.2.10 Additional System Function

3.2.10.1 Configuration management

Software and Data Maintenance System provides CM tool(s) to support configuration management of all artifacts developed as part of the Project

Failure Modes Considered:

N/A

3.2.10.2 ACSES II System Data Maintenance

The ACSES II is a safety critical system consisting of many subsystems that pull their data from a common database (Topographical Database – TopoDB) in order to ensure safe operation of the system.

Failure Modes Considered:

SDMT Errors SHA-73

Data Entry Errors PHA-39, SHA-226, SHA-11, SHA-36, SHA-48,

Civil Data Verification SHA-10, SHA-13, SHA-53

3.2.10.3 System Initialization

Onboard

When the Onboard is initially powered on, the Onboard assumes it is in Non-ACSES territory, regardless of its current location, as defined in the ACSES Modes section of this document. If a departure test is required, as defined in the Departure Test section of this document, then one should be performed. The ACSES system allows the train to move without performing a departure test upon power-up and reset.

Office

The active STS in a control center waits for active state communication message from UIS, DMS, WCC, and RGS located in the same control center as a response to STS status message before the STS accepts “Controlling State” command.

The initial Safety TSR Server would have no active or scheduled TSRs until they are entered through the Select-Check-Execute process defined within this document. If a TSR server is brought online while another TSR server is active, then the two servers would be synchronized while the currently active TSR server remains as the controlling TSR server. The controlling TSR server does not change until a fail-over occurred or a command from the NMS was issued

3.2.10.4 Security

See System Vulnerability Assessment[14].

3.2.10.5 ADDC and Single Sign On

The Active Directory Domain Controller (ADDC) Server is used to provide Single Sign-On (SSO) administration and management for all the Office and RWPS Subsystems in the ACSES II system. ADDC provides ability for the System Administrator to configure access rights to the office applications. Individual office application with the support from ADDC provide access rights to functions and features of the application as defined by the different user classifications assigned to individual user groups

See System Vulnerability Assessment[14].

3.2.11 Roadway Worker Protection

3.2.11.1 RWPS

Roadway worker protection is provided by the ACSES II through the use of TSRs requested from an Employee in Charge (EIC) using the Roadway Worker Protection System (RWPS). The RWPS consists of a dedicated set of servers and EIC input devices (portable handheld units as well as truck mounted terminals) that communicate with the ACSES II Office system through the Railroad Gateway Server (RGS).

At a high level, the EIC has the capability to request a Work Zone TSR be placed in order to protect a crew of workers for a specified section of track (start and end limits set by the EIC). The request is transmitted through the RWPS Office system to the ACSES II Office system where a dispatcher begins the Select-Check-Execute process in order to place the TSR. The EIC is informed of the current status of the TSR request as well as able to access a TSR list from the RWPS terminal device.

Additionally, secondary EICs can be protected under the primary EICs work zone by being attached, electronically, to the specific work zone. The primary EIC cannot release a work zone until all secondary EICs have been released from the specific work zone. This ensures that all work crews are accounted for when attempting to delete a Work Zone TSR.

4 Methodology

The System SHA verifies implementation of the safety requirements, derived to mitigate the primary hazards inherent with the railway system. Primary hazards that the ACSES II system must control are identified based in the System PHA [2].

4.1 Analysis Process

The SHA is developed by expansion of the system-related hazards and resolutions presented in the PHA to identify faults to the subsystem level. The SHA also incorporates the safety-critical detailed functional requirements of the system as given in the System Level Requirements Specifications [16], combined specific domain knowledge of the safety critical functions of train control systems.

The hazards analyzed in the SHA are primarily those that may cause serious injury or significant damage to equipment or infrastructure. Each hazard is then analyzed to determine what specific safety-critical functions or processes of the <subsystem> will eliminate or mitigate the unsafe effects. These resolutions are then established as requirements to be implemented in the system design. Proper implementation greatly increases the level of safety assurance provided.

As defined in Reference [5] [21], a process of determining hazard risk is followed which first categorizes hazards by their severity, then derives the probability that a hazard will occur, in order to assign a Hazard Risk Index (HRI) level. An initial HRI is assigned to each hazard based on the unsafe result without applying mitigation strategies. Design and/or procedural resolution(s) to the faults that lead to the hazards are then proposed. A residual HRI is assigned based on the nominal effectiveness of the proposed resolutions.

It is the task of the implementation level verification(s) and the Verification and Validation Program to confirm that the resolutions provided by the ACSES II design as explained in Reference [20] are effective in mitigating the hazard to the assessed residual risk index level.

5 System Hazard Analysis Results Table

The analysis and assessment results are presented in table format which contains the following columns:

Table 6: Hazard Table Column Definition / Description

Column Title	Description
ID	A direct cross-reference from the SHA to the entry for each hazard into the Project Hazard Log [1].
Subsystem or Interfaces	Subsystem to which this Hazard Interfaces.
Source of Hazard	A unique identification number is provided per line to simplify hazard location in the tables.
Hazard Description	Description of the hazard.
Primary Cause	Description of the possible causes which might be at the origin of the hazard, as identified at the FFT Level.
Initial Risk Index	The ranking of the severity of the hazard is performed per the description of the analysis process in Section 4.1
Mitigation / Controls / Safeguards)	Description of how the subsystem or components will mitigate the hazard.
Final Risk Index	The residual (or final) Hazard Risk Index (HRI) number based on the expected effectiveness of the listed mitigation, control, or safeguard.
Safety Requirement ID	An Identification Number to the Safety Requirement Derived from the Mitigation for the Hazard.
Responsibility	System Component or Subsystem Component to which the responsibility for this hazard and corresponding mitigation have been allocated.
Remarks	General remarks to the identified hazards, relative to the analyses or safety program.

5.1 System Hazard Analysis Table

The System Hazard Analysis is presented in Tabular form as per column Description given in Table 6 above. The System Hazard Analysis table is provided in Attachment – System Hazard Analysis Table see section 7.

5.2 New Hazards Introduced by SHA

The following entries were added based upon the completion of the SHA.

HL-644

HL-645

HL-646

HL-647

HL-648

6 Conclusion

The LIRR PTC System Hazard Analysis (SHA) has verified the potential hazards in the design and operation of the ACESS II System.

In Section 5.1, the analysis table corresponding to the System Hazards, as derived with regard to the Subsystem Hazard Analyses, was presented. This analysis was verified through and further analyzed in this document. The result shows that those hazards can be mitigated to a tolerable level and can be considered to have no significant hazardous effect on the operation of the ACSES II system once mitigations are applied.

7 Attachment – System Hazard Analysis Table

See 3035823_Rev_A Attachment A –

This spreadsheet is a filtered view of the Project Hazard Log from Sources set from SHA. The baseline used for this export was version 8.0 JW1 (View was set to LIRR_SHA)

ID	Subsystem or Interfaces	Source of Hazard	Hazard Description	Primary Cause (FFT Level 2)	Risk - Before	Safety Requirements ID	SA_LIRR_Status	Responsibility	Risk Mitigation	Remarks
HL- 358	Office	SHA-99	Onboard Receives incorrect TSR	STS Computer Failure	IB	SR_217 SR_518 SR_521	Closed	Office Safety	IE	
HL- 536	Onboard	SHA-98	Onboard Receives incorrect TSR	Failure of Onboard to process Transponder data correctly	IC	SR_544	Closed	Onboard Safety	IE	
HL- 535	Onboard	SHA-97	Onboard Receives incorrect TSR	Onboard incorrectly processes the TSR data	IC	SR_509 SR_510	Closed	Onboard Safety	IE	
HL- 357	Comms	SHA-96	Antennae Mast Collapse - Incorrect Design	Incorrect maintenance of Antennae Mast	IB	SR_216	Mitigated	System Safety	IE	No SLR Req
HL- 356	Comms	SHA-95	Antennae Mast Collapse - Incorrect Design	Mas Failure or Foundation Failure	IB	SR_216	Mitigated	System Safety	IE	No SLR Req
HL- 534	Onboard	SHA-94	Train Speed in MTEA area not correctly controlled by ACSES	Failure of Onboard to receive Transponder Data	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	Coverage of LIRR PTCIP Hazard 1B - No Speed Control
HL- 533	Onboard	SHA-93	Train Speed in MTEA area not correctly controlled by ACSES	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	Coverage of LIRR PTCIP Hazard 1B - No Speed Control
HL- 532	Onboard/ Onboard-Speed Sensor	SHA-92	Train Speed in MTEA area not correctly controlled by ACSES	Failure of Onboard to receive speed data	IC	SR_11	Closed	Onboard Safety	IE	Coverage of LIRR PTCIP Hazard 1B - No Speed Control
HL- 531	Railroad	SHA-91	Train speed not correctly controlled by Engineer.	Onboard Powered down after exit into MTEA	IB	SR_69	Mitigated	Railroad	IE	Coverage of LIRR PTCIP Hazard 1B - No Speed Control
HL- 530	Onboard	SHA-90	Train speed not correctly controlled by Engineer.	Failure of Onboard to receive Transponder Data	IC	SR_351 SR_390 SR_570 SR_571	Closed	Railroad	IE	
HL- 355	Railroad	SHA-89	Train speed not correctly controlled by Engineer.	Failure of Onboard to process Transponder data correctly	IB	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 354	Onboard	SHA-88	Train speed not correctly controlled by Engineer.	Failure of Onboard to receive speed data	IC	SR_11 SR_506	Closed	Onboard Safety	IE	

HL- 353	Railroad	SHA-87	Train speed not correctly controlled by Engineer.	Train exits to MTEA not properly speed controlled by Engineer.	IB	SR_69	Mitigated	System Safety	ID	
HL- 529	Onboard	SHA-86	Mainline Incursion	Failure of Onboard to receive Transponder Data	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 528	Onboard	SHA-85	Mainline Incursion	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570	Closed	Onboard Safety	IE	
HL- 527	Onboard	SHA-84	Non ACSES II Train overruns a stop signal.	Failure of Onboard to receive Transponder Data	IC	SR_478 SR_570	Closed	Onboard Safety	IE	
HL- 526	Onboard	SHA-83	Non ACSES II Train overruns a stop signal.	Failure of Onboard to process Transponder data correctly	IC	SR_139 SR_478 SR_570	Closed	Onboard Safety	IE	
HL- 525	Onboard	SHA-82	Incorrect Movement Authority received by Onboard	Failure of Onboard to receive Transponder Data	IC	SR_388 SR_478 SR_570	Closed	Onboard Safety	IE	
HL- 524	Onboard	SHA-81	Incorrect Movement Authority received by Onboard	Failure of Onboard to process Transponder data correctly	IC	SR_139	Closed	Onboard Safety	IE	
HL- 521	Onboard	SHA-78	ACSES II train location incorrect	Failure of Onboard to receive Transponder Data	IC	SR_478 SR_570	Closed	Onboard Safety	IE	
HL- 520	Onboard	SHA-77	ACSES II train location incorrect	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570	Closed	Onboard Safety	IE	
HL- 519	Onboard/ Onboard-Speed Sensor	SHA-76	ACSES II train location incorrect	Failure of Onboard to receive speed data	IC	SR_11	Closed	Onboard Safety	IE	
HL- 518	Onboard/ Onboard-Speed Sensor	SHA-75	ACSES II not measuring speed correctly	Failure of Onboard to receive speed data	IC	SR_11	Closed	Onboard Safety	IE	
HL- 517	Office	SHA-74	ACSES II not enforcing Speed correctly.	Failure of Office database to define correct TSR for work areas	IB	SR_22 SR_394 SR_507	Closed	System Safety	IE	
HL- 516	Office	SHA-73	ACSES II not enforcing Speed correctly.	Failure of Office database to define correct TSR	IB	SR_22 SR_468 SR_469	Closed	System Safety	IE	

HL- 515	Onboard	SHA-72	ACSES II not enforcing Speed correctly.	Failure of Onboard to process TSR data correctly	IC		SR_139 SR_467 SR_509 SR_510	Closed	Onboard Safety	IE	Coverage of LIRR PTCIP Hazard 1E - TSR
HL- 512	Onboard - Train Mission Switch	SHA-69	ACSES II not enforcing Speed correctly.	Failure between Onboard and Train ACSES cut out switch	IC		SR_196 SR_197	Closed	Onboard Safety	IE	
HL- 511	Onboard	SHA-68	ACSES II not enforcing Speed correctly.	Failure of Onboard to receive ACSES cut out input data	IC		SR_360	Mitigated	Onboard Safety	IE	Install Manual Link needed
HL- 510	Onboard	SHA-67	ACSES II not enforcing Speed correctly.	Failure of Onboard to receive ACSES cut out input data	IC		SR_196	Closed	Onboard Safety	IE	
HL- 509	Onboard	SHA-66	ACSES II not enforcing Speed correctly.	Failure of Onboard to receive Transponder Data	IC		SR_388	Closed	Onboard Safety	IE	
HL- 508	Onboard	SHA-65	ACSES II not enforcing Speed correctly.	Failure of Onboard to process Transponder data correctly	IC		SR_139 SR_572	Mitigated	Onboard Safety	IE	
HL- 507	Onboard/ Onboard- Speed Sensor	SHA-64	ACSES II not enforcing Speed correctly.	Failure of Onboard to receive speed data	IC		SR_11	Closed	Onboard Safety	IE	
HL- 506	Onboard	SHA-63	Mainline Incursion	Failure of Onboard to receive Transponder Data	IC		SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 505	Onboard	SHA-62	Mainline Incursion	Failure of Onboard to process Transponder data correctly	IC		SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 504	Onboard	SHA-61	Non ACSES II Train overruns a stop signal.	Failure of Onboard to receive Transponder Data	IC		SR_388	Closed	Onboard Safety	IE	
HL- 503	Onboard	SHA-60	Non ACSES II Train overruns a stop signal.	Failure of Onboard to process Transponder data correctly	IC		SR_139	Closed	Onboard Safety	IE	
HL- 502	Railroad	SHA-59	Non ACSES II Train overruns a stop signal.	Engineer fails to obey operating procedures and stop at red signal.	IB		SR_69	Mitigated	System Safety	ID	
HL- 352	Onboard	SHA-58	Incorrect Movement Authority received by Onboard	Onboard uses a stale WIU message to proceed through an interlocking that another train traversed through.	IC		SR_214 SR_215	Closed	System Safety	IE	

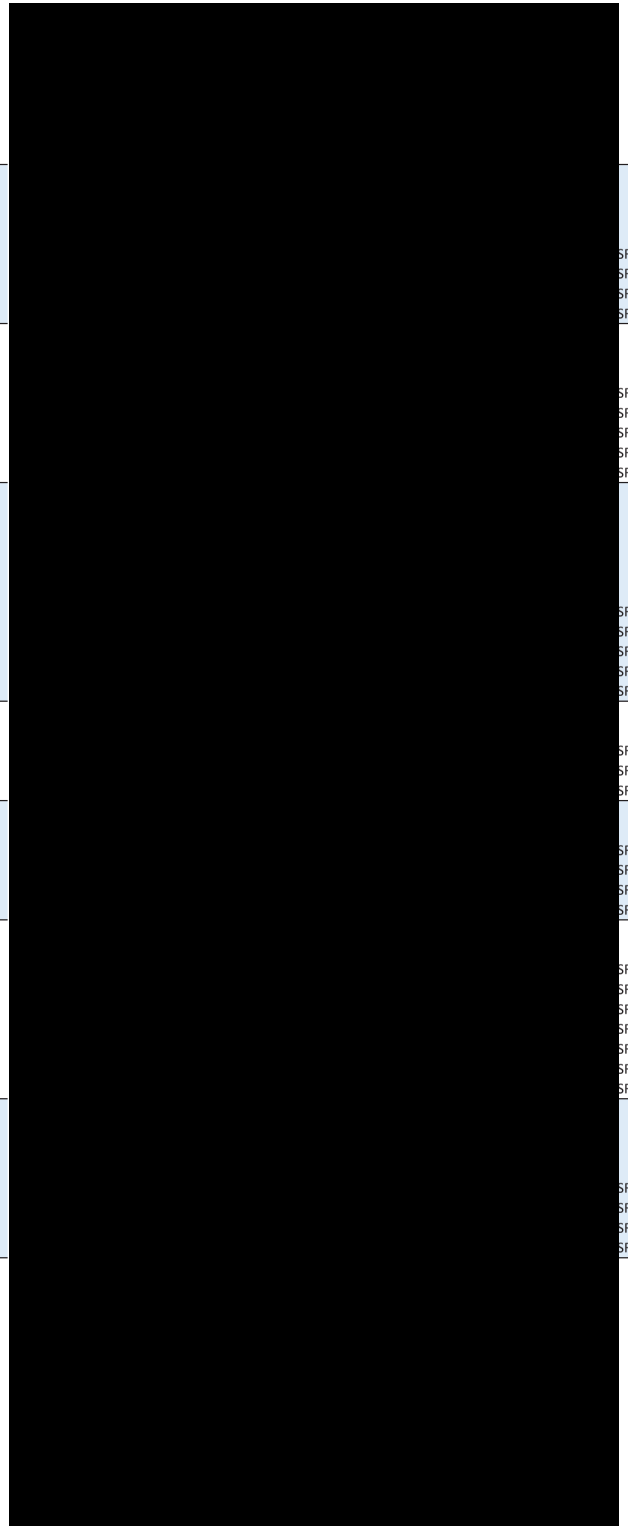
HL- 351	Railroad	SHA-57	Incorrect Movement Authority received by Onboard	ACSES II allows train to operate above 15MPH after the operation of ASB.	IB	SR_86 SR_540 SR_541 SR_542	Closed	Railroad	IE	ASB / CMB
HL- 470	WIU Onboard Operations	SHA-56	Incorrect Movement Authority received by Onboard	ACSES II allows PTSO in area without main signals when ASC is cut out.	IC	SR_325	Closed	Wayside safety	IE	
HL- 349	Railroad	SHA-55	Incorrect Movement Authority received by Onboard	The ATC fails to provide the correct signaling status	IB	SR_209 SR_534	Closed	Railroad	IE	
HL- 348	Onboard	SHA-54	Incorrect Movement Authority received by Onboard	Failure of Onboard to receive Transponder Data	IC	SR_388	Closed	System Safety	IE	
HL- 347	Transponder	SHA-53	Incorrect Movement Authority received by Onboard	Failure of Transponder database to define correct distances and location	IB	SR_22 SR_324	Closed	Transponder Safety	IE	
HL- 346	Onboard	SHA-52	Incorrect Movement Authority received by Onboard	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570 SR_571	Closed	System Safety	IE	
HL- 345	Onboard	SHA-51	Incorrect Movement Authority received by Onboard	Onboard incorrectly process the WIU message.	IC	SR_410 SR_511 SR_523	Closed	Onboard Safety	IE	
HL- 344	WIU	SHA-50	Incorrect Movement Authority received by Onboard	Failure of the interface between the WIU and ATC.	IB	SR_208	Closed	System Safety	IE	
HL- 343	WIU	SHA-49	Incorrect Movement Authority received by Onboard	WIU incorrectly process movement authority Data.	IB	SR_204 SR_504 SR_511	Closed	Wayside Safety	IE	

HL- 469	WIU	SHA-48	Incorrect Movement Authority received by Onboard	Failure of WIU Database to correctly define inputs to movement authority	IB	SR_22 SR_512 SR_522	Closed	Wayside Safety	IE	
HL- 341	WIU	SHA-47	Incorrect Movement Authority received by Onboard	WIU Computer Failure	IB	SR_204 SR_511 SR_512 SR_522	Closed	Wayside Safety	IE	
HL- 338	Onboard	SHA-44	ACSES train performance characteristics not programmed correctly.	Incorrect train performance characteristic programmed into the Onboard causes the Onboard to fail to perform the correct functionality.	IC	SR_203	Closed	Onboard Safety	IE	
HL- 337	Onboard	SHA-43	ACSES train performance characteristics not programmed correctly.	Onboard incorrectly processes the train data	IC	SR_139	Closed	Onboard Safety	IE	
HL- 501	Onboard	SHA-42	ACSES II train location incorrect	Failure of Onboard to receive Transponder Data	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 500	Onboard	SHA-41	ACSES II train location incorrect	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570	Closed	Onboard Safety	IE	
HL- 499	Onboard/ Onboard-Speed Sensor	SHA-40	ACSES II train location incorrect	Failure of Onboard to receive speed data	IC	SR_11	Closed	Onboard Safety	IE	
HL- 336	Onboard	SHA-39	ACSES II train location incorrect	Incorrect train location calculated from incorrect front of train offsets programmed into the Onboard.	IC	SR_203 SR_324	Mitigated	Onboard Safety	IE	Manual Link Neede
HL- 335	Transponder	SHA-38	ACSES II train location incorrect	Incorrect train location defined due to data corruption during programming of transponder memory	IB	SR_194	Closed	Transponder Safety	IE	Manual Link Neede

HL- 334	Transponder	SHA-36	ACSES II train location incorrect	Failure of TopoDB to define correct placement of Transponder	IB		SR_22 SR_142 SR_324 SR_514	Closed	Transponder Safety	IE	
HL- 333	Onboard	SHA-35	ACSES II train location incorrect	Failure of Onboard to receive Transponder Data	IC		SR_478 SR_570 SR_571	Closed	System Safety	IE	
HL- 332	Onboard	SHA-34	ACSES II train location incorrect	Failure of Onboard to process Transponder data correctly	IC		SR_478 SR_570 SR_571	Closed	System Safety	IE	
HL- 331	Onboard	SHA-33	ACSES II train location incorrect	Failure of Onboard to receive speed data	IC		SR_11	Closed	Onboard Safety	IE	
HL- 672	Transponder	SHA-320	Train violates Home Signal after turnback.	Interoperable Train fails to read turnback packages and enforce PTS.	IB		SR_557	Mitigated	System Safety	ID	
HL- 330	Onboard	SHA-32	ACSES II train location incorrect	Onboard incorrectly processes the train location data	IC		SR_139 SR_474 SR_548	Closed	Onboard Safety	IE	
HL- 329	Onboard	SHA-31	ACSES II not measuring speed correctly	Failure of Onboard to receive speed data	IC		SR_11 SR_506	Closed	Onboard Safety	IE	
HL- 458	Dispatcher to Office Office	SHA-30	ACSES II not enforcing Speed correctly.	Incorrect TSR entered by the Office personnel	IB		SR_318 SR_519 SR_520	Closed	System Safety	IE	
HL- 327	Onboard - Office	SHA-29	ACSES II not enforcing Speed correctly.	Failure of Onboard to receive TSR Data	IC		SR_430	Canceled	System Safety	IE	Duplicate of PHL-251 Duplicate of PHL-252

HL- 433	WIU ATC	SHA-289 PHA-80	ATC fails to reduce the speed of a train after entering ASC from ABS Territory	ATC is High Energy Cutout when operating in ABS Territory. When entering ACSES territory the signal state could be Restricted or Stop and Proceed which are considered permissive by ACSES. If the ATC fails to wakeup and restrict the speed of the train the train could overspeed into the next ASC block cause a collision.	IC	SR_309 SR_310 SR_311	Closed	Railroad	IE	ABS / CMB
HL- 326	Office	SHA-287 PHA-89	STS Database Incorrect	The vital data used by STS to verify TSR Requests is incorrect	IC	SR_200 SR_201 SR_202	Closed	Office Safety	IE	
HL- 474	Transponder Office Onboard	SHA-286 PHA-73	Train exceeds speed for a section of track	ACSES II not receiving lowest speed limit that is in effect	IC	SR_63 SR_64 SR_328 SR_329 SR_330 SR_331 SR_332 SR_333 SR_334 SR_335 SR_409 SR_478 SR_506	Closed	Onboard Safety Transpodner Safety	IE	Removed Transponder Message dulication. Current OBC does not enforce Speed restrictions after a missed TP so not needed.
HL- 16	Office Onboard Comms	SHA-285 PHA-22	Train violates a speed restriction established to provide protection from an unsafe condition at a certain location.	On-board receives incorrect Mandatory Directive	IC	SR_317	Closed	System Safety	IE	Coverage of LIRR PTCIP Hazard 1D and 1E - PSR and TSR enforcement
HL- 436	Office	SHA-284 PHA-91	UIS Database Incorrect	The UIS database has incorrect data	IC	SR_116 SR_314 SR_315	Closed	Office Safety	IE	

HL- 442	Onboard Onboard Parameter Programming Tool	SHA-283 PHA-12	Train Speed not correctly enforced by ACSES II	ACSES II wrongly locating train relative to Limit of Movement Authority	IC	SR_3 SR_65 SR_66 SR_432	Closed	Onboard Safety	IE	Linking to Op Procedure and Installation Procedure for insallation verification to be done.
HL- 198	Office / Onboard	SHA-281 PHA-59	Train violates a TSR in an adjacent RR	TSR is not communicated from the adjacent RR	IC	SR_55 SR_56 SR_57 SR_392 SR_470	Closed	System Safety	ID	Point TSR will be at MAS
HL- 205	On-board	SHA-280 PHA-66	Train Speed not correctly enforced by ACSES II	ACSES II wrongly locating train relative to Limit of Movement Authority	IIIB	SR_3 SR_63 SR_64 SR_65 SR_66	Closed	System Safety	IIIE	
HL- 468	Office	SHA-28	ACSES II not enforcing Speed correctly.	Failure of Office database to define correct TSR	IB	SR_22 SR_323 SR_324	Closed	Office Safety	IE	
HL- 644	OBC - WIU	SHA-279 SYS_IHA_56	Onboard recieves correct WIU data but form wrong WIU	OBC reqeust to WIU corrupted - WIU responds with wrong signal or wrong WIU responds	IB	SR_78 SR_410 SR_429 SR_476	Closed	OBC	IE	Exported from WIU need to link
HL- 394	WIU - Interface to Points and Signals	SHA-278 SYS_IHA_50	WIU Configuration error which results in WIU to send an ATCS message with a less restrictive movement authority than intended	Error in Installation Instructions. Error in configuration files	IB	SR_34 SR_235 SR_236 SR_237 SR_238 SR_239 SR_516	Closed	Wayside Safety System Safety	IE	
HL- 670	Onboard	SHA-277	Train Exceeds ACSES braking Profile	Service Brake Rate fails to acheive calcualted rate for ACSES Enforcement	IC	SR_2 SR_531 SR_532 SR_535	Closed	Onboard Safety	IE	



HL- 232	OBC to Train	SHA-276 SYS_IHA_27	OBC interface to Reverse Train Line fails open.	Open circuit	IB		SR_96 SR_97 SR_263	Closed	Onboard Safety	IE	
HL- 231	OBC to Train	SHA-276 SYS_IHA_26	OBC interface to Forward Train Line fails short circuit	Short circuit	IB		SR_95 SR_97 SR_263	Closed	Onboard Safety	IE	
HL- 230	OBC to Train	SHA-276 SYS_IHA_25	OBC interface to Forward Train Line fails open.	Open circuit	IB		SR_95 SR_97 SR_263	Closed	Onboard Safety	IE	
HL- 229	OBC to Train	SHA-276 SYS_IHA_24	OBC interface to Service Brake Train Line shorts.	Short Circuit.	IB		SR_97 SR_189 SR_263	Closed	Onboard Safety	IE	
HL- 228	OBC to Train	SHA-276 SYS_IHA_23	OBC interface to Service Brake Train Line Fails open.	Open Circuit	IB		SR_94 SR_97 SR_263	Closed	Onboard Safety	IE	
HL- 411	Onboard	SHA-275 Sys-OHA-51	Failure to perform the departure test on the 24 hour cycle. Possible equipment failure not detected.	Equipment failure on onboard not detected.	IC		SR_262 SR_263	Mitigated	Onboard Safety	ID	RR to address departure test requirements.
HL- 489	Railroad	SHA-274 Sys-OHA-59 Sys-OHA-62	Train overspeeds through a established Temporary Speed Enforcement	ACSES indicates No TSR Data to the Train Engineer but the train Engineer does not have or does not enforce current speed Restriction	IC		SR_128 SR_352 SR_530	Closed	Railroad	ID	Coverage of LIRR PTCIP Hazard 1E -TSR
HL- 216	Office to OBC	SHA-273 SYS_IHA_09	Onboard fails to received TSR data and fails to reduce speed at TSR that is now active but is not in the trains list of TSRs	Loss of Interface	IB		SR_69 SR_75 SR_76 SR_77 SR_80 SR_84 SR_421 SR_422 SR_423 SR_458	Closed	System Safety	ID	

HL- 462	Onboard	SHA-272 PHA-81	Failure to Acknowledge Overspeed	The operator fails to Ack the overspeed alarm or the Ack button fails in the inactive position.	IC	SR_319 SR_320 SR_500 SR_539	Closed	Onboard Safety	IE	N/A
HL- 481	Onboard Office WIU RWPS	SHA-271 PHA-93	Communication Delay	ACSES data is not updated and the system reacts to old data.	IC	SR_63 SR_64 SR_82 SR_101 SR_328 SR_330 SR_331 SR_336 SR_341 SR_342 SR_343 SR_344 SR_345	Closed	Wayside Safety Onboard Safety	IE	
HL- 680	Onboard	SHA-271	Turnback protection disabled as train moves thorugh a Back to back interlocking.	OBC disables Turnback after reading DS Set	IC	SR_566		Transponder	IE	Back to Back ABS / CMB
HL- 248	Train Engineer to OBC	SHA-270 SYS_IHA_43	ADU fails to provide updated information to the Train Engineer.	Loss of Interface	IB	SR_121 SR_122 SR_123 SR_125 SR_126 SR_496	Closed	System Safety	IE	
HL- 679	Onboard	SHA-270	Train performing turnback in back to back embedded signal area releases PTS for wrong signal infomration	Train used radio information for a turnback package read in trail that is no longer valid	IC	SR_565		Transponder	IE	Back to Back ABS / CMB
HL- 325	Onboard	SHA-27	ACSES II not enforcing Speed correctly.	Failure of Onboard to process TSR data correctly	IC	SR_139 SR_509 SR_510 SR_529	Closed	System Safety	IE	

HL- 350	WIU Onboard Operations	SHA-269 PHA-88	ATC Cutout	ACSES does not detect that the ATC is cutout and lets the train into the next block without safe train separation	IC	SR_210 SR_211 SR_212 SR_325 SR_477 SR_497	Closed	Wayside safety	IE	ASC Only
HL- 249	Train Engineer to OBC	SHA-268 SYS_IHA_44	ADU fails to provide updated information to the Train Engineer.	Incorrect Transfer of information.	IB	SR_121 SR_122 SR_123 SR_125 SR_126 SR_496	Closed	System Safety	IE	
HL- 238	OBC to Train	SHA-266 SYS_IHA_33	OBC interface to ATC fails short circuit	Open circuit	IB	SR_97 SR_100 SR_101 SR_263	Closed	Onboard Safety	IE	
HL- 669	OBC	SHA-265	Train not stoped when OBC determine train is stopped (V Zero Function)	Speed Sensor Failure or SW failure	IB	SR_11 SR_106 SR_139 SR_188 SR_479 SR_528	Closed	Onboard Safety	IE	
HL- 233	OBC to Train	SHA-264 SYS_IHA_28	OBC interface to Reverse Train Line fails short circuit	Short circuit	IB	SR_96 SR_97 SR_263	Closed	Onboard Safety	IE	
HL- 281	On-Board	SHA-263 Sys-OHA-18	Train Engineer fails to detect and safely react to train system failures (e.g. damaged wheels, propulsion failures, brake failures)	Train Engineer Error	IIB	SR_165 SR_475	Canceled	System Safety	IID	Removed from System OHA Rev _A.
HL- 466	OBC to Decelerometer	SHA-262 SYS_IHA_60	The interface between decelerometer and OBC fails	Incorrect Grade compensated	IB	SR_447 SR_448	Closed	System Safety	IE	

HL- 220	TP to OBC	SHA-261 SYS_IHA_16	Onboard system receives data from the transponder that is not programmed into the transponder. (I.E data is corrupted over the RF Link)	Incorrect Transfer of information.	IB		SR_64 SR_69 SR_73 SR_89 SR_90 SR_91 SR_92 SR_389 SR_432	Closed	System Safety	IE	
HL- 438	Onboard	SHA-260 PHA-11	Train Speed not correctly enforced by ACSES II	Train exceeds ACSES target speed profile as speed measurement sensor fails to detect the speed of the train.	IC		SR_11 SR_528	Closed	Onboard Safety	IE	N/A
HL- 424	Wayside	SHA-260	Train Engineer falls to stop and Stop and proceed aspects in ABS territory and ASC is cutout.	Operator Error	IC		SR_292 SR_293 SR_294 SR_543	Closed	Wayside Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program ABS / CMB
HL- 446	Onboard Onboard Parameter Programming Tool	SHA-259 PHA-13	Train Speed not correctly enforced by ACSES II	Train performance characteristics not programmed correctly	IC		SR_316	Closed	Onboard Safety	IE	N/A
HL- 409	Onboard	SHA-258 Sys-OHA-50	Improper entry of offset distance, antenna to front of vehicle.	Configuration update not performed on spare equipment.	IC		SR_254 SR_255 SR_256 SR_257	Mitigated	Onboard Safety	ID	
HL- 645	Operations	SHA-257	Train Operator moves the train at a slow speed and is able to proceed past PTS Enforcement targets.	Train Engineer Error	IB		SR_479	Mitigated	Railroad	ID	
HL- 648	Onboard	SHA-256	Train requests incorrect signal status from Wayside due to back to back signals.	ISRRequest sent by OBC not resolved by DS/HS transponder packets in seperate TP. Back to back requires these packets in the same TP set.	IB		SR_481	Closed	OBC	IE	Clear mitigation not yet decided. Back to Back ABS / CMB

[redacted]

HL- 647	Operation	SHA-255	Loss of TSR, PSR and MAS enforcement when reverser changes from current direction of travel to opposing directin.	OBC Type approved SW removes all Speed enforcmeent when direction changes not when TP read in opposing direction.	IIIB	SR_480	Mitigated	Railroad	IIID	Rated a III - Very few trains reverese and then resume in same direction. Next TP read will reset TSR and PSR/MAS enforcement. Not appliable for turnback locations.
HL- 646	Operations	SHA-254	Train engineer able to drive the train past signals or zero speed restriction start locations.	Train Engineer Error	IB	SR_479	Mitigated	Railroad	ID	ACSES will command braking to enforce PTS and TSR but delay in braking system may cause the tran to stop past start of enforcement espceciall if trian enginer accelerates near enforcement location. Also slow speed movement not protected by ACSES.
HL- 649	Operations	SHA-253	Train operator accelerates near PTS enforcement area (especially accurate stop areas). Delay in OBC / Rolling stock reaction causes train to stop past PTS target.	Train Engineer Error	IB	SR_482	Mitigated	Railraod	ID	ACSES will command brake eforcement durring such events but the delay in rolling stock and OBC enforcement may cause the train to exceed PTS enforcement targets.
HL- 626	Comms	SHA-252	Equipment Tool Design - Obtrusive shape of MCP	Obtrusive shape of MCP mouinted above doorat 6'4"	IIIC	SR_418 SR_419	Closed	Comms Safety	IIID	DE/DM train type only
HL- 419		SHA-251	STS sends a message to a Locomotive ID of an adjacent railroad to the same locomotive number of this railroad.	TSR Data between office and Onboard corrupted.	IB	SR_80 SR_523	Closed	Onboard safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

[redacted]

HL- 221	TP to OBC	SHA-250 SYS_IHA_15	Onboard system fails to read a transponder.	OBC fails to read a transponder.	IB	SR_63 SR_64 SR_69 SR_90 SR_93 SR_140 SR_431 SR_473 SR_478 SR_525 SR_555 SR_570 SR_571	Closed	System Safety	IE	
HL- 421	Office	SHA-249	Both redundant STS servers become active controlling at the same time.	Redundancy Design	ID	SR_287 SR_288	Closed	Office Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program Mitigated for only one control center
HL- 425	System	SHA-248	Train Engineer exceeds FRA Rules for operating speeds after an en route failure of the ATC or ACSES (both required for PTC coverage)	Operator Error	IC	SR_295 SR_296 SR_297	Mitigated	System Safety Onboard	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 426	Wayside	SHA-247	ACSES II train does not enforce civil speed or PSR enforcement in MBS areas.	Transponder programming does not contailn correct infomration to provide enforcement	IC	SR_298 SR_299	Closed	Transponder Safety Onboard Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program MBS

[redacted]

HL- 429	Onboard	SHA-246	Accurate stop packages can use standard DS packet with Q bit set. If a tenant OBC is not programmed to handle the Q Bit it will interrupt the distance to DS in 10 yard increments instead of 1ft increments and overshoot the PTS.	OBC incorrectly reads Transponder packets and interrupts PTS distance incorrectly.	IC	SR_300 SR_301 SR_302	Closed	Transponder Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 624	Operations	SHA-245	Freight Train Overspeeds within an interlocking.	ACSES does not enforce Freight Interlocking speeds in interlockings.	IB	SR_396 SR_407	Closed	Railroad	IE	Found in Transponder Design Reivew for Shey Stadium
HL- 430	Onboard	SHA-244	OBC uses a PTS Hold to retain a PTS status from the WIU after passing the PTS location. This function is needed where TP must be installed behind the signal or where a train could shunt itself. This function could cause the train to not enforce a PTS where the train should be stopped.	PTS hold function causes a train to ignore a stop command.	IC	SR_304 SR_305 SR_524 SR_538	Closed	Onboard Safety	IE	Modified from System Engineering Discussion.
HL- 416	OBC	SHA-243	ACSES can only process a maximum of 8 tracks per line. MNR/LIRR has lines with more than 8 tracks. Therefore ACSES cannot provide safe speed or PTS enforcement for TSR's or PTS on tracks 9 and above.	Railroad has more than 8 tracks.	IC	SR_280 SR_281 SR_282 SR_517	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 415	OBC	SHA-242	OBC when performing the accurate stop may read a partial HS set that may release PTS enforcement.	Transponder layout distances not sufficient to prevent HS TP's from being read during an accurate stop.	IC	SR_279 SR_513 SR_538	Closed	Onboard Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 413	Transponder	SHA-241	When the PTSO is generated through the cab signaling release the onboard system does not know the exact path the train will take through the interlocking and may select the wrong PSR to enforce.	Design Error	ID	SR_268 SR_269 SR_298 SR_335 SR_396	Closed	Transponder Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

HL- 412	RWPS	SHA-240	RWPS Removes a TSR without ensuring all EIC are clear of work area	Operator Error	IC	SR_264 SR_265 SR_266 SR_267 SR_451 SR_455 SR_456 SR_457 SR_460	Closed	RWPS Safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 382	Office	SHA-239	Train violates SAR TSR without proper authorization.	Train Engineer uses Ack for an overpseed event that occurs near SAR TSR and inadvertenly clears TSR.	IB	SR_47 SR_232 SR_494 SR_495 SR_550	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 618		SHA-238	Train violates a work zone in an Adj Railroad	OBC does not slow down on the current line before braking curve for speed restriction on Adj RR.	IB	SR_398 SR_399	Closed	Office Safety	IE	
HL- 422	Office	SHA-237	TSR request lost because TSR storage exceeded.	To many TSR's for a defined area are requested.	IB	SR_289 SR_290 SR_533	Closed	Office Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 423		SHA-236	ACSES position error is 5% and is not considered in OBC enforcement of speed restrictions	ACSES position error not considered	IB	SR_291	Closed	Onboard Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

HL- 617	Onboard	SHA-235	Nested Interlocking where second radio in interlocking is failed to the second interlocking with permissive cab and where a speed beyond the ilk on a different track's brake distance exntends into the current ILK	The OBC will not consider this speed restriction until the train passes the exit TP set of the first ILK and recieves a list of possible exit tracks (which include the other track) .	IC	[redacted]	SR_69 SR_396 SR_397	Closed	Onboard Safety	ID	Addresses S9 from Safety Integrated Issues List Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 420		SHA-233	Train exceeds speed for a section of track	ACSES II not receiving lowest speed limit that is in effect	IB		SR_286 SR_500 SR_506 SR_517 SR_526	Closed	Office Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 46	Transponder	SHA-232	Some train types do not have physical clearance to enter the East Side Access tunnels. The ACSES system will enforce a stop on all East Side Access routes for trains that cannot clear the tunnel.	Train fails to read Transponder set with Route Dependent Speed Restriction	IB		SR_50 SR_51 SR_52 SR_53 SR_466	Mitigated	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 44	Onboard	SHA-231	Interoperable trains stopping at an accurate station stop may stop at the station such that the end of the train is beyond the platform.	Interoperable train SW uses the wrong accuracy for the accurate stop and stops with part of the train beyond the platform.	IIIC		SR_47 SR_48 SR_49	Mitigated	System Safety	IIIE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

HL- 39	Onboard Transponder	SHA-230	Transponder Data Incorrect	Transponder programmed with incorrect data or the incorrect packet programmed into the wrong transponder.	IC	SR_42 SR_43 SR_44 SR_45 SR_537 SR_549 SR_552	Closed	Wayside Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 38	Onboard	SHA-229	As cab signaling is cut out in ABS/CMB areas ACSES does not display the maximum train speed on the ADU and this could cause excessive overspeeds.	Original ACSES design does not display MAS speed on ADU when ASC is cut-out.	IC	SR_41 SR_125	Closed	System Safety	IE	MAS speed will not be displayed in MTEA or MBS areas with ASC cut-out. Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program. ABS/CMB
HL- 37	Onboard WIU	SHA-228	Train collision is due to Route to next home signal not being clear and ACS non operable to prevent collision.	Route is not cleared and ACSES performed PTSO without intervening system to prevent collision.	IC	SR_40	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program ASC Only
HL- 36	Onboard	SHA-227	Train released by train operator by ASB in cab for PTS collides with a train in the route.	Train allowed to travel at speed where train engineer can not intervene to stop a collision	IC	SR_38 SR_39 SR_568 SR_569	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program ABS/CMB

[redacted]

HL- 35	Onboard WIU	SHA-226	Onboard uses the wrong speed to control the speed of the train for the exit the train is actually taking. WIU message has an error or was unable to send a message for the actual speed to take.	Failure of the WIU to Onboard Message to send correct exit speed to the train.	IC	SR_22 SR_429 SR_511	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 34	Transponder Operations	SHA-225	Train will be unable to determine where home signal is located if the trailing end fails to read Transponder set when entering the turnback.	Improper layout of transponder, or Not enough space to apply ACSES.	IB	SR_36 SR_37	Closed	Wayside Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 33	Operations	SHA-224	Train will be unable to determine where the home signal is located if the trailing end fails to read Transponder set when entering the turnback.	Trailing end fails to read Transponder set when entering the turnback.	IB	SR_34 SR_35	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 32	Office	SHA-223	Office fails to retain Zero speed restriction for an MBS area occupied by train.	Cold start of STS would remove all active TSR's.	IB	SR_32 SR_33 SR_218 SR_462	Closed	Office Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program Left open for PCC/BCC connections Mitigated for only one control center
HL- 31	Operations	SHA-222	Operations fails to activate Zero Speed restrictions for a train allowed to enter MBS area.	Office Failure causes TSR request to be rejected. No Request Made.	IB	SR_31 SR_318	Closed	System Safety	IE	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program

[redacted]

HL- 30	Operations	SHA-221	Train Allowed to enter MBS area when another train of the same type is Occupying that area	Temporal Speed restrictions are removed form the Onboard when rebooted. Train will not receive TSR list until it reads transponder in MBS area.	IB	SR_29 SR_30	Closed	System Safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 29	Operations	SHA-220	A train that does not have permission to occupy the MBS area is permitted by verbal authorization to enter the MBS areas with a Zero Speed restriction active for its type of train.	Temporal Speed restrictions are removed form the Onboard when rebooted. Train will not receive TSR list until it reads transponder in MBS area.	IB	SR_29 SR_30	Mitigated	System Safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program Need to confirm that TSR is held after comm loss
HL- 418	Office	SHA-219	TSR is requested with a removals date and time but conditions change and TSR should not be removed when scheduled	Dispatcher enters incorrect time	IC	SR_284	Closed	Office Safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 417	Office	SHA-218	Scheduled TSR not executed because times requested for activation is not in the future or time for removal is before implementation time.	Dispatcher fails to enter the correct start time for TSR.	IC	SR_283	Closed	Office Safety	ID	Hazards identified by sources other than analyses will be reviewed for inclusion during updates to existing and execution of planned analyses of the safety program
HL- 263	Transponder	SHA-217	ACSES II not enforcing Speed correctly.	Transponder with Cutover Message installed in incorrect location.	IB	SR_22 SR_142	Mitigated	System Safety	IE	
HL- 262	Railroad	SHA-216	Unsafe switch Movement MBS Territory	Unsafe switch Movement MBS Territory	IB	SR_141	Mitigated	System Safety	ID	
HL- 615	Onboard	SHA-215	ACSES II train location incorrect In ABS Territory	Incorrect train location calculated from incorrect front of train offsets programmed into the Onboard.	IC	SR_203 SR_394	Closed	Onboard Safety	ID	ABS / CMB
HL- 614	Onboard	SHA-214	ACSES II train location incorrect In ABS Territory	Failure of Onboard to receive Transponder Data	IC	SR_388	Closed	Onboard Safety	ID	ABS / CMB

[redacted]

HL- 613	Onboard	SHA-213	ACSES II not enforcing Speed correctly. In ABS Territory	Failure of Onboard to process TSR data correctly	IC	SR_139 SR_509 SR_510	Closed	Onboard Safety	ID	ABS / CMB
HL- 319	Onboard	SHA-21	ACSES II not enforcing Speed correctly.	Train Engineer fails to follow the procedure during train mission failure	IC	SR_330	Mitigated	System Safety	IE	
HL- 611	Onboard	SHA-208	ACSES II not enforcing Speed correctly. In ABS Territory	Failure of Onboard to receive Transponder Data	IC	SR_388 SR_478	Closed	Onboard Safety	ID	ABS / CMB
HL- 610	Onboard	SHA-207	ACSES II not enforcing Speed correctly. In ABS Territory	Failure of Onboard to receive speed data	IC	SR_11	Closed	Onboard Safety	ID	ABS / CMB
HL- 261	Onboard	SHA-206	Wrong train type allowed to proceed through ESA tunnel.	Onboard receives incorrect data from the Transponder.	IC	SR_140	Mitigated	System Safety	IE	
HL- 260	Onboard	SHA-205	Wrong train type allowed to proceed through ESA tunnel.	Onboard computer failure	IC	SR_139	Closed	Onboard Safety	IE	
HL- 259	Transponder	SHA-204	Wrong train type allowed to proceed through ESA tunnel.	Transponder failure prevents Onboard from getting route dependent speed restriction.	IB	SR_138	Closed	System Safety	IE	
HL- 258	Transponder	SHA-203	Wrong train type allowed to proceed through ESA tunnel.	Transponder not programmed with Route dependent Speed restriction	IB	SR_89 SR_432	Closed	System Safety	IE	
HL- 256	Transponder	SHA-201	Train violates a home signal after a turnback.	Transponder at a turnback station does not have turnback packet.	IB	SR_89 SR_432	Closed	System Safety	IE	
HL- 255	Transponder	SHA-200	Train violates a home signal after a turnback.	Transponder location not sufficient to allow last Onboard to clear the transponder.	IB	SR_36	Closed	System Safety	IE	
HL- 318	Onboard	SHA-20	ACSES II not enforcing Speed correctly.	Failure between Onboard and Train ACSES cut out switch	IC	SR_196	Closed	Onboard Safety	IE	
HL- 254	Transponder	SHA-199	Train violates a home signal after a turnback.	Train location in platform did not allow last Onboard to clear transponder location	IB	SR_135 SR_136	Closed	System Safety	ID	
HL- 253	Comms	SHA-198	Train violates a work zone in an Ad Railroad.	Radio failure near Adjacent Railroad Boundary.	IB	SR_133 SR_134	Mitigated	System Safety	IE	
HL- 609	Office	SHA-197	Train violates a work zone in an Ad Railroad.	Failure of Local Office Server	IB	SR_392 SR_393	Closed	Railroad	IE	

HL- 381	Office	SHA-196	Train violates a work zone in an Ad Railroad.	Failure of Adjacent Office Server	IB		SR_55 SR_392	Closed	Railroad	ID	Point TSR will be at MAS Speed.
HL- 380	Comms Office Railroad	SHA-195	Train violates a work zone in an Ad Railroad.	Communication failure between Local and Adjacent Office Server	IB		SR_229 SR_230 SR_231	Mitigated	System Safety	IE	
HL- 608	Transponder	SHA-194	Transponder Fails to respond to scanner and provide data to train.	Transponder installation causes the air gap between the scanner and transponder to be less than 9 in or more than 13 in.	IB		SR_90 SR_390 SR_391	Closed	Onboard Safety	IE	
HL- 607	Onboard	SHA-193	Transponder Fails to respond to scanner and provide data to train.	EMI/EMC prevents transponder form responding to scanner.	IC		SR_389 SR_427	Closed	Transponder Safety	IE	
HL- 606	Onboard	SHA-192	Transponder Fails to respond to scanner and provide data to train.	Scanner in Onboard fails	IC		SR_388	Closed	Onboard Safety	IE	
HL- 605	Onboard	SHA-191	Transponder Fails to respond to scanner and provide data to train.	Transponder Failure prevents Onboard from getting Transponder Data	IC		SR_388	Closed	Onboard Safety	IE	
HL- 604	Onboard	SHA-190	Office to Onboard communication Failure	New TSR does not reach Onboard due to communication failure.	IC		SR_386 SR_387	Closed	Onboard Safety	IE	
HL- 317	Onboard	SHA-19	ACSES II not enforcing Speed correctly.	Failure of the ACSES cut out switch to detect an ACSES cut out	IC		SR_196 SR_197	Closed	Onboard Safety	IE	
HL- 603	RWPS	SHA-189	Fire	ACSES II equipment provides inadequate cooling or ventilation.	IB		SR_385 SR_463	Closed	RWPS Safety	IE	
HL- 602	Transponder	SHA-188	Fire	ACSES II equipment provides inadequate cooling or ventilation.	IB		SR_384	Closed	Transponder Safety	IE	
HL- 601	Comms	SHA-187	Fire	ACSES II equipment provides inadequate cooling or ventilation.	IB		SR_383	Closed	Comms Safety	IE	
HL- 600	Office	SHA-186	Fire	ACSES II equipment provides inadequate cooling or ventilation.	IB		SR_382	Closed	Office Safety	IE	
HL- 599	WIU	SHA-185	Fire	ACSES II equipment provides inadequate cooling or ventilation.	IB		SR_381	Closed	WIU Safety	IE	

HL- 598	Onboard	SHA-184	Fire	ACSES II equipment provides inadequate cooling or ventilation.	IC		SR_380	Closed	OBC Safety	IE	
HL- 379	Onboard WIU Office RWPS Transponder Comms	SHA-183	Fire	ACSES II equipment provides inadequate cooling or ventilation.	IC		SR_227 SR_228	Mitigated	System Safety	IE	Manual Link Neede
HL- 597	RWPS	SHA-182	Electrocution - Maint	ACSES II equipment provides inadequate maintenance procedures.	IIB		SR_378 SR_379	Closed	RWPS Safety	IIE	Manual Link Required
HL- 596	Transponder	SHA-181	Electrocution - Maint	ACSES II equipment provides inadequate maintenance procedures.	IIB		SR_412	Closed	Transpodner Safety	IIE	Manual Link Required
HL- 595	Comms	SHA-180	Electrocution - Maint	ACSES II equipment provides inadequate maintenance procedures.	IIB		SR_376 SR_377	Closed	Comms Safety	IIE	Manual Link Required
HL- 498	Onboard	SHA-18	ACSES II not enforcing Speed correctly.	Failure of Onboard to receive ACSES cut out input data	IC		SR_360	Closed	Onboard Safety	ID	Link to Instal and maintenance manua
HL- 594	Office	SHA-179	Electrocution - Maint	ACSES II equipment provides inadequate maintenance procedures.	IIB		SR_374 SR_375	Closed	Office Safety	IIE	Manual Link Required
HL- 593	WIU	SHA-178	Electrocution - Maint	ACSES II equipment provides inadequate maintenance procedures.	IIB		SR_373	Closed	WIU Safety	IIE	
HL- 378	Onboard WIU Office RWPS Transponder Comms	SHA-177	Electrocution - Maint	ACSES II equipment provides inadequate maintenance procedures.	IIC		SR_226 SR_377	Closed	System Safety	IIE	Manual Link Neede
HL- 592	Office	SHA-176	Radiation	ACSES II equipment accessible to passengers in public areas	IIB		SR_221 SR_227	Closed	Onboard Safety	IIE	
HL- 591	Transponder	SHA-175	Radiation	ACSES II equipment accessible to passengers in public areas	IIB		SR_371 SR_372	Closed	Transponder Safety	IIE	
HL- 377	Comms	SHA-174	Radiation	ACSES II equipment accessible to passengers in public areas	IIB		SR_224 SR_225	Closed	Comms Safety	IIE	

[redacted]

HL- 590	Office	SHA-173	Radiation	ACSES II equipment accessible to passengers in public areas	IIB	SR_369 SR_370 SR_490	Closed	Office Safety	IIE	
HL- 589	WIU	SHA-172	Radiation	ACSES II equipment accessible to passengers in public areas	IIB	SR_221 SR_367 SR_368	Closed	System Safety	IIE	
HL- 376	Onboard	SHA-171	Radiation	ACSES II equipment accessible to passengers in public areas	IIC	SR_221 SR_222 SR_223	Closed	Onboard Safety	IIE	
HL- 588	Onboard	SHA-170	Staff struck by Train - Onboard receives TSR with higher speed then intended	Failure of Onboard to process Transponder data correctly	IC	SR_139	Closed	Onboard Safety	IE	
HL- 316	Onboard	SHA-17	ACSES II not enforcing Speed correctly.	Failure of Onboard to receive ACSES cut out input data	IC	SR_196	Closed	System Safety	IE	
HL- 587	Office	SHA-169	Staff struck by Train - Onboard receives TSR with higher speed then intended	RWPS Failure causes TSR Request Error	IB	SR_129	Mitigated	Office Safety	ID	
HL- 586	Office	SHA-168	Staff struck by Train - Onboard receives TSR with higher speed then intended	Failure of Office to process Onboard Message correctly	IB	SR_363	Closed	Office Safety	IE	
HL- 585	Onboard	SHA-167	Staff struck by Train - Onboard receives TSR with higher speed then intended	Failure of Onboard to process Transponder data correctly	IC	SR_478	Closed	Onboard Safety	IE	
HL- 582	Onboard	SHA-164	Staff struck by Train	Failure of Onboard to receive Transponder Data	IC	SR_388	Canceled	Onboard Safety	IE	Duplcate of HL-573
HL- 581	Onboard	SHA-163	Staff struck by Train	Failure of Onboard to process Transponder data correctly	IC	SR_139	Canceled	Onboard Safety	IE	Duplcate of HL 572
HL- 580	Onboard/ Onboard-Speed Sensor	SHA-162	Staff struck by Train	Failure of Onboard to receive speed data	IC	SR_11	Canceled	Onboard Safety	IE	Duplcate of HL 571
HL- 579	Onboard/ Onboard-Speed Sensor	SHA-161	Staff struck by Train	Failure of Onboard to receive speed data	IC	SR_11	Canceled	Onboard Safety	IE	Duplcate of HL 571
HL- 578	Onboard	SHA-160	Staff struck by Train	Failure of Onboard to process TSR data correctly	IC	SR_139 SR_509 SR_510	Closed	Onboard Safety	IE	
HL- 315	Onboard	SHA-16	ACSES II not enforcing Speed correctly.	Onboard incorrectly process the ACSES cut out input data	IC	SR_11	Closed	System Safety	IE	
HL- 575	Onboard	SHA-157	Staff struck by Train	Failure of Onboard to receive ACSES cut out input data	IC	SR_360	Mitigated	Onboard Safety	ID	Duplate of HL 574
HL- 574	Onboard	SHA-156 SHA-157	Staff struck by Train	Failure of Onboard to receive ACSES cut out input data	IC	SR_196	Closed	Onboard Safety	IE	Manual Link Required

HL- 573	Onboard	SHA-155 SHA-164	Staff struck by Train	Failure of Onboard to receive Transponder Data	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 572	Onboard	SHA-154 SHA-163	Staff struck by Train	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 571	Onboard/ Onboard- Speed Sensor	SHA-153 SHA-161 SHA-162	Staff struck by Train	Failure of Onboard to receive speed data	IC	SR_11	Closed	Onboard Safety	IE	
HL- 570	Railroad	SHA-152	ACSES II Train Derails on a curve	Incorrect Speed Data submitted for entry to the database	IB	SR_366 SR_506	Closed	Railroad	IE	
HL- 314	Railroad	SHA-15	ACSES II not enforcing Speed correctly.	Failure of ATC to enforce Track Speed	IB	SR_195 SR_505 SR_506	Closed	Railroad	IE	
HL- 567	Onboard	SHA-149	ACSES II Train Derails on a curve	Failure of Onboard to receive Transponder Data	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 566	Onboard	SHA-148	ACSES II Train Derails on a curve	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 565	Onboard/ Onboard- Speed Sensor	SHA-147	ACSES II Train Derails on a curve	Failure of Onboard to receive speed data	IC	SR_11	Canceled	Onboard Safety	IE	Duplcate of HL 564
HL- 564	Onboard/ Onboard- Speed Sensor	SHA-146 SHA-147	ACSES II Train Derails on a curve	Failure of Onboard to receive speed data	IC	SR_11	Closed	Onboard Safety	IE	
HL- 375	Onboard	SHA-145	ACSES II Train Derails on a curve	Failure of Onboard to process TSR data correctly	IC	SR_139	Closed	Onboard Safety	IE	
HL- 374	Onboard	SHA-143	ACSES II Train Derails on a curve	Failure of Onboard to receive Train Type input data	ICB	SR_199 SR_357	Closed	Onboard Safety	IE	
HL- 562	Onboard	SHA-142	ACSES II Train Derails on a curve	Failure of Onboard to receive ACSES cut out input data	IC	SR_360	Mitigated	Onboard Safety	ID	Manual Link Required
HL- 373	Onboard	SHA-141	ACSES II Train Derails on a curve	Failure of Onboard to receive ACSES cut out input data	IC	SR_196	Closed	Onboard Safety	IE	

HL- 372	Onboard	SHA-140	ACSES II Train Derails on a curve	Failure of Onboard to receive Transponder Data	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 313	Transponder	SHA-14	ACSES II not enforcing Speed correctly.	Incorrect track speed defined due to data corruption during programming of Transponder Memory	IB	SR_193 SR_194	Closed	System Safety	IE	
HL- 371	Onboard	SHA-139	ACSES II Train Derails on a curve	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570 SR_571	Closed	System Safety	IE	
HL- 370	Onboard	SHA-138	ACSES II Train Derails on a curve	Failure of Onboard to receive speed data	IC	SR_11 SR_506	Closed	System Safety	IE	
HL- 561	Railroad	SHA-137	ACSESS II Train derails on a hand thrown switch	System detects switch opening but can not stop train in time.	IB	SR_365	Mitigated	Railroad	ID	
HL- 560	Railroad	SHA-136	ACSESS II Train derails on a hand thrown switch	System detects switch opening but can not stop train in time.	IB	SR_364	Mitigated	Railroad	IE	
HL- 559	Onboard	SHA-135	ACSES II Train derails on a hand switch thrown in ATC (ASC, ABS or CMB)	Failure of Onboard to receive Transponder Data	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 558	Onboard	SHA-134	ACSES II Train derails on a hand switch thrown in ATC (ASC, ABS or CMB)	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 557	Onboard	SHA-132	ACSES II Train derails on switch	Failure of Onboard to receive Transponder Data	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 556	Onboard	SHA-131	ACSES II Train derails on switch	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570 SR_571	Closed	Onboard Safety	IE	
HL- 312	Transponder	SHA-13	ACSES II not enforcing Speed correctly.	Failure of TopoDB to define correct placement of Transponder	IB	SR_22 SR_324	Closed	System Safety	IE	

HL- 553	Onboard	SHA-128	ACSES II Train derails on switch	Failure of Onboard to receive Transponder Data	IC	SR_478 SR_570 SR_571	Closed	System Safety	IE	
HL- 552	Onboard	SHA-127	ACSES II Train derails on switch	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570	Closed	Onboard Safety	IE	
HL- 551	Onboard/ Onboard-Speed Sensor	SHA-126	ACSES II Train derails on switch	Failure of Onboard to receive speed data	IC	SR_11	Canceled	Onboard Safety	IE	duplicate of 550 canceled
HL- 550	Onboard/ Onboard-Speed Sensor	SHA-125 SHA-126	ACSES II Train derails on switch	Failure of Onboard to receive speed data	IC	SR_11	Closed	Onboard Safety	IE	
HL- 549	Office	SHA-124	ACSES II Train derails on switch	Failure of Office database to define correct TSR for work areas	IB	SR_22 SR_394 SR_507	Closed	Office Safety	IE	
HL- 548	Office	SHA-123	ACSES II Train derails on switch	Failure of Office database to define correct TSR	IB	SR_22 SR_507	Closed	System Safety	IE	
HL- 369	Onboard	SHA-122	ACSES II Train derails on switch	Failure of Onboard to process TSR data correctly	IC	SR_139	Closed	System Safety	IE	
HL- 311	Onboard	SHA-12	ACSES II not enforcing Speed correctly.	Failure of Onboard to receive Transponder Data	IC	SR_388	Closed	System Safety	IE	
HL- 545	Onboard	SHA-119	ACSES II Train derails on switch	Failure of Onboard to receive ACSES cut out input data	IC	SR_360	Mitigated	Onboard Safety	ID	Manual Link Required
HL- 544	Onboard	SHA-118	ACSES II Train derails on switch	Failure of Onboard to receive ACSES cut out input data	IC	SR_196	Closed	Onboard Safety	IE	
HL- 543	Onboard	SHA-117	ACSES II Train derails on switch	Failure of Onboard to receive Transponder Data	IC	SR_388	Closed	Onboard Safety	IE	
HL- 542	Onboard	SHA-116	ACSES II Train derails on switch	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570	Closed	Onboard Safety	IE	
HL- 368	Onboard	SHA-115	ACSES II Train derails on switch	Failure of Onboard to receive speed data	IC	SR_11 SR_506	Closed	System Safety	IE	
HL- 541	Office	SHA-114	Highway crossing warning system fails	EIC Failure causes TSR Request error	IB	SR_129	Mitigated	Office Safety	ID	Coverage of LIRR PTCIP Hazard 9B - Train to Road Vehicle Collilsion - H'way activiation failure

HL- 540	Office	SHA-113	Highway crossing warning system fails	Failure of Office to process Onboard Message correctly	IB	SR_363	Closed	Office Safety	IE	Coverage of LIRR PTCIP Hazard 9B - Train to Road Vehicle Collilsion - H'way activiation failure
HL- 539	Onboard	SHA-112	Highway crossing warning system fails	Failure of Onboard to process Transponder data correctly	IC	SR_478 SR_570 SR_571	Closed	Office Safety	IE	Coverage of LIRR PTCIP Hazard 9B - Train to Road Vehicle Collilsion - H'way activiation failure
HL- 367	Railroad	SHA-111	Highway crossing warning system fails	Operation and Maintenance staff fail to respond to reputable reports of highway arming system failure	IB	SR_155	Mitigated	System Safety	ID	
HL- 366	Transponder, Comms	SHA-110	Onboard, WIU, and Transponder Equipment must be maintained so as to not foul train movement	Transponder and Radio Equipment is maintained such that if fouls train movement	IB	SR_220	Closed	Transponder Safety	IE	
HL- 310	Transponder	SHA-11	ACSES II not enforcing Speed correctly.	Failure of Transponder database to define correct ACSES Data	IB	SR_22 SR_324 SR_537 SR_549	Closed	System Safety	IE	
HL- 365	Onboard	SHA-109	Onboard, WIU and Transponder Equipment must be maintained so as to not foul train movement	Onboard Equipment is maintained such that it fouls train movement	IC	SR_15	Closed	Onboard Safety	IE	
HL- 364	Transponder, Comms	SHA-108	Onboard, WIU, and Transponder Equipment must be located so as to not foul train movement	Transponder and Radio Equipment is installed such that if fouls train movement	IB	SR_220	Closed	Transponder Safety	IE	
HL- 363	Onboard	SHA-107	Onboard, WIU, and Transponder Equipment must be located so as to not foul train movement	Onboard Equipment is installed such that it fouls train movement	IC	SR_15	Closed	Onboard Safety	IE	
HL- 362	Office	SHA-106	Onboard Receives incorrect TSR	Railroad Network Failure between Control Centers causes both Office's to be controlling.	IB	SR_118 SR_119	Mitigated	Office Safety	IE	

[redacted]

HL- 361	Office	SHA-105	Onboard Receives incorrect TSR	Dispatcher Error causes TSR Request error	IB	SR_128 SR_129	Mitigated	Office Safety	ID	To reduce system Risk noted that Paper TSR process is not be abondanded and that this process can be used to check the TSRs within the system to detect manual entry errors as well as UIS errors.
HL- 360	Office	SHA-104	Onboard Receives incorrect TSR	EIC Failure causes TSR Request error	IB	SR_128 SR_129	Mitigated	Office Safety	ID	To reduce system Risk noted that Paper TSR process is not be abondanded and that this process can be used to check the TSRs within the system to detect manual entry errors as well as UIS errors.
HL- 359	Office	SHA-103	Onboard Receives incorrect TSR	UISS Failure causes TSR Request Error	IB	SR_128 SR_129	Mitigated	Office Safety	ID	To reduce system Risk noted that Paper TSR process is not be abondanded and that this process can be used to check the TSRs within the system to detect manual entry errors as well as UIS errors.
HL- 538	Office	SHA-101	Onboard Receives incorrect TSR	Failure of Office to process Onboard Message correctly	IB	SR_217	Closed	Office Safety	IE	
HL- 537	Office	SHA-100	Onboard Receives incorrect TSR	Office incorrectly processes TSR Request and/or Onboard TSR message.	IB	SR_32 SR_472	Closed	Office Safety	IE	
HL- 309	Transponder	SHA-10	ACSES II not enforcing Speed correctly.	Failure of TopoDB to define Transponder Installation correctly for the territory	IB	SR_22 SR_468 SR_469	Closed	System Safety	IE	
HL- 308	Onboard	SHA-09	ACSES II not enforcing Speed correctly.	Failure of Onboard to process Transponder data correctly	IC	SR_11	Closed	System Safety	IE	
HL- 307	Onboard	SHA-08	ACSES II not enforcing Speed correctly.	Engineer accelerates before train passes TSR locations.	IC	SR_190 SR_191	Closed	System Safety	IE	
HL- 306	Onboard	SHA-07	ACSES II not enforcing Speed correctly.	Service Brake Interface Failure	IC	SR_189	Closed	Onboard Safety	IE	

HL- 497	Onboard	SHA-06	ACSES II not enforcing Speed correctly.	The speed sensor incorrectly reads the speed	IC		SR_102 SR_359	Closed	Onboard Safety	ID	Link to Instal and maintenance manua
HL- 496	Onboard	SHA-05	ACSES II not enforcing Speed correctly.	Failure of the speed sensor to detect speed	IC		SR_359	Mitigated	Onboard Safety	ID	Link to Instal and maintenance manual
HL- 305	Onboard	SHA-04	ACSES II not enforcing Speed correctly.	Failure of the speed sensor to detect speed	IC		SR_187 SR_188	Closed	Onboard Safety	IE	No SLR Req.
HL- 304	Onboard	SHA-03	ACSES II not enforcing Speed correctly.	Failure of Onboard to receive speed data	IC		SR_11	Closed	System Safety	IE	
HL- 303	Onboard	SHA-02	ACSES II not enforcing Speed correctly.	Onboard incorrectly processes the speed data	IC		SR_139 SR_505 SR_506 SR_572	Closed	Onboard Safety	IE	
HL- 302	Onboard	SHA-01	ACSES II not enforcing Speed correctly.	Onboard Main Computer Failure	IC		SR_139	Closed	Onboard Safety	IE	
HL- 684	STS - Adj STS	SHA_353	ACSES train fails to enforce Vitally scheduled TSR after crossing boundary	Vitally scheduled TSR are not sent to Adj STS until enforcement occurs in MTA and there is a chance that train crosses with prior list without Scheudled TSR.	IC		SR_133 SR_575	Mitigated	Railroad	ID	
HL- 683	Onboard	SHA_352	ACSES train failes to enforce Temporary Speed Restrictions	Location of train exit track unknown so Onboard fails to enforce correct Temprorary Speed Restrictions	IC		SR_567	Mitigated	Onboard WIU	IE	Failure of mesage will enforce TSR on all tracks
HL- 681	Railroad	SHA_350	Tenant train authorized for interlocking by ACSES based on prior signal data.	Tenant trains not compliant with back to back ACSES design allowed to operate in territory with back to back signal. (Failure occurs after tenant train losses radio commuication in ACSES (authorized by ATC for PTS in back to back area)	ID		SR_47	Mitigated	Railraod	IE	
HL- 671	Transponder	SHA_301	Maintainer or Track worker falls on track.	Maintenance Error	IIIC		SR_558	Mitigated	Transponder Safety	IIID	
HL- 477	Operations Office	SHA_288 PHA-76	Non ACSES II train runs afoul of an ACSES II train.	Non ACSES II train overruns a temporal separation	IC		SR_339 SR_340	Mitigated	Railroad	IE	

Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

System Interface Hazard Analysis

CDRL 2-131-20

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Jason Weighley System Safety Engineer	Jason W Weighley	Jason W Weighley 2019.07.17 07:58:13 -04'00'
Verified:	Aaron Graham System Safety Engineer	Aaron Graham	Aaron Graham 2019.07.17 13:28:48 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.07.17 15:40:37 -04'00'
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group	Phil Magloire	Phil Magloire 2019.07.17 15:33:03 -04'00'
BT/SRA Review:	NA		
BT/SRA Review:	NA		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3035828

Effective Date:	Revision:	Language:
2019-07-17	_D	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2014-09-30	First issue
_A	2015-10-02	Submitted for PDR. Aligned with Subsystem IHAs for PDR
-A1	2016-09-30	Updated to resolve Customer comments
A2	2017-06-13	Update as per RR comments
A3	2017-09-01	Update as per RR Comments
A4	2017-11-27	Further updates, as per another round of RR comments.
A5	2018-01-23	Updated as per second round of RR comments
_B	2018-02-23	Updated as per RR comments
B1	2018-04-06	Updated as per RR comments
_B2	2018-04-20	Updated to address wording of ADU Flahing red mitigation, removed TBD and corrected severity of Train Engineer interface
_B3	2018-05-17	Updated as per additional comments from RR.
_B4	2018-07-10	Updated as per additional comments from RR.
_C	2018-07-18	Updated for formal release after working group approval
_D	2019-07-17	Updated for PTCSP comments

Table of Contents

Section	Subject	Page
1	**Executive Summary**	9
2	**Introduction**	9
2.1	**Compliance Matrix**	9
2.2	**Reference Documents**	11
2.3	**Glossary**	13
3	**ACSES II System Interfaces**	14
3.1	**System Interfaces – Definitions**	15
3.1.1	Internal Interfaces	16
3.1.1.1	Communications to Onboard	16
3.1.1.2	Communications to Wayside	16
3.1.1.3	Communications to Office	16
3.1.2	External Interfaces	16
3.1.2.1	Onboard External Interfaces	16
3.1.2.2	Wayside External Interfaces	16
3.1.2.3	Office External Interfaces	16
3.1.3	User Interfaces	16
3.1.3.1	Office and Maintenance User Interfaces	16
3.1.3.2	Onboard User Interfaces	17
3.2	**Users**	17
3.2.1	Train Engineer	17
3.2.2	Dispatcher(s)	17
3.2.2.1	Dispatcher	17
3.2.2.2	Chief Dispatcher / Assistant Chief Dispatcher	18
3.2.3	Employee-In-Charge	18
3.2.4	Maintenance Staff	18
3.2.5	System Administrators	18
3.2.6	ACSES II System Maintainers	19
3.3	**Analysis Methodology**	19
3.4	**Risk Assessment Classification Frame Work**	20
4	**ACSES II System Internal Interfaces – Attributes**	23
4.1	**Communications to Onboard**	23
4.1.1	OBC to WIU	23
4.1.1.1	Physical Attribute	24
4.1.1.2	Functional Attribute	24
4.1.1.3	Loss of Interface	24
4.1.1.4	Corrupted Interface	25
4.1.2	OBC to STS – Interface I	25
4.1.2.1	Physical Attribute	25

4.1.2.2 Functional Attribute 25
4.1.2.3 Information Attribute 26
4.1.2.4 Loss of Interface 26
4.1.2.5 Incorrect Information in Interface 26
4.1.3 OBC to STS – Interface II 26
4.1.3.1 Physical Attribute 26
4.1.3.2 Functional Attribute 27
4.1.3.3 Information Attribute 27
4.1.3.4 Loss of Interface 27
4.1.3.5 Incorrect Data in Interface 27
4.1.4 Transponder to OBC 27
4.1.4.1 Physical Attribute 28
4.1.4.2 Functional Attribute 28
4.1.4.3 Information Attribute 28
4.1.4.4 Loss of Interface 28
4.1.4.5 Incorrect Information in Interface 28

4.2 Communications to Wayside 29
4.2.1 WIU to Office 29
4.2.1.1 Physical Attribute 29
4.2.1.2 Functional Attribute 29
4.2.1.3 Information Attribute 29
4.2.1.4 Loss of Interface 29
4.2.1.5 Incorrect Information in Interface 30
4.2.2 WIU to OBC 30
4.2.2.1 Physical Attribute 30
4.2.2.2 Functional Attribute 30
4.2.2.3 Information Attribute 30
4.2.2.4 Loss of Interface 31
4.2.2.5 Incorrect Data in Interface 31

4.3 Communications to Office 31
4.3.1 STS to RGS 31
4.3.1.1 Physical Attribute 31
4.3.1.2 Functional Attribute 32
4.3.1.3 Information Attribute 32
4.3.1.4 Loss of Interface 32
4.3.1.5 Incorrect Data in Interface 33
4.3.2 RWPS to STS 33
4.3.2.1 Physical Attribute 33
4.3.2.2 Functional Attribute 33
4.3.2.3 Information Attribute 34
4.3.2.4 Loss of Interface 34
4.3.2.5 Incorrect Data in Interface 34

5 ACSES II System External Interfaces – Attributes 34

5.1 Onboard External Interfaces 35
5.1.1 OBC to Vehicle Interface 35

5.1.1.1 Physical Attribute 35
5.1.1.2 Functional Attribute 35
5.1.1.3 Information Attribute 35
5.1.1.4 Loss of Interface 35
5.1.1.5 Incorrect Information in Interface 35
5.1.2 OBC to (Existing) ATC Interface 35
5.1.2.1 Physical Attribute 35
5.1.2.2 Functional Attribute 36
5.1.2.3 Information Attribute 36
5.1.2.4 Loss of Interface 36
5.1.2.5 Incorrect Information in Interface 36
5.1.3 OBC to Brake Interface 36
5.1.3.1 Physical Attribute 36
5.1.3.2 Functional Attribute 36
5.1.3.3 Information Attribute 36
5.1.3.4 Loss of Interface 36
5.1.3.5 Incorrect Information in Interface 37
5.1.4 OBC to Speed Sensor 37
5.1.4.1 Physical Attribute 37
5.1.4.2 Functional Attribute 37
5.1.4.3 Information Attribute 37
5.1.4.4 Loss of Interface 37
5.1.4.5 Incorrect Information in Interface 37
5.1.5 OBC to Decelerometer 38
5.1.5.1 Physical Attribute 38
5.1.5.2 Functional Attribute 38
5.1.5.3 Information Attribute 38
5.1.5.4 Loss of Interface 38
5.1.5.5 Incorrect Information in Interface 39

5.2 Office External Interfaces 39
5.2.1 Office to Adjacent RR STS Server 39
5.2.1.1 Physical Attribute 39
5.2.1.2 Functional Attribute 39
5.2.1.3 Information Attribute 39
5.2.1.4 Loss of Interface 40
5.2.1.5 Incorrect Data in Interface 40
5.2.2 IXL to WIU 40
5.2.2.1 Physical Attribute 40
5.2.2.2 Functional Attribute 40
5.2.2.3 Information Attribute 40
5.2.2.4 Loss of Interface 40
5.2.2.5 Incorrect Data in Interface 40
5.2.3 GPS to GCS 41
5.2.3.1 Physical Attribute 41
5.2.3.2 Functional Attribute 41
5.2.3.3 Information Attribute 41
5.2.3.4 Loss of Interface 41

5.2.3.5 Incorrect Data in Interface 41
5.2.4 GPS to BCM 41
5.2.4.1 Physical Attribute 41
5.2.4.2 Functional Attribute 41
5.2.4.3 Information Attribute 41
5.2.4.4 Loss of Interface 42
5.2.4.5 Incorrect Data in Interface 42

6 ACSES II System User Interfaces – Attributes 42

6.1 Office and Maintenance User Interfaces 42
6.1.1 Dispatcher to UISS 42
6.1.1.1 Physical Attribute 42
6.1.1.2 Functional Attribute 42
6.1.1.3 Loss of Interface 42
6.1.1.4 Incorrect Data in Interface 42
6.1.2 EIC to RWPS (Employee-In-Charge Interface) 43
6.1.2.1 Physical Attribute 43
6.1.2.2 Functional Attribute 43
6.1.2.3 Loss of Interface 43
6.1.2.4 Incorrect Data in Interface 43
6.1.3 Maintenance Staff to WIU 43
6.1.3.1 Physical Attribute 43
6.1.3.2 Functional Attribute 43
6.1.3.3 Loss of Interface 43
6.1.3.4 Incorrect Data in Interface 44
6.1.4 Maintenance Staff to RWPS 44
6.1.4.1 Physical Attribute 44
6.1.4.2 Functional Attribute 44
6.1.4.3 Loss of Interface 44
6.1.4.4 Incorrect Data in Interface 44

6.2 Onboard User Interfaces 44
6.2.1 Train Engineer to ADU 44
6.2.1.1 Physical Attribute 44
6.2.1.2 Functional Attribute 44
6.2.1.3 Loss of Interface 45
6.2.1.4 Incorrect Data in Interface 45
6.2.2 Train Engineer to Ack 45
6.2.2.1 Physical Attribute 45
6.2.2.2 Functional Attribute 45
6.2.2.3 Loss of Interface 45
6.2.2.4 Incorrect Data in Interface 45
6.2.3 Train Engineer to PTS Push-Button 45
6.2.3.1 Physical Attribute 45
6.2.3.2 Functional Attribute 46
6.2.3.3 Loss of Interface 46
6.2.3.4 Incorrect Data in Interface 46

7 ACSES II System External Power Interfaces – Attributes 46

7.1 Power to Office 46
7.1.1 Power Interface To Office 46
7.1.1.1 Physical Attribute 46
7.1.1.2 Functional Attribute 46
7.1.1.3 Information Attribute 46

7.2 Power to Wayside 46
7.2.1 Power Interface to WIU 46
7.2.1.1 Physical Attribute 46
7.2.1.2 Functional Attribute 46
7.2.1.3 Information Attribute 47

8 Interface Hazard Analysis 48

8.1 Safety Requirement Management 48

8.2 Hazard Log Tracking 48
8.2.1 Interface Analysis Fields 48

9 Interface Hazard Analysis Table 49

10 Conclusions 65

List of Figures

Figure 1: Overview of ACSES II System 14
Figure 2: Interface between Subsystems 15
Figure 3: Onboard Computer to Wayside Interface Unit 24
Figure 4: Onboard to Safety Temporary Speed Restriction Server 25
Figure 5: Safety Temporary Speed Restriction Server to Wayside Communications Controller 26
Figure 6: Onboard to Transponder 27
Figure 7: Wayside Interface Unit to Network Management System 29
Figure 8: Wayside Interface Unit to Onboard Computer 30
Figure 9: Safety Temporary Speed Restriction Server to Railroad Gateway Server 31
Figure 10: Railway Worker Protection System to Safety TSR Server Subsystem 33

List of Tables

Table 1: Compliance Matrix 9
Table 2: Reference Documents 11
Table 3: Terms Specific to this Document 13
Table 4: Acronyms Specific to this Document 13
Table 5: Hazard Severity Classifications 20
Table 6: Hazard Probability Classifications 21
Table 7: Hazard Risk Assessment Matrix 22
Table 8: Hazard Risk Index (HRI) 22
Table 9: IHA matrix description 48
Table 10 System IHA Table 49
Table 11: The mitigations from the IHA analysis 65
Table 12: Safety Related Application Condition 76

1 Executive Summary

The Interface Hazard analysis covers interfaces external to the ACSES II System as well as interfaces between subsystems. Interfaces within each subsystem will be covered by an analysis for each subsystem.

The process followed was to analyze the external and internal interfaces between the external and internal interfaces to the ACSES II system. A complete description of the interfaces is provided in 3.1. For Each defined interface, the interface was examined to determine the impact to system operation for loss of the interface or incorrect data transmission. If the impact of interface was significant then mitigation was proposed by safety engineering and recorded in the hazard analysis table. The hazards raised by this analysis were then transferred to the Hazard Log and linked to appropriate Safety Requirements. The security of the wireless communication will be analyzed in the System Vulnerability Assessment (CDRL 2-137) and will not be covered in the analysis provided in this document.

The closure of each hazard in the Hazard Log process is handled within the System Product Safety Plan but a high level overview is provided in this document in section 8.1.

2 Introduction

This analysis covers interfaces external to the ACSES II system and interfaces between ACSES II subsystems. The interfaces were determined from an analysis of the System Architecture Drawing [3]. Each interface (direct and indirect) was analyzed to determine any hazards associated to loss of the interface, timing issues with the interface, required alarm notifications and safe default states to interface failures. This is documented in section 4.

A description of each subsystem to subsystem interface is provided as well as a reference to the design documentation that will provide the full details for each interface. The overall logical interfaces are analyzed for the failure modes and safe default states.

The subsystem interface will not focus on redundancy and assurance of information during redundancy as this is defined with the subsystem IHA analysis.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part 1	12.10.6.A	Interface Hazard Analysis	IHA to be performed by SI	3

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.6.B		The SI shall combine the subsystem IHAs into an overall system IHA for the ACSES system.	4,
	12.10.6.C.1		The IHA shall Address Physical, functional and all other interface attributes	4
	12.10.6.C2		The IHA shall Address loss or incorrect transfer of information between ACSES II Subsystems	4
	12.10.6.C.3		The IHA shall Address Timing issues associated with the transfer of information	4
	12.10.6.C.4		The IHA shall Address Redundancy management and assurance of information during redundancy handover	4
	12.10.6.C.5		The IHA shall Address required alarm notifications and safe default actions for interface failures.	4
	12.10.6.C.6		The IHA shall Address Handover of information between wayside and onboard	4
	12.10.6.C.7		The IHA shall Address Testing of interfaced subsystems to ensure correct operating of subsystems and overall system.	4
Vol 2 Part 1	9.3.H.5	Interface Hazard Analysis	IHA part of Hazard Identification Process	4

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624
[2]	Removed	
[3]	LIRR System Architecture drawing Package	3038055
[4]	System Description Document (CDRL 2-27)	3035724
[5]	System Product Safety Plan (CDRL 2-123-20)	3035815
[6]	Office Interface Control Document (CDRL 6-018)	3035958
[7]	MCM – OBC Interface Control Document	3040403
[8]	RWPS Interface Control Document (CDRL 2-225)	3035874
[9]	Transponder Interface Control Document (CDRL 4-002)	3035877
[10]	WIU Interface Control Document (CDRL 4-016)	3035890
[11]	Onboard Interface Control Document (CDRL 5-002)	3035903
[12]	ACSES II Message Description Document	3041417
[13]	Project Hazard Log (CDRL 2-126-20)	3035819
[14]	MIL-STD-882C, System Safety Program Requirements	MIL–STD-882C
[15]	AREMA, Communications and Signals Manual – 2009 Section Parts 16, 17, 21, and 23.	Revision 2001
[16]	CENELEC EN50126, Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)	EN50126: 1999
[17]	CENELEC Standard. Railway Applications – Communication, signaling and processing systems – Safety related electronic systems for signaling.	EN50129: 2003
[18]	Certifiable Items List (CDRL 2-125-20)	3035818
[19]	Office Subsystem Interface Hazard Analysis (CDRL 2-131-22)	3037428

Reference Number	Document Name	Identification Number
[20]	Transponder Subsystem Interface Hazard Analysis (CDRL 2-131-25)	3037434
[21]	COMMS Subsystem Interface Hazard Analysis (CDRL 2-131-23)	3037430
[22]	Onboard Interface Hazard Analysis (CDRL 2-131-21)	3037426
[23]	RWPS Interface Hazard Analysis (CDRL 2-131-26)	3037436
	Addenda to CDRL 6-018	
[24]	STS – UIS ICD (CDRL 6-018-001)	3034870
[25]	STS – WCC ICD (CDRL 6-018-002)	3038473
[26]	STS – RGS ICD (CDRL 6-018-003)	3038475
[27]	STS – DMS ICD (CDRL 6-018-004)	3038472
[28]	STS – NMS (CDRL 6-018-005)	3038471
[29]	UIS – DMS ICD (CDRL 6-018-006)	3044894
[30]	UIS – NMS ICD (CDRL 6-018-007)	3050288
[31]	UIS – RWPS (CDRL 6-018-008)	3044893
[32]	WCC – DMS ICD (CDRL 6-018-009)	3040410
[33]	WCC – NMS (CDRL 6-018-010)	3050289
[34]	RGS – DMS ICD (CDRL 6-018-011)	3046058
[35]	RGS – NMS (CDRL 6-018-012)	3050290
[36]	DMS – NMS (CDRL 6-018 Addendum)	3050287
[37]	BCM – WCC ICD (CDRL 6-018 Addendum)	3044047
[38]	Onboard Subsystem Description Document (SysDD)	3035902
	Review Records	
[39]	3035874_Rev___RWPS_ICDReview_Record	2014-9-19
[40]	3035890_Rev_B_WIUICDReview_Record_	2015-07-16
[41]	3040403_Rev_C_MMC-obc_ICDReview_Record	10/10/2017
[42]	STS_DMS_ICD Review Record	8/05/2015
[43]	STS_NMS_ICD Review Record	03/26/2016

Reference Number	Document Name	Identification Number
[44]	STS_RGS_ICD Review Record	02/02/2015
[45]	STS_UIS_ICD Review Record	08/21/2015
[46]	STS_WCC_ICD Review Record	08/05/2015

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in Table 3 and Table 4 respectively.

Table 3: Terms Specific to this Document

Term	Definition
Non-Safety Related	A classification of a product that has no safety implications
Stale	A message is detected as more than 42 seconds old.

Table 4: Acronyms Specific to this Document

Acronym	Definition
Adj	Adjacent
CRC	Cyclic Redundancy Code (72 bits)
ICD	Interface Control Documents
ISP	Internet Service Provider
PDR	PTC Data Radio
PIU	Portable Interface Unit
PTE	Portable Test Equipment
RCF	Radio Configuration Files
SRAC	Safety Related Application Condition
UIS	Redundant User Interface

3 ACSES II System Interfaces

ACSES II is a vital train control system that provides supplemental functionality to the existing railroad system in order to comply with FRA 49 CFR 236 subpart I functionality. The intention of ACSES II is to supplement the existing functionality of the ATC system in order to provide an FRA compliant system for PTC. Figure 1 provides a high-level illustration of the ACSES II system implementation and Figure 2 provides a high-level illustration of the ACSES II System interface between subsystems.

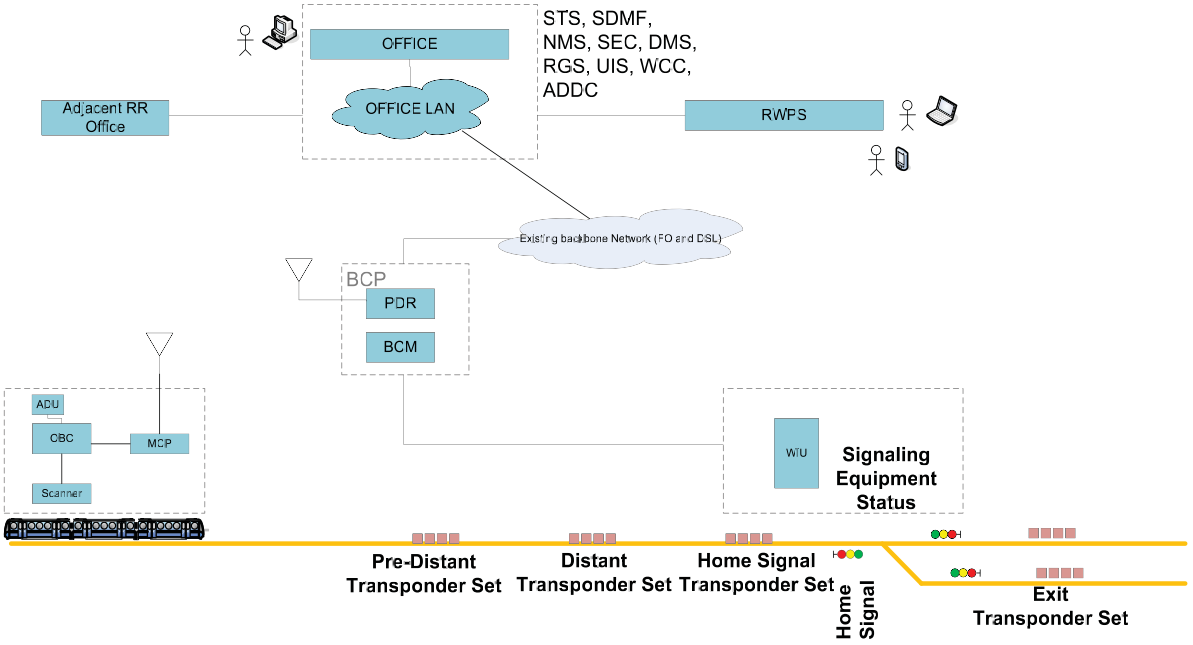


Figure 1: Overview of ACSES II System

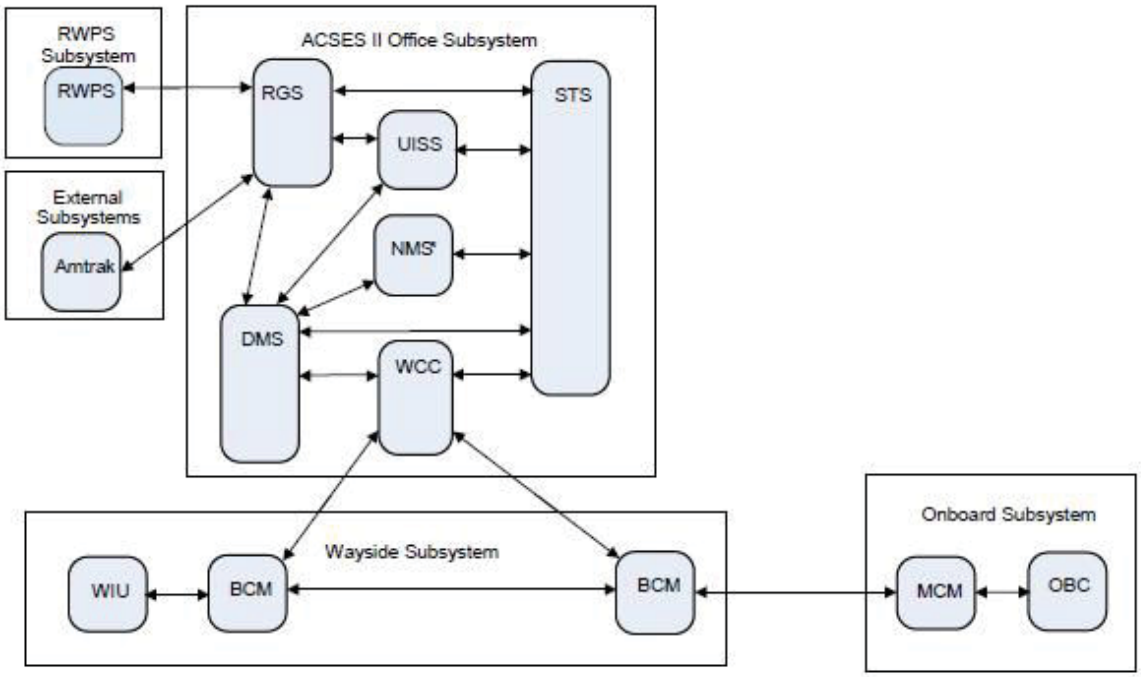


Figure 2: Interface between Subsystems

3.1 System Interfaces – Definitions

The Interface Hazard Analysis (IHA) analyzes each interface to the LIRR ACSES II System to identify the Hazards associated with the failure modes of each interface. Each interface description was reviewed in the SDD [4] and ICDs [6], [7], [8], [9], [10], [11] [12] to confirm the attributes of the interface.

The first attribute reviewed was the physical medium used to provide the interface. The second attribute reviewed in the design documentation for each interface was the system functionality performed by each interface. If a function identified in the CIL (2-125) and defined as being safety related was implemented by an interface, the interface was reviewed to determine if any hazard could arise from the loss of the interface, or if the data within the interface was corrupted without detection. The safety critical interfaces were also reviewed to determine what hazards could arise if a message arrived too early or late.

The design documentation was reviewed to determine the information passed on each interface that was not involved in system safety critical functionality. If the interface passes alarm data, an analysis of the system was performed to determine the impact on the system from the loss of the interface. The next analysis done was to determine if the interface is lost what safe default state the data from the interface should be assumed to prevent hazardous events.

3.1.1 Internal Interfaces

The Internal interfaces to the ACSES II System are defined below.

3.1.1.1 Communications to Onboard

- OBC (via MCM) to WIU (via BCM);
- OBC (via MCM) to STS Interface I (via RGS) and Interface II (via BCM); and,
- Transponder to OBC (via Transponder Antenna System).

3.1.1.2 Communications to Wayside

- WIU (via BCM) to Office (via WCC); and,
- WIU (via BCM) to OBC (via MCM), Interface I;
- WIU (via BCM / RGS) to OBC (via ISP Cell Network / MCM), Interface II.

3.1.1.3 Communications to Office

- STS (via RGS) to OBC (via ISP Cell Network);
- STS (via MCM) to OBC (via BCM) and,
- RWPS (via 220 MHz Radio) to STS (via RGS).

3.1.2 External Interfaces

The external interfaces to the ACSES II Systems are defined below.

3.1.2.1 Onboard External Interfaces

- OBC to Vehicle Interface (via ADU);
- OBC to (Existing) ATC Interface; and,
- OBC to Brake Interface.

3.1.2.2 Wayside External Interfaces

- WIU to IXL; and,
- GPS to BCM.

3.1.2.3 Office External Interfaces

- Office (via RGS) to Adjacent RR STS Server; and,
- GPS to GCS.

3.1.3 User Interfaces

The user interfaces to the ACSES II System are defined below.

3.1.3.1 Office and Maintenance User Interfaces

- Dispatcher(s) to UISS;
- EIC to RWPS (EIC Interface)

- Maintenance Staff to WIU;
- Maintenance Staff to NMS;
- Maintenance Staff to RWPS;
- System Administrator(s); and,
- ACSES II System Maintainer(s).

3.1.3.2 Onboard User Interfaces

- Train Engineer to ADU (Train Engineer Interface);
- Train Engineer to Acknowledge Button (Ack); and
- Train Engineer to PTS Push-Button (PB).

3.2 Users

The interfaces that exist outside of the system have not been evaluated as part of this analysis. For instance, the Train Engineer and Dispatcher will need to interface to perform their roles, but this is outside the scope of this analysis and is covered in the Operating Hazard Analysis. The OHA only covers the need of the operating rules and procedures. The Human Factor Analysis will need to determine if the interfaces provided allow the proper and safe implementation of those procedures on the system. If the mitigations indicate that users must interface, then operation procedures and experts should indicate how this interface will be made.

3.2.1 Train Engineer

The Train Engineer will directly interface with the system through the Onboard subsystem ADU and switch components. The ADU will provide the engineer with information needed to properly control the train speed. If the train engineer does not obey the speed curves, the ADU will provide a warning and indication of the pending intervention by the Onboard subsystem. The ADU will also provide important status information to the Train engineer. This status information will be used by the Train Engineer to determine the proper operating mode of the system.

This analysis will cover that the information on the ADU covers all information needed for the train engineer to perform his role. The Human Factors analysis will need to indicate if this information is properly displayed.

3.2.2 Dispatcher(s)

3.2.2.1 Dispatcher

The Dispatcher will interface to the UISS component of the Office subsystem to request the addition and removal of TSR's. The UISS will also be able to provide the current TSR status for an assigned area to each dispatcher. This analysis will cover that the information on the UIS covers all information needed for the dispatcher to perform his role. The Human Factors analysis will need to indicate if this information is properly displayed.

3.2.2.2 Chief Dispatcher / Assistant Chief Dispatcher

Reviews and approves TSR in the Select – Check – Execute process. Assigns territories to Dispatchers. The user interface for the Chief Dispatcher / Asst. Chief Dispatcher is identical to the UIS interface for the dispatcher with additional functionality.

This analysis will cover that the information on the UIS covers all information needed for the dispatcher to perform his role. The Human Factors analysis will need to indicate if this information is properly displayed.

3.2.3 Employee-In-Charge

The Employee-In-Charge will be able to request and remove TSR's for work zones through the Employee-In-Charge terminal components of the RWPS. The Employee-In-Charge terminal will also indicate active TSR's for an assigned area as well as the primary and secondary EIC's for those TSR's. This analysis will cover that the information on the UIS covers all information needed for the dispatcher to perform his role. The Human Factors analysis will need to indicate if this information is properly displayed.

3.2.4 Maintenance Staff

Maintenance staff will work through multiple components of the system to program and configure the components of the subsystem.

The Onboard subsystem has a Portable Interface Unit (PIU) that is used for downloading the OBC event recorder log files, uploading system updates, configuring the OBC, and general troubleshooting.

The Communications subsystem will provide tools for each component. The MCM has a portable diagnostic tool that is used for uploading system updates (such as MCM and RCF files). The MCM portable diagnostic tool must be directly connected to the diagnostic port on the MCM.

The PTC Data Radio (PDR) has a portable diagnostic tool used for configuring the data radio. The BRCM and BCM will have a portable diagnostic tool that is used for updating the software of these units. In addition, maintainers can remotely login to the MCM, BCM and PDR to review log files.

The transponders have a Portable Test Equipment (PTE) diagnostic tool for programming and verifying data within transponders.

This analysis will review the interfaces between the system/subsystems and the maintenance and the diagnostic tools listed above to determine any hazards associated with these interfaces.

3.2.5 System Administrators

This user may define new reports as needed for operations based on the data reported back by the ACSES system. This user may also add roles and users to the system as needed to support operations.

The interfaces for the System Administrator are not covered in this analysis.

3.2.6 ACSES II System Maintainers

Interfaces that allow troubleshooting and analysis of the system performance allow the system maintainer to find system errors and determine the maintenance to be performed.

The DMS will provide reports and the ability to playback data for the system maintainer to review system performance and determine the actions needed by maintenance staff. The ability to remotely review onboard event logs will also be available.

The analysis evaluates if hazards can arise from the use of the maintenance tools when setting parameters such as reprogramming after replacing a failed transponder or when uploading train configuration data into the onboard following an equipment replacement.

The interfaces for the System Administrator are not covered in this analysis.

3.3 Analysis Methodology

The Interface Hazard Analysis (IHA) was performed to identify and evaluate hazards between subsystems, and their potential effect on the overall ACSES II system safety and operation of the PTC system. The system IHA was generated by the System Safety Engineer. The IHA was reviewed by the subsystem lead engineers. The System IHA focused on the interfaces between the ACSES II subsystems and the external interfaces to the ACSES II system.

The analysis identified the cause and effect of possible independent, dependent and simultaneous failures that could present a hazardous condition. The analysis was also subjected to design review in order to verify that design modifications do not introduce new hazards or increase the risk from existing hazards.

For each interface reviews focused on the failures from the following:

- Loss or incorrect transfer of information
- Timing issues associated with the interfaces
- Required alarm notifications and safe default actions for interface failures.
- Handover of information between wayside and onboard.

The IHA includes applicable interfaces with Track and infrastructure, Line and Signal Controllers, etc.

The system architecture drawing [3] was reviewed to determine the interfaces between the subsystems. Each interface description was reviewed in the SDD[4] and ICD's [6], [7], [8], [9], [10], [11] [12] to confirm the attributes of the interface. A review log [39], [40], [41], [42], [43], [44], [45] and [46] was made for each interface for the review list above. Where this list showed a hazard, this was added to another table attached to this report. The hazard table at the back of this report was prepared in line with the Risk management assessment defined in the SPSP [5]. After review by the System Safety Engineer, subsystem safety engineers and the Subsystem leads the hazard table was added to the Project Hazard Log [13].

3.4 Risk Assessment Classification Frame Work

Throughout the product development lifecycle, risk assessment practices are applied to guide the implementation of mitigating actions to control or eliminate each identified hazard such that the risk introduced by each is acceptable. Risk assessment and management is a decision-making process consisting of evaluation and control of the severity and probability of a potentially hazardous event. As hazard analyses are performed, Bombardier will identify hazards that will require resolution through this mechanism.

The classification of severity for hazards will be based on the four categories from MIL-STD-882C [14] and AREMA section 17.3.5 [15] identified in Table 5 ranging from Category I (Catastrophic) to Category IV (Negligible). The severity classification assigned to each hazard will provide a qualitative indication of the worst-case consequences that could occur if the hazard is not eliminated or controlled.

Probability classifications will be based on the five categories from MIL-STD-882C [14] and AREMA section 17.3.5 [15] as shown in Table 6. These range from Category A (Frequent) to Category E (Improbable). The assigned probability will be based on the likelihood that a particular hazard and effect would occur in the planned life expectancy of the product. To assist in assigning the specific categories of probability, Table 6 shows definitions for both a specific individual item (i.e. a specific component of the system) as well as for the fleet or overall inventory of the system. The table also provides the Mean Time Between Events (MTBE) to guide the consistent application of the classifications. Note that since the probability categories are applied to hazards of all severities (even category IV), it is not appropriate to use Mean Time Between Hazardous Events (MTBHE) in Table 6 as all events may not be truly hazardous in nature and therefore MTBE is used.

Table 5: Hazard Severity Classifications

Description	Category	Definition
Catastrophic (1 Yr.-death)	**I**	Death, system loss, or severe environmental damage.
Critical (21-363 Days)	**II**	Severe injury, severe occupational illness, major system or environmental damage.
Marginal (8-20 Days)	**III**	Minor injury, minor occupational illness, or minor system or environmental damage.
Negligible (0-7 Days)	**IV**	Less than minor injury, occupational illness, or less than minor system or environmental damage.

Table 6: Hazard Probability Classifications

Description	Level	# of accidents # of employees	Specific individual item	Fleet or inventory	Numerical range of failure rate (f/Hr) for fleet/inventory
Frequent	**A**	(> .24)	Likely to occur frequently.	Continuously experienced.	Greater that 10^{-1}
Probable	**B**	(0.16 – 0.24)	Will occur several times in the life of an item.	Will occur frequently.	$\geq 1.39 \times 10^{-3}$ to $\leq 1.0 \times 10^{-1}$
Occasional	**C**	(0.10 – 0.15)	Likely to occur sometime in the life of an item.	Will occur several times.	$\geq 1.14 \times 10^{-5}$ to $\leq 1.39 \times 10^{-3}$
Remote	**D**	(0.02 – 0.09)	Unlikely but possible to occur in the life of an item.	Unlikely but can reasonably be expected to occur.	$\geq 5.12 \times 10^{-7}$ to $\leq 1.14 \times 10^{-5}$
Unlikely	**E**	(<0.01)	So unlikely, it can be assumed occurrence may not be experienced.	Unlikely to occur, but possible.	Less than 5.12×10^{-7}

The combination of the hazard severity and hazard frequency forms a Hazard Risk Index (HRI). The resulting Hazard Risk Assessment Matrix is obtained from MIL-STD-882C [14] as shown in Table 7 and Table 8.

The HRI presents the hazard analysis results in a format useful to the decision maker in determining whether hazards should be eliminated, controlled, or accepted. This provides a logical basis for management decision-making, considering both the severity and probability of any individual hazard in a weighted fashion.

Table 7: Hazard Risk Assessment Matrix

	Catastrophic	Critical	Marginal	Negligible
Frequent	**IA**	**IIA**	**IIIA**	**IVA**
Probable	**IB**	**IIB**	**IIIB**	**IVB**
Occasional	**IC**	**IIC**	**IIIC**	**IVC**
Remote	**ID**	**IID**	**IIID**	**IVD**
Improbable	**IE**	**IIE**	**IIIE**	**IVE**

Table 8: Hazard Risk Index (HRI)

Hazard Risk Index	Acceptance Criteria
IA, IIA, IIIA, IB, IIB, IC	**Unacceptable**
ID, IIC, IID, IIIB, IIIC	**Undesirable** - Requires solution acceptable to Bombardier Project Manager.
IE, IIE, IIID, IIIE, IVA, IVB	**Acceptable with review -** Requires review.
IVC, IVD, IVE	**Acceptable** - Review not required.

It should also be noted that these hazard classifications are consistent with CENELEC standards ([15] [16]) which define a sixth probability classification and different numerical ranges but similar severity definitions. As long as the definitions are applied consistently throughout all product safety analyses, the resulting risk assessment will be consistent and sufficiently accurate to guide the development process.

By assigning a Hazard Risk Index (HRI), a determination can be made as to how the hazards should be addressed, in the order of precedence shown below:

1. **Design for minimum risk**: Eliminate hazards by safety-critical design. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level through design concept and implementation.
2. **Incorporate safety devices**. If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk shall be reduced to a level acceptable through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks of safety devices when applicable.

3. **Provide warning devices**. When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, warning devices shall be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems.
4. **Develop rules, procedures and training**. Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training shall be used. Procedures may include the use of personal protective equipment. Such practices shall be evaluated for completeness, clarity, and applicability where necessary to provide adequate safety. Such methods may also include warnings and equipment labeling.

   Note: The use of warnings, cautions, or other written advisory shall not be used as the only risk reduction method for Category I or II severity hazards unless approved. Safety-critical tasks may require personnel proficiency in specific areas; the need for personnel proficiency certification will be identified in the analysis.

Hazard severity, before and after mitigation; provides a measure of the worst credible accident resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction. The hazard severity ranking of “AFTER mitigation” takes into account the actual design and architecture of the system (fail-safe design, maintenance procedures, etc.) and uses following rationale:

- Failures of components related to non-vital systems lead to hazard category IV when an independent vital subsystem protects them.
- The failure of a safety-related system, dependent on external requirements (e.g. periodic maintenance, periodic adjustments, cycle checking, or daily safety test) will lead to a hazard with a severity category I.
- A (Vital) fail-safe system will fail into a restrictive mode. The use of a fail-safe system can reduce the probability of the hazard occurrence for the item to an extent where it can be assumed that the hazard may not occur. This leads to a hazard probability of category E.

4 ACSES II System Internal Interfaces – Attributes

4.1 Communications to Onboard

The internal interfaces between subsystems of the contract are described in detail below. The interfaces in this section are described by the Onboard ICD [11] and the MDD [12].

4.1.1 OBC to WIU

The purpose of this interface is for the OBC to obtain the status of the approach interlocking from WIU, via the hardwired MCM-to-BCM interface.

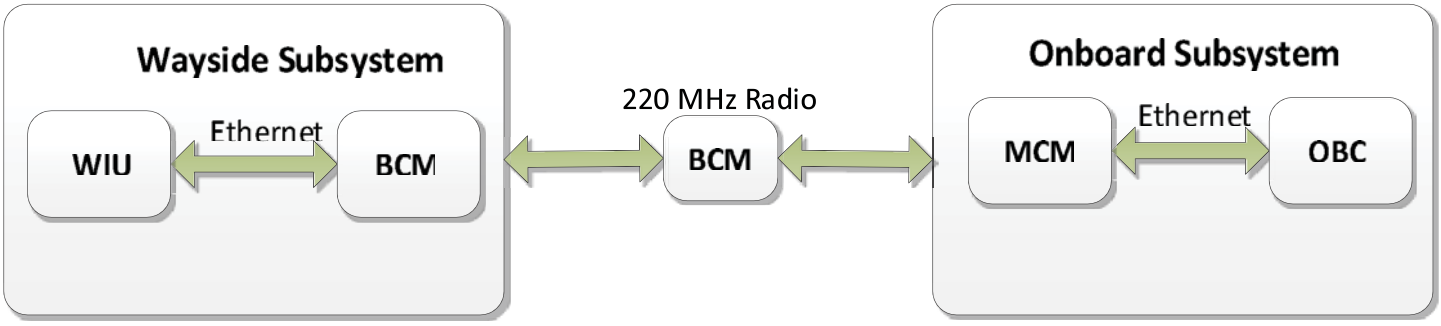


Figure 3: Onboard Computer to Wayside Interface Unit

4.1.1.1 Physical Attribute

The ACSES II OBC communicates to the wayside through the Mobile Communications Manager (MCM) which can use several radio frequencies to communicate to the Base Communications Manager (BCM). The different radio frequencies will be detailed in the Communications IHA. The use of different radios will not impact the safety analysis presented here.

4.1.1.2 Functional Attribute

Health messages are passed between the WIU and OBC to determine the health of this interface. Signal address information is passed from the OBC to MCM to setup the Radio with the correct frequency and power. Once the request sent by OBC the WIU respond to the request with the following information:

- Home signal status (Go or No go)
- Tracks crossed in interlocking and Exit information
- “C” Signal data
- Nested interlocking information (Next WIU: Controlling grade, distance, ATCS address)

As this message contains the vital and safety related data, it must be protected by CRC and checked for staleness. A CRC requirement of 72 bits and a staleness criterion of 42 seconds have been calculated Addendum 5 [38] .

4.1.1.3 Loss of Interface

If the OBC to WIU interface is lost (data not executed by the receiving end, or the communication is disconnected), the OBC shall enforce all PTS stops until the ISResp is received or the ATC releases this stop enforcement. The Train Engineer may also use the PTS bypass PB if approved by the Dispatcher. The Cellular network is a possible alternative source of the ISResp if the OBC to WIU connection is lost. The Cellular interface is tested in the departure test. A failure will prevent that train from entering service.

4.1.1.4 Corrupted Interface

The OBC shall check that the CRC encoded by the WIU matches the CRC calculated by the OBC for the data within this message. Any mismatch of data will be reported as an error through the MTA Error message. Also a staleness check using the time stamp will also be implemented to detect stall data in each message.

4.1.2 OBC to STS – Interface I

The purpose of this interface is for the OBC to communicate train status with the Office, and receive information such as TSR from the Office.

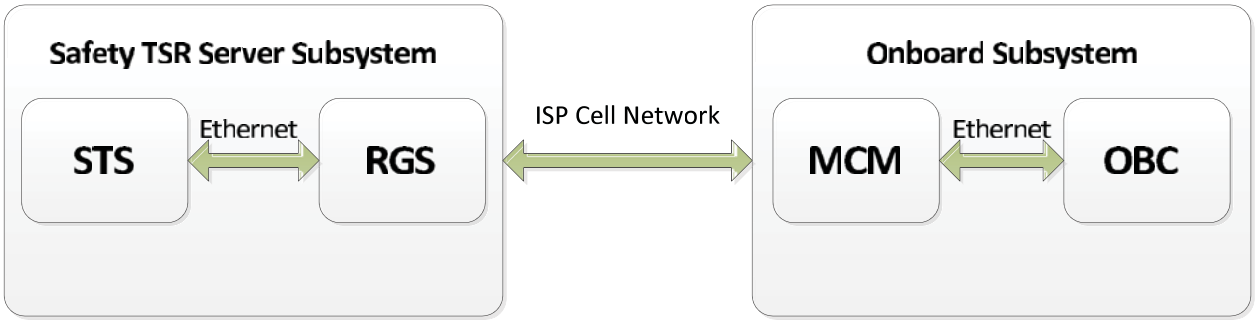


Figure 4: Onboard to Safety Temporary Speed Restriction Server

4.1.2.1 Physical Attribute

The Mobile Communications Manager (MCM) of the MCP communicates to ACSES II OBC over an Ethernet link. The ACSES II OBC communicates to the wayside through the Mobile Communications Package (MCP) in defined areas can route these requests through the cellular modem to the office RGS. The cellular connection will need to be protected by a VPN with adequate encryption to protect the data from external users of the cellular service.

4.1.2.2 Functional Attribute

TSR List Train Request is sent by the OBC to the STS. The request is repeated until the complete list is received by the OBC from the STS. As this message is vital is must be protected by CRC and checked for staleness.

TSR List Train Answer is sent by the STS in response to the request. This list has the TSR to be enforced in the next three interlockings. If no change in the list a special no change response is sent to the train. As this message is vital is must be protected by CRC and checked for staleness.

ISReq is sent by the OBC to the WIU after passing PDS TP set or DS TP set every 6 seconds until the HS TP is passed. ISResp is sent by the WIU in response to the ISReq. As this message is vital is must be protected by CRC and checked for staleness.

ISResp has two different messages one for LoMA and one without LoMA. Both messages have the signal status, speed change data and exit track data. LoMA has in in addition grade between interlocking, next BCP number and next WIU assignment and next signal assignment. As this message is vital is must be protected by CRC and checked for staleness.

4.1.2.3 Information Attribute

Missed Transponder alarms are sent in the Maintenance Train Alarm messages through this interface to the DMS in the Office. Maintenance Train Alarm messages will have TSR request errors, ISReq errors and transponder communication errors. Maintenance Train Alarms are sent as polling allows but are prioritized below TSR and ISReq requests. Additional Onboard alarms will also be sent to the DMS.

4.1.2.4 Loss of Interface

A loss of this interface will need to be detected by the OBC. The OBC will indicate loss of TSR information to the train engineer. The loss of ISResp information will cause the PTS enforcement to be active at every interlocking unless released by the ATC aspects.

4.1.2.5 Incorrect Information in Interface

The OBC shall check that the CRC encoded by the STS or WIU matches the CRC calculated by the OBC for the data within this message. Any mismatch of data will be reported as an error through the MTA Error message. A staleness check will also be implemented to detect stall data in each message.

4.1.3 OBC to STS – Interface II

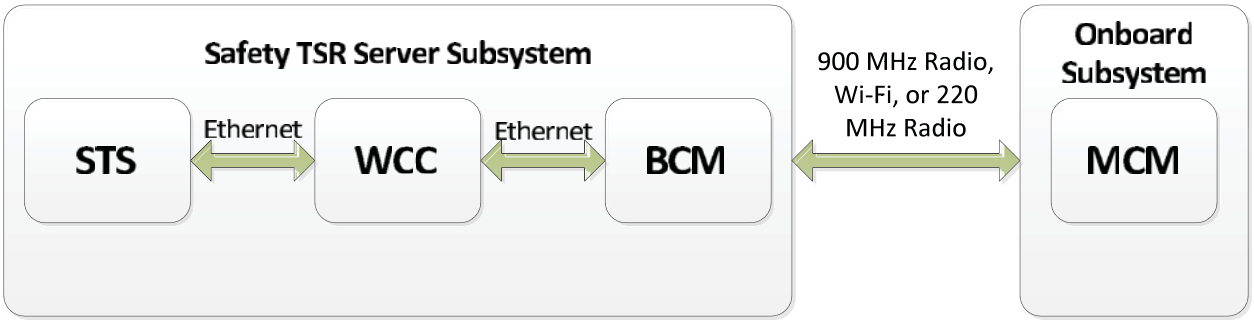


Figure 5: Safety Temporary Speed Restriction Server to Wayside Communications Controller

4.1.3.1 Physical Attribute

This interface is an Ethernet interface implemented by the Office LAN. The interface is described in the System Description Document [4].

The WCC will route the TSR messages to the correct BCM for transmission to the train via the correct radio frequency (900, Wi-Fi, or 220 MHz). This interface will be detailed in the communications IHA as it is internal to the communications subsystem. The PDR to PDR interface is also detailed in the communications IHA.

4.1.3.2 Functional Attribute

Data and polling messages are sent over this interface. The data messages include TSR List Train Request, TSR List Train Answer, TSR List No Change. The polling messages include WCC Poll Request and WCC Poll Reply.

The data messages implement the ability of the onboard to send TSR requests to the STS and the STS to reply with a list of TSR's for a specific location. The no change response would be used when the list sent by the train is the current list for that area.

4.1.3.3 Information Attribute

The WIU will indicate the health of the STS to WCC link to the NMS based on the response to the poll messages.

4.1.3.4 Loss of Interface

The loss of the WCC to STS interface would be indicated on the NMS. The loss of this interface would cause the loss of TSR information to the train which would cause the onboard system to display the "No TSR Data" indication on the ADU. The onboard system would enforce a penalty brake upon indication of No TSR data until the train engineer presses the Ack. Any TSR currently enforced would be released after the Ack (except temporal separation TSRs). Upon this indication manual TSR enforcement would be required based on communication between the Dispatcher and the Train Engineer.

4.1.3.5 Incorrect Data in Interface

The STS must calculate a CRC on the TSR data and send this with the data to the train. The OBC will use this CRC and verify the data processed matches the CRC within the message. If any error on CRC calculations is found the message will be ignored and the OBC will send an alarm to the DTS.

4.1.4 Transponder to OBC

The purpose of this interface is for the OBC to determine its position, using the location of the Transponder(s).

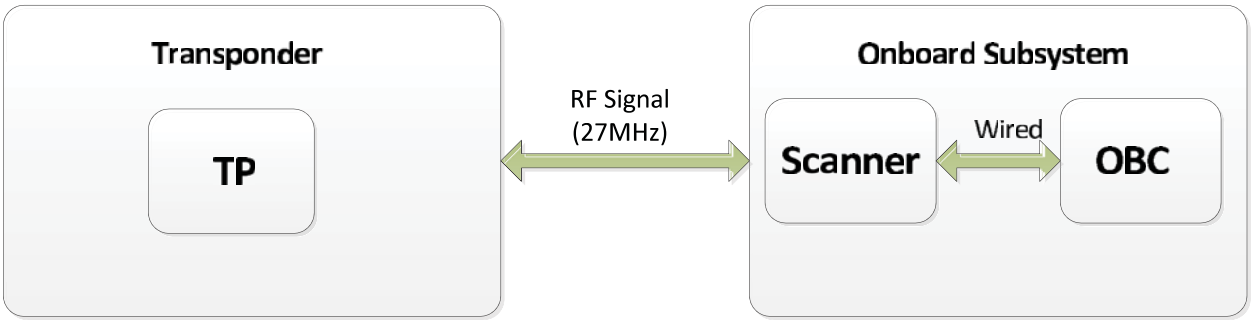


Figure 6: Onboard to Transponder

4.1.4.1 Physical Attribute

RF Interface that allows the onboard scanner to power the transponder response when a train passes over the transponder. The scanner uses a 27 MHz signal and the transponder response is a 4.5 MHz signal.

4.1.4.2 Functional Attribute

The transponder packets define the identification of the railroad, line, track number and position in the TP set of this transponder. This allows the train to determine its current location and direction on the system. The transponder will also provide the linking distance to the next transponder set. Active speed restrictions (MAS and PSR) and the distance to start and end (if applicable). PTS target distances. Radio address and channel number for wayside communication. As this message is vital it must be protected by CRC and checked for staleness.

4.1.4.3 Information Attribute

The OBC determines from transponder data the next available transponder data to be read in the direction of travel. If the Onboard fails to read the next transponder, the onboard system will send an alarm to the NMS. Any error or transponders not read correctly will be reported by the onboard to the DMS system.

4.1.4.4 Loss of Interface

Without the transponder information the onboard system is unable to enforce the safe operating speed as it is missing updated MAS/PSR information from the transponder. The onboard may also be unable to enforce the next PTS. The ability to enforce the PTS requires it reads either the PDS or DS prior to reaching the Home Signal.

The OBC reads the linking distances in the transponder packets and determines the window for which the next transponder should be read based on this distance. If a transponder is read outside of this window then an error is sent to the NMS and error log. The OBC on detecting an error will keep enforcing PTS but stop all TSR enforcement. The ADU train speed will be set to "- -" and a missed transponder indication will be shown to indicate the system is operating in degraded mode. The train engineer must revert to an operating procedure that will enforce train stops and speed restrictions. The OBC will enforce an overall maximum speed of 59 MPH.

Upon successfully reading the next transponder the system will return to normal operation.

All PSR and MAS packets will be enforced with redundant packets in different transponder sets to mitigate the impact of a missed transponder

4.1.4.5 Incorrect Information in Interface

The OBC shall check that the CRC encoded in the transponder packet matches the CRC calculated by the OBC for the data within this message. Any mismatch of data will be reported as an error through the MTA Error message. The OBC will display a "- -" on the ADU to indicate a misread transponder. See above for the system reaction.

All PSR and MAS packets will be enforced with redundant packets in different transponder sets to mitigate the impact of a missed transponder.

4.2 Communications to Wayside

This interface is described in System Description Document [4]. This is the primary interface of the WIU to send and receive messages from the Onboard and Office. There are no direct users for this interface.

4.2.1 WIU to Office

The purpose of this interface is for the transmission of status messages and alarms, as well as controlling switchover and shutdown within control centers and between control centers.

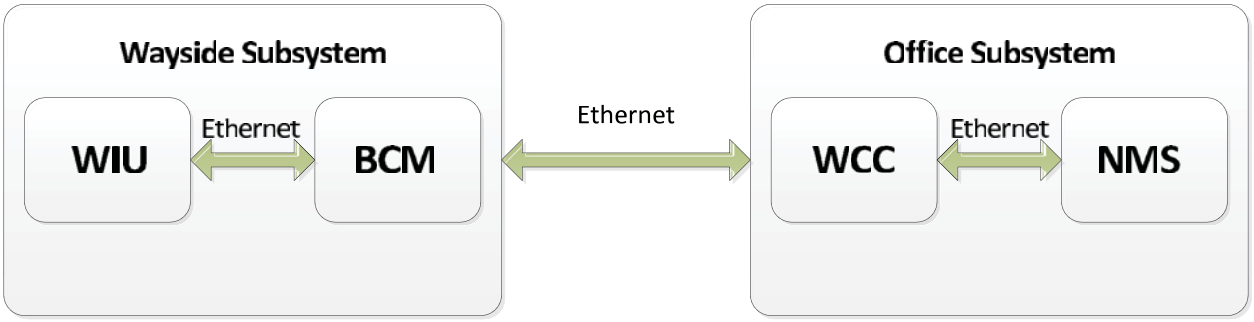


Figure 7: Wayside Interface Unit to Network Management System

4.2.1.1 Physical Attribute

This interface is an Ethernet interface through the wayside Layer 2 and Layer 3 switches to the ground based network of the railroad to complete the network. All NMS bound messaging will use SNMP V2.0 format. The interface is described in the System Description Document [4].

4.2.1.2 Functional Attribute

The WIU will send the NMS a limited set of data. The NMS can request an update from this data as required. The data that can be polled includes latest software revisions, name, and up time. The WIU will also respond to NMS inquiries to indicate health of the connection.

4.2.1.3 Information Attribute

The WIU will send NMS data on changes to system health, system in edit mode, or configuration changed. In addition, errors such as invalid address, invalid encoder number, invalid signal number, message number error, message version number error and loss of time source will be sent.

4.2.1.4 Loss of Interface

The loss of this interface will not impact the safety of the operation of the system. The NMS will monitor and indicate the loss of response of connected configured devices to the maintenance users.

4.2.1.5 Incorrect Information in Interface

Incorrect data sent via the WIU to NMS interface will cause false maintenance requests but will not impact the operation of the system.

4.2.2 WIU to OBC

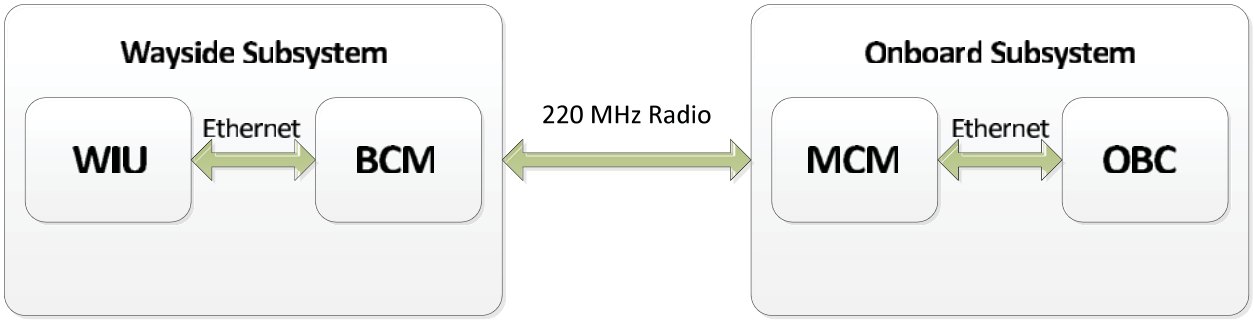


Figure 8: Wayside Interface Unit to Onboard Computer

4.2.2.1 Physical Attribute

This interface is an Ethernet interface that uses the Layer 2 and Layer 3 network switches. The interface is described in the System Description Document [4]. This section will analyze the BCM connection to the communication subsystem RF connections. Three RF frequency bands are possible (220 MHz, Wi-Fi, or 900 MHz).

4.2.2.2 Functional Attribute

The BCM will send the WIU the ISReq received from the train. The WIU will respond to the BCM with the appropriate ISResp for that request. Two types of ISResp exist one with LoMA and one without.

ISResp has information on the signal status, exit track, C Signal status, and speed restrictions within the interlocking. If a LoMA response is given it will also have the distance to next interlocking, worst case grade to next interlocking, next WIU Address the next interlocking signal and the next BCP address.

ISReq will indicate the signal required for status. No CRC is provided for this message as the signal ID and Train ID is repeated in the ISResp. No other safety data is included in the ISReq.

4.2.2.3 Information Attribute

The WIU to BCM interface receives train error messages and forwards these messages to the DMS for processing.

4.2.2.4 Loss of Interface

If the WIU to BCM interface is lost, the OBC shall enforce all PTS stops until the ISResp is received or the ATC releases this stop enforcement. The Train Engineer may also use the PTS bypass PB if approved by the Dispatcher. The Cellular network is a possible alternative source of the ISResp if the WIU to BCM connection is lost. The same safety criteria for the WIU and BCM will be applied.

The connection of the WIU and BCM to the network is monitored by the NMS.

4.2.2.5 Incorrect Data in Interface

The ISReq data for the WIU ID, signal ID, and BCM ID is returned to the train in the ISResp and checked by the OBC for validity of the correct data. Any corruption in the ISReq will result in the WIU sending an error message to the DMS or a response with incorrect data that will not release the PTS.

The ISResp data packet has a built in CRC that the onboard must verify and a timestamp for staleness checking. If the onboard is unable to verify the CRC or timestamp an error message will be sent to the DMS and the onboard will ignore the data.

4.3 Communications to Office

This interface is described in System Description Document [4]. This is the primary interface of the Office to send and receive messages from the Onboard, and WIU. There are no direct users for this interface.

4.3.1 STS to RGS

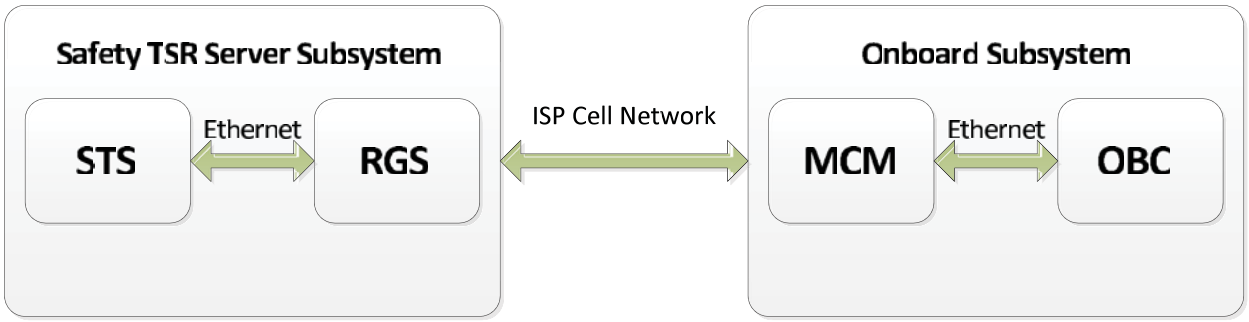


Figure 9: Safety Temporary Speed Restriction Server to Railroad Gateway Server

4.3.1.1 Physical Attribute

This interface between the STS and the RGS is an Ethernet interface implemented by the Office LAN. The interface will be made through a firewall. The interface is described in the System Description Document [4].

The interface between the STS and RGS will be used to send TSR count request, TSR count and TSR list data between the adjacent railroad and the local STS.

The interface between the RGS and the MCM is an ISP Cell Network.

This interface will be used when the WCC determines the train TSR request originated from the cellular connection and not the BCM. The STS response will be routed to the ISP for sending to the train. The security analysis of this connection will be analyzed in the System Vulnerability Assessment.

4.3.1.2 Functional Attribute

Data and polling messages are sent over this interface. The data messages include TSR List, TSR List Count Request, TSR Count Update, TSR DB Update, TSR DB update notification, TSR List STS Count request, TSR List STS Answer, TSR List No Change (cellular only), and TSR List STS Complete Request.

The data messages between the STS and RGS implement the ability of local and adjacent railroad STS servers to synchronize boundary TSR data.

The data messages between the RGS and the MCM implement the ability of the onboard to send TSR requests to the STS and the STS to reply with a list of TSR's for a specific location. The no change response would be used when the list sent by the train is the current list for that area.

The polling messages Inter-STS ATCS poll request and Inter STS ATCS poll reply provide a method of confirming the link between the STS servers is healthy. The RGS – STS Status message notifies the STS on the health of the RGS. The STS – RGS Status allows the STS to inform the RGS on the health and controlling status of the STS.

4.3.1.3 Information Attribute

The STS will indicate the health status of the STS – RGS and STS to adjacent railroad STS link status to the NMS.

4.3.1.4 Loss of Interface

The loss of the RGS – STS interface will cause the local STS to remove the adjacent railroad speed restrictions as these could change while the connection is down. The local STS will place a point TSR near the adjacent railroad boundary to restrict the speed of trains entering the adjacent railroad. In addition, manual communication between the dispatchers of the two railroads should ensure that the train engineer of any trains crossing the boundary are informed of changing speed restrictions in the other railroad.

The loss of the RGS – STS interface will be indicated on the UIS and the NMS.

The loss of the WCC to STS interface would be indicated on the NMS. The loss of this interface would cause the loss of TSR information to the train which would cause the onboard system to display the "No TSR Data" indication on the ADU. Upon this indication manual TSR enforcement would be required based on communication between the Dispatcher and the Train Engineer.

4.3.1.5 Incorrect Data in Interface

Incorrect TSR data would impact the TSR enforced by the local STS for the adjacent railroad or the adjacent railroad STS enforcement of local TSR's. The STS must calculate a CRC on the TSR data and send this with the data to the adjacent railroad. The adjacent railroad STS will use this CRC and verify the data processed matches the CRC within the message. If any error on CRC calculations is found the message will be ignored and the adjacent railroad. If the local STS detects an incorrect CRC on the adjacent railroad STS messages a message will be sent to the local DMS.

The STS must calculate a CRC on the TSR data and send this with the data to the train. The OBC will use this CRC and verify the data processed matches the CRC within the message. If any error on CRC calculations is found the message will be ignored and the OBC will send an alarm to the DTS.

4.3.2 RWPS to STS

The design of the RWPS interface is described below. The safety requirements described here in the analysis will drive the design.

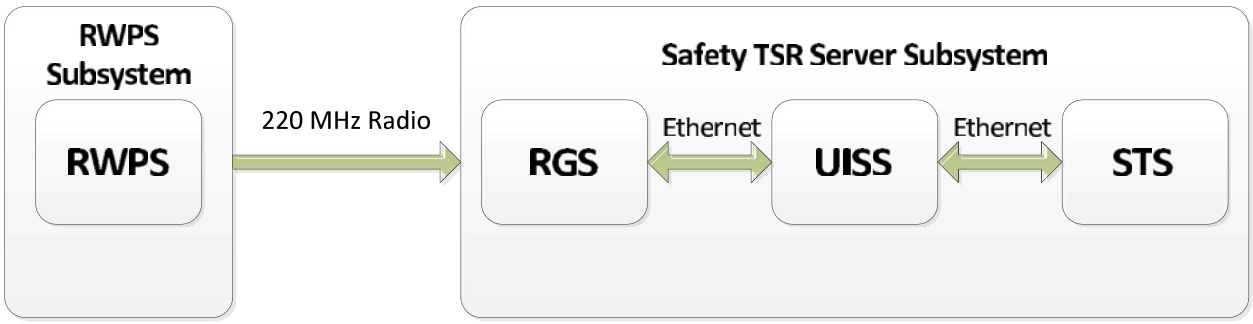


Figure 10: Railway Worker Protection System to Safety TSR Server Subsystem

4.3.2.1 Physical Attribute

Ethernet interface that utilizes the RGS and firewall to enable the connection between the RWPS and its UIS.

4.3.2.2 Functional Attribute

This interface allows the following functional messages to be sent TSR List Request, Speed Restriction Request, EIC Access request, TSR List Response, Speed Restriction Response, and EIC Access response. These messages allow the EIC to view speed restrictions active in their assigned areas, request new speed restrictions and assign authority of speed restriction to an employee in change.

Poll messages of Keep alive are also sent to indicate the health status of the link between the RWPS and the UIS.

4.3.2.3 Information Attribute

The UIS and the RWPS will report to the NMS the health status of the interface by monitoring the response to the keep alive messages.

4.3.2.4 Loss of Interface

The loss of the RGS to UIS interface would be indicated on the NMS. The loss of this interface would cause the loss of TSR information on the RWPS. Connection status of the RWPS to UIS must be indicated on the EIC Terminals.

The loss of the interface on the UIS may require the Dispatcher to log in as a supervisor to allow TSR's with assigned EIC's to be removed. The STS must process this request by the UIS supervisor to remove TSR's with assigned EIC's.

4.3.2.5 Incorrect Data in Interface

As the RWPS is sending TSR requests to the UIS and STS, the data within that request must be checked. The UIS and STS will both perform a check on the data sent by the RWPS. This check will employ verification checks to the UIS and STS database as well as confirmation of the data within the request via a CRC that the RWPS places in the message. Any errors in the request will be returned to the RWPS in the reply and indicated to DMS and NMS.

As the RWPS is a non-safety subsystem the data requested must be confirmed via the Select – Check-Execute process by independent Dispatcher and supervisor before being enforced by the STS.

The RWPS must not convert any TSR request data into any other format other than that entered by the employee in charge. This will limit the integrity of the software from making errors that cannot be detected by the Select – Check Execute process.

5 ACSES II System External Interfaces – Attributes

External interfaces to the ACSES II System include both those to devices and those to users. User interfaces include both those in the office and those onboard. Since this is external to ACSES II system, the Safety Related Application Conditions (SRAC) may identified and assign a unique ID. The following are the external interfaces to the system that are further analyzed in this document:

- OBC to Vehicle Interface;
- OBC to (Existing) ATC Interface;
- OBC to Brake Interface;
- OBC to Speed sensor;
- OBC to Decelerometer;
- Office to Adjacent RR STS Server;
- WIU to IXL;
- GPS to GCS;
- GPS to BCM;
- Dispatcher(s) to UISS;
- EIC to RWPS (Employee-In-Charge Interface);

- Maintenance Staff to NMS;
- Maintenance Staff to WIU;
- Train Engineer to ADU (Train Engineer Interface);
- Train Engineer to Ack;
- Train Engineer to PTS PB.

5.1 Onboard External Interfaces

5.1.1 OBC to Vehicle Interface

5.1.1.1 Physical Attribute

The physical connections of the ACSES II OBC to the vehicle will depend on the vehicle application. Vital signal inputs will be used to collect the vehicle interface information. See the OBC HIA[6] for further details.

5.1.1.2 Functional Attribute

This interface will be used to collect forward, reverse, A Cab / B Cab key, A-Cab / B-Cab Stop Release PB, and A-Cab / B-Cab Alarm inputs to OBC. These are safety related inputs to OBC and OBC vital functions ensure that the inputs are vital.

5.1.1.3 Information Attribute

This interface will be recorded in the onboard event recorders.

5.1.1.4 Loss of Interface

As these signals are hardwired the interface will be designed so that if the wiring breaks the onboard will assume a safe restrictive state.

5.1.1.5 Incorrect Information in Interface

The analysis assumes that the OBC vital functions will discard when receive incorrect input data's.

5.1.2 OBC to (Existing) ATC Interface

5.1.2.1 Physical Attribute

The physical connections of the ACSES II OBC to the ATC will depend on the vehicle application. Two basic approaches are used: one for a Siemens ATC and another for a non-Siemens ATC. Where a Siemens ATC is used communication will be over a serial bus link. Where a non-Siemens ATC is present an AIU component will be installed and a serial bus link will be established between the OBC and the AIU.

5.1.2.2 Functional Attribute

Data shared on this link is the aspect information, ATC cutout, ACSES cutout, ATC brake and emergency brake commands.

5.1.2.3 Information Attribute

Aspect indications will be displayed on the ADU. ATC Cutout will be used by ACSES to determine the applicability of C Signal functionality. ACSES cutout will be displayed on the ADU.

It is assumed this data will be vital when received.

5.1.2.4 Loss of Interface

A loss of ATC interface will cause the OBC to determine the ATC is cutout with no aspect indicated.

5.1.2.5 Incorrect Information in Interface

For the AIU to OBC or Siemens ATC to OBC interface [11], the OBC shall check that the CRC encoded by the ATC matches the CRC calculated by the OBC for the data within this message. Any mismatch of data will be reported as an error through the MTA Error message. A staleness check will also be implemented to detect stale data in each message.

The interface of the AIU to the legacy ATC is assumed to be vital and will be hardwired.

5.1.3 OBC to Brake Interface

5.1.3.1 Physical Attribute

This interface shall be a hardwired connection based on the vehicle type. For LIRR vehicles, the interface methods include single P-wire control, magnet valve (pneumatic actuating), and vital relay interfacing.

5.1.3.2 Functional Attribute

This interface is used by the onboard computer to apply the brakes. This interface shall be vital and failsafe.

It is assumed that the vehicle brake system shall apply the brakes in a vital manner.

5.1.3.3 Information Attribute

The information shall be in the form of energy applied to hold off the braking system (Fail safe).

5.1.3.4 Loss of Interface

This interface shall be designed vitally such that the loss of the interface from the OBC will enforce the brakes to be applied.

[IHA-SARC-02]-The OBC shall vitally designed to enforce braking when the interface between OBC to brake interface is lost.

5.1.3.5 Incorrect Information in Interface

Incorrect information to brake interface lead to emergency break. The interface between the OBC and the existing vehicle emergency brakes is through a vital relay.

5.1.4 OBC to Speed Sensor

5.1.4.1 Physical Attribute

This interface shall be a hardwired connection and sending speed pulses from the tachometer to the Tach I/O PCB in the OBC. The sensor is driven from a 60-tooth gear

5.1.4.2 Functional Attribute

This function is a type-approved ACSES II function. The OBC interfaces with the vehicle speed sensor to calculate the train speed. The train speed is derived from the number of teeth of the gear per revolution and the size of the wheel that the OBC is configured for a specific vehicle type. Also, the speed sensor pulse shift provides the rotation sense of the wheel.

The train speed is measured using pulses representing speed. The OBC calculates the train speed by measuring the frequency of the speed sensor signal by counting pulses over fixed time durations

The speed sensors are checked three different ways to ensure proper functionality:

1. When not in motion, an inductive pulse is sent to the sensor coil. And, a pulse train test is performed, and the circuit will verify the pulse count. This check ensures that no short circuits are present.

2. A DC bias test is continually performed to check for open circuits.

3. Periodically, the microprocessor routes the bus clock into the counter input to verify the counter increments properly at high counts.

5.1.4.3 Information Attribute

This interface will be recorded in the onboard event recorders.

5.1.4.4 Loss of Interface

As these signals are hardwired the interface will be designed so that if the wiring breaks the onboard will assume a safe restrictive state.

[IHA-SARC-03]-The speed sensor pulse inputs received by OBC shall be Safety Critical.

5.1.4.5 Incorrect Information in Interface

The analysis assumes that the pulse of speed sensor is safety critical when received and OBC confirms the pulse vitality by performing a vital check.

Failure of the speed sensor or its associated circuitry results in a penalty brake application. Sensor tests are performed on a regular basis. Circuit continuity is periodically verified with a DC bias measurement while the vehicle is stopped or moving. While stopped, operation of the internal pulse counting electronics and measurements of the inductive response of the sensor tests are also performed.

Also, the speed sensor is crosschecked with a decelerometer to detect for speed errors.

When the OBC detects a speed sensor failure, the train engineer is notified with the following indications to take actions.

- An audible alarm is generated.
- LIRR – ADU indicate flashing red on the ACSES indicator when an OBC fault is detected .

5.1.5 OBC to Decelerometer

5.1.5.1 Physical Attribute

The physical serial connections of the ACSES II OBC to the Decelerometer will depend on the vehicle application. This input will provide vital acceleration information.

5.1.5.2 Functional Attribute

The decelerometer is a vital, microcontroller-based device whose primary function is to provide grade-compensated deceleration sensing in railroad applications. It is designed to operate and report deceleration measured within the range of a typical service or emergency brake rate. It utilizes an inclinometer and automatically performs certain self-tests and diagnostics to monitor its integrity, checking its calibration and dynamic range. The OBC uses decelerometer input to suppress audible alarm and penalty brake application and to implement spin/slide (slip/slide) compensation, brake assurance (where applicable), and cross check with speed sensor.

5.1.5.3 Information Attribute

This interface will be recorded in the onboard event recorders.

5.1.5.4 Loss of Interface

If the decelerometer completely fails and is unable to function, the OBC determines that communication with the decelerometer has failed and defaults to a brake rate of 0 mph/s.

With a brake rate of 0 mph/s under the decelerometer failure condition, the OBC loses suppression, slip/slide compensation capability, brake assurance function (LIRR only), and acceleration cross-check capability (cross-check with speed sensor).

When the decelerometer is failed, the ADU indicate flashing red on the ACSES indicator when an OBC fault is detected.

Upon detecting the decelerometer failure, if the permanent suppression input is OFF and the OBC detects that there is no speed sensor pulse count, the OBC requests a penalty brake application. While the OBC still detects that there is no speed sensor pulse count, if the permanent suppression input becomes ON, the penalty brake application is released.

[IHA-SARC-04]-The decelerometer inputs received by OBC shall be vital.

5.1.5.5 Incorrect Information in Interface

The Decelerometer serial link is implemented with vital techniques, e.g. CRC and stale data detection (time stamp). In addition, measured speed and deceleration are crosschecked, identifying a failure in the subsystem, leading to brake application.

5.2 Office External Interfaces

5.2.1 Office to Adjacent RR STS Server

5.2.1.1 Physical Attribute

This interface is an Ethernet interface implemented by the Office LAN. The interface will be made through a firewall. The interface is described in the System Description Document [4].

This interface will be used to send TSR count request, TSR count and TSR list data between the adjacent railroad and the local STS.

5.2.1.2 Functional Attribute

Data and polling messages are sent over this interface. The data messages include TSR List, TSR List Count Request, TSR Count Update, TSR DB Update, TSR DB update notification, TSR List STS Count request, TSR List STS Answer, and TSR List STS Complete Request.

The data messages implement the ability of local and adjacent railroad STS servers to synchronize boundary TSR data.

The polling messages Inter-STS ATCS poll request and Inter STS ATCS poll reply provide a method of confirming the link between the STS servers is healthy. The RGS – STS Status message notifies the STS on the health of the RGS. The STS – RGS Status allows the STS to inform the RGS on the health and controlling status of the STS.

5.2.1.3 Information Attribute

The STS will indicate the health status of the STS – RGS and STS to adjacent railroad STS link status to the NMS.

5.2.1.4 Loss of Interface

The loss of the RGS – STS interface will cause the local STS to remove the adjacent railroad speed restrictions as these could change while the connection is down. The local STS will place a point TSR near the adjacent railroad boundary to restrict the speed of trains entering the adjacent railroad. In addition, manual communication between the dispatchers of the two railroads should ensure that the train engineer of any trains crossing the boundary are informed of changing speed restrictions in the other railroad.

The loss of the RGS – STS interface will be indicated on the UIS and the NMS.

5.2.1.5 Incorrect Data in Interface

Incorrect TSR data would impact the TSR enforced by the local STS for the adjacent railroad or the adjacent railroad STS enforcement of local TSRs. The STS must calculate a CRC on the TSR data and send this with the data to the adjacent railroad. The adjacent railroad STS will use this CRC and verify the data processed matches the CRC within the message. If any error on CRC calculations is found the message will be ignored and the adjacent railroad. If the local STS detects an incorrect CRC on the adjacent railroad STS messages a message will be sent to the local DMS.

5.2.2 IXL to WIU

5.2.2.1 Physical Attribute

A parallel interface will be employed through the existing vital relays and/or parallel interface to existing interlocking computers.

5.2.2.2 Functional Attribute

Status of switch positions and signal status will be collected by the WIU. The interface hazard analysis looked at detection of health of the interface between WIU and the legacy interlocking.

5.2.2.3 Information Attribute

The wayside status information sends to/from IXL and WIU via Vital Signal Logic.

5.2.2.4 Loss of Interface

The loss of the IXL to WIU interface will cause the WIU to report routes are not available to trains. So the ISResp will not show a clear route. ATC can provide an aspect to releases the PTS or the Train engineer could use the PTS PB with Dispatcher approval.

5.2.2.5 Incorrect Data in Interface

As this interface is hardwired this is not applicable. The analysis assumes the wayside signal system is vital.

5.2.3 GPS to GCS

5.2.3.1 Physical Attribute

Physical GPS Antenna RF connection to the Grand Master Clock.

5.2.3.2 Functional Attribute

The GPS signal to the grand master clock is used to synchronize the time source sent over the network. The alignment to GPS is necessary as the primary timing source to the BCM for the PDR synchronization is GPS.

5.2.3.3 Information Attribute

The grandmaster clock will report GPS signal and strength to the NMS.

5.2.3.4 Loss of Interface

The loss of the GPS to GCS may cause the 220 MHz radio time slot to drift and cause interface or failure to complete radio transmissions. In non-tunnel applications the primary timing source will be a GPS antennae to the BCM. To mitigate the loss of 220 MHz cellular PDR's and Wi-Fi PDR's are present in the system.

The failure of radio communication would prevent the release of PTS or additional TSR information from being received by the train but would not directly impact the safety of the system.

5.2.3.5 Incorrect Data in Interface

Incorrect transmission or receipt of the time synchronization pulse would cause the radio communication to fail. Please see loss of interface section above for details.

5.2.4 GPS to BCM

5.2.4.1 Physical Attribute

GPS antenna to PPS (1 pulse per second) TTL clock signal input to PDR.

5.2.4.2 Functional Attribute

Provides time synchronization for each PDR to align time slots on 220 MHz radio.

5.2.4.3 Information Attribute

Each PDR can be configured for two time sources, one is the GPS the other is the GCS network source. For tunnel areas only, the network time source will be available.

5.2.4.4 Loss of Interface

The loss of the GPS to BCM may cause the 220 MHz radio time slot to drift and cause interface or failure to complete radio transmissions. In non-tunnel applications the primary timing source will be a GPS antennae to the BCM. To mitigate the loss of 220 MHz cellular PDR's and Wi-Fi PDR's are present in the system.

The failure of radio communication would prevent the release of PTS or additional TSR information from being received by the train but would not directly impact the safety of the system.

5.2.4.5 Incorrect Data in Interface

Incorrect transmission or receipt of the time synchronization pulse would cause the radio communication to fail. Please see loss of interface section above for details.

6 ACSES II System User Interfaces – Attributes

6.1 Office and Maintenance User Interfaces

6.1.1 Dispatcher to UISS

6.1.1.1 Physical Attribute

A standard workstation and special designed application software provides the interface for the Dispatcher to the UISS.

6.1.1.2 Functional Attribute

This interface provides the Dispatcher with the ability to enter the TSR Request information and the Supervisor and Dispatcher the information on enforced TSR's in their territories to make operational decisions for the railroad. The supervisor is also provided information to review the TSR requests to perform the select check execute function responsibilities.

TSR information includes the passenger speed, freight speed, start milepost, end milepost, and TSR type.

6.1.1.3 Loss of Interface

TSR requests would not be able to be made for addition or removal of the TSR. A manual procedure to keep paper records of all enforced TSRs must be maintained.

6.1.1.4 Incorrect Data in Interface

The UISS is to pass the Dispatcher TSR request data without changes to the STS for verification. The STS will require the UISS get confirmation of the TSR request from a supervisor within a timeout period of the TSR request to confirm the information entered by the Dispatcher is correct and that the UISS did not alter the data.

6.1.2 EIC to RWPS (Employee-In-Charge Interface)

EIC's are designated as Primary or Secondary RWPS terminal users. The Primary EIC defines the limits of TSR and requests TSR to be implemented through the ACSES II system. The Secondary EIC (with Primary EIC's approval) can be attached to or released from an existing TSR. When there are no secondary EICs attached remaining on to the TSR, the Primary EIC is able to request the work zone TSR to be deleted from ACSES II system.

6.1.2.1 Physical Attribute

The primary interface for Employee-in-Charge (EIC) and the ACSES II system. This display will indicate the list of TSRs for the assigned area and any secondary EIC's attached to those TSR's.

6.1.2.2 Functional Attribute

Displays current TSR list for an assigned area.

6.1.2.3 Loss of Interface

If the EIC terminal detects no response from the RWPS server it will be indicated on the EIC terminal display.

6.1.2.4 Incorrect Data in Interface

The TSR list received by the EIC Terminal from the RWPS, UIS, and STS server will be checked for any corruption in transmission. If the data is found to be incorrect no data will be displayed.

6.1.3 Maintenance Staff to WIU

Maintenance staff will work through multiple components of the system to program and configure the components of the subsystem.

6.1.3.1 Physical Attribute

The WIU has a Diagnostic Tool (DT) that is used for downloading the local event logs and configuring each WIU.

6.1.3.2 Functional Attribute

The WIU vitally monitor the status of wayside devices (Switches and Signals) and send the status to Office and OBC upon request of interlocking status. The interlocking status includes the signal status (including interlocking speed), tracks to be crossed (including distance to change track), exit track (including distance to exit track), and any additional LoMA information to the next interlocking when nested.

6.1.3.3 Loss of Interface

The maintenance staff can't download even logs and/or configure the WIU.

6.1.3.4 Incorrect Data in Interface

The configuration data corrupted during the maintenance, the WIU calculate its own CRC and check against the built in CRC of the configuration data. If the check fails, the WIU reject the configuration data update.

6.1.4 Maintenance Staff to RWPS

Maintenance staff will work through multiple components of the system to program and configure the components of the subsystem.

6.1.4.1 Physical Attribute

The primary interface of the RWPS to the maintainer will be through the NMS.

6.1.4.2 Functional Attribute

The NMS in RWPS network will monitor all the equipment connected to the RWPS network and provide appropriate alarms/alerts to the authorized RWPS maintainers.

6.1.4.3 Loss of Interface

There is no monitoring (alarm/alerts) of all the hardware components of RWPS Office.

6.1.4.4 Incorrect Data in Interface

The data is protected from the RWPS server is sent to the EIC terminal using an HTTP checksum (which runs TCP/IP in the background) to detect any corruption of data.

6.2 Onboard User Interfaces

6.2.1 Train Engineer to ADU

6.2.1.1 Physical Attribute

The ADU is the primary interface to the ATC and ACSES systems. This display functions as the ATC signal aspects and displays ACSES related information. ACSES information displayed includes the currently enforced speed, the current speed of the train, missing transponder alarm indication and no TSR data indication.

The ADU communicates independently with the ATC and ACSES OBC. If the ATC is not a Siemens ATC, then an AIU is installed to communicate between the ADU and ATC.

6.2.1.2 Functional Attribute

Displays current track speed, current train speed, and ATC aspect information. Also displays indications for missed transponders and no TSR data.

The ADU is dark when the train is not configured for the cab for which the ADU is installed in to be the lead cab.

6.2.1.3 Loss of Interface

The ADU will not show any information or be a blank screen if loss of interface to the ATC or AIU occurs. The OBC shall still enforce penalty braking regardless of operator action or inaction. The ATC shall also enforce penalty braking regardless of operator action or inaction.

6.2.1.4 Incorrect Data in Interface

The information from the ATC/AIU and ACSES provided over serial interfaces to the ADU shall be protected by vital means including CRC and stale data detection.

6.2.2 Train Engineer to Ack

6.2.2.1 Physical Attribute

A pushbutton installed on the onboard to allow the train engineer to acknowledge alerts issued by the system. The acknowledgement will hold off brake enforcement until the train crosses the brake enforcement curve.

6.2.2.2 Functional Attribute

The onboard uses a vital digital input to detect the state of this pushbutton.

6.2.2.3 Loss of Interface

The design of this interface shall cause the onboard to assume no acknowledgement should this interface be lost.

6.2.2.4 Incorrect Data in Interface

The onboard design shall detect transitions in the activation of the pushbutton. The onboard shall not assume that the pushbutton being in the acknowledge state for long periods of time is an active acknowledgement by the operator. The input being active more than a set time period will enforce brake application. This mitigates a button stuck in the ACK position either through failure or the Engineer holding the button down continuously.

6.2.3 Train Engineer to PTS Push-Button

6.2.3.1 Physical Attribute

A pushbutton installed on the onboard to allow the train engineer to manually release a PTS enforced brake application when stopped and drive per manual operating procedures. This pushbutton is only active when the train is stopped and the PTSO from the WIU or ATC is not available. This pushbutton must be installed so that the operator must leave his accustomed position in the cab per 49 CFR Subpart E 236.506. The onboard after it releases the brakes enforces a 15 MPH speed limit until a transponder with inexact linking distance and then a transponder with exact linking distance is read.

6.2.3.2 Functional Attribute

The onboard uses a vital digital input to detect the state of this pushbutton.

6.2.3.3 Loss of Interface

The design of this interface shall cause the onboard to not release the brake enforcement should this interface be lost.

6.2.3.4 Incorrect Data in Interface

The onboard design shall detect transitions in the activation of the pushbutton. The onboard shall not assume that the pushbutton being in the release state for long periods of time is an active release by the operator. The input being active more than a set time period will enforce brake application. This mitigates a button stuck in the ACK position either through failure or the Engineer holding the button down continuously.

7 ACSES II System External Power Interfaces – Attributes

7.1 Power to Office

7.1.1 Power Interface To Office

7.1.1.1 Physical Attribute

Direct, copper-wired interface to two separate power supplies in each Office location. UPS for the power is supplied by the customer.

7.1.1.2 Functional Attribute

120 V 60 Hz AC Power.

7.1.1.3 Information Attribute

N.A.

7.2 Power to Wayside

7.2.1 Power Interface to WIU

7.2.1.1 Physical Attribute

Direct copper wired interface at each interlocking where WIU is to be installed.

7.2.1.2 Functional Attribute

120 V 60 Hz AC Power.

7.2.1.3 Information Attribute

Not Applicable.

8 Interface Hazard Analysis

8.1 Safety Requirement Management

For each hazard defined the SLR was reviewed for existing requirements that mitigated the hazard. These requirements were marked safety. Where mitigations were needed but didn't exist the System Safety Engineer worked with System engineering to add SLR requirements to cover the mitigations. All of these requirements were reviewed and linked to the appropriate hazard log entries. These requirements will also be linked to verification evidence in the form of functional test cases or analyses that prove the mitigations required are in place to eliminate the hazards. This traceability of safety requirements to the test cases will be provided in the RTM once the test cases are fully defined. The full safety requirement management process is defined in the SPSP [5].

8.2 Hazard Log Tracking

Please refer to the System Product Safety Plan 2-123-20)[5] for details on how the hazard tracking will be performed. The Hazard Log will be maintained in DOORS and the hazards defined in this analysis will be added to the Hazard Log.

8.2.1 Interface Analysis Fields

This section defines the columns of the analysis tables appended to the document.

Table 9: IHA matrix description

Definition	Description
System IHA ID	Unique identifier for each defined hazard of each interface.
Assigned Interface	Definition of the subsystems involved in the interface. If the interface is to an external system component, that component is identified. All user interfaces are defined with the user role and subsystem that provides the interface.
Physical Interface Types	This field describes the type of physical interface, e.g., radio frequency (RF), 220 MHz, etc.
Hazard Cause	Primary reason the hazard occurs.
Hazard Description	A scenario of a system failure that could occur if the interface provides incorrect data or fails to provide any data.
Hazard Effects	This field defines the accident that could occur from the scenario description.
Initial Risk Index	Hazard Severity and Frequency before mitigation and/or safeguard is implemented.
Final Risk Index	Hazard Severity and Frequency after successful implementation of the mitigation and/or safeguard.
Mitigation / Control / Safeguards	Description of the requirements and process required to mitigate or eliminate the hazard from occurring.
Remarks	Comments about the analysis, if any.

9 Interface Hazard Analysis Table

Table 10 System IHA Table

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
ACSES II Internal Interfaces:									
SYS_IHA_01	Interface between Onboard and WIU	Ethernet / Radio (220MHz) interface	Loss of Interface between Onboard and WIU.	OBC uses stale WIU information to allow a train through an interlocking that has changed state.	Collision Derailment	IB	IE		
SYS_IHA_02	Interface between Onboard and WIU	Ethernet / Radio interface	Loss of Interface between Onboard and WIU.	OBC uses stale WIU information to allow a train to pass restrictive signal.	Collision	IB	IE		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_03	Interface between Onboard and WIU	Ethernet / Radio interface	Loss of Interface between Onboard and WIU.	OBC uses stale WIU information to allow a train to enter occupied track block.	Collision	IB	IE		
SYS_IHA_04	Interface between Onboard and WIU	Ethernet / Radio interface	Onboard received Corrupted message from WIU.	OBC received corrupt WIU message	Collision	IB	IE		
SYS_IHA_05	Interface between Onboard and WIU	Ethernet / Radio interface	Onboard received delayed message from WIU.	OBC process stale WIU message.	Collision	IC	IE		
SYS_IHA_06	Interface between Onboard and WIU	Ethernet / Radio interface	Onboard received resequence message from WIU.	OBC receive messages in out of sequence from WIU	Collision	IB	IE		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_07	Interface between Onboard and WIU	Ethernet / Radio interface	Inserted message into the Onboard message from WIU.	Inserted message on the message transfer between Onboard and WIU.	Collision	IB	IE		
SYS_IHA_08	Interface between Onboard and WIU	Ethernet / Radio interface	Onboard received repeated message from WIU.	OBC receive same messages from WIU	Collision	IB	IE		
SYS_IHA_09	Interface between Onboard and STS	Ethernet / Radio interface	Loss of Interface between Onboard and STS.	Onboard fails to receive the latest TSR data	Collision Overspeed Injury	IB	ID		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_10	Interface between Onboard and STS	Ethernet / Radio interface	Onboard received Corrupted message from STS.	The TSR list received from STS is corrupted.	Collision Overspeed Injury	IB	IE		
SYS_IHA_11	Interface between Onboard and STS	Ethernet / Radio interface	Onboard received delayed message from STS.	OBC process stale STS message.	Collision Overspeed Injury	IC	IE		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_12	Interface between Onboard and STS	Ethernet / Radio interface	Onboard received resequencing message from STS.	OBC receive messages in out of sequence from STS	Collision	IB	IE		
SYS_IHA_13	Interface between Onboard and STS	Ethernet / Radio interface	Inserted message into the Onboard message from STS.	Inserted message on the message transfer between Onboard and STS.	Collision	IB	IE		
SYS_IHA_14	Interface between Onboard and STS	Ethernet / Radio interface	Onboard received repeated message from STS.	OBC receive same messages from STS	Collision	IB	IE		
SYS_IHA_15	Interface between Onboard and Transponder	RF	Loss of Interface	Onboard system fails to read a transponder.	Collision Overspeed	IB	IE		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_16	Interface between Onboard and Transponder	RF	Onboard received Corrupted message from TP.	The Transponder data received by Onboard is corrupted	Collision, Overspeed	IB	IE		
SYS_IHA_17	Interface between Onboard and Transponder	RF	Onboard received resequencing message from Transponder.	OBC receive messages is in out of sequence from Transponder	Collision	IB	IE		
SYS_IHA_18	Interface between Onboard and Transponder	RF	Inserted message into Transponder.	Install a transponder with incorrect messages which read by Onboard.	Collision	IB	IE		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_19	Interface between Onboard and Transponder	RF	Onboard received repeated message from Transponder.	OBC receive same messages from Transponder sets	Collision	IB	IE		
ACSES II External Interfaces:									
SYS_IHA_20	Interface between WIU and Legacy IXL (Relay)	Parallel	Open Circuit	WIU fails to update an input state when the input is disconnected.	Collision	IB	IE		
SYS_IHA_21	Interface between WIU and Legacy IXL (Relay)	Parallel	Short Circuit.	WIU fails to update an input state when the input circuit shorts.	Collision	IB	IE		
SYS_IHA_22	Interface between WIU and Legacy IXL (Relay)	Parallel	Noise voltage on Legacy Interlocking interface.	WIU fails to update an input state when the input circuit has noise	Collision	IB	IE		
SYS_IHA_23	Interface between Onboard and Service Brake Train Line	Parallel	Open Circuit	OBC interface to Service Brake Train Line Fails open.	Over speed	IB	IE		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_24	Interface between Onboard and Service Brake Train Line	Parallel	Short Circuit.	OBC interface to Service Brake Train Line shorts.	Over speed	IB	I E		
SYS_IHA_25	Interface between Onboard and Forward Train Line	Parallel	Open circuit	OBC interface to Forward Train Line fails open.	Over speed	IB	I E		
SYS_IHA_26	Interface between Onboard and Forward Train Line	Parallel	Short circuit	OBC interface to Forward Train Line fails short circuit	Over speed	IB	I E		
SYS_IHA_27	Interface between Onboard and Reverse Train Line	Parallel	Open circuit	OBC interface to Reverse Train Line fails open.	Over speed	IB	I E		
SYS_IHA_28	Interface between Onboard and Reverse Train Line	Parallel	Short circuit	OBC interface to Reverse Train Line fails short circuit	Over speed	IB	I E		
SYS_IHA_29	Interface between Onboard and Cab Makeup Train Line	Parallel	Open circuit	OBC interface to Cab Makeup Train Line fails open circuit	Over speed	IB	I E		
SYS_IHA_30	Interface between Onboard and Cab Makeup Train Line	Parallel	Short circuit	OBC interface to Cab Makeup Train Line fails short circuit	Over speed	IB	I E		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_31	Interface between Onboard and Ack Train Line	Parallel	Open circuit	OBC interface to Ack Train Line fails open circuit	Over speed	IB	I E		
SYS_IHA_32	Interface between Onboard and Ack Train Line	Parallel	Short circuit	OBC interface to Ack Train Line fails short circuit	Over speed	IB	I E		
SYS_IHA_33	Interface between Onboard and ATC	Parallel	Open circuit	OBC interface to ATC fails short circuit	Over speed	IB	I E		
SYS_IHA_34	Interface between Onboard and ATC	Parallel	Short circuit	OBC interface to ATC fails open circuit	Over speed	IB	I E		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_35	Interface between Onboard and Speed Sensor	Discrete Signal	Open Circuit	OBC interface to the Speed Sensors is disconnected	Over speed	IB	I E		
SYS_IHA_36	Interface between Onboard and Speed Sensor	Discrete Signal	Noise on Speed Sensor circuit	OBC Detects noise on Speed Sensor as train speed	Over speed	IB	I E		
SYS_IHA_37	Office to Adj RR	Ethernet	Loss of Interface	Interface between the Adj RR STS server and the local STS server fails.	Overspeed	IB	IE		
SYS_IHA_38	Office to Adj RR	Ethernet	Incorrect Transfer of information.	Adj RR TSR List message is corrupted in transit to local system.	Overspeed	IB	IE		
SYS_IHA_39	RWPS to Office	Ethernet	Loss of Interface	TSR Request from RWPS fails to be set.	Overspeed	IB	IE		
SYS_IHA_40	RWPS to Office	Ethernet	Incorrect Transfer of information.	TSR request message from RWPS is corrupted before Office receives.	Overspeed	IB	IE		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_41	RWPS to EIC	Through Internet	Loss of Interface	TSR Request from EIC fails to be set.	Overspeed	IB	IE		
SYS_IHA_42	RWPS to EIC	Through Internet	Incorrect Transfer of information.	TSR request from EIC is incorrect.	Overspeed	IB	IE		
SYS_IHA_43	ADU to Engineer	Graphical Display	Loss of Interface with ACSES II Onboard.	ADU fails to provide information to the Train Engineer due to loss of interface.	Overspeed	IB	IE		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
									Intent is for the OBC/ ATC to correctly enforce the speed no matter what the ADU does or doesn't display. Corrected Final Severity based on this.
SYS_IHA_44	ADU to Engineer	Graphical Display	Incorrect Transfer of information.	ADU display incorrect information to the Train Engineer.	Overspeed	IB	IE		Intent is for the OBC/ ATC to correctly enforce the speed no matter what the ADU does or doesn't display. Corrected Final Severity based on this.
SYS_IHA_45	ADU to Engineer	Graphical Display	Timing Issues with Data Transfer	ADU display stale information to the Train Engineer.	Overspeed	IVB	IVE		Intent is for the OBC/ ATC to correctly enforce the speed no matter what the ADU does or doesn't display. Corrected Final Severity based on this.
SYS _IHA_46	Office to Dispatcher	Graphical Display	Loss of Interface	An Office workstation fails to provide updated information to the Dispatcher.	Overspeed	IB	ID		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_47	Office to Dispatcher	Graphical Display	Incorrect Transfer of Information	An Office workstation fails to provide updated information to the Dispatcher.	Overspeed	IB	ID		
SYS_IHA_48	Office to Dispatcher	Graphical Display	Timing Issues with Data Transfer	An Office workstation fails to provide updated information to the Dispatcher.	Overspeed	IB	ID		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_49	Interface Onboard to Transponder	Onboard to Transponder RF Interface	Partial TP message set read	Onboard partially reads a TP set.	Collision / Overspeed	IB	IE		
SYS_IHA_50	Interface WIU to Legacy IXL	Wiring between WIU and Legacy Interlocking	Installation Instructions not followed	Error in vital input installation / wiring results in the WIU detecting a signal with less Restrictive Speed than intended	Collision / Derailment	IB	IE		
SYS_IHA_51	WIU – Legacy IXL	WIU wiring to Legacy IXL for point and signal status	Legacy IXL HW or SW Failure	Vital input delivered incorrect state by Legacy IXL which results in WIU send an ATCS message with a less restrictive movement authority then intended causing the OBC to show less restrictive movement authority than intended.	Collision / Derailment	IC	IE		
SYS_IHA_52	WIU – Legacy IXL	WIU interface to points and signals	Error in Installation Instructions. Error in configuration files	WIU Configuration error which results in WIU to send an ATCS message with a less restrictive movement authority than intended	Collision / Derailment	IB	IE		(WIU_IHA_6)

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_53	WIU – Legacy IXL	WIU interface to points and signals	Installation Instructions are not followed	WIU Configuration error which results in WIU to send an ATCS message with a less restrictive movement authority than intended	Collision / Derailment	IB	IE		(WIU_IHA_7)
SYS_IHA_54	WIU – Main WIU	Serial Interface – Ethernet	Application was not validated and properly tested.	Auxiliary WIU communication to main WIU contains less restrictive value than intended due to application program.	Collision / Derailment	IB	IE		(WIU_IHA_10)
SYS_IHA_55	OBC to ADU	Serial Interface – Ethernet	ADU Failure or OBC Failure	Displaying an incorrect aspect when operating with ATC cutout / Overspeed Cutout could result in a collision or derailment due to an over-speed condition.	Collison / Derailment	IB	IE		(SIIHO-03)
SYS_IHA_56									This hazard has been removed since it's only applicable to MNR
SYS_IHA_57	OBC to PTS PB	PTS PB allows Train Engineer to bypass PTS stop.	PTS PB failure	OBC accepts PTS PB input when the train engineer did not press the PB.	Collision / Derailment	IB	IE		
SYS_IHA_58	Interface between Onboard and Transponder Scanner	Parallel	Short Circuit	OBC interface to Transponder Scanner Train Line fails short circuit	Overspeed	IB	IE		

System IHA ID	Assigned Interface	Physical Interface Types	Hazard Cause	Hazard Description	Hazard Effects	Initial Risk Index	Final Risk Index	[redacted]	Remark
SYS_IHA_59	Interface between Onboard and STS	Ethernet / Radio interface	Onboard received Corrupted message from STS.	The TSR list received is not from STS is corrupted.	Collision Overspeed Injury	IB	IE		
SYS_IHA_60	Interface between Onboard and Decelerometer	Serial link	Incorrect grade-compensated	The interface between Decelerometer and Onboard fails	Overspeed	1B	1E		

10 Conclusions

The ACSES II Signaling System is made up of several interfaces between subsystems, people, and the environment. This report defines the system interfaces, identifies potential hazards, and shows that mitigations have been identified for the potential hazards. The Table 11 below listing all the unique mitigations identified during this analysis. Also, the Table 11 presents the mitigation type, i.e. whether the mitigation is functional, Operational, SRAC and/or Exported constrains (EC) to appropriate subsystem stakeholders. The overall design concepts incorporate adequate control over interfaced functions to prevent any potential hazards from affecting system safety.

The Safety Related Application Conditions (SRAC) has been identified during the external interface analysis and it is presented in Table 12 below..

The Table 11 description as follows:

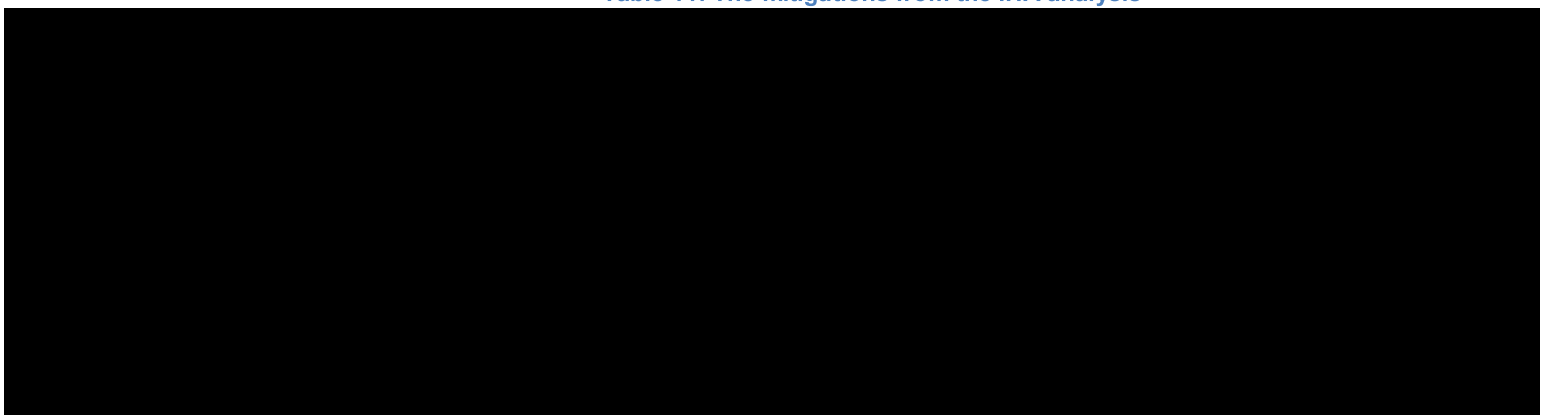
Sys-IHA-ID – Unique System Interface Hazard ID.

Description – The unique mitigations from Interface Hazard Analysis Table

Mitigation Type – Whether the mitigation is a functional, Operational, SARC and/or ECS (Exported Constraints to Stake holder).

Cross Ref. – Cross references to Interface Hazard Analysis

Table 11: The mitigations from the IHA analysis



Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

System Fault Tree Analysis

CDRL 2-132-20

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	PM	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Wilton D. Alston Safety Engineer		Wilton D. Alston 2019.07.18 17:11:47 -04'00'
Verified:	Jason Weighley Safety Engineer		Jason W Weighley 2019.07.18 16:25:55 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.07.19 11:16:55 -04'00'
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group		Phil Magloire 2019.07.19 10:55:48 -04'00'
BT/SRA Review:	NA Title		
BT/SRA Review:	NA Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3035830

Effective Date:	Revision:	Language:
2019-07-18	_E	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2016-12-01	First issue.
_A	2017-12-02	Released.
_B	2016-12-06	Updated.
_B1	2017-09-01	Updated as per initial review comments on DRAFT, trees completely reworked, table(s) showing all events and gates, and traceability to subsystem trees, added.
_B2	2017-09-29	Updated as per comments from subsystem review, as well as additional comments on draft. Added traceability information as per subsystem FTAs.
_B3	2017-10-24	Updated as per comments from 2017-09-29 document submission, including updated trees.
_B4	2017-11-01	Updated as per comments from SYSTRA/AECOM from Review Form SI-RVW-0245 6-720-CDRL-20, Rev_B
_B5	2017-12-15	Updated as per comments from SYSTRA/AECOM from Review Form SI-RVW-0245 6-720-CDRL 2-132-20, Rev_B
_B6	2018-01-10	Updated as per comments from SYSTRA/AECOM from Review Form SI-RVW-0245 6-720-CDRL 2-132-20, Rev_B5
_B7	2018-02-14	Updated as per comments from SYSTRA/AECOM from Review Form SI-RVW-0245 6-720-CDRL 2-132-20, Rev_B6
_B8	2018-03-23	Updated as per comments from SYSTRA/AECOM from Review Form SI-RVW-0245 6-720-CDRL 2-132-20, Rev B7
_B9	2018-04-20	Updated to add RWPS Terminal Events.
_B10	2018_06_05	Updated to add RWPS
B11	2018_09_10	Updated to align with WIU FTA
_C	2018-11-19	Released for Baseline 3.2 aligned for OBC FTA changes. Updated to align with further OBC FTA changes, and respond to peer review.
_D	2019-04-04	Released for System Baseline 3.4 and to Resolve RR comments against Rev_C SI_RVW_0770
_E	2019-07-18	Updated to align with Rev_E OBC Fault Tree. Seperated Territories

Table of Contents

Section	Subject	Page
1	**Executive Summary**	7
2	**Introduction**	7
	2.1 Compliance Matrix	7
	2.2 Reference Documents	9
	2.3 Glossary	10
3	**Analysis Prerequisites**	11
	3.1 System Design	11
	3.2 General Assumptions	12
	3.3 Boundary Conditions	12
	3.4 Fault Types	12
	3.4.1 Internal ACSES II Fault Types	14
	3.4.2 External Fault Types	15
4	**Fault Tree Process**	15
	4.1 Fault Tree Tool	15
	4.2 Fault Tree Logic Gates	15
	4.3 Fault Tree Logic Events	16
5	**Fault Tree Methodology**	17
6	**Coverage Table, Traceability, Results, and Conclusions**	19
	6.1 Events Coverage and Traceability Table – ATC Territory	19
	6.2 Events Coverage and Traceability Table – CMB Territory	26
	6.3 Results and Conclusions	32
7	**Appendix – Fault Tree Diagrams**	33
	7.1 Trees for ATC Territory	33
	7.2 Trees for ABS/CMB Territory	63
8	**Appendix – Fault Tree Cut-Set Analysis**	91
	8.1 ATC Territory – Fault(s) with w Higher Than e^{-9}	91
	8.2 CMB Territory – Fault(s) with w Higher Than e^{-9}	92

List of Figures

Figure 1: System Architecture 11
Figure 2 – ATC Territory FTA Page 1: Top-Level Fault Tree for ACSES II System (ATC Territory) 33
Figure 3 – ATC Territory FTA Page 2: Collision Fault Tree for ACSES II System 34
Figure 4 – ATC Territory FTA Page 3: Overspeed Fault Tree for ACSES II System 35
Figure 5 – ATC Territory FTA Page 4: Human Error Leads to Overspeed 36
Figure 6 – ATC Territory FTA Page 5: Failure of Onboard to Enforce Speed 37
Figure 7 – ATC Territory FTA Page 6: Failure of Onboard to Correctly Process Transponder Data 38
Figure 8 – ATC Territory FTA Page 7: Transponder Data Errors 39
Figure 9 – ATC Territory FTA Page 8: Failure of Onboard to Correctly Process Wayside Data 40
Figure 10 – ATC Territory FTA Page 9: Wayside Delivers Erroneously Permissive Status to Onboard 41
Figure 11 – ATC Territory FTA Page 10: Onboard Subsystem Failure or Faults 42
Figure 12 – ATC Territory FTA Page 11: Interface (Transmission) Failure to Onboard Causes Incorrect Data 43
Figure 13 – ATC Territory FTA Page 12: Failure of Onboard to Correctly Process TSR Data 44
Figure 14 – ATC Territory FTA Page 13: Failure of Onboard to Correctly Process Vehicle Data 45
Figure 15 – ATC Territory FTA Page 14: Failure of ADU Leads to 46
Figure 16 – ATC Territory FTA Page 15: Vital Speed Protection Systems Cut-Out 47
Figure 17 – ATC Territory FTA Page 16: Unsafe Train Entry / Exit 48
Figure 18 – ATC Territory FTA Page 17: Onboard Fails to Enforce Positive Train Stop (PTS) 49
Figure 19 – ATC Territory FTA Page 18: Unsafe Enforcement of Positive Train Stop (PTS) 50
Figure 20 – ATC Territory FTA Page 19: ATC Fails to Automatically Cut-In 51
Figure 21 – ATC Territory FTA Page 20: Train Violates Positive Train Stop (PTS) 52
Figure 22 – ATC Territory FTA Page 21: Operational Error by Train Engineer or Dispatcher 53
Figure 23 – ATC Territory FTA Page 22: Obstruction on Track 54
Figure 24 – ATC Territory FTA Page 23: Failure to Establish TSR or Enforce TSR 55
Figure 25 – ATC Territory FTA Page 24: Derailment 56
Figure 26 – ATC Territory FTA Page 25: Unsafe Switch Movement or Positioning 57
Figure 27 – ATC Territory FTA Page 26: Unsafe Switch Movement 58
Figure 28 – ATC Territory FTA Page 27: Personnel or Passenger Death or Injury 59
Figure 29 – ATC Territory FTA Page 28: Select-Check-Execute Failure Combined with RWPS and Crew Procedure Failure 60
Figure 30 – ATC Territory FTA Page 29: RWPS Subsystem Faults 61

Figure 31 – FTA Page 30: Fire 62
Figure 32 – ABS / CMB Territory FTA Page 1: Top-Level Fault Tree for ACSES II System (ABS/CMB Territory) 63
Figure 33 – ABS/CMB Territory FTA Page 2: Collision Fault Tree for ACSES II System 64
Figure 34 – ABS/CMB Territory FTA Page 3: Overspeed Fault Tree for ACSES II System 65
Figure 35 – ABS/CMB Territory FTA Page 4: Human Error Leads to Overspeed 66
Figure 36 – ABS/CMB Territory FTA Page 5: Failure of Onboard to Enforce Speed 67
Figure 37 – ABS/CMB Territory FTA Page 6: Failure of Onboard to Correctly Process Transponder Data 68
Figure 38 – ABS/CMB Territory FTA Page 7: Transponder Data Errors 69
Figure 39 – ABS/CMB Territory FTA Page 8: Failure of Onboard to Correctly Process Wayside Data 70
Figure 40 – ABS/CMB Territory FTA Page 9: Wayside Delivers Erroneously Permissive Status to Onboard 71
Figure 41 – ABS / CMB Territory FTA Page 10: Onboard Subsystem Failure or Faults 72
Figure 42 – ABS / CMB Territory FTA Page 11: Interface (Transmission) Failure to Onboard 73
Figure 43 – ABS / CMB Territory FTA Page 12: Failure of Onboard to Correctly Process TSR Data 74
Figure 44 – ABS/ CMB Territory FTA Page 13: Failure of Onboard to Correctly Process Vehicle Data 75
Figure 45 – ABS CMB Territory FTA Page 14: Failure of ADU Leads to Overspeed 76
Figure 46 – ABS / CMB FTA Page 15: Unsafe Train Entry / Exit Between ACSES II Territories 77
Figure 47 – ABS / CMB FTA Page 16: Onboard Fails to Enforce Positive Train Stop (PTS) 78
Figure 48 – ABS / CMB FTA Page 17: Unsafe Enforcement of Positive Train Stop (PTS) 79
Figure 49 – ABS / CMB FTA Page 18: Train Violates Positive Train Stop (PTS) 80
Figure 50 – ABS / CMB FTA Page 19: Obstruction on Track 81
Figure 51 – ABS / CMB FTA Page 20: Failure to Establish TSR or Enforce TSR After Highway Obstruction 82
Figure 52 – ABS / CMB FTA Page 21: Derailment 83
Figure 53 – ABS / CMB FTA Page 22: Unsafe Switch Movement or Positioning 84
Figure 54 – ABS / CMB FTA Page 23: Unsafe Switch Movement 85
Figure 55 – ABS / CMB FTA Page 24: Human Error and Interlocking Failure in MBS Territory 86
Figure 56 – ABS / CMB FTA Page 25: Personnel or Passenger Death or Injury 87
Figure 57 – ABS / CMB FTA Page 26: Select-Check-Execute Failure Combined with RWPS and Crew Procedure Failure 88
Figure 58 – ABS / CMB FTA Page 27: Work Crew Error Combined with RWPS Fault 89
Figure 59 – ABS / CMB FTA Page 28: Fire 90

List of Tables

Table 1: Compliance Matrix 7
Table 2: Reference Documents 9
Table 3: Terms Specific to this Document 10
Table 4: Acronyms Specific to this Document 10
Table 5: Fault Categorization 13
Table 6: Basic Event Traceability to Exported Subsystem(s) – ATC Territory 19
Table 7: Basic Event Traceability to Exported Subsystem(s) – ABS / CMB Territory 26
Table 8: Cut-Set Analysis – ATC Territory – Fault(s) with **w** Higher Than e^{-9} 91
Table 9: Cut-Set Analysis – CMB Territory – Fault(s) with **w** Higher Than e^{-9} 92

1 Executive Summary

This document is a high Level analysis of system faults to identify system fault events and to quantify safety targets for each ACSES II subsystem contained in the LIRR PTC System.

The System Fault Tree analysis will cover the full extent of operations of the LIRR ACSES II System including all subsystems, safety related interfaces, operating environments, and malfunctions to the system. This fault tree will confirm the safety targets assigned to each subsystem. The System Fault Tree analysis excludes:

- Tenant railroad equipment except for ensuring interoperability;
- External equipment located outside of the LIRR ACSES II system boundary that does not interface to the ACSES II system. Where external equipment does interface to the system this FTA will only analyze the effects of Failures of the External equipment and not the cause within that equipment. Failure rates for external equipment will be provided by others;
- Environmental conditions exceeding the specifications listed in Vol 2 Part 1 Section 5.3.9 of the contract specification; and,
- Other external factors, such as, vandalism, gas-build, rolling stock, and construction.

2 Introduction

This analysis looks at the system level faults that combine to form the identified accidents described in the PHA [2] analysis. The faults have been analyzed and derived into the subsystem faults that contribute to each accident. The hazard log will be updated to link each fault tree event back to an entry in the Project Hazard Log [3] where the appropriate mitigation and description is described.

Each subsystem will derive its own Fault Tree that expands the Terminal or Basic events from this System FTA into further fault detail and provides a further analysis that contributes to the events identified in this system level analysis.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
2	12.10.8	Fault Tree Analysis	Detailed description of required content of the System FTA, listed here.	3

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.8, Subsection A		A system-level Fault Tree Analysis (FTA), CDRL 2-132, shall be submitted by the SI. The system-level FTA shall be used to allocate quantified targets to the ACSES II Subsystems. The ACSES II Subsystem FTA shall be used as part of the evidence to support compliance with the quantified safety requirements allocated to the ACSES II Subsystems	
	12.10.8, Subsection B		The FTA analysis shall furnish a structured means of identifying faults associated with the ACSES II System and ACSES II Subsystem, which must be mitigated, and shall identify the system functions requiring fail-safe implementation. The FTA shall identify the system and subsystem faults, starting with the top level ACSES II System design and the SHL-identified hazards, clearly identifying the logical combinations of faults which are contributors to the hazard, and subsequently developed to the subsystem and interface level.	
	12.10.8, Subsection C		The system-level FTA terminal events shall be used as the top-level events of detailed Fault Tree Analyses (FTAs), which analyze the hardware, and software of each ACSES II Subsystem performing vital functions. System level FTA terminal faults shall be reviewed for possible transfer to the Project Hazard Log for action, tracking, and review	

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.8, Subsection D		The Fault Tree Analysis deliverables shall contain, as a minimum, the following elements: 1. A discussion of the analytic techniques used to generate the fault tree. 2. Explanation of the types of faults considered part of the ACSES II and those, which are external to the ACSES II, if any. 3. A comprehensive FTA diagram, using a graphical tool, which is suitable for the presentation of the tree logic in a clear and understandable manner. The symbols used and their meaning shall be explained in the text. Each fault or hazard shall be uniquely identified by a reference number.	
	12.10.8, Subsection E		Reference from the unique terminal faults to where their resolution is addressed (e.g., further safety analysis, specific design techniques, Safety V&V, test). Subsequent to the system-level FTA, the ACSES II Subsystem suppliers shall submit FTA(s) to identify the elements that can combine to result in Category I events. The ACSES II Subsystem suppliers shall submit FTA as an input to the overall system-level FTA to be produced by the SI.	

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624
[2]	Preliminary Hazard Analysis CDRL 2-127	3035821
[3]	Project Hazard Log CDRL 2-126-20	3035819
[4]	ISOGRAPH Reliability Workbench, Version 12.0	N.A
[5]	System Design Description CDRL 2-27	3035724
[6]	LIRR System Architecture	3038633
[7]	LIRR System PSP CDRL 2-123-20	3035815

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in

Table 3 and Table 4 respectively.

Table 3: Terms Specific to this Document

Term	Definition
Fault Tree top event	Top event of a fault tree, corresponding to a top-level hazard
Fault Tree basic events	Lower level event in fault tree, usually corresponding to a hazard from the list of hazards.

Table 4: Acronyms Specific to this Document

Acronym	Definition
FTA	Fault Tree Analysis
PHA	Preliminary Hazard Analysis
MTTHE	Mean Time to Hazardous Event
NA	Not Applicable
TBD	To Be Determined

3 Analysis Prerequisites

3.1 System Design

A full detailed description of the system design is provided by the System Design Description [5]. Additional details and system architecture is provided in the LIRR System Architecture Description [6].

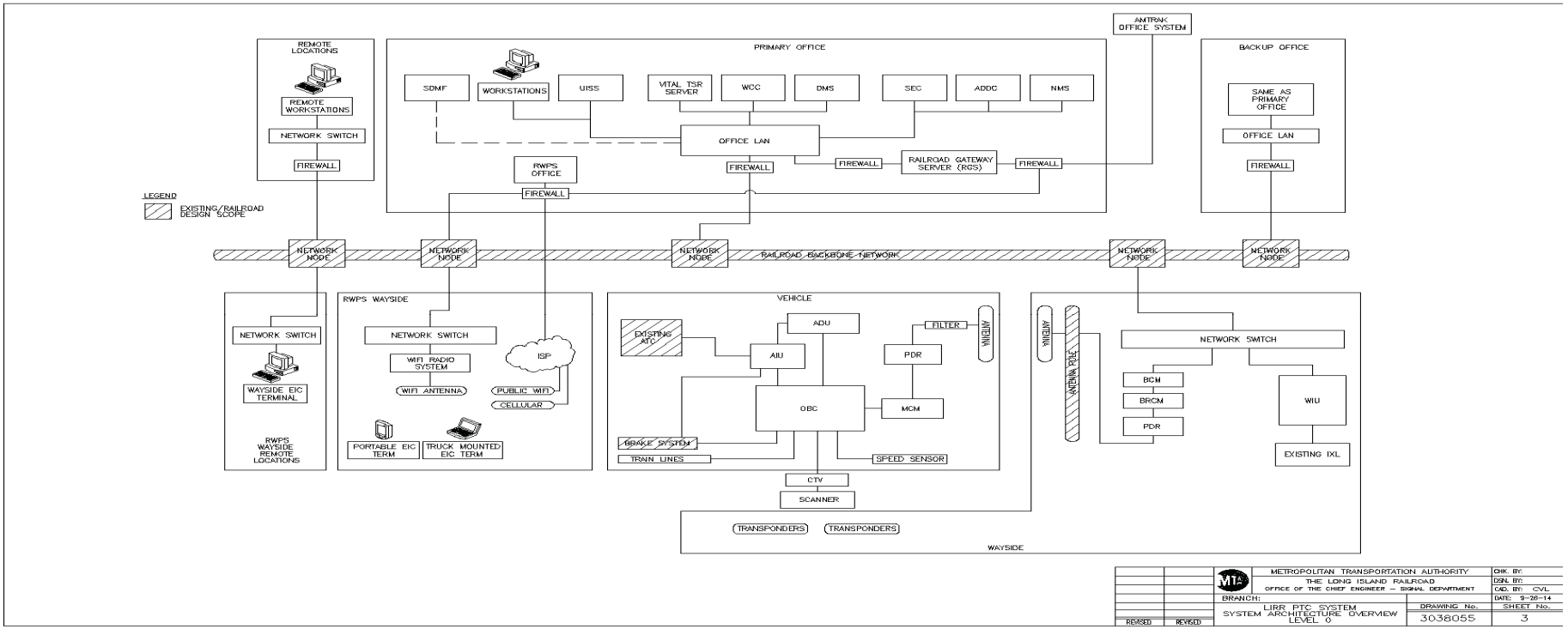


Figure 1: System Architecture

3.2 General Assumptions

The following general assumptions apply to the System FTA.

- The analysis covers normal operation of the equipment. The equipment is correctly installed.
- The analysis covers anticipated operation, including degraded mode, component failure, and human error.
- This analysis covers the Office, Onboard, Comms, RWPS, Wayside and Transponder subsystems and their interfaces as shown in Figure 1.
- External systems that interface to the system will be analyzed only to determine the impact of the external system failure. No other analysis on the external system will be performed. This includes the existing wayside Interlocking (ASC, ABS and CMB), Train lines, and onboard ATC systems.
- Changes in Operation caused by the differently-signaled territories within the LIRR system will be addressed in the System OHA and will also be addressed in this analysis, resulting in two (2) complete trees, one covering ATC Territory and one covering CMB Territory.
- In the cases of processor-based subsystems / components, an MTTHE for each processor-based subsystem or component, or both, has been used as appropriate relevant terminal events, indicating the safety-critical behavior of the integrated hardware/software subsystem or component, or both.

3.3 Boundary Conditions

The following general assumptions apply to the System FTA

- The Preliminary Hazard Analysis [2] used as a basis for the FTA.

3.4 Fault Types

The effects of the system faults mitigated by ACSESS II that could otherwise result in the accidents/mishaps defined in the Preliminary Hazard Analysis and can be categorized into the events presented in

Table 5. The consequences are defined in terms of accidents/mishaps that can occur in the operation of the railway, and are identified based on:

- Understanding the high-level general overview of the ACSES II System and the railroad system as show in the System Description Document, with portions of the ACSES II System, specifically the subsystem functionality, being treated as a “Black Box”; and,
- Experience in previous PTC System projects.

Table 5: Fault Categorization

Fault – Top Level Events	Faults Breakdown
Collision	Includes Train-to-Train and Train-to-Object obstruction events, as well as various Overspeed events. • Overspeed • Unsafe Train Entry / Exit between ACSES Territories (and Other Systems) • Unsafe Enforcement of a Positive Train Stop (PTS) • Train Violates Positive Train Stop (PTS), including East Side Access Entry (Tunnel Collision Avoidance) • Obstruction on Track
Derailment	Includes Train crossing misaligned switches, as well as overspeed events: • Overspeed • Unsafe Switch Movement • Front of Train Encroaches into Interlocking Due to Incorrect Position Calculation
Personnel or Passenger Death or Injury	Includes Train personnel, passengers (or trespassers) struck by trains and other staff-related injuries, as defined in the PHA: • Work Zone Protection • Train Engineer Applies Unnecessary Penalty or Emergency Break • Overspeed • Electrical Shock or Electrocution • Passengers or Staff Affected by EMI/EMC
Fire	This is an Undeveloped Fault. The design of the ACSES II shall incorporate fire retardant materials as possible.

The system was analyzed based on the functional description breakdown provided in the System Design Description [5]. Each subsystem, based on its assigned functionality, was analyzed to determine what accidents / mishaps would occur based on the assigned functionality and defined interfaces. The analysis also looked at the data contained and used by each subsystem to determine where that data, and the process used to develop that data, would also contribute to the defined accidents/mishaps.

3.4.1 Internal ACSES II Fault Types

The following list is a list of the Faults relevant to the LIRR ACSES II System. Some of these faults are relevant to portions of the system that reside below the subsystem level. Only the subsystem level faults or vital components will be analyzed in this System Fault Tree on the LIRR ACSES II System. The components that could fail that are below the subsystem level are shown for information.

Onboard Subsystem Failures

- OBC H/W Failure(s)
    - AIU Failure
    - ADU Failure
    - Train Type Selector Failure (MNR ONLY)
    - MCM Failure
- Onboard-to-WIU Interface Failure
- Onboard-to-STS Interface Failure
- Onboard-to-Transponder Interface Failure
- Onboard-to-ATC Interface Failure
- Speed Sensor Failure

Wayside Subsystem Failures

- WIU H/W Failure
- WIU Configuration Data Failure

Office Subsystem Failures

- Office H/W Failure(s)
    - STS Failure
    - UIS Failure
    - NMS Failure
    - WCC Failure
    - RGS Failure
- Office Database Failure
- TSR Request Failure

Transponder Subsystem Failures

- Transponder Failure
- Transponder Data Failure

RWPS Subsystem Failures

- TSR Request Failure
- TSR Removal Failure
- TSR Attachment Failure

3.4.2 External Fault Types

The following external Faults are derived from the System Fault Tree Analysis:

- Signaling Logic Fails to provide correct Interlocking Status to WIU
- Onboard Cab Signaling Fails to Enforce Train Speed
- Adjacent Railroad STS Failure
- Adjacent Railroad OBC Failure
- Adjacent Railroad WIU Failure
- Obstruction on Track
- Duplicate Train IDs Between Railroads

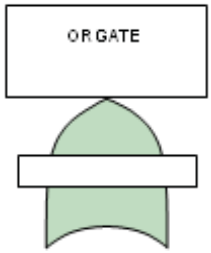
4 Fault Tree Process

In this document, fault trees were developed to illustrate the relationship between the primary hazards and their potential causative fault events. The following sections, including the definitions for the symbols used in the fault tree diagrams, provides additional insight into the process shown in this document. The complete set of graphical trees is shown in the Appendix. Additionally, because LIRR has two (2) distinct territories with varying levels of equipment to vitally ensure safety—Automatic Train Control (ATC) versus Controlled Manual Block (CMB)—these territories are treated separately, with a tree being developed for each. As a result, there are subsections in the following sections to cover ATC and CMB territories separately. The development of the FTA is identical for each..

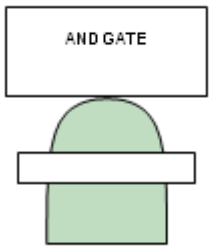
4.1 Fault Tree Tool

Fault trees are designed using the ISOGRAPH Reliability Workbench [4] software.

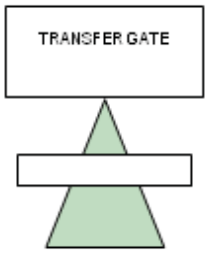
4.2 Fault Tree Logic Gates



OR Gate – The event described by the gate text occurs if at least *one* of the underlying events occur. Logically, there must be at least two input events to an OR Gate.

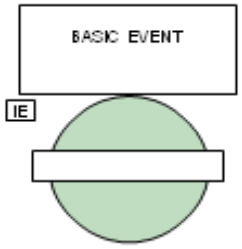


AND Gate – The event described by the gate text occurs if *all* the underlying events occur. Logically, there must be at least two input events to an AND Gate.

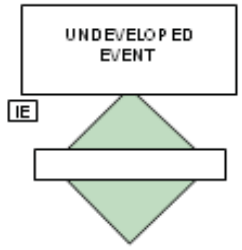


TRANSFER Gate – Transfer to other fault tree page. It is used to link logic in separate areas of a fault tree. When you insert a transfer gate, both a transfer in gate and a transfer out gate are inserted. The transfer in gate links to the transfer out gate, which represents the top gate of another fault tree. The transfer can also be to more than one out gate.

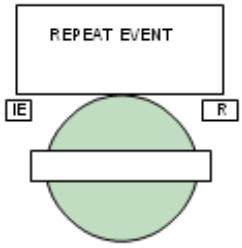
4.3 Fault Tree Logic Events



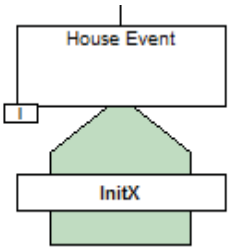
Basic Event – Primary event, e.g. component failure or human error. A Basic event represents the lowest level, or terminating event, in a fault tree. It has no inputs. It simply represents the occurrence of an event in the system being analyzed. A Basic event is either a component-level event that is not further resolved or an external event. Basic events can include hardware or software failures, human errors, and system failures.



Undeveloped Event – An Undeveloped event is used if the information necessary for developing the event is not currently available, or when the event is out-of-scope or not applicable to the analysis. This category of events is applicable to existing, standard, railroad operations that are not changed by the introduction of ACSES II.



Repeat Event – “R” Indicates that this event has been used elsewhere in the fault tree diagrams.



A “house” shaped symbol represents an event that occurs outside the scope of the subsystem under analysis, but represents an initiating event relating to the subsystem and if the analysis were to be quantified it can be assumed to have a probability of occurrence of 1 in most cases. The House event represents mechanisms that are outside the associated subsystem boundaries, but are relevant to understanding the hazard potential within the subsystem in question.

5 Fault Tree Methodology

The fault tree employs a Top-Down Methodology, whereby general categories of faults, such as Collision, Derailment, and Overspeed, are analyzed in an ever-expanding manner, identifying contributing faults. These contributing faults are further decomposed until a final fault, referred to as a Terminal Event, is discovered. These Terminal Events are thereafter exported to the ACSES II Subsystem that will be responsible for them. This system FTA ends at the identification of those Terminal Events. The Events Coverage and Traceability Table, shown in Section 6.1 shows the results of the exportation to subsystems. The identified Terminal Events fall into several categories, each of which could be treated differently with regard to determining the overall system failure rate. These categories, and how they are treated is below:

- All Subsystems: These faults that are mitigated by functionality or requirements placed on all subsystems, such as fire retardancy.
- Comm: These faults are mitigated by the functionality in the Communications Subsystem.
- Human Error: These faults will have the standard failure rate for a trained person, which will be 10^{-3} failures/hour.
- Office: These faults are mitigated by functionality in the Office Subsystem;
- Onboard: These faults are mitigated by functionality in the Vehicle Subsystem;
- Railroad: These are faults that are mitigated by standard RR practice(s).
- RWPS: These are faults that are mitigated by the Railway Worker Protection System
- Transponder: These faults are mitigated primarily by the Transponder portion of the Wayside Subsystem;
- Wayside: These faults are mitigated primarily by the WIU portion of the Wayside Subsystem.

The completed subsystem analyses will contain failure probabilities for these events, which will be incorporated into the System FTA, to derive a system rate. In cases where analysis via Fault Tree Analysis has taken place, a reference to the event of interest on the corresponding subsystem tree is shown, with a designation such as “SISSO,” which is used on the Onboard FTA.

Assumptions used for the methodology used in this analysis are shown below:

- For the purposes of completing a full quantitative FTA, the mission time will be set to 20 years, or 175,200 hours, which is the number of hours in 20 years.

- In the cases of “Interface” faults, the responsibility will generally be placed upon the subsystem that is receiving the data, e.g., FFT1.1.4.1.2 Interface Failure Between Onboard and Transponder Causes Corrupted or Incorrect Data, is exported to the Onboard system for mitigation.
- In the cases of faults that are allocated to the Communications Subsystem, no FTA will be generated, but a generic failure rate will be used in this analysis.

6 Coverage Table, Traceability, Results, and Conclusions

6.1 Events Coverage and Traceability Table – ATC Territory

Basic Event Traceability Table Key

In the table below, which shows all the BASIC or Terminal Events from the System FTA, the following columns are found:

- **Name** – The designation of the Event or Gate in the System FTA;
- **Description** – The description of the Event or Gate from the System FTA;
- **Exported Subsystem** – The subsystem to which the Terminal Event has be exported. For items that are out of the scope of ACSES II, "Out-of-Scope" is shown. For items related to operating procedures or existing RR responsibility, "Operation/Manual" or "Railroad" are shown, respectively. For items covered by existing Type Approved Functions, "*Legacy*" is shown.;
- **w** – The failure rate for the fault, either as shown on the subsystem tree, or as derived from industry standards.
- **Model Name or Subsystem Reference** – The designation of the Event or Gate in the Subsystem FTA, if applicable;
- **Subsystem FTA Event Description** – The description of the event from the subsystem tree that corresponds to, or which has been allocated to, the event shown from the System FTA, if applicable.
- **Comments** – Relevant Comments about the Event or Gate, if applicable.

Table 6: Basic Event Traceability to Exported Subsystem(s) – ATC Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	[redacted]	Model Name or Subsystem Reference	Subsystem FTA Event Description	Comments
1	FFT1.1.1	Brake Assurance Function Not Enforced. [Onboard]	Onboard		Onboard_FT1	Brake assurance function not enforced	
2	FFT1.1.2.1	Train Engineer Fails to Follow Procedures. [Human Error]	Human Error		Human Error		
3	FFT1.1.2.2	ATC Fails to Enforce Civil Speed. [Legacy]	Legacy		Design Mitigation		
4	FFT1.1.3.1.2	ADU Displays PTC-Related Aspect Despite ACSES II Being Cut-Out. [Onboard]	Onboard		Onboard_FT2	ADU displays aspect incorrectly	

Table 6: Basic Event Trace [redacted] Subsystem(s) – ATC Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	Model Name or Subsystem Reference	Subsystem FTA Event Description	Comments
5	FFT1.1.3.3.1	ADU Displays an Incorrect Aspect. [Onboard]	Onboard	Onboard_GT1	ADU incorrectly displays a different aspect	
6	FFT1.1.3.6	ADU Fails to Send PTS Stop Request to AIU. [Onboard]	Onboard	Onboard_FT5	ADU fails to send PTS stop request to AIU	
7	FFT1.1.4	Vehicle Service Penalty Brake Fails. [Legacy]	Legacy	Design Mitigation		
8	FFT1.1.4.1.1.2	Transponder Not Detectable. [Transponder]	Transponder	Transponder_H1		
9	FFT1.1.4.1.1.3	Transponder Bogus Telegram. [Transponder]	Transponder	Transponder_H4		
10	FFT1.1.4.1.2	Interface Failure Between Onboard and Transponder Causes Corrupt or Incorrect Data. [Onboard]	Onboard	Onboard_FT6	Interface failure between onboard and transponder causes corrupt or incorrect data	
11	FFT1.1.4.1.3	Transponder Installation Errors. [Transponder]	Transponder	Transponder_H7		
12	FFT1.1.4.1.3.1	Onboard Processes Data From Incorrect Transponder. [Onboard]	Onboard	Onboard_FT7	Onboard process incorrect transponder data	
13	FFT1.1.4.1.3.2	OBC Fails to Process Transponder Message. [Onboard]	Onboard	Onboard_GT15	Replaced with GT15, GT15 referenced in FT13	
14	FFT1.1.4.1.3.3	Train Reads Transponder from Another Track. [Onboard]	Onboard	Onboard_FT27	Train reads transponder from another track	
15	FFT1.1.4.1.4	Incorrect Data Programmed Into Transponder. [Transponder]	Transponder	Transponder_H6		

Table 6: Basic Event Tracea [redacted] d Subsystem(s) – ATC Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	[redacted]	Model Name or Subsystem Reference	Subsystem FTA Event Description	Comments
16	FFT1.1.4.2.1	Interface Failure Wayside-WIU. [Wayside]	Wayside		Wayside_GATE01		
17	FFT1.1.4.2.2	Onboard Fails to Process Wayside (Data Radio) Message Correctly. [Onboard]	Onboard		Onboard_FT8	Onboard processes incorrect data radio message	
18	FFT1.1.4.2.9.2	Communication Error WIU-OBC. [Wayside]	Wayside		Wayside_GATE02		
19	FFT1.1.4.2.9.3	Maintenance Error. [Wayside]	Wayside		Wayside_GATE03		
20	FFT1.1.4.2.9.4	Communication Failure WIU-Main. [Wayside]	Wayside		Wayside_GATE04		
21	FFT1.1.4.2.9.5	WIU Software Failure. [Wayside]	Wayside		Wayside_GATE05		
22	FFT1.1.4.2.9.6	WIU Hardware Failure. [Wayside]	Wayside		Wayside_EVENT 69		
23	FFT1.1.4.3.2.1	EMI from Nearby Source Causes Unsafe Operation. [Onboard]	Onboard		Onboard_FT9	EMI from Nearby Source Causes Unsafe Operation	
24	FFT1.1.4.3.2.2	EMI from Onboard Components Causes Unsafe Operation. [Onboard]	Onboard		Onboard_FT10	EMI from Onboard Components Causes Unsafe Operation	
25	FFT1.1.4.3.5.2	Interface (Transmission) Failure Causes Incorrect Data. [Comm]	Comm		Design Mitigation		
26	FFT1.1.4.3.5.3	Message Sent to Incorrect Train. [All Subsystems]	All Subsystems		Design Mitigation		
27	FFT1.1.4.3.6	Onboard Fails to Process an Overspeed. [Onboard]	Onboard		Onboard_FT16	OBC Fails to enforce overspeed	

Table 6: Basic Event Tracea [redacted] d Subsystem(s) – ATC Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	[redacted]	Model Name or Subsystem Reference	Subsystem FTA Event Description	Comments
28	FFT1.1.4.4.1.1	Primary PH04; Overspeed Due to STS Error. [Office]	Office		Office Overspeed		
29	FFT1.1.4.4.1.2	Primary PH06; Insufficient Protection for Railway Worker. [Office]	Office		Office PH06		
30	FFT1.1.4.4.1.4	STS Failure Leads to Hazardous Output. [Office]	Office		Office STS Output		
31	FFT1.1.4.4.2	Incorrect TSR Enforcement; Mishandling of TSR. [Onboard]	Onboard		Onboard_FT11	Incorrect TSR enforcement	
32	FFT1.1.4.5.2	Corrupt Vehicle Type Parameter(s) Used by OBC. [Onboard]	Onboard		Onboard_FT18	Corrupt vehicle parameter used by OBC	
33	FFT1.1.5	Onboard Subsystem(s) Fails to Measure Speed Correctly. [Onboard]	Onboard		Onboard_FT19	Vehicle speed measured incorrectly	
34	FFT1.3.1.1	Dispatcher Gives Unsafe Order to Pass Restrictive Signal. [Human Error]	Human Error		Human Error		
35	FFT1.3.4	Existing ATC Faills to Maintain Movement Authority. [Legacy]	Legacy		Design Mitigation		
36	FFT1.3.5.5	Existing ATC Fails. [Legacy]	Legacy		Design Mitigation		
37	FFT1.4.3.2.1	Train Engineer Fails to Follow Procedure. [Human Error]	Human Error		Human Error		
38	FFT1.4.3.2.2	Dispatcher Issues Improper Exit Order. [Human Error]	Human Error		Human Error		

Table 6: Basic Event Tracea [redacted] Subsystem(s) – ATC Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	Model Name or Subsystem Reference	Subsystem FTA Event Description	Comments
39	FFT1.4.3.4	OBC Allows East Side Access to Non-Approved Vehicle. [Onboard]	Onboard	Onboard_FT22	OBC allows east side access to non-approved vehicle	
40	FFT1.4.4	Train passes PTS without confirmation that signals are clear. [Onboard]	Onboard	Onboard_FT23	Train passes PTS without confirmation that signal is clear	
41	FFT1.5.4.1	SAR Failure Not Detected. [Onboard]	Onboard	Onboard_FT24	SAR failure not detected	
42	FFT1.5.4.2.1	Failure to Establish Stop-And-Release TSR After Problem Reported. [Human Error]	Human Error	Human Error		
43	FFT2.1	Front of Train Offset is Incorrect. [Onboard]	Onboard	Onboard_FT25	Front of train offset is incorrect	
44	FFT2.2.1	Train Engineer Passes Red Signal. [Human Error]	Human Error	Human Error		
45	FFT2.2.2	ATC Fails to Protect Against Unsafe Movement of Switch. [Legacy]	Legacy	Design Mitigation		
46	FFT2.2.3.1.2	Dispatcher Commands Unsafe Switch Movement. [Human Error]	Human Error	Human Error		
47	FFT2.2.4	WIU Misreports Status of a Switch. [Legacy]	Legacy	Design Mitigation		
48	FFT3.1.2.1.1	RWPS Fails to Properly Create a TSR. [RWPS]	RWPS	Non-Vital System		
49	FFT3.1.2.1.2	RWPS Erroneously Requests Removal of a TSR. [RWPS]	RWPS	Non-Vital System		

Table 6: Basic Event Tracea [redacted] d Subsystem(s) – ATC Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	[redacted]	Model Name or Subsystem Reference	Subsystem FTA Event Description	Comments
50	FFT3.1.2.1.3	RWPS Fails to Properly Attach to an Existing TSR. [RWPS]	RWPS		Non-Vital System		
51	FFT3.1.2.2	Work Crew Fails to Follow Procedure. [Human Error]	Human Error		Human Error		
52	FFT4.1	ACSES II Design Shall Incorporate Non-Toxic, Non-Explosive, and Flame-Retardant Materials. [All Subsystems]	All Subsystems		Design Mitigation		
53	FFT1.1.1	Brake Assurance Function Not Enforced. [Onboard]	Onboard		Onboard_FT1	Brake assurance function not enforced	
54	FFT1.1.2.2	ATC Fails to Enforce Civil Speed. [Legacy]	Legacy		Design Mitigation		
55	FFT1.1.3.1.2	ADU Displays PTC-Related Aspect Despite ACSES II Being Cut-Out. [Onboard]	Onboard		Onboard_FT2	ADU displays aspect incorrectly	
56	FFT1.1.3.2.2	ACSES II Cut-Out Switch Failure. [Onboard]	Onboard		Onboard_FT3	ACSES cut-out switch failure	
57	FFT1.1.3.3.1	ADU Displays an Incorrect Aspect. [Onboard]	Onboard		Onboard_GT1	ADU incorrectly displays a different aspect	
58	FFT1.1.3.6	ADU Fails to Send PTS Stop Request to AIU. [Onboard]	Onboard		Onboard_FT5	ADU fails to send PTS stop request to AIU	
59	FFT1.1.4	Vehicle Service Penalty Brake Fails. [Legacy]	Legacy		Design Mitigation		
60	FFT1.1.4.1.1.2	Transponder Not Detectable. [Transponder]	Transponder		Transponder_H1		

Table 6: Basic Event Tracea [redacted] d Subsystem(s) – ATC Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	[redacted]	Model Name or Subsystem Reference	Subsystem FTA Event Description	Comments
61	FFT1.1.4.1.1.3	Transponder Bogus Telegram. [Transponder]	Transponder		Transponder_H4		
62	FFT1.1.4.1.2	Interface Failure Between Onboard and Transponder Causes Corrupt or Incorrect Data. [Onboard]	Onboard		Onboard_FT6	Interface failure between onboard and transponder causes corrupt or incorrect data	

6.2 Events Coverage and Traceability Table – CMB Territory

Basic Event Traceability Table Key

In the table below, which shows all the BASIC or Terminal Events from the System FTA, the following columns are found:

- **Name** – The designation of the Event or Gate in the System FTA;
- **Description** – The description of the Event or Gate from the System FTA;
- **Exported Subsystem** – The subsystem to which the Terminal Event has be exported. For items that are out of the scope of ACSES II, "Out-of-Scope" is shown. For items related to operating procedures or existing RR responsibility, "Operation/Manual" or "Railroad" are shown, respectively. For items covered by existing Type Approved Functions, "*Legacy*" is shown.;
- **w** – The failure rate for the fault, either as shown on the subsystem tree, or as derived from industry standards.
- **Model Name or Subsystem Reference** – The designation of the Event or Gate in the Subsystem FTA, if applicable;
- **Subsystem FTA Event Description** – The description of the event from the subsystem tree that corresponds to, or which has been allocated to, the event shown from the System FTA, if applicable.
- **Comments** – Relevant Comments about the Event or Gate, if applicable.

Table 7: Basic Event Traceability to Exported Subsystem(s) – ABS / CMB Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	[redacted]	Model Name or Subsystem Reference	Subsystem FTA Event Description (Latest)	Comments
1	FFT1.1.1	Brake Assurance Function Not Enforced. [Onboard]	Onboard		Onboard_FT1	Brake assurance function not enforced	
2	FFT1.1.2.1	Train Engineer Fails to Follow Procedures. [Human Error]	Human Error		Human Error		
3	FFT1.1.3.1.2	ADU Displays PTC-Related Aspect Despite ACSES II Being Cut-Out. [Onboard]	Onboard		Onboard_FT2	ADU displays aspect incorrectly	
4	FFT1.1.3.2.2	ACSES II Cut-Out Switch Failure. [Onboard]	Onboard		Onboard_FT3	ACSES cut-out switch failure	
5	FFT1.1.3.3.1	ADU Displays an Incorrect Aspect. [Onboard]	Onboard		Onboard_GT1	ADU incorrectly displays a different aspect	

Table 7: Basic Event Traceability to Exported Subsystem(s) – ABS / CMB Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	[redacted]	Model Name or Subsystem Reference	Subsystem FTA Event Description (Latest)	Comments
6	FFT1.1.3.6	ADU Fails to Send PTS Stop Request to AIU. [Onboard]	Onboard		Onboard_FT5	ADU fails to send PTS stop request to AIU	
7	FFT1.1.4	Vehicle Service Penalty Brake Fails. [Legacy]	Legacy		Design Mitigation		
8	FFT1.1.4.1.1.2	Transponder Not Detectable. [Transponder]	Transponder		Transponder_H1		
9	FFT1.1.4.1.1.3	Transponder Bogus Telegram. [Transponder]	Transponder		Transponder_H4		
10	FFT1.1.4.1.2	Interface Failure Between Onboard and Transponder Causes Corrupt or Incorrect Data. [Onboard]	Onboard		Onboard_FT6	Interface failure between onboard and transponder causes corrupt or incorrect data	
11	FFT1.1.4.1.3	Transponder Installation Errors. [Transponder]	Transponder		Transponder_H7		
12	FFT1.1.4.1.3.1	Onboard Processes Data From Incorrect Transponder. [Onboard]	Onboard		Onboard_FT7	Onboard process incorrect transponder data	
13	FFT1.1.4.1.3.2	OBC Fails to Process Transponder Message. [Onboard]	Onboard		Onboard_GT15	Replaced with GT15, GT15 referenced in FT13	
14	FFT1.1.4.1.3.3	Train Reads Transponder from Another Track. [Onboard]	Onboard		Onboard_FT27	Train reads transponder from another track	
15	FFT1.1.4.1.4	Incorrect Data Programmed Into Transponder. [Transponder]	Transponder		Transponder_H6		
16	FFT1.1.4.2.1	Interface Failure Wayside-WIU. [Wayside]	Wayside		Wayside_GATE01		
17	FFT1.1.4.2.2	Onboard Fails to Process Wayside (Data Radio) Message Correctly. [Onboard]	Onboard		Onboard_FT8	Onboard processes incorrect data radio message	
18	FFT1.1.4.2.9.2	Communication Error WIU-OBC. [Wayside]	Wayside		Wayside_GATE02		

Table 7: Basic Event Traceability to Exported Subsystem(s) – ABS / CMB Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	[redacted]	Model Name or Subsystem Reference	Subsystem FTA Event Description (Latest)	Comments
19	FFT1.1.4.2.9.3	Maintenance Error. [Wayside]	Wayside		Wayside_GATE03		
20	FFT1.1.4.2.9.4	Communication Failure WIU-Main. [Wayside]	Wayside		Wayside_GATE04		
21	FFT1.1.4.2.9.5	WIU Software Failure. [Wayside]	Wayside		Wayside_GATE05		
22	FFT1.1.4.2.9.6	WIU Hardware Failure. [Wayside]	Wayside		Wayside_EVENT 69		
23	FFT1.1.4.3.2.1	EMI from Nearby Source Causes Unsafe Operation. [Onboard]	Onboard		Onboard_FT9	EMI from Nearby Source Causes Unsafe Operation	
24	FFT1.1.4.3.2.2	EMI from Onboard Components Causes Unsafe Operation. [Onboard]	Onboard		Onboard_FT10	EMI from Onboard Components Causes Unsafe Operation	
25	FFT1.1.4.3.5.1	Interface Failures Between Onboard and STS Causes Corrupted or Incorrect Data. [Onboard]	Onboard		Onboard_FT13	Interface failures between onboard and STS causes corrupted or incorrect Data	
26	FFT1.1.4.3.5.10	Onboard Main PCB Failure Causes Incorrect Message Processing. [Onboard]	Onboard		Onboard_FT14	Onboard main PCB failure causes incorrect message processing	
27	FFT1.1.4.3.5.2	Interface (Transmission) Failure Causes Incorrect Data. [Comm]	Comm		Design Mitigation		
28	FFT1.1.4.3.5.3	Message Sent to Incorrect Train. [All Subsystems]	All Subsystems		Design Mitigation		
29	FFT1.1.4.3.6	Onboard Fails to Process an Overspeed. [Onboard]	Onboard		Onboard_FT16	OBC Fails to enforce overspeed	
30	FFT1.1.4.4.1.1	Primary PH04; Overspeed Due to STS Error. [Office]	Office		Office Overspeed		

Table 7: Basic Event Traceability to Exported Subsystem(s) – ABS / CMB Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	[redacted]	Model Name or Subsystem Reference	Subsystem FTA Event Description (Latest)	Comments
31	FFT1.1.4.4.1.2	Primary PH06; Insufficient Protection for Railway Worker. [Office]	Office		Office PH06		
32	FFT1.1.4.4.1.4	STS Failure Leads to Hazardous Output. [Office]	Office		Office STS Output		
33	FFT1.1.4.4.1.4	STS Failure Leads to Hazardous Output. [Office]	Office		Office STS Output		
34	FFT1.1.4.4.2	Incorrect TSR Enforcement; Mishandling of TSR. [Onboard]	Onboard		Onboard_FT11	Incorrect TSR enforcement	
35	FFT1.1.4.5.2	Corrupt Vehicle Type Parameter(s) Used by OBC. [Onboard]	Onboard		Onboard_FT18	Corrupt vehicle parameter used by OBC	
36	FFT1.1.5	Onboard Subsystem(s) Fails to Measure Speed Correctly. [Onboard]	Onboard		Onboard_FT19	Vehicle speed measured incorrectly	
37	FFT1.2.1.1	Train Engineer Drives Train Into or Out of ACSES II Territory Without Authorization. [Human Error]	Human Error		Human Error		
38	FFT1.2.2.1	Train Not Protected by Absolute Block Authority [Railroad]	Railroad		Human Error		
39	FFT1.3.1.1	Dispatcher Gives Unsafe Order to Pass Restrictive Signal. [Human Error]	Human Error		Human Error		
40	FFT1.4.1.2	Onboard Failure Causes Incorrect Train Position Calculation. [Onboard]	Onboard		Onboard_FT20	OBC failure causes incorrect train position calculation	
41	FFT1.4.2	OBC Fails to Enforce Immediate PTS During Turnback. [Onboard]	Onboard		Onboard_FT21	OBC fails to enforce immediate PTS during turnback	
42	FFT1.4.3.2.1	Train Engineer Fails to Follow Procedure. [Human Error]	Human Error		Human Error		

Table 7: Basic Event Traceability to Exported Subsystem(s) – ABS / CMB Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	[redacted]	Model Name or Subsystem Reference	Subsystem FTA Event Description (Latest)	Comments
43	FFT1.4.4	Train passes PTS without confirmation that signals are clear. [Onboard]	Onboard		Onboard_FT23	Train passes PTS without confirmation that signal is clear	
44	FFT1.5.4.1	SAR Failure Not Detected. [Onboard]	Onboard		Onboard_FT24	SAR failure not detected	
45	FFT1.5.4.2.1	Failure to Establish Stop-And-Release TSR After Problem Reported. [Human Error]	Human Error		Human Error		
46	FFT2.1	Front of Train Offset is Incorrect. [Onboard]	Onboard		Onboard_FT25	Front of train offset is incorrect	
47	FFT2.2.1	Train Engineer Passes Red Signal. [Human Error]	Human Error		Human Error		
48	FFT2.2.1.1.1.1	Interlocking Fails to Signal Improperly Lined Switch. [Legacy]	Legacy		Design Mitigation		
49	FFT2.2.1.2.1	Switch Moved Against Operating Procedures. [Human Error]	Human Error		Human Error		
50	FFT2.2.1.3	Existing Signaling System Fails to Protect. [Legacy]	Legacy		Design Mitigation		
51	FFT2.2.3.1.2	Dispatcher Commands Unsafe Switch Movement. [Human Error]	Human Error		Human Error		
52	FFT2.2.4	WIU Misreports Status of a Switch. [Legacy]	Legacy		Design Mitigation		
53	FFT3.1.2.1.1	RWPS Fails to Properly Create a TSR. [RWPS]	RWPS		Non-Vital System		
54	FFT3.1.2.1.2	RWPS Erroneously Requests Removal of a TSR. [RWPS]	RWPS		Non-Vital System		

Table 7: Basic Event Traceability to Exported Subsystem(s) – ABS / CMB Territory

Count	System FTA Event Name	System FTA Event Description	Exported Subsystem(s)	[redacted]	Model Name or Subsystem Reference	Subsystem FTA Event Description (Latest)	Comments
55	FFT3.1.2.1.3	RWPS Fails to Properly Attach to an Existing TSR. [RWPS]	RWPS		Non-Vital System		
56	FFT3.1.2.2.1	Work Crew Fails to Follow Procedure. [Human Error]	Human Error		Human Error		
57	FFT3.1.2.3	Training is Ineffective in Assuring Procedural Compliance. [Railroad]	Railroad		Human Error		
58	FFT3.1.2.3.1	Select-Check-Execute Procedure Failure. [Human Error]	Human Error		Human Error		
59	FFT3.6	Electrical Shock or Electrocution. [All Subsystems]	All Subsystems		Design Mitigation		
60	FFT3.7	Passengers or Staff Affected by EMI/EMC. [All Subsystems]	All Subsystems		Design Mitigation		
61	FFT4.1	ACSES II Design Shall Incorporate Non-Toxic, Non-Explosive, and Flame-Retardant Materials. [All Subsystems]	All Subsystems		Design Mitigation		

6.3 Results and Conclusions

The System Fault Tree Analysis demonstrates that causative faults at the system level are precipitated by one of the following events:

1. Failure in an identified subsystem of the ACSES II system;
2. Failure in external systems affecting the ACSES II system; or,
3. Human errors in following rules, regulations, or procedures of the railroad.

For any of these types of events, a terminal event exists in the system fault tree diagram. Failures which are identified as occurring in an identified subsystem are further developed in detail in the subsystem fault trees provided as separate CDRL documents of the LIRR system.

Ultimately, the Terminal Events shown in the table above must be included either as Initiating Events in the appropriate Subsystem Fault Tree, or as second-level Events that lead directly to the Top-Most Event in the Subsystem Fault Tree. The status of that traceability is (and will be) shown in the table above, along with the failure corresponding failure probability.

This version of the System FTA includes quantification of all faults shown, both for those faults allocated to the various subsystems, as well as those shown only on the System FTA. This quantification allows for calculation of the System MTTHE. A Risk Assessment, as per CFR 49 §236.1015(d)(3) will be demonstrate that the ACSES II system being installed on LIRR meets the risk criteria generally accepted, i.e., industry-standard, for a vital system. The Cut Set Analysis[1] found in the Appendix to this document will be used as input to that Risk Assessment, along with the full System FTA.

Failure rate FFT1 needs to be reviewed with the Railroad. The exact process and procedures to prevent non equipped ACSES trains and trains with ACSES that are cut-out and being allowed to enter the system is not fully understood by the SI. These events are not protected by ACSES and must rely on procedures and operation rules that must be properly enforced to maintain system safety.

Failure rate FFT3 needs to be reviewed with the railroad as well. This rate will also be reviewed by the SI again for correctness as some of the events seem to low given the subsystem tests have been performed and all subsystems have passed EMI/EMC testing. The review with the Railroad will need to focus on proper modeling of the work zone protection rules and the addition of operating procedures and other restrictions not enforced by ACSES to ensure proper protection of work zones and work crews.

[1] A **cut-set analysis** determines a distinct path of failure leading to the top undesired event, referred to as the Fault Tree top event in this analysis. A minimal cut-set is the unique path of failure to the Fault Tree top event.

8 Appendix – Fault Tree Cut-Set Analysis

Cut-Set Analysis Table Key

In the table below, which provides both a unique and minimal cut-set, shows those Terminal Events, or combinations of Terminal Events that directly affect the overall system MTTHE, the following columns are found:

- **Gate Name** – The designation of the upper-most gate affected by the cut-set. The term, "FFT_TOP" means that the overall MTTHE is directly affected by the cut-set;
- **Count** – An ordinal count, showing the number of entries in the table;
- **Cut Set** – The identifier for either the specific Terminal Event, or the combination of Terminal Events of which the Cut Set is composed.;
- **Cut Set Description** – The description, as derived from the System FTA Terminal Event. In the case where multiple Terminal Events comprise the Cut Set, a "::" is shown to indicate the joining of two, or more, Terminal Events.
- **Set Failure Frequency** – The MTTHE for the Terminal Event, if a single Terminal Event accounts for the Cut Set, or the aggregate MTTHE, for a combination of Terminal Events comprising the Cut Set;
- **1st Subsystem** – The ACSES II subsystem to which the Terminal Event has been attributed. In the case where multiple Terminal Events comprise the Cut Set, the first one in the set.
- **Comments** – Relevant Comments about the Cut Set, if applicable.

8.1 ATC Territory – Fault(s) with w Higher Than e^{-9}

Table 8: Cut-Set Analysis – ATC Territory – Fault(s) with **w** Higher Than e^{-9}

Gate Name	Count	Cut Set	Cut Set Description	Set Failure Frequency	1st Subsystem	Comments
			None.			

The purpose of this ATC Territory Fault Tree Cut-Set Analysis is to illustrate and identify any Terminal Events that directly affect the MTTHE predicted by the full Fault Tree. In this case, all such Terminal Events, i.e., those that have a failure rate higher than e^{-9}, are mitigated either via vital systems or a combination of vital systems and other means. As such, no entries are applicable for this table. ATC Territory meets the requirement for vital overlay without further analysis.

8.2 CMB Territory – Fault(s) with w Higher Than e^{-9}

Table 9: Cut-Set Analysis – CMB Territory – Fault(s) with **w** Higher Than e^{-9}

Gate Name	Count	Cut Set	Cut Set Description	[redacted]	1st Subsystem	Comments
FFT_TOP	1	FFT2.2.3.1.2 ::FFT3.1.2.3	Dispatcher Commands Unsafe Switch Movement. [Human Error] ::Training is Ineffective in Assuring Procedural Compliance. [Railroad]		[Human Error]	Existing procedures and/or Operating Rules in place.

The purpose of this CMB Territory Fault Tree Cut-Set Analysis is to il erminal Events that directly affect the MTTHE predicted by the full Fault Tree. In this case, several such Te that have a failure rate higher than e^{-9}, exist. That means that these faults are not mitigated sufficiently by vit ion of vital systems and other means. As such, these Faults will be further analyzed in the Risk Assessment.

Metropolitan Transportation Authority
Long Island Rail Road / Metro-North Railroad
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712/29544

System Preliminary Hazard Analysis
CDRL 2-127

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	PM	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Jason Weighley Sfatey Engineer	Jason Weighley	2016-11-18
Verified:	Theresa Barbour Safety Engineer	T Barbour	2016-11-18
Approved:	Anthony DeFrancisco Project Director	Anthony DeFrancisco	11/16/16
SI Quality Process Review:	Joe Castellani BT Quality Assurance Group	Joseph Castellani	2016-11-18
BT/SRA Review:	N/A Title		
BT/SRA Review:	N/A Title		

N. Mistah 2016-11-22 7:00

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2016, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2016 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3035821

Effective Date:	Revision:	Language:
2016-11-18	_D	EN

Released Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2014-03-10	First issue
_A	2014-07-31	Document updated to address CDR comments applicable to SRR.
_B	2014-08-27	Updated disclaimer on signature page
_C	2015-09-25	Submitted for PDR
_C.1	2016-07-29	Draft update to address RR Comments
_C.2	2016-10-19	Updated to respond to commetns from _C.1
_C.3	2016-10-31	Updated to resolve comments from _C.2 review
_C.4	2016-11-14	Aligned with Hazard Log. Resolved internal comments.
_D	2016-11-18	Released for Approval

Table of Contents

Section	Subject	Page
1	**Executive Summary**	6
2	**Introduction**	6
2.1	**Objective**	6
2.2	**Scope**	6
2.3	**Compliance Matrix**	7
2.4	**Reference Documents**	12
2.5	**Glossary**	14
3	**System Overview**	16
3.1.1	Office System	17
3.1.2	Onboard System	18
3.1.3	Wayside System	18
3.1.4	Communication system	18
3.1.5	RWPS	19
4	**Methodology**	19
4.1	**System Interfaces**	21
4.1.1	Human Interfaces	22
4.2	**Operating and Test Conditions Analyzed.**	22
4.3	**Operating Environments**	23
4.4	**Safety Related Equipment**	24
4.5	**System Failure Modes Considered**	24
4.6	**Training and Emergency Preparedness**	25
4.7	**Risk Assessment Classification Frame Work**	25
5	**Identification of Primary Hazards**	29
5.1	**Top Level Hazard Consequences –Accident Types**	29
5.1.1	Collision between Trains	30
5.1.1.1	A01- Head on Collision	30
5.1.1.2	A11. Collision at 15MPH	30
5.1.1.3	A02- Rear End Collision	30
5.1.1.4	A03- Fouling Side-Swipe (Convergent Collision)	31
5.1.2	Collision with obstructions	31
5.1.2.1	A04 – Collision with Bumper Block	31
5.1.2.2	A05- Collision with Object on Track of Infrastructure	31
5.1.2.3	A06- Collision with road vehicle or pedestrian	31
5.1.3	Derailment	31
5.1.3.1	A07- Derailment	31
5.1.4	Personal – Staff or Passenger	31
5.1.4.1	A08- Staff Struck by Train	31
5.1.4.2	A09- Non-Vehicular death or Injury (Staff or Passenger)	32

5.1.4.3 A10- PTC Equipment Damaged by Fire or Fire Suppression Measures 32
5.2 Primary Hazard Identification 32
5.2.1 Primary Hazard List 32
5.2.2 Primary Hazard and Consequence Table 34
5.3 PTC System Related Primary Hazards 34
5.3.1 PH01- Undetected Obstruction on Track 34
5.3.2 PH02- Unsafe Movement Authority Issued 35
5.3.3 PH03- Train Violates Movement Authority 36
5.3.4 PH04- Overspeed 36
5.3.5 PH05- Unsafe Switch Movement 37
5.3.6 PH06 Insufficient Protection for Person on Track/Unsafe Track Area 38
5.3.7 PH07- Unsafe Train Entry / Exit between PTC Territory and Other Systems 38
5.3.8 PH08- Unauthorized Access to PTC System 39
5.3.9 PH09- EMI/EMC Disturbance Contributing to Signalling and Train Control Hazards 39
5.3.10 PH10- Toxic or Explosive Materials 40
5.3.11 PH11- Fire, Smoke 40
6 Hazard Assessment & PHA Result Table 41
6.1 Hazard Analysis Table 43
6.2 Hazard Analysis Results 67
7 Functional Safety Requirements 68
7.1 Function Classification 68
7.2 Safety Requirement 69
8 Conclusion 75

List of Figures

Figure 1: PTC ACSES II System Architecture 17

List of Tables

Table 1: Compliance Matrix 7
Table 2: Reference Documents 12
Table 3: Terms Specific to this Document 14
Table 4: Acronyms Specific to this Document 16
Table 5: Hazard Severity Classifications 26
Table 6: Hazard Probability Classifications 26
Table 7: Hazard Risk Assessment Matrix 27
Table 8: Hazard Risk Index (HRI) 27

Table 9: Consequence Categorization 29
Table 10: PTC System Primary Hazards 32
Table 11: Primary Hazard & Consequence Cross Reference 34
Table 12: Hazard Table column Definition/Description 41
Table 13: LIRR / MNR Hazard Analysis 44
Table 14: Summary of Identified Hazards 67
Table 15: Function Classification 68
Table 16: Safety Requirements 69

1 Executive Summary

This document records the Preliminary Hazard Analysis of the LIRR / MNR PTC system. This analysis forms the initial safety demonstration document; its purpose is to identify the potential hazardous events that can occur as a result of operating the PTC system on the right of way.

The analysis evaluates the severity and identifies the causes of hazardous events in order to develop safety requirements. These identified hazards will be further broken down and analyzed in greater detail in the System Hazard Analysis to assess their compliance with the Safety requirements.

2 Introduction

2.1 Objective

This PHA is undertaken in order to identify hazards related to the design and operation of the LIRR / MNR PTC system. This is to aid the derivation and verification of the PTC system safety requirements.

This document provides an initial list of hazards, which require tracking mitigation resolution during the PTC system design and development. The PHA is the foundation for further system and subsystem level hazard analyses.

2.2 Scope

This analysis will cover the full extent of operations of the LIRR/MNR PTC System including all subsystems, hazardous components, safety related interfaces, operating environments, Human Interfaces, Safety Concepts, Operations and Maintenance procedures, Training, Safety Related equipment, and malfunctions to the system. This analysis excludes:

- Tenant railroad equipment except for ensuring interoperability.
- External equipment located outside of the LIRR/MNR PTC system boundary;
- Misuse (intended) of the LIRR/MNR PTC equipment, operating and maintenance procedures;
- Environmental conditions exceeding the contract specifications;
- Catastrophic natural events (lightning, flooding, earthquake, etc.); and
- Other external factors, such as, vandalism, fire, smoke, gas-build, electrification, rolling stock and construction.
- Security mitigations will be covered by the System Vulnerability Assessment and are not included in this analysis.

2.3 Compliance Matrix

Table 1: Compliance Matrix

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Requirement Summary (2)	Document Section Reference
1	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2	A. The SI shall perform and document a Preliminary Hazard Analysis (PHA) [CDRL 2-127], starting with the ACSES II hazards defined in the Type Approved ACSES II PHL, identifying the system hazards, conditions that could result in the hazard, and the mitigation strategy for protecting and maintaining the safety of the ACSES II System.			Section 5.3; Section 6.1
2	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2	B. The PHA shall be performed in general conformance to MIL-STD-882C including the following:	1. Hazard severity and probability for each hazard and the level achieved after mitigation;		Section 4 [*PHA regarding mitigation will identify Potential mitigation]*
3	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		2. Safety provisions and alternatives needed to eliminate the hazards or reduce their associated risk to a level acceptable to the Engineer;		Section 6.1 [*PHA will identify System (high) level potential mitigations with regard to Safety order of precedence as identified in Mil-Std-882C to achieve the a Risk level as defined in the Safety Plan Risk Acceptability matrix.*]

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Requirement Summary (2)	Document Section Reference
4	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		3. The following as minimum shall be considered in the hazard analysis:	a. ACSES II Subsystems and components;	Section 4[*PHA will be done at to System (high) level and will not go into subsystem and component details. Each subsystem will generate a separate PHA that will go to sufficient detail.*]
5	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			b. Hazardous components;	[*Covered by the Subsystem PHAs][25], [26], [27], [28], [29], [30]*
6	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			c. Safety related interfaces;	4.1
7	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			d. Operating environments, including vehicles, track beds, wayside rooms and huts, control centers, and other required ACSES II installation sites.	4.3
8	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			e. Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures;	4.2

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Requirement Summary (2)	Document Section Reference
9	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			f. Human interface;	4.1.1
10	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			g. Safety concepts and dependencies;	4.4
11	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			h. Operations and Maintenance procedures;	4.2
12	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			i. Training and emergency preparedness;	Section 6.1[*This document will address System Issues. The subsystem PHA's will address subsystem and component issues.*]
13	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			j. Safety related equipment, safeguards, and possible alternate approaches (e.g., system redundancy; fail safe design considerations using hardware or software controls);	4.4

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Requirement Summary (2)	Document Section Reference
14	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			k. Malfunctions to the system, subsystems, or software. Each malfunction shall be specified, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and/or design changes developed.	4.5
15	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2	C. Functional failure analysis shall be derived from the Preliminary Hazard Analysis (PHA) and subsequent Hazard Analyses, including subsystem HA's. Hardware items on this list as applicable. This analysis looks at software's relationship to hardware.			Please see documents: [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44]
16	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2	D. A Preliminary Hazard Report shall be furnished as part of the PHA by the SI including for each hazard the following:	1. Hazard Description;		6
17	Contract 1712 Vol 2	Vol 2 PART I rev1.01-		2. Safety Requirement(s), with reference to		6

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Requirement Summary (2)	Document Section Reference
		Section 12.10.2		the RTM (Section 6.6);		
18	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		3. Hazard Cause;		6
19	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		4. Hazard Control;		6
20	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		5. Hazard Detection Method;		6
21	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		6. Safety Verification Method (analysis, test, demonstration, or inspections), with reference to Subsystem Test Plan (Section 10.4.1);		6
22	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		7. Status		6

2.4 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	PDM 3035624
[2]	System Description Document CDRL 2-27	PDM 3035724
[3]	MIL-STD-822C	
[4]	System Product Safety Plan LIRR CDRL 2-123-20 System Product Safety Plan MNR CDRL 2-123-10	PDM 3035815 PDM 3036437
[5]	RAM Program Plan CDRL 2-139	PDM 3035841
[6]	FRA PTC ACSES II Type Approval (FRA-TA-2010-001)	FRA-TA-2010-001 (Regulation.gov)
[7]	FRA Approved LIRR PTC DP	FRA-2010-0031-0013
[8]	FRA Draft LIRR PTC SP FRA Draft MNR PTC SP	NA NA
[9]	FRA Type Approved ACSES II Preliminary Hazard List	FRA-2010-0029-0042
[10]	Requirement Management Plan	PDM 3035705
[11]	LIRR System Architecture Drawing Package	3038055
[12]	Transponder - SDD	3035882
[13]	WIU - SDD	3035895
[14]	Onboard - SDD	3035908
[15]	Office - SDD	3035950
[16]	RWPS – SDD	3035851
[17]	Comms – SDD	3035962
[18]	LIRR Operational Concepts	NA
[19]	MNR Operational Concepts	NA
[20]	AREMA, Communications and Signals Manual – 2009 Section Parts 16, 17, 21, and 23.	2001

Reference Number	Document Name	Identification Number
[21]	CENELEC EN50126, Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)	EN50126:1999
[22]	CENELEC Standard. Railway Applications – Communication, signaling and processing systems – Safety related electronic systems for signaling.	EN50129:2003
[23]	Pilot Program Plan (CDRL 2-019-20 and 2-019-10)	3035622 3035623
[24]	System Vulnerability Assessment (CDRL 2-137)	3035840
[25]	Onboard PHA	3036405
[26]	WIU PHA	3036409
[27]	Transponder PHA	3036413
[28]	Office PHA	3035822
[29]	Comms PHA	3036420
[30]	RWPS PHA	3036416
[31]	LIRR System IHA	3035828
[32]	MNR System IHA	3043905
[33]	LIRR Onboard IHA	3037426
[34]	LIRR WIU IHA	3037432
[35]	LIRR Transponder IHA	3037434
[36]	LIRR Office IHA	3037428
[37]	LIRR Comms IHA	3037430
[38]	LIRR RWPS IHA	3037436
[39]	MNR Onboard IHA	3037427
[40]	MNR WIU IHA	3037433
[41]	MNR Transponder IHA	3037425
[42]	MNR Office IHA	3037429
[43]	MNR Comms IHA	3037431

Reference Number	Document Name	Identification Number
[44]	MNR RWPS IHA	3037437

2.5 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in Table 3 and Table 4 respectively.

Table 3: Terms Specific to this Document

Term	Definition
Preliminary Hazard Analysis (PHA)	An analysis performed on the potential hazards identified in the PHL, to provide an initial risk assessment of the hazards, and to identify requisite controls and follow-on actions.
Product	A train control system, subsystem, or component. Or An element of the physical or system architecture, specification tree, or system breakdown structure that is a subordinate element to the system or subsystem and which is wholly documented in a separate way, and considered as a terminal branch of the specification tree.
Qualitative Argument of Safety	Argument provided by the application of the safety assurance methodology that hazards are eliminated or controlled to an acceptable level. The norms for acceptability are usually based upon MIL-STD-882C[3], or similar documents.
Quantitative Proof of Safety	A measure of safety, stated in terms of a Mean Time To Hazardous Events (MTTHE) or Mean Time Between Hazardous Events (MTBHE), usually obtained by mathematical analysis of the safety assurance mechanisms used in the product/system, or by modeling and simulation techniques applied to the hardware and software of the product/system.
Review	The assessment of a work product's content to verify adherence to defined standards, guidelines, specifications and procedures.
Risk	An expression combining the probability of the mishap occurring with the severity of the consequences of the mishap, used to rank hazards.

Term	Definition
Risk Assessment	The process of determining the amount of risk associated with use of the product under all intended operating conditions. Intended operating conditions include normal operations, degraded operations, and operation under failure conditions including unintended human error. Risk assessment techniques for any product may include qualitative, semi-quantitative and quantitative approaches.
Safety-Critical Classification	A classification of products that have at least one hazard that can lead directly to a mishap.
Safety-Related Classification	A classification of products which do not lead directly to a mishap but which may significantly increase the overall risk of a mishap.
Safety Life Cycle	The additional series of activities carried out in conjunction with the system life cycle for safety related systems.
Self-Revealing Component Failures	Component failures whose effects on system operation are immediately and clearly apparent to a properly trained person.
Subsystem Hazard Analysis (SSHA)	An analysis that looks at each subsystem or component and identifies hazards associated with operating or failure modes and is especially intended to determine how operation, unintended human error or failure of components affects the overall safety of the subsystem.
System Hazard Analysis (SHA)	An analysis that determines how system operation and failure modes can affect the safety of the system and its subsystems. Note: Specifically, the SHA examines all subsystem interfaces and interfaces with other systems for: Compliance with safety criteria called out in the applicable system/subsystem requirements documents. Possible combinations of independent or dependent failures that can cause hazards to the system or personnel. Failures of controls and safety devices should be considered. How normal operations of systems and subsystems can degrade the safety of the system. How design changes to system, subsystems, or interfaces, logic, and software can create new hazards to equipment and personnel.

Table 4: Acronyms Specific to this Document

Acronym	Definition
AARA	Association of American Railroads
CRL	Customer Requirement List
HL	Hazard Log
PHL	Preliminary Hazard List
SLR	System Level Requirements
SPSP	System Product Safety Plan
SSHA	Subsystem Hazard Analysis

3 System Overview

ACSES incorporates both the Automatic Speed Control (ASC) and, as an overlay to the ASC System, the speed and stop enforcement including the transponder and data radio subsystems. ACSES enforces positive stop at home signals, and enforces permanent and temporary speed restrictions. ACSES uses data obtained from passive track-mounted transponders and a data radio to impose permanent and temporary speed limits. The Onboard System responds to data acquired from transponders and through the data radios. The Onboard System calculates a speed profile for both warning and enforcement from the track profile and vehicle performance characteristics.

The ACSES System Architecture can be divided into equipment systems, such as:

- Office Subsystem
- Onboard Subsystem
- Wayside Subsystem
    - o Transponder Subsystem
    - o WIU Subsystem
- Communication Subsystem
- RWPS Subsystem

The ACSES system basic architecture and interfaces between the subsystems is presented in Figure 1 below. The System Architecture Drawing Package [11] defines the formal architecture of ACSES. The system design is documented by the System Design Description [2].

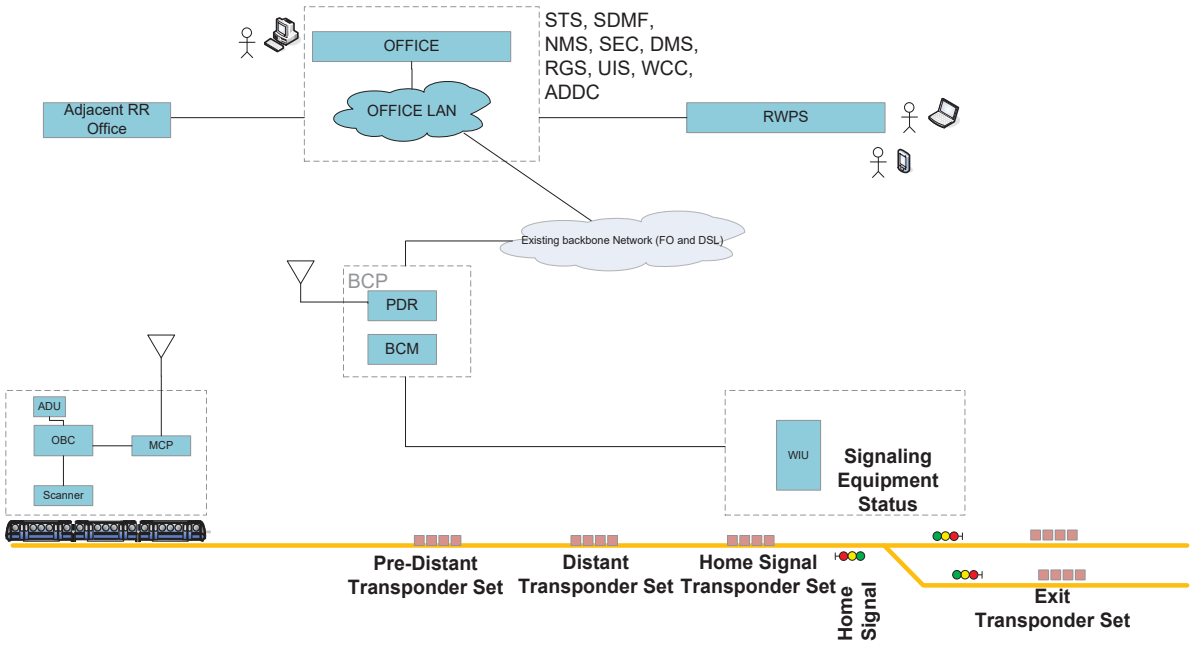


Figure 1: PTC ACSES II System Architecture

3.1.1 Office System

The Control Center System includes all ACSES II components necessary to integrate the dispatcher and field functions in order to issue temporary speed restrictions, store critical and non-critical data, provide maintenance and reporting functions, and provide all interfaces to the Wayside Systems for ACSES II operations. The Office system is fully described by the Office SDD [15]. This office equipment set includes:

- Safety TSR Server (STS) -Vital
- Wayside Communication Controller (WCC)
- Data Maintenance System (DMS)
- ACSES II Network Management System (ACSES II NMS)
- User Interface System (UIS)
- ACSES II Office Local Area Network (ACSES II LAN)
- Active Directory Domain Controller (ADDC)
- Railroad Gateway Server (RGS)
- Software and Data Maintenance Facility (SDMF)
- Security Server (SEC)

The Safety TSR Server (STS) will be the single point of execution for office safety critical logic functions and will calculate all safety critical parameters for the ACSES II System.

3.1.2 Onboard System

The onboard is a vital subsystem that is located in the train and controlling the train's movement through requesting an application of the train's brakes upon detecting unsafe/undesirable conditions. The onboard platform supports both Cab Signal System functions only and ACSES II functions as an overlay to the existing cab signaling system. The onboard system is described by the Onboard SDD [14]. The Onboard ACSES II system equipment set consists of the following key elements:

- Onboard Computer -Vital
- Transponder Antenna and CTV
- Speed Sensor
- Decelerometer
- Vital interface to ATC (via AIU where applicable)
- Train Engineer ACSES Display Unit (ADU)
- Acknowledge Switch
- Event Recorder System
- ACSES Alert – for providing audible alerts to the train engineer.
- Absolute Stop Bypass pushbutton
- Cut-out switch

3.1.3 Wayside System

The wayside components will be installed at the existing interlocking locations and integrated with the communications network. These wayside components include: the Wayside Interface Unit (WIU); data radio; Communication Managers; interfaces to the existing signal logic and communications network; and any necessary supporting equipment (power supplies, etc.). Additional wayside components include passive track-mounted apparatus (transponders), and data radio antenna installations, both of which will be installed based upon site-specific requirements determined during system design. The WIU is described by the WIU SDD [13]. The transponder is described by the Transponder SDD [12]. The ACSES II wayside components include:

- Track-mounted passive transponder - Vital
- Wayside Interface Unit (WIU) - Vital
- Miscellaneous hardware, wire cabling, and connections

3.1.4 Communication system

The communication components will be installed at the existing interlocking locations and integrated with the communications network. The communication system is described by the Comms SDD. [17] These components include:

<u>Wayside</u>

- Data radio
- WiFi and Cellular
- Base Communications Manager (BCM)

- RTU – Remote Terminal unit for monitoring status
- uRTU – micro Remote Terminal Unit for monitoring status in the CIL
- L2 and L3 network switches
- Any necessary supporting equipment (power supplies, antennae, filters, fibers, etc.).

Onboard

- Data Radio
- WiFi and Cellular
- MCM
- Any necessary supporting equipment (power supplies, antennae, filters, fibers, etc.)

3.1.5 RWPS

The roadway worker protection system will be installed in the BCC and PCC on each railroad. The RWPS will be connected to the Office sub system to allow roadway workers to request TSR's and determine the active TSR's on the system. The RWPS is described by the RWPS SDD [16]. The RWPS system components include:

- Roadway Worker Protection Server
- Employee In Charge Terminal
- Data Maintenance System (DMS)
- ACSES II Network Management System (ACSES II NMS)
- User Interface System (UIS)
- ACSES II Office Local Area Network (ACSES II LAN)
- Active Directory Domain Controller (ADDC)

Please refer to CDRL 2-27 System Description Document [2]

4 Methodology

The PHA identifies the primary hazards inherent with the railway system. Primary hazards that the ACSES II PTC system must control are identified based of on Railway Application principles of railway Automatic Train Control Signaling system, past experience with similar PTC systems, and the context and specifics of the LIRR Operation Concepts [18] and MNR Operation Concepts [19].

The analysis investigates hazards around the boundary of the ACSES II system and its environment by treating the ACSES II system as a black box. The system boundary is defined in terms of its equipment interface to the railway system, the environment, and people, and in terms of its primary functions within the railway system.

The PHA determines the ACSES II system's contribution to the primary hazards and defines the role and responsibilities of the ACSES II system in the mitigation of each of the primary hazards. Out of these roles and responsibilities, a set of system hazards is deduced. System hazards are defined as conditions associated with the physical and functional boundaries of the ACSES II system.

This analysis uses a "top-down" deductive approach to systematically and comprehensively identify hazards associated with the ACSES II system design and operation. The primary hazards (top events)) are decomposed into contributing lower level hazards (trigger events) associated with the ACSES II system functions, equipment and interfaces.

The analysis provides, for each potential hazard, the preventive and control measures that if assured, guarantee that an undesired event will not occur or its residual risk is at an acceptable level.

The identification of hazards at the Preliminary level is based on the best available data, including mishap data from similar PTC or advanced train control systems and other lessons learned from similar projects. The analytical process took into considerations the following factors in the identification process of hazards:

a) Hazardous components including the use of toxic or flammable materials;

b) Interfaces between subsystems and the interfaces between the PTC system and existing LIRR / MNR System and third parties;

c) Electromagnetic interference;

d) Fire/explosive initiation and propagation;

e) Contributions to hazards by hardware and software elements;

f) Human errors including incorrect inputs and commands to The System;

g) Environmental impacts including shock, vibration, extreme temperatures, noise, electrostatic discharge, lightning;

h) Human factors impacts by operators and maintainers;

i) System malfunctions; and

j) Errors arising from the application of design tools or processes including database errors and performance parameters

The following documents were used as an input to the preliminary hazard analysis: System Design Description and the Preliminary Hazard List from the contract specification.

The PHA process uses the SDD as the primary input document. A preliminary Hazard list from the specification was also used as a starting point as was the Hazard log from the Amtrak ACSES FRA submittal.

Output Document	Required Inputs from Project	Comments
Preliminary Hazard Analysis (PHA) Matrix –Table **13**	1. System Design Description (SDD) 2. Preliminary Hazard List (From LIRR PTCDP) 3. Subsystem Design Description	.

The initial hazard lists were reviewed by the safety engineer for each subsystem, System Integration engineers, and subsystem lead engineers, for acceptability and then transferred to the LIRR/MNR lists. The SDD was then reviewed for each function to determine the hazards for each function and the potential failure modes of the system. For each subsystem the interfaces, human interfaces, and equipment locations were reviewed to add relevant failures for each function. These hazards were then ranked for initial severity and frequency based on expert opinion. The mitigation for each hazard was then determined with system integration engineers and system engineering, with emphasis on PTC mitigation of each hazard if possible. A final residual risk and severity was determined based on the agreed mitigation and expert opinion on the reduction that mitigation would provide. The final output is the preliminary hazard log report contained in Table 13: LIRR / MNR Hazard Analysis and maintained in the final hazard log

The safety mitigations found during this analysis will be assigned to the SLR and tracked as marked safety requirements in the SLR. Any mitigation that has been assigned type railroad is a Safety Related Application Condition (SRAC). A document of all the SRAC's will be generated by the SI and formally agreed and accepted with the railroad prior to revenue service of the system. Details of this process will be in the System Product Safety Plan.

4.1 System Interfaces

From the System Architecture Drawing Package [11] the following system level interfaces were analyzed. Interfaces listed below are documented by the System Design Description [2].

Onboard computer to Office

Onboard computer to Transponder

Onboard computer to WIU

WIU to Wayside Interlocking Signal

Office to Adj Railroad STS

Office to Cellular connection

Office to RWPS

Office to Comms

WIU to NMS

WIU to Comms

Onboard Computer to Train

ADU to Train Engineer

Office to User Interface

RWPS to EIC

RWPS to RGS

RWPS User Interface

4.1.1 Human Interfaces

Of the interfaces listed above the below listed interfaces provide interfaces to end users. Please note subsystem maintenance and diagnostic interfaces will be listed in the subsystem PHA.

RWPS User Interface – Interface not designed and to be analyzed later.

EIC Terminal Device Interface – Interface not designed and to be analyzed later.

SDMF User Interface - Interface not designed and to be analyzed later.

ADU to Train Engineer

Office to User Interface

Train Engineer to Train (Components like Reverser, Ack pushbutton, and brake application)

4.2 Operating and Test Conditions Analyzed.

The following list of test conditions from the Pilot Program Plan [23] was analyzed for possible hazards.

Normal Operation in ASC Territory

Normal Operation in ABS Territory

Normal Operation in MBS Territory

Operation in ASC Territory with ASC Cutout onboard

Operation in ASC Territory with Failed ATC

Operation in ABS Territory with Failed ATC

Operation with missing Transponder

Operation with failed Radio

Operation with WIU Failure

Departure Test

Train Type modified in Operation

Operation in a construction zone area – I.E. transponder ignored.

Departing terminal with ACSES inactive – ADU to display '- -' and missing transponder indication to also be light.

OBC reset in construction zone area.

Operation in MTEA areas (Yard and Sidings)

Entry to ACSES

Exit from ACSES

Operation when TP data is migrated from Speed Enforcement to full PTS

Operation without WIU for testing.

Operation without Office for testing.

Operation with Stale WIU Data

Operation with Stale STS Data

ESA Operation

Turnback Operation

Operation with a TSR enforcement

Operation with a reported failed highway crossing

OBC failure enroute.

4.3 Operating Environments

The following operating environments were considered in the generation of this document.

Wayside cases

Primary Office control center.

Backup office control center

Office Workstations

Control Tower rooms

CIL (WIU)

C-Case

Tunnels

Onboard equipment lockers

Onboard under train equipment

Onboard roof top equipment

Onboard Comm Panels

Onboard ADU / User Interfaces

Highway crossing

In Track Locations

EIC Handheld use locations

EIC Truck mounted Equipment

4.4 Safety Related Equipment

The following concepts from IEEE 1483 Safety Assurance will only be considered for all safety critical subsystems used in ACSES.

- Checked Redundancy
- Numerical Assurance
- N-Version Programming
- Diversity
- Self-Checking

The following subsystems of ACSES are assumed based on the specification and existing hazard analysis to be safety critical subsystems that must use one of the above concepts.

- WIU
- STS
- OBC – Onboard Computer
- OBC – AIU
- Transponder

4.5 System Failure Modes Considered

The following failure modes of the system were analyzed.

- Missing / Failed / Removed Transponders
- Loss of WIU interlocking response / WIU failure.
- Loss of Office communication
- Onboard ATC cutout
- Onboard failures
- Office to Adj RR Office Communication Failure
- Primary Control Center Failures
- Loss of communication between primary / backup offices.
- EIC to RWPS Loss of communication.
- EIC Failures
- RWPS to Office Failures

4.6 Training and Emergency Preparedness

The following Training and Emergency Procedures were considered:

- Train Operation without ACSES procedures.
- Yard Operation
- MBS Territory Switch Operation
- Temporal Separation Procedure
- TSR procedures
- Maintenance Procedures.

4.7 Risk Assessment Classification Frame Work

Throughout the product development lifecycle, risk assessment practices are applied to guide the implementation of mitigating actions to control or eliminate each identified hazard such that the risk introduced by each is acceptable. Risk assessment and management is a decision-making process consisting of evaluation and control of the severity and probability of a potentially hazardous event. As hazard analyses are performed, Bombardier will identify hazards that will require resolution through this mechanism.

The classification of severity for hazards will be based on the four categories from MIL-STD-882C [3]12 and AREMA section 17.3.5 [20] identified in Table **5** ranging from Category I (Catastrophic) to Category IV (Negligible). The severity classification assigned to each hazard will provide a qualitative indication of the worst-case consequences that could occur if the hazard is not eliminated or controlled.

Probability classifications will be based on the five categories from MIL-STD-882C and AREMA section 17.3. as shown in Table **6**. These range from Category A (Frequent) to Category E (Improbable). The assigned probability will be based on the likelihood that a particular hazard and effect would occur in the planned life expectancy of the product. To assist in assigning the specific categories of probability, Table **6** shows definitions for both a specific individual item (i.e. a specific component of the system) as well as for the fleet or overall inventory of the system. The table also provides the Mean Time Between Events (MTBE) to guide the consistent application of the classifications. Note that since the probability categories are applied to hazards of all severities (even category IV), it is not appropriate to use Mean Time Between Hazardous Events (MTBHE) in Table **6** as all events may not be truly hazardous in nature and therefore MTBE is used.

Table 5: Hazard Severity Classifications

Description	Category	Definition
Catastrophic (1 Yr.-death)	**I**	Death, system loss, or severe environmental damage.
Critical (21-363 Days)	**II**	Severe injury, severe occupational illness, major system or environmental damage.
Marginal (8-20 Days)	**III**	Minor injury, minor occupational illness, or minor system or environmental damage.
Negligible (0-7 Days)	**IV**	Less than minor injury, occupational illness, or less than minor system or environmental damage.

Table 6: Hazard Probability Classifications

Description	Level	# of accidents # of employees	Specific individual item	Fleet or inventory	Numerical range of failure rate (f/Hr) for fleet/inventory
Frequent	**A**	(> .24)	Likely to occur frequently.	Continuously experienced.	Greater that 10^{-1}
Probable	**B**	(0.16 – 0.24)	Will occur several times in the life of an item.	Will occur frequently.	$\geq 1.39 \times 10^{-3}$ to $\leq 1.0 \times 10^{-1}$
Occasional	**C**	(0.10 – 0.15)	Likely to occur sometime in the life of an item.	Will occur several times.	$\geq 1.14 \times 10^{-5}$ to $\leq 1.39 \times 10^{-3}$
Remote	**D**	(0.02 – 0.09)	Unlikely but possible to occur in the life of an item.	Unlikely but can reasonably be expected to occur.	$\geq 5.12 \times 10^{-7}$ to $\leq 1.14 \times 10^{-5}$
Unlikely	**E**	(<0.01)	So unlikely, it can be assumed occurrence may not be experienced.	Unlikely to occur, but possible.	Less than 5.12×10^{-7}

The combination of the hazard severity and hazard frequency forms a Hazard Risk Index (HRI). The resulting Hazard Risk Assessment Matrix is obtained from MIL-STD-882C as shown in Table 7 and Table 8.

The HRI presents the hazard analysis results in a format useful to the decision maker in determining whether hazards should be eliminated, controlled, or accepted. This provides a logical basis for management decision-making, considering both the severity and probability of any individual hazard in a weighted fashion.

Table 7: Hazard Risk Assessment Matrix

	Catastrophic	Critical	Marginal	Negligible
Frequent	**IA**	**IIA**	**IIIA**	**IVA**
Probable	**IB**	**IIB**	**IIIB**	**IVB**
Occasional	**IC**	**IIC**	**IIIC**	**IVC**
Remote	**ID**	**IID**	**IIID**	**IVD**
Improbable	**IE**	**IIE**	**IIIE**	**IVE**

Table 8: Hazard Risk Index (HRI)

Hazard Risk Index	Acceptance Criteria
IA, IIA, IIIA, IB, IIB, IC	**Unacceptable**
ID, IIC, IID, IIIB, IIIC	**Undesirable** - Requires solution acceptable to Bombardier Project Manager.
IE, IIE, IIID, IIIE, IVA, IVB	**Acceptable with review -** Requires review.
IVC, IVD, IVE	**Acceptable** - Review not required.

It should also be noted that these hazard classifications are consistent with CENELEC standards ([21], [22]) which define a sixth probability classification and different numerical ranges but similar severity definitions. As long as the definitions are applied consistently throughout all product safety analyses, the resulting risk assessment will be consistent and sufficiently accurate to guide the development process.

By assigning a Hazard Risk Index (HRI), a determination can be made as to how the hazards should be addressed, in the order of precedence shown below:

1. **Design for minimum risk**: Eliminate hazards by safety-critical design. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level through design concept and implementation.

2. **Incorporate safety devices**. If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk shall be reduced to a level acceptable through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks of safety devices when applicable.
3. **Provide warning devices**. When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, warning devices shall be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems.
4. **Develop rules, procedures and training**. Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training shall be used. Procedures may include the use of personal protective equipment. Such practices shall be evaluated for completeness, clarity, and applicability where necessary to provide adequate safety. Such methods may also include warnings and equipment labeling.
5. **Note**: The use of warnings, cautions, or other written advisory shall not be used as the only risk reduction method for Category I or II severity hazards unless approved. Safety-critical tasks may require personnel proficiency in specific areas; the need for personnel proficiency certification will be identified in the analysis.

Hazard severity, before and after mitigation; provides a measure of the worst credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction. The hazard severity ranking of “AFTER mitigation” takes into account the actual design and architecture of the system (fail-safe design, maintenance procedures, etc.) and uses following rationale:

- Failures of components related to non-vital systems lead to hazard category IV when an independent vital subsystem protects them.
- The failure of a safety-related system, dependent on external requirements (e.g. periodic maintenance, periodic adjustments, cycle checking, or daily safety test) will lead to a hazard with a severity category I.
- A (Vital) fail-safe system will fail into a restrictive mode. The use of a fail-safe system can reduce the probability of the hazard occurrence for the item to an extent where it can be assumed that the hazard may not occur. This leads to a hazard probability of category E.

5 Identification of Primary Hazards

The primary hazards, which must be controlled by the PTC System, are identified in this section. Each primary hazard is presented with descriptions and analysis in terms of its consequences (e.g. resulting accidents or mishaps), in a manner to derive the hazard contributors.

5.1 Top Level Hazard Consequences –Accident Types

The effects of the primary hazards can be categorized into the Accident/Mishap presented in Table 9. The consequences are defined in terms of accidents/mishaps that can occur in the operation of the railway, and are identified based on:

- Understanding the high-level general overview of the PTC System and the railroad system as show in the System Description Document [2], with the PTC System treated as a “Black Box” and
- Experience in previous PTC System projects.

Table 9: Consequence Categorization

Consequence – General	Consequence - Specific Accident/Mishap
Collision between trains	A01. Head-On Collision between trains
	A11. Collision between trains at 15MPH or less. (ASC territory only)
	A02. Rear end Collision with train
	A03. Fouling, Side-swipe (convergent collision)
Collision with obstructions	A04. Collision with bumper block
	A05. Collision with object on track or infrastructure
	A06. Collision with road vehicle or pedestrian after entering a highway or pedestrian grade crossing.
Derailment	A07. Derailment. The train leaves the track on which it is travelling.

Consequence – General	Consequence - Specific Accident/Mishap
Personnel - Staff or Passenger death or injury	A08. Staff struck by train
	A09. Non-vehicular death or injury (Staff or Passenger)
Fire	A10. PTC equipment damaged by fire or fire suppression measures.

5.1.1 Collision between Trains

A collision between trains can be a head-on, rear-end, or side-swipe (or convergent collision). These four cases are described in greater detail below.

5.1.1.1 A01- Head on Collision

A head-on collision is defined as a collision between two trains travelling in converging directions along the same path. A head on collision can result in multiple fatalities, loss of rolling stock, damage to infrastructure, and loss of system operations in the area where the collision has occurred.

5.1.1.2 A11. Collision at 15MPH

A rear end collision is defined as a collision between two trains travelling in the same direction, where the following train overtakes and collides with the rear end of the leading train. This scenario will include scenarios where the lead train is stopped. This accident is focused on cases where the speed difference is controlled to less than 15MPH by the ATC design. A rear end collision at 15MPH can result in multiple injuries, damage to rolling stock, and loss of system operations in the area where the collision has occurred.

5.1.1.3 A02- Rear End Collision

A rear end collision is defined as a collision between two trains travelling in the same direction, where the following train overtakes and collides with the rear end of the leading train. This scenario will look include scenarios where the lead train is stopped and when the lead train is at speed. For this accident type the ATC is not available or installed. A rear end collision can result in multiple fatalities, loss of rolling stock, damage to infrastructure, and loss of system operations in the area where the collision has occurred.

5.1.1.4 A03- Fouling Side-Swipe (Convergent Collision)

A side-swipe or convergent collision is defined as a collision between two trains where the trains are travelling in different paths, but collide due to proximity in the fouling area of an interlocking, or due to dynamic violation of the expected train envelope when travelling in parallel tracks. A side-swipe collision can result in multiple fatalities, loss of rolling stock, damage to infrastructure, and loss of system operations in the area where the collision has occurred.

5.1.2 Collision with obstructions

5.1.2.1 A04 – Collision with Bumper Block

A collision with a Bumper Block is defined as the collision of one train with the Bumper Block that protects the end of a physical section of track. A collision with a Bumper Block can result in multiple fatalities, loss of rolling stock, damage to infrastructure, and loss of system operations in the area where the collision has occurred.

5.1.2.2 A05- Collision with Object on Track of Infrastructure

This is defined as a collision of one train with the infrastructure. This may occur where an object is overhanging or on the track, or where train equipment is outside of the expected train envelope. A collision of this type can result in multiple fatalities, loss of rolling stock, damage to infrastructure, and loss of system operations in the area where the collision has occurred.

5.1.2.3 A06- Collision with road vehicle or pedestrian

This is defined as collision with a road vehicle or pedestrian after entering a highway or pedestrian grade crossing.

5.1.3 Derailment

5.1.3.1 A07- Derailment

A derailment occurs when a train leaves the tracks on which it is travelling. A derailment of this type can result in multiple fatalities, loss of rolling stock, damage to infrastructure, and loss of system operations in the area where the collision has occurred.

5.1.4 Personal – Staff or Passenger

5.1.4.1 A08- Staff Struck by Train

In cases where personnel are sent into the track areas to perform maintenance activities, a failure to properly provide protection can result in these personnel can be struck by a passing train

5.1.4.2 A09- Non-Vehicular death or Injury (Staff or Passenger)

This accident category considers other types or injuries and illnesses that can occur in the railway environment during use by passengers and during operation or maintenance by personnel. The term non-vehicular is used to denote the fact that the injuries are not sustained as a result of another mishap involving the train. Examples include:

- Electrocution
- Radiation (EMI/EMC)
- Asphyxia, suffocation
- High or low temperature related injuries
- Toxicity
- Fire

5.1.4.3 A10- PTC Equipment Damaged by Fire or Fire Suppression Measures

This accident category is concerned with equipment damaged by fire or fire suppression measures. This category is primarily concerned with the equipment damage, whereas Non-Vehicular Death or Injury (A09) examined in section 5.1.4.2 explores the toxicity, asphyxia, and suffocation that may also result from smoke and fire.

5.2 Primary Hazard Identification

Primary hazards are the necessary conditions required to exist for an accident type as described in Section 5.1 to occur. These primary hazards are identified in Table 10 and correlated to accident types in Table 11

5.2.1 Primary Hazard List

Table 10: PTC System Primary Hazards

ID	Primary Hazard Description	Mitigated or Controlled by PTC System
PH01	Undetected Obstruction on Track	Yes
PH02	Unsafe Movement Authority Issued	Yes
PH03	Train Violates Movement Authority	Yes

ID	Primary Hazard Description	Mitigated or Controlled by PTC System
PH04	Overspeed	Yes
PH05	Unsafe Switch Movement	No
PH06	Insufficient Protection for Person on Track/Unsafe Track Area	Yes
PH07	Unsafe Train Entry / Exit between PTC Territory and Other Systems	Yes
PH08	Unauthorized Access to PTC System	Yes
PH09	EMI/EMC Disturbance Contributing to Signalling and Train Control Hazards	Yes
PH10	Toxic or Explosive Materials	Partially
PH11	Fire, Smoke	Partially

5.2.2 Primary Hazard and Consequence Table

Table 11: Primary Hazard & Consequence Cross Reference

Primary Hazard ID	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10	A11
PH01			X		X	X	X	X			
PH02		X	X	X	X	X	X	X			X
PH03	X	X	X	X	X	X	X	X			X
PH04	X	X		X	X	X	X	X			X
PH05	X		X	X	X	X	X	X			X
PH06			X		X	X	X	X			
PH07	X	X	X			X	X	X			X
PH08	X	X	X	X	X	X	X	X			X
PH9	X	X		X	X	X	X	X	X	X	X
PH10									X	X	
PH11									X	X	

5.3 PTC System Related Primary Hazards

This section presents primary hazards, the hazards identified are those that have an impact with the PTC functionality being implemented, with descriptions and analysis in terms of its consequences. Mitigations considered for these hazard include safety restrictions on existing equipment, safety requirements for ACSES and operational procedures and rules to be implemented by the railroad.

5.3.1 PH01- Undetected Obstruction on Track

In this primary hazard, the focus is on the detection of obstructions on or near the tracks.

If an obstruction exists and is detected by the PTC System, the system will react and restrict the movement authority of approaching trains. If an obstruction exists but is not detected by the PTC System, the hazard can lead to collision or derailment.

Obstructions are categorized as follows:

- Detectable obstructions
- Un-detectable obstructions

Detectable obstruction could be a static obstruction (e.g. track end/buffer, tunnel clearance or boundary of PTC controlled area) or a dynamic obstruction (e.g. other train moving along the track, switch). For this PTC system the underlying signaling system (ASC, ABS or CMB) must provide full detection of detectable obstructions.

Un-detectable obstruction are those which cannot be detected by PTC System, like a person (Staff or Trespassers) on the track, vehicles on grade crossings, or falling objects from PTC equipment or environment. For PTC only the reported failures of grade crossings are considered as the grade crossings are part of the existing signaling system and not part of the analysis to be performed by the system integrator. Broken rail in MBS areas would also be considered an undetectable obstruction.

In order to prevent train movement into or within an area with un-detectable obstructions, the PTC System provides functionalities (Work Zone command, Temporary Speed Restrictions) for the operator to protect relevant track areas. This is only a partial mitigation as the Control Operator must first be made aware of the undetected obstruction.

The Control Operator shall take responsibility to activate work zone speed restrictions or temporary speed restrictions in required situations (hazardous situation or personnel working / walking on track). Appropriate procedures or operational rules must be defined. However, as failure of these functionalities may cause a hazard, the PTC System still has responsibility to ensure these functionalities are working properly.

Individual hazards have been assigned to cover the above primary hazard type. The mitigations to be employed to protect this hazard type are the tunnel clearance protection function, Work zone temporary speed restrictions, C Function, and temporary speed restrictions. Please refer to Table 13: LIRR / MNR Hazard Analysis for a detailed list of hazards related to this hazard type.

5.3.2 PH02- Unsafe Movement Authority Issued

Limit of authority is an area reserved for and exclusively used by a train, Limit of Authority is unsafe if it conflicts with any existing Limit of Authority, or overlaps obstructions.

ACSES will enforce a stop at all signals until a release is provided by the existing signalling system indication of the signal state not being at stop through the existing signalling system or PTC interface to that system. The WIU will also confirm that the switch states for the indicated signal is an approved route.

The existing interlocking shall enforce that the route set through the interlocking is not conflicting with any other route through the interlocking. The existing interlocking shall also vitally check the switch status is correct prior to implementing the signal.

ACSES shall ensure that a full block ahead of the train is available before releasing the PTS, if the ASC is cut out.

Please refer to **Table** 13: LIRR / MNR Hazard Analysis for a detailed list of hazards related to this hazard type. All hazards will be tracked to closure in the Project Hazard Log.

5.3.3 PH03- Train Violates Movement Authority

A train that is violating its movement authority for PTC is a train that is exceeding the calculated ACSES II speed profile for a Positive Train Stop. ACSES will enforce a stop at all signals until a release is provided by the existing signalling system indication of the signal state not being at stop through the existing signalling system or ACSES interface to that system.

ACSES will enforce work zone speed restrictions and prevent train incursions into established work zone limits.

ACSES shall enforce stops over all hand operated points on the mainline where the operating speed is greater than 20 MPH and/or travel through that switch shall create a potential collision with a train on the mainline.

Please refer to Table 13: LIRR / MNR Hazard Analysis for a detailed list of hazards related to this hazard type. All hazards will be tracked to closure in the Project Hazard Log.

5.3.4 PH04- Overspeed

A train is defined to be in an overspeed condition when it travels at a speed exceeding the authorized limit that is known to be safe. Speed limits are defined by track speed, PSR, Route dependent PSR, interlocking speeds, Temporary Speed restrictions and Work Zone specified speed limits.

For LIRR if the speed of the train exceeds the full service brake penalty speed for a period of time then ACSES II will apply the emergency brake.

Please refer to Table 13: LIRR / MNR Hazard Analysis for a detailed list of hazards related to this hazard type. All hazards will be tracked to closure in the Project Hazard Log.

PTC system mitigations include enforcement of TSRs, Enforcement of PSRs, enforcement of TSR’s near line boundaries, enforcement of Route dependent speed restrictions, retention of TSR’s after loss of communication with the Wayside, indication of loss of transponder data, Indication of loss of communication with Wayside, and loss of communication with adjacent railroads.

Non PTC system mitigations include Train engineer adherence to speed restrictions issued from Dispatcher not in the ACSES system, Train engineer adherence of speed restrictions for the length of the train, and ATC enforcement of interlocking speeds and PSR’s.

Please refer to Table 13: LIRR / MNR Hazard Analysis for a detailed list of hazards related to this hazard type. All hazards will be tracked to closure in the Project Hazard Log.

5.3.5 PH05- Unsafe Switch Movement

Generally a switch can be moved for following reasons:

- Switch move is commanded by the system; (ATC System function)
- Switch hand-cranked (by wayside personnel)
- Switch random failure.

The Unsafe Switch movement categorized as follows:

1. Switch move while the switch is locked (ATC System Failure)

Once a switch is locked by the interlocking for a train, this switch shall not be allowed to move for any reason. The switch is allowed to be moved only when the Movement Authority reservation of this switch has been released and other vital conditions for switch move are satisfied. The ATC system is to be designed to prevent this failure from occurring.

When the ATC system moves the switch the ATC system shall confirm the switch is in the correct position to allow the route established. Switch position will be monitored by PTC only for determining proper speed through an interlocking. Protection for incorrect routes shall be implemented by the ATC.

2. Switch moves under train or while train is approaching (ATC System Failure)

Commanding a switch to move while a train is occupying the switch block or while train is approaching is a hazard, as a train might be travelling over this switch while the switch is moved. The ATC system is to be designed to prevent this failure from occurring.

This means that the system fails to detector lock the switch while the over-switch block or approaching block is occupied. Switch moves under an occupying train or while a train is approaching.

3. Un-commanded switch move (Considered by PH-05)

Un-commanded switch move may be caused by manual operation by wayside personnel or by switch random failure.

ACSES shall enforce stops over all hand operated points on the mainline where the operating speed is greater than 20 MPH and/or travel through that switch shall create a potential collision with a train on the mainline.

Note: Acts of Vandalism are addressed in PH08.

Please refer to Table 13: LIRR / MNR Hazard Analysis for a detailed list of hazards related to this hazard type. All hazards will be tracked to closure in the Project Hazard Log.

5.3.6 PH06 Insufficient Protection for Person on Track/Unsafe Track Area

In order to protect authorized personnel working on or along the track, the operator shall either restrict train movement within the relevant area by means of Work Zone protection, or by temporary slower speed restriction for the area where people are authorized to be working along tracks. For PTC this function is performed by RWPS and the Office Subsystems. All RWPS TSR's will be enforced by the STS/Office subsystem and will be retained regardless of RWPS status.

Level crossings are installed along the right-of-way in order to facilitate automobiles and/or pedestrian crossings. These crossing are considered to be an obstacle to a train if they are not in the activated position as a person or automobile may be present on the track; however, if the crossing is activated, it is assumed that the track is clear of automobiles and persons. There are no technical means deployed by MNR and LIRR by which to detect persons and/or vehicles on the tracks.

There are no technical means deployed to detect a person intruding into the tracks, so the PTC System has no direct responsibility to control the prevention of this hazard.

Unsafe track reported by maintenance or operations shall be reported by the dispatcher who will generate a TSR to protect the unsafe track. If the track is not safe for any movement a zero speed TSR shall be requested. If the track speed can be reduced to mitigate the track safety issue then the TSR shall be established for the location and possible position error (5%) to protect train operation.

The PTC system shall allow operations to create TSR's to mitigate for unsafe track areas or staff on track. The railroad shall implement physical security to mitigate intruders.

Please refer to Table 13: LIRR / MNR Hazard Analysis for a detailed list of hazards related to this hazard type. All hazards will be tracked to closure in the Project Hazard Log.

5.3.7 PH07- Unsafe Train Entry / Exit between PTC Territory and Other Systems

Unsafe train entry /exit may occur due to interlocking failures, a train engineer fouling his/her limit of authority, or unsafe limit of authority on the interface between those systems.

Unsafe entry/exit of an interoperable train at an adjacent railroad boundary due to incorrect or missing TSR information communicated to the train.

In cases where the ATC is High Energy Cutout (HECO), such as entering ASC from ABS territory, it is possible for the ACSES to receive a Restricted or Stop and proceed signal which is a permissive signal for ACSES but if the ATC does not properly receive the cut in loop the train may overspeed into the next block.

Please refer to Table 13: LIRR / MNR Hazard Analysis for a detailed list of hazards related to this hazard type. All hazards will be tracked to closure in the Project Hazard Log.

5.3.8 PH08- Unauthorized Access to PTC System

The scope of analysis of this hazard is confined to access to PTC equipment, physical or virtual, which could lead to unintentional or intentional damage to the PTC System, leading to any of the previously described primary hazards. Hazards related to malicious misuse of the system are outside of the scope of this analysis but will be addressed in the System Vulnerability Assessment [24].

Unauthorized Access to PTC System includes:

- Accessing the system through the human-machine interfaces for operations and maintenance;
- Malicious attacks through open transmission in the system communication network.
- Malicious attacks through closed transmission in the system communication network.
- Trespassers causing malicious damage to equipment.

The PTC System with human-machine interfaces shall be protected by password to avoid unauthorized access. Relevant areas with PTC equipment shall be accessed only by authorized personnel (like operator or maintainer). The customer has in place security policy to prevent unauthorized physical access.

Mitigation of this hazard is generally in the form of security for the system, both in the physical sense, closed media transmission, and by means of appropriate protocols, which will prevent any unauthorized changes to the system hardware, software, configuration data, or interfaces to the trackside equipment.

Please refer to Table 13 for a detailed list of hazards related to this hazard type. All hazards will be tracked to closure in the Project Hazard Log.

5.3.9 PH09- EMI/EMC Disturbance Contributing to Signalling and Train Control Hazards

EMI/EMC disturbance can cause discrete transmissions to be falsely permissive. EMC/EMI disturbance can also cause computer systems to malfunction. In the worst case, this can lead to various signalling or train control hazards. The hazard of an EMI/EMC disturbance contributing to signalling or train control hazards will be handled through the EMI/EMC design by ensuring that the design follows relevant international standards.

This hazard can be caused by one of the following contributing factors:

- ACSES II system equipment immunity against EMI/EMC is insufficient;
- PTC system failure to detect and safely react to corruption of data caused by EMI/EMC or lightning;
- PTC system failure to detect and safely react to internal fault caused by EMI/EMC or Lightning.

Please refer to Table 13: LIRR / MNR Hazard Analysis for a detailed list of hazards related to this hazard type. All hazards will be tracked to closure in the Project Hazard Log.

5.3.10 PH10- Toxic or Explosive Materials

This hazard is only partially controlled by the ACSES II System in the sense that the ACSES II System by design must use non-toxic materials and/or gas such as zero halogen wire insulation.

This hazard can only be mitigated by preventing usage of toxic, explosive, and flammable materials in the ACSES II system design.

Please refer to Table **13**: LIRR / MNR Hazard Analysis for a detailed list of hazards related to this hazard type. All hazards will be tracked to closure in the Project Hazard Log.

5.3.11 PH11- Fire, Smoke

A Fire in any structure housing ACSES II equipment can result in multiple fatalities, loss of rolling stock, damage to infrastructure, and loss of system operations in the area where the fire has occurred.

This hazard can only be mitigated by preventing usage of toxic, explosive, flammable materials in the ACSES II system design.

This hazard can be caused by one of the following contributing factors:

- Flammable materials are used to build the ACSES II system equipment;
- Insufficient protection against over voltage conditions at the PTC system electric equipment;
- Insufficient protection against shorted electric circuits within the PTC system equipment;
- Overheated ACSES II system equipment.

Please refer to Table **13**: LIRR / MNR Hazard Analysis for a detailed list of hazards related to this hazard type. All hazards will be tracked to closure in the Project Hazard Log.

6 Hazard Assessment & PHA Result Table

The contributors to the primary hazards identified in section 5 are categorized and summarized in this section. The hazard analysis tables presented in this section include the assessment of applicability of the hazard contributors to the ”Interlocking”, PTC, System operation and support, and exported hazards that are outside of the scope of the PTC system to mitigate. As well, the initial risk assessment, the proposed mitigation requirements, and the residual risk assessment based on the implementation of the mitigations are presented.

The hazard status was not added to the table as all the hazards in this report are open. Current status will be reported from the project hazard log.

All exported hazards will be documented in a Safety Related Application Conditions (SRAC) document that will be agreed with the railroad. All operating and maintenance procedures will require that proper training evidence be provided that shows training has occurred for all impacted users of the system.

The hazards in the following table have been added to the Project Hazard Log. Final resolution and tracking of these hazards will be reported from the Project Hazard Log.

Security mitigations are not included in this analysis. Security will be addressed in the System Vulnerability Analysis.

The analysis and assessment results are presented in table format which contains the following columns:

Table 12: Hazard Table column Definition/Description

Column Title	Description
PHA ID#	A unique identification number is provided per line to simplify hazard location in the tables
Event	List of potential hazardous events that could occur on the LIRR / MNR Right of Way with PTC equipped trains.
Primary Hazard ID	A unique identification number for the Primary Hazard
Primary Hazard	The hazard that could lead to an Accident/Mishap. Defined as per definitions in Section 5.2.1
Hazard Description	Description of the hazard
Potential Cause	Description of the possible causes which might be at the origin of the hazard
Effect	The effect (e.g. hazard consequences) of the hazard on the system. Please refer to section 5.1 for more details.

Initial Risk Assessment	IS - Severity- The severity of the hazard consequences; (Refer to the System Product Safety Plan [4]) IF – Frequency - The frequency of occurrence of the hazard condition; (Refer to the System Product Safety Plan [4])
Final Risk Assessment	FS - Severity- The severity of the hazard consequences; (Refer to the System Product Safety Plan [4]) FF – Frequency - The frequency of occurrence of the hazard condition; (Refer to the System Product Safety Plan [4])
Sub-Syst/ I'face	Identification of the subsystem or interfaces that can contribute to the hazardous event: Onboard; Wayside; Data Communication System; Office; RWPS, STS database.
SR ID	A unique identification assigned to a Safety Requirement. To be updated in the project hazard log to the mitigating system level requirement used to track safety mitigations.
Type	Type of control measure; can be one or more of Design, Operation, Maintenance. Any requirement marked as Railroad indicates a Safety Related Application Condition (SRAC) that needs to be agreed with the railroad prior to allowing revenue service that the safety requirement is implemented by existing equipment and or data not under the scope of this analysis.
Function involved	ACSES II System level function description. Reference to SDD function reviewed where hazards was generated from.
Safety Verification Method	Method to be used to provide verification evidence that the hazard is closed. Note this will be justified further in the project hazard log after linking to the final requirements and test cases is completed.

6.1 Hazard Analysis Table

The Hazard Analysis is presented in Tabular form as per the column Definition/Description given Table 12 above. Refer to Table 13.

Table 13: LIRR / MNR Ha

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	Type	Function involved	Safety Verification Method
PHA-01	Head on collision between 2 trains	PH04	Overspeed	Train exceeds speed for a section of track.	Train Operator fails to enforce safe speed in a section of track.	Collision; Derailment;	II	B	I	E	On-Board	PHA-SR-07	Design	Braking Curve Compensation.	Test
											Onboard	PHA-SR-06	Design		Test
PHA-02	Head on collision between 2 trains	PH04	Overspeed	Train exceeds speed for a section of track	Train exceeds ACSES target speed profile as speed measurement sensor fails to detect the speed of the train.	Collision; Derailment;	I	B	I	E	On-board	PHA-SR-15	Design	Braking Curve Compensation.	Analysis Test
PHA-73	Head on collision between 2 trains	PH04	Overspeed	Train exceeds speed for a section of track	ACSES II not receiving lowest speed limit that is in effect	Collision; Derailment;	I	B	I	E	Transponder Office Onboard	PHA-SR-42	Design	MAS Enforcement, PSR Enforcement.	Analysis
												PHA-SR-36	Design	Braking Curve Compensation.	Test
												PHA-SR-35	Design	TSR Enforcement.	Test
												PHA-SR-95			
												PHA-SR-43	Design	TSR Enforcement	Test

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	Type	Function involved	Safety Verification Method
												PHA-SR-44	Design	PSR Enforcement.	Test
												PHA-SR-30	Op	TSR Enforcement PSR Enforcement	Analysis
PHA-04	Head on collision between 2 trains	PH03	Train violates Movement Authority	One or more trains' authority limit not correctly enforced by ACSES II	ACSES II wrongly locating train relative to Limit of Movement Authority	Collision	I	B	I	E	On-board	PHA-SR-04	Design	Location Determination	Test
PHA-05	Head on collision between 2 trains	PH03	Train violates Movement Authority	One or more trains' authority limit not correctly enforced by ACSES II	Train performance characteristics not programmed correctly	Collision	I	B	I	E	On-board Onboard parameter programmer tool	PHA-SR-17	Design	Braking Curve Compensation, Front of Train Offset by Direction, Wheel Diameters	Test
PHA-06	Head on collision between 2 trains	PH03	Train violates Movement Authority	One or more trains' authority limit not correctly enforced by ACSES II	Train Type wrongly identified by Engineer on at least Train types BL-20 & GP-35/8	Collision	I	B	I	E	LIRR/MNR personnel	PHA-SR-25	Ops	Train Types	Analysis
											Onboard	PHA-SR-45	Design	Train Types	Test
											Onboard	PHA-SR-46	Design	ACSES Display	Analysis
PHA-07	Head on collision between 2 trains	PH02	Unsafe Movement Authority Issued	One or more trains; authority limit not correctly enforced by ACSES II	On-board enforces unsafe Limit of Movement Authority from Wayside	Collision	I	B	I	E	Wayside/ On-Board	PHA-SR-12	Design	PTS Enforcement, TSR Enforcement,	Analysis

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
PHA-08	Head on collision between 2 trains	PH03	Train violates Movement Authority	Non ACSES II train runs afoul of an ACSES II train.	Non ACSES II train overruns a stop signal	Collision	I	B	I	E	Locomotive Engineer, Tennant Locomotive Engineer Maintenance Operator, Tennant Maintenance Operator	PHA-SR-20		Ops	NA	Analysis
PHA-09	Head on collision between 2 trains	PH07	Unsafe Train Entry/Exit	Non ACSES II train runs afoul of an ACSES II train.	Driver fails to obey red signal or ATC fails to stop train from entering mainline.	Collision	I	B	I	E	Operations	PHA-SR-11		Design	Yard and Siding Entry Protection, Exiting ACSES Territory	Test
PHA-10	Rear End Collision Between Two Trains	PH03	Train violates Movement Authority	Train exceeds zero speed for a section of track	Train Operator fails to enforce safe speed in a section of track	Collision	I	B	I	E	On-Board	PHA-SR-07		Design	Braking Curve Compensation.	Test
												PHA-SR-06		Design		Test
PHA-11	Rear End Collision Between Two Trains	PH03	Train violates Movement Authority	Train not correctly enforced by ACSES II	Train exceeds ACSES target speed profile as speed measurement sensor fails to detect the speed of the train.	Collision	I	B	I	E	On-board	PHA-SR-15		Design	Braking Curve Compensation.	Analysis Test
PHA-12	Rear End Collision Between Two Trains	PH03	Train violates Movement Authority	Train not correctly enforced by ACSES II	ACSES II wrongly locating train relative to Limit of Movement Authority	Collision	I	B	I	E	On-board	PHA-SR-04		Design	Location Determination	Test
									I	D	Transponder	PHA-SR-31		Maintenance	Location Determination	Analysis
									I	E	Onboard Transponder	PHA-SR-75		Design	Location Determination	Analysis

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	Type	Function involved	Safety Verification Method
									I	D	Maintenance	PHA_SR_81	Maintenance	Location Determination	Analysis
PHA-13	Rear End Collision Between Two Trains	PH03	Train violates Movement Authority	Train not correctly enforced by ACSES II	Train performance characteristics not programmed correctly	Collision	I	B	I	E	On-board Onboard programing Tool	PHA-SR-17	Design	Braking Curve Compensation, Front of Train Offset by Direction, Wheel Diameters	Test
PHA-14	Rear End Collision Between Two Trains	PH03	Train violates Movement Authority	Train not correctly enforced by ACSES II	Train Type wrongly identified by Engineer on at least Train types BL-20 & GP-35/8	Collision	I	B	I	E	Locomotive Engineer Onboard	PHA-SR-25	Ops	Train Type	Analysis
PHA-15	Rear End Collision Between Two Trains	PH02	Unsafe Movement Authority Issued	Train not correctly enforced by ACSES II	On-board enforces unsafe Limit of Movement Authority from Wayside	Collision	I	B	I	E	Wayside/On-Board	PHA-SR-12	Design	-PTS Enforcement,	Analysis
PHA-16	Rear End Collision Between Two Trains	PH03	Train violates Movement Authority	Non ACSES II train runs afoul of an ACSES II train.	Non ACSES II train overruns a stop signal	Collision	I	B	I	E	LIRR/MNR personnel	PHA-SR-20	Ops	Yard and Siding Entry Protection, Exiting ACSES Territory	Analysis
PHA-17	Rear End Collision Between Two Trains	PH07	Unsafe Train Entry/Exit	Train exceed limit authority near ACSES entry / Exit	Driver fails to obey red signal or ATC fails to stop train from entering mainline.	Collision	I	B	I	E	Wayside Onboard	PHA-SR-11	Design	Yard and Siding Entry Protection, Exiting ACSES Territory	Test

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
PHA-18	ACSES II Train collides with bumper block	PH04	Overspeed	Train speed not controlled correctly by Engineer.	Train in Yard Mode under Engineer's control subject to restricted speed limit not properly controlled by Engineer.	Collision with Bumper Block	II	B	II	C	LIRR/MNR personnel	PHA-SR-21		Ops	Exiting ACSES Territory	Analysis
											Interlocking	PHA-SR-51		Design	Exiting ACSES Territory	Test
											Onboard Transponder	PHA-SR-52		Design	Exiting ACSES Territory	Test
PHA-19	ACSES II Train collides with bumper block	PH04	Overspeed	Train speed excessive coming into terminal and not controlled by Engineer.	ACSES II not correctly enforcing Yard Mode speed.	Collision with Bumper Block	I	B	I	E	On-Board/	PHA-SR-10		Design;	Exiting ACSES Territory	Test
											Onboard	PHA_SR_7		Design	Exiting ACSES Territory	Test
											Interlocking	PHA-SR-51		Design	Exiting ACSES Territory	Test
PHA-20	Antenna masts collapse	PH06	Insufficient Protection for Person on Track/Unsafe Track Area	Mast falls on tracks, within the clearance space for the train, or roadways /walkways,	Incorrect foundations or structural design	Collision with Object on track or Infrastructure. Non-Vehicular death or injury (Staff or Passenger)	I	B	I	D	Wayside	PHA-SR-13		Design	Data Radio Transmission	Analysis Post Installation Check

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
PHA-21	Antenna masts collapse	PH06	Insufficient Protection for Person on Track/Unsafe Track Area	Mast falls on tracks, equipment or passers by	Incorrect maintenance	Collision with Object on track or Infrastructure. Non-Vehicular death or injury (Staff or Passenger)	I	B	I	D	Wayside	PHA-SR-16		Maint.	Data Radio Transmission	Analysis Post Installation Check
PHA-22	On-Track equipment Struck by train	PH01	Undetected obstruction on track	Train violates a speed restriction established to provide protection from an unsafe condition at a certain location.	On-board receives incorrect Mandatory Directive	Collision; Derailment	I	B	I	E	Office/On-Board	PHA-SR-24		Ops/ Maint	TSR Enforcement	Analysis
									I	E	Office / Onboard	PHA-SR-28		Design	TSR Enforcement	Analysis
PHA-23	ACSES II Equipt. Struck by train	PH01	Undetected obstruction on track	ACSES equipment installed such that it interferes with train movement.	On board equipment not correctly installed	Collision with Object on track or Infrastructure	I	B	I	E	On-board	PHA-SR-08		Design/ Install.	NA	Analysis Installation Checklist Post Installation Checkout
PHA-24	ACSES II Equipt. Struck by train	PH01	Undetected obstruction on track	ACSES equipment installed such that it interferes with train movement. When equipment is	Wayside equipment not correctly installed	Collision with Object on track or Infrastructure	I	B	I	E	Transponder, Wayside	PHA-SR-26		Install/Maint.	-NA	Analysis

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	Type	Function involved	Safety Verification Method
				maintained it shall also be clear of the track.											
												PHA-SR-27	Install/Maint.	-NA	Analysis
PHA-25	Highway crossing warning systems do not activate or activate late for a train	PH06	Insufficient Protection for Person on Track/Unsafe Track Area	ACSES II not sending TSR in time.	Highway crossing failure not reported	Collision with Road vehicle or pedestrian	I	C	I	C	Operations	PHA-SR-05	Ops	Stop and Release TSR	Analysis
							I	C	I	D	Office / Onboard	PHA-SR-47	Design	Stop and Release TSR	Test
							I	C	I	E	Onboard	PHA-SR-65	Design	Stop and Release TSR	Test
PHA-26	ACSES II Train Derails on switch	PH04	Overspeed	Train exceeds speed for a section of track	Train Operator fails to enforce safe speed in a section of track	Derailment	I	B	I	E	On-Board	PHA-SR-07	Design	Braking Curve Compensation.	Test
									I	E	Onboard	PHA-SR-06	Design	Brake Assurance	Test
PHA-27	ACSES II Train Derails on switch	PH04	Overspeed	Train not correctly enforced by ACSES II	Train exceeds ACSES target speed profile as speed measurement sensor fails to detect the speed of the train.	Derailment	I	B	I	E	On-board	PHA-SR-15	Design	Braking Curve Compensation.	Test Analysis

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	Type	Function involved	Safety Verification Method
PHA-28	ACSES II Train Derails on switch	PH04	Overspeed	Train not correctly enforced by ACSES II	ACSES II wrongly locating train relative to Limit of Movement Authority	Derailment	I	B	I	E	On-board	PHA-SR-04	Design	Location Determination	Test
											Transponder Onboard	PHA-SR-36	Design	Location Determination	Test
											Transponder	PHA-SR-31	Maintenance	Location Determination	Analysis
											Onboard Transponder	PHA-SR-75	Design	Location Determination	Analysis
									I	D	Maintenance	PHA_SR_81	Maintenance	Location Determination	Analysis
PHA-29	ACSES II Train Derails on switch	PH04	Overspeed	Train not correctly enforced by ACSES II	Train performance characteristics not programmed correctly	Derailment	I	B	I	E	On-board On-board programming tool	PHA-SR-17	Design	Braking Curve Compensation, Front of Train Offset by Direction, Wheel Diameters	Test Analysis
PHA-30	ACSES II Train Derails on switch	PH04	Overspeed	Train not correctly enforced by ACSES II	Train Type wrongly identified by Engineer on at least Train types BL-20 & GP-35/8	Derailment	I	B	I	E	Locomotive Engineer Onboard	PHA-SR-25	Ops	Train Type	Analysis
PHA-31	ACSES II Train Derails on switch	PH05	Unsafe Switch Movement	Train not correctly enforced by ACSES II.	On-board enforces unsafe Limit of Movement Authority from Wayside.	Derailment	I	B	I	E	Wayside/On-Board	PHA-SR-12	Design	-PTS Enforcement,	Test

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
PHA-32	ACSES II Train derails on hand thrown switch in ATC (ASC, ABS or CMB)	PH02	Unsafe Movement Authority Issued	Train not correctly enforced by ACSES II.	On-board enforces unsafe Limit of Movement Authority from Wayside.	Derailment	I	B	I	E	Wayside/On-Board	PHA-SR-12		Design	-PTS Enforcement	Analysis
PHA-33	ACSES II Train derails on hand thrown switch	PH08	Unauthorized access to ACSES II System	Train detects switch opening but cannot stop in time.	Vandalism	Derailment	I	B	I	E	Wayside/On-Board	PHA-SR-22		Design; Maint.	- Braking Curve Compensation.	Analysis Post Installation Checkout
PHA-34	ACSES II Train Derails on Curve	PH04	Overspeed	Train exceeds speed for a section of track	Train Operator fails to enforce safe speed in a section of track	Derailment	I	B	I	E	On-Board	PHA-SR-07		Design	Braking Curve Compensation	Test
												PHA-SR-06		Design		
PHA-35	ACSES II Train Derails on curve	PH04	Overspeed	Train not correctly enforced by ACSES II	Train exceeds ACSES target speed profile as speed measurement sensor fails to detect the speed of the train.	Derailment	I	B	I	E	On-board	PHA-SR-15		Design	Braking Curve Compensation	Test Analysis
PHA-36	ACSES II Train Derails on curve	PH04	Overspeed	Train not correctly enforced by ACSES II	ACSES II wrongly locating train relative to Limit of Movement Authority	Derailment	I	B	I	E	On-board	PHA-SR-04		Design	Location Determination	Test
											Transponder Onboard	PHA-SR-36		Design	Location Determination	Test

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
											Transponder	PHA-SR-31		Maintenance	Location Determination	Analysis
											Onboard Transponder	PHA-SR-75		Design	Location Determination	Analysis
									I	D	Maintenance	PHA_SR_81		Maintenance	Location Determination	Analysis
PHA-37	ACSES II Train Derails on curve	PH04	Overspeed	Train not correctly enforced by ACSES II	Train performance characteristics not programmed correctly	Derailment	I	B	I	E	On-board On-board programing tools	PHA-SR-17		Design	Braking Curve Compensation, Front of Train Offset by Direction, Wheel Diameters	Test Analysis
PHA-38	ACSES II Train Derails on switch	PH04	Overspeed	Train not correctly enforced by ACSES II	Train Type wrongly identified by Engineer on at least Train types BL-20 & GP-35/8	Derailment	I	B	I	E	LIRR/MNR personnel	PHA-SR-25		Ops	Train Type	Analysis
											Onboard	PHA-SR-45		Design	Train Type	Test
											Onboard	PHA-SR-46		Design	ACSES Display	Analysis
PHA-39	ACSES II Train Derails on curve	PH04	Overspeed	ACSES II train derails as train speed is higher then safe operating speed.	ACSES II speed limit on curve is incorrect	Derailment	I	B	I	E	Data	PHA-SR-23		Railroad	MAS Enforcement, PSR Enforcement	Test Analysis
											Transponder	PHA-SR-18		Design/ Install	MAS Enforcement, PSR Enforcement	Analysis
											Transponder	PHA-SR-53		Design	MAS Enforcement, PSR Enforcement	Analysis
PHA-40	Staff Struck by train	PH04	Overspeed	Train exceeds speed for a section of track	Train Operator fails to enforce safe speed in a section of track	Derailment; Staff Struck by Train	I	B	I	E	On-Board	PHA-SR-07		Design	Braking Curve Compensation	Test

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	Type	Function involved	Safety Verification Method
												PHA-SR-06	Design		
PHA-41	Staff Struck by train	PH04	Overspeed	Train not correctly enforced by ACSES II	Train exceeds ACSES target speed profile as speed measurement sensor fails to detect the speed of the train.	Derailment; Staff Struck by Train	I	B	I	E	On-board	PHA-SR-15	Design	Braking Curve Compensation	Test Analysis
PHA-42	Staff Struck by train	PH04	Overspeed	Train not correctly enforced by ACSES II	ACSES II wrongly locating train relative to Limit of Movement Authority	Derailment; Staff Struck by Train	I	B	I	E	On-board	PHA-SR-04	Design	Location Determination	Test
											Transponder Onboard	PHA-SR-36	Design	Location Determination	Test
											Transponder	PHA-SR-31	Maintenance	Location Determination	Analysis
											Onboard Transponder	PHA-SR-75	Design	Location Determination	Analysis
									I	D	Maintenance	PHA_SR_81	Maintenance	Location Determination	Analysis
PHA-43	Staff Struck by train	PH04	Overspeed	Train not correctly enforced by ACSES II	Train performance characteristics not programmed correctly	Derailment; Staff Struck by Train	I	B	I	E	On-board On-board programing tools	PHA-SR-17	Design	Braking Curve Compensation, Front of Train Offset by Direction, Wheel Diameters	Test Analysis
PHA-44	Staff Struck by train	PH04	Overspeed	Train not correctly enforced	Train Type wrongly identified by Engineer on at	Derailment; Staff	I	C	I	E	Locomotive Engineer Onboard	PHA-SR-25	Ops	Train Type	Analysis

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	Type	Function involved	Safety Verification Method
				by ACSES II	least Train types BL-20 & GP-35/8	Struck by Train					Onboard	PHA-SR-45	Design	Train Type	Test
											Onboard	PHA-SR-46	Design	ACSES Display	Analysis
PHA-46	Staff Struck by train	PH04	Overspeed	Train violates a speed restriction established to provide protection from an unsafe condition at a certain location.	On-board receives incorrect Mandatory Directive	Derailment; Staff Struck by Train	I	C	I	E	Office/On-Board	PHA-SR-24	Ops/ Maint	-TSR Enforcement, Roadway Worker Protection	Test
												PHA-SR-28	Design	TSR Enforcement, Roadway Worker Protection	Analysis Test
									I	D	Operations	PHA_SR_	Ops	TSR Enforcement, Roadway Worker Protection	Analysis
PHA-47	Radiation effects	PH09	EMI/EMC Disturbance contributing to Signaling and Train Control Hazards	Person in the presence of a radiating ACSES II object.	Radiating devices accessible to passengers in public area	Non-Vehicular death or injury (Staff or Passenger)	II	B	II	D	Comms, Onboard, RWPS	PHA-SR-09	Design	N/A	analysis
									II	D	RWPS	PHA-SR-101	Design	Roadway Worker Protection	Analysis
									II	E	Comms, Onboard, RWPS	PHA-SR-102	Maintenance	NA	Analysis
PHA-48	Electrocution	PH06	Insufficient Protection for Person on Track/Unsafe Track Area	Person in contact with or near an electrical power source.	Material with electrical potential accessible to passengers in public area.	Non-Vehicular death or injury (Staff or Passenger)	I	B	I	E	All s/systems	PHA-SR-02	Design	N/A	Inspection\ First Article Inspection

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
PHA-49	Electrocution	PH06	Insufficient Protection for Person on Track/Unsafe Track Area	Person in contact with or near an electrical power source.	Inadequate maintenance procedures	Non-Vehicular death or injury (Staff or Passenger)	I	B	I	E	All s/systems	PHA-SR-14		Maint.	N/A	Analysis
PHA-50	Fire	PH11	Fire, Smoke	Burns to passengers, crew and third parties	Underrated cables, incorrect materials selection etc.	Non-Vehicular death or injury (Staff or Passenger)	I	B	I	E	All s/systems	PHA-SR-01		Design	N/A	Analysis First Article Inspection
PHA-51	Fire	PH11	Fire, Smoke	Inhalation damage to passengers, crew, and third parties	, Underrated cables, incorrect materials selection, etc.	Non-Vehicular death or injury (Staff or Passenger)	I	B	I	E	All s/systems	PHA-SR-03		Design	N/A	Analysis First Article Inspection
PHA-59	Train overspeeds in Adj Railroad	PH04	Oversepeed	Train violates a TSR in an adjacent RR	TSR is not communicated from the adjacent RR	Staff struck by Train, Derailment	I	B	I	D	Office	PHA-SR-37		Design	Shadowed TSR	Test
							I	B	I	E	Office	PHA-SR-56		Design	Shadowed TSR	Test
PHA-60	Head on Collision between two trains.	PH03	Train Violates Movement Authority	Train violates Home Signal after turnback.	If the train tail is not past the HS transponder when the turnback is performed the tail OBC will not be able to enforce a PTS.	Collision.	I	B	I	C	Operations	PHA-SR-54		Operations	Turnback Function	Analysis Analysis
							I	B	I	E	Transponder	PHA-SR-38		Design / Operations	Turnback Function	Test Analysis

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	Type	Function involved	Safety Verification Method
PHA-61	Head on Collision between two trains.	PH03	Train Violates Movement Authority	Train location incorrectly calculated	Offset distance of Scanner for rolling stock is not considered in train calculation	Train violates target PTS due to incorrect assumption of scanner offset.	I	B	I	E	Onboard	PHA-SR-39	Design	Front of Train Offset by Direction	Test Post Installation Check
PHA-62	Collision with Object on track or infrastructure	PH01	Undetected Obstruction on Track	Wrong train type allowed to proceed into ESA tunnel.	Train type that cannot clear ESA tunnel misses transponder with tunnel package for that train type	Train enters ESA Tunnel and collides with tunnel	I	B	I	E	Transponder, Onboard	PHA-SR-40	Design	East Side Access Entry	Test Analysis
PHA-63	Train derails	PH04	Overspeed	One or more trains not correctly enforced by ACSES.	ACSES reduces the train speed so that the front of the train enters the TSR at the correct speed, but the Train engineer accelerates past TSR restriction before rear of train is past TSR location.	Train derails due overspeed	I	B	I	C	Operations	PHA-SR-29	Operations	East Side Access Entry	Analysis Training
PHA-64	Collision at 15MPH	PH03	Train violates Movement Authority in ASC Territory	Train not correctly enforced by ACSES II	ACSES II not enforcing speed	Lower speed (15mph) collision	III	B	III	E	On-Board	PHA-SR-07	Design	Braking Curve Compensation	Test
												PHA-SR-06	Design	PTS Enforcement	Test
PHA-65	Collision at 15MPH	PH03	Train violates Movement Authority in ASC Territory	Train not correctly enforced by ACSES II	ACSES II not measuring speed correctly	Lower speed (15mph) collision	III	B	III	E	On-board	PHA-SR-15	Design	Braking Curve Compensation	Test Analysis

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
PHA-66	Collision at 15MPH	PH03	Train violates Movement Authority in ASC Territory	Train not correctly enforced by ACSES II	ACSES II wrongly locating train relative to Limit of Movement Authority	Lower speed (15mph) collision	III	B	III	E	On-board	PHA-SR-04		Design	Location Determination Location Determination	Test
											Transponder Onboard	PHA-SR-36		Design	Location Determination	Test
											Transponder	PHA-SR-31		Maintenance	Location Determination	Analysis
									I	D	Maintenance	PHA_SR_81		Maintenance	Location Determination	Analysis
PHA-67	Collision at 15MPH	PH03	Train violates Movement Authority in ASC Territory	Train not correctly enforced by ACSES II	Train performance characteristics not programmed correctly	Lower speed (15mph) collision	III	B	III	E	On-board On-board programing tools	PHA-SR-17		Design	Braking Curve Compensation, Front of Train Offset by Direction, Wheel Diameters	Test
									III	E	On-board On-board Programing Tools	PHA-SR-103		Design	Braking Curve Compensation, Front of Train Offset by Direction, Wheel Diameters	Test
PHA-68	Collision at 15MPH	PH03	Train violates Movement Authority in ASC Territory	Train not correctly enforced by ACSES II	Train Type wrongly identified by Engineer on at least Train types BL-20 & GP-35/8	Lower speed (15mph) collision	III	B	III	C	LIRR/MNR personnel	PHA-SR-25		Ops	Train Type	Analysis
							III	B	III	E	Onboard	PHA-SR-45		Design	Train Type	Test

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	Type	Function involved	Safety Verification Method
							III	B	III	E	Onboard	PHA-SR-46	Design	ACSES Display	Analysis
PHA-69	Collision at 15MPH	PH02	Unsafe Movement Authority Issued in ASC Territory	Train not correctly enforced by ACSES II	On-board enforces unsafe Limit of Movement Authority from Wayside	Lower speed (15mph) collision	III	B	III	E	Wayside, On-Board,	PHA-SR-12	Design	PTS Enforcement	Analysis
PHA-70	Collision at 15MPH	PH03	Train violates Movement Authority in ASC Territory	Non ACSES II train runs afoul of an ACSES II train.	Non ACSES II train overruns a stop signal	Lower speed (15mph) collision	III	B	III	E	LIRR/MNR personnel	PHA-SR-20	Ops		Analysis
PHA-71	Collision at 15MPH	PH07	Unsafe Train Entry/Exit in ASC Territory	Non ACSES II train runs afoul of an ACSES II train.	Driver fails to obey red signal or ATC fails to stop train from entering mainline.	Lower speed (15mph) collision	III	B	III	E	Wayside Onboard	PHA-SR-11	Design	Yard and Siding Entry Protection, Exiting ACSES Territory	Test
PHA-72	ACSES II Train derails on hand thrown switch in MBS	PH05	Unsafe Switch Movement	Train not correctly enforced by operations.	Operating staff to check DSI per rule book.	Derailment	I	C	I	C	Operations	PHA-SR-41	Ops	Manual Block System Territory (MBS)	Analysis
PHA-74	Head on collision betwee	PH04	Unsafe Movement Authority Issued	One or more trains; authority limit not	On-board enforces unsafe Limit of Movement	Collision	I	C	I	E	Wayside	PHA-SR-48	Design	PTS Enforcement	Test

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	Type	Function involved	Safety Verification Method
	n 2 trains			correctly enforced by ACSES II	Authority from Wayside						Onboard	PHA-SR-34	Design	PTS Enforcement	Test
											Wayside	PHA-SR-49	Design	PTS Enforcement	Test
											ATC Interlocking	PHA-SR-67	Railroad	PTS Enforcement	Analysis
PHA-83	ACSES II train derails on Switch	PH05	Unsafe Switch Movement	Switch movement not correctly enforced by ATC.	Existing ATC (ABS, CMB, or ASC) moves a switch under a train or as a train approaches.	Derailment	I	E	I	E	ATC Interlocking	PHA-SR-67	Railroad	PTS Enforcement	Analysis
PHA-76	Head on collision between 2 trains	PH03	Train violates Movement Authority	Non ACSES II train runs afoul of an ACSES II train.	Non ACSES II train overruns a temporal separation	Collision	I	C	I	E	Operations	PHA_SR-50	Ops	Manual Block System Territory (MBS)	Analysis
									I	E	Office	PHA-SR-64	Design	Manual Block System Territory (MBS)	Test
PHA-75	Head on collision between 2 trains	PH03	Train violates Movement Authority	Service Brake Failure.	ACSES requests a service brake application as the train is not within the ACSES speed profile but fails to apply the service brakes	Collision	I	B	I	D	Operations	PHA-SR-55	Ops	Departure Test	Analysis

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
PHA-77	Staff Struck by train	PH04	Overspeed	EIC to RWPS Loss of Communication	TSR Request from EIC fails to be set.	Derailment; Staff Struck by Train	I	C	I	D	Office	PHA-SR-58		Design	Roadway Worker Protection System	Test
											RWPS	PHA-SR-59		Design	Roadway Worker Protection System	Test
											RWPS	PHA-SR-60		Design	Roadway Worker Protection System	Test
											Operation	PHA-SR-61		Ops	Roadway Worker Protection System	Analysis
PHA-78	Staff struck by Train	PH04	Overspeed	EIC to RWPS Incorrect Transfer	TSR Request from EIC is not correct.	Derailment; Staff Struck by Train	I	C	I	D	RWPS Communications	PHA_SR-62		Design	Roadway Worker Protection System	Test
											Office	PHA-SR-63		Design	Roadway Worker Protection System	Test
PHA-79	Train to Train Collision – Operating over a switch in wrong	PH02	Unsafe Movement Authority Issued	MBS area switch protection	Train is operated in MBS area over a switch in the incorrect position	Collision	I	C	I	E	Office	PHA-SR-64		Design	Manual Block System Territory (MBS)	Test
									I	D	Operation	PHA-SR-41		Ops	Manual Block System Territory (MBS)	Analysis

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
	position								I	D	Operation	PHA-SR-50		Ops	Manual Block System Territory (MBS)	Analysis
PHA-80	Rear End Collision	PH07	Train Entering ASC from ABS	ATC fails to reduce the speed of a train after entering ASC from ABS Territory	ATC is High Energy Cutout when operating in ABS Territory. When entering ACSES territory the signal state could be Restricted or Stop and Proceed which are considered permissive by ACSES. If the ATC fails to wakeup and restrict the speed of the train the train could overspeed into the next ASC block cause a collision.	Collision	I	C	I	E	Wayside	PHA-SR-68		Design	PTS Enforcement	Test
						Collision	I	C	I	C	ATC / Interlocking	PHA-SR-69		Railroad	NA	NA (outside scope of contract)
PHA-81	Head on collision between 2 trains	PH04	Overspeed	Failure to Acknowledge Overspeed	The operator fails to Ack the overspeed alarm or the Ack button fails in the inactive position.	Derailment Collision	I	C	I	E	Onboard	PHA-SR-70		Design	PTS Enforcement	Test
PHA-82	Head on collision between 2 trains	PH04	Overspeed	Failure of Ack Button	The Ack button fails in the Ack position.	Derailment Collision	I	C	I	E	Onboard	PHA-SR-71		Design	PTS Enforcement	Test

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
PHA-84	Head on collision between 2 trains	PH03	Train violates Movement Authority	Reverse Moves	Train Engineer activates the cab in the tail of the train and pushes the train in reverse onto the mainline violates a signal.	Collision Derailment	I	C	I	E	ATC / Interlocking	PHA-SR-72		External	NA	NA (outside scope of contract)
PHA-85	Head on collision between 2 trains	PH03	Train violates Movement Authority	Loss of communication between WIU and OBC	The OBC allows a train to pass a PTS without getting confirmation from the WIU that the signal is clear	Collision	I	C	I	E	Onboard	PHA-SR-76		Design	PTS Enforcement	Test
							I	C	I	D	Operations	PHA-SR-77		Design	PTS Enforcement	Test
PHA-86	Head on Collision Between 2 trains	PH03	Train violates Movement authority	Loss of comms between ATC and OBC (including AIU)	The OBC allows a train to enter an interlocking based on ATC data when the ATC is not communicating.		I	C	I	E	Onboard	PHA-SR-78		Design	PTS Enforcement	Test
PHA-87	Head on collision between 2 trains	PH04	Overspeed	Train exceeds speed for a section of track.	Brake Assurance Function does not protect from 42 MPH to 16 MPH.	Collision	I	C	I	D	Onboard	PHA-SR-79		Design	PTS Enforcement	Analysis
							I	C	I	C	Operations	PHA-SR-80		Ops	PTS Enforcement	Analysis

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
PHA-88	Read End Collision between 2 trains	PH02	Unsafe Movement Authority Issued	ATC Cutout	ACSES does not detect that the ATC is cutout and lets the train into the next block without safe train separation	Collision	I	C	I	E		PHA-SR-82		Design	C Signal	Test
									I	E		PHA-SR-83		Design	C Signal	Test
									I	C		PHA-SR-84		Ops	C Signal	Analysis
									I	C		PHA-SR-85		External		N/A
PHA-89	ACSES II Train Derails on switch	PH04	Overspeed	STS Database Incorrect	The vital data used by STS to verify TSR Requests is incorrect	Derailment	I	C	I	E	Office	PHA-SR-86		Design	TSR Enforcement	Test
									I	D	Office	PHA-SR-87			TSR Enforcement	Analysis
									I	E	Office	PHA-SR-88		Maintenance	TSR Enforcement	Test
PHA-90	ACSES II Train Collision betwee	PH03	Train Passes Signal at Red	WIU Data incorrect	The vital application data / program has incorrect data.	Collision	I	C	I	E	WIU	PHA-SR-89		Design	PTS Enforcement	Test

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
	n 2 Trains								I	D	WIU	PHA-SR-90			PTS Enforcement	Analysis
									I	E	WIU	PHA-SR-91		Maintenance	PTS Enforcement	Test
PHA-91	ACSES II Train Derails on switch	PH04	Overspeed	UIS Database Incorrect	The UIS database has incorrect data	Collision	I	C	I	E	Office	PHA-SR-92		Design	TSR Enforcement	Test
									I	E	Office	PHA-SR-93		Design	TSR Enforcement	Test
									I	D	Office	PHA-SR-94		Operations	TSR Enforcement	Analysis
PHA-92	ACSES II Train Derails on switch	PH04	Overspeed	TP data incorrect	Transponder programmed with incorrect data or the incorrect packet programmed into the wrong transponder.	Derailment	I	C	I	D	Transponder	PHA-SR-96		Design		Analysis
									I	D	Transponder	PHA-SR-97		Ops		Test
PHA-93	Head on collision betwee	PH03	Train Violates Movement Authority	Communication Delay	ACSES data is not updated and the system reacts to old data.	Collision	I	C	I	E	Onboard	PHA-SR-36		Design	PSR Enforcement	Test

PHA ID#	Event	Primary Hazard ID	Primary Hazard	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Sub-Syst/ I'face	SR_ID	[redacted]	Type	Function involved	Safety Verification Method
	n 2 trains								I	E	Onboard	PHA-SR-34		Design	PTS Enforcement	Test
									I	E	Onboard	PHA-SR-35		Design	TSR Enforcement	Test
									I	D	Office	PHA-SR-98				
									I	E	Onboard	PHA-SR-99				
									I	E	Onboard	PHA-SR-100				
									I	E	WIU	PHA-SR-49				
									I	E	RWPS	PHA-SR-59				
									I	E	Onboard	PHA-SR-78				

6.2 Hazard Analysis Results

The PHA identified the Possible Causes as the contributors to the Primary Hazards and these are listed in Table 14. These will be further decomposed into their contributing events in the SHA.

Table 14: Summary of Identified Hazards

Primary Hazard ID	Potential Cause
PH01	On board equipment not correctly installed
PH01	Wayside equipment not correctly installed
PH01	On-board receives incorrect Mandatory Directive
PH01	Tunnel package missing from Transponder near ESA Tunnel
PH02	On-board enforces unsafe Limit of Movement Authority from Wayside
PH02	Train is operated in MBS territory over a switch in the incorrect position.
PH03	Non ACSES II train overruns a stop signal
PH03	ACSES II not enforcing speed
PH03	Train performance characteristics not programmed correctly
PH03	Train Type on at least Train types BL-20 & GP-35/8 wrongly identified by Engineer
PH03	Transponder Installed at incorrect location
PH03	Transponder programmed with incorrect or missing data
PH03	ACSES Cut Out
PH03	WIU Communication Failure
PH03	Transponder Communication Failure
PH03	Scanner Offset Location
PH03	ACSES II wrongly locating train relative to limit of movement authority
PH03	ACSES II not measuring speed correctly
PH03	NonACSES II train overruns a temporal separation
PH03	Failure to perform the departure test on the 24 hour cycle. Possible equipment failure not detected.
PH03	Train Reverse Moves violates mainline.
PH03	OBC to ATC communication Failure
PH04	ACSES II not correctly enforcing Yard Mode speed.
PH04	Train Operator fails to enforce safe speed in a section of track.
PH04	ACSES II not measuring speed correctly
PH04	ACSES II speed limit on curve is incorrect
PH04	ACSES II wrongly locating train relative to Limit of Movement Authority
PH04	Train in Yard Mode under Engineer's control subject to restricted speed limit not properly controlled by Engineer.
PH04	ASC Cut Out
PH04	Office to Train Communication Failure
PH04	TSR communication from Adj Railroad
PH04	Train accelerates before clearing TSR Location
PH04	ACSES II not receiving lowest speed limit that is in effect.
PH04	TSR is not communicated from the Adjacent RR.
PH04	TSR Request from EIC fails to be set.
PH04	TSR Request from EIC is not correct.
PH04	Error in Operator Ack of Overspeed

Primary Hazard ID	Potential Cause
PH04	Overspeed in Brake Assurance
PH04	ACSES does not detect that the ATC is cutout and lets the train into the next block without safe train separation
PH04	The vital data used by STS to verify TSR Requests is incorrect
PH04	The vital application data / program has incorrect data.
PH04	The UIS database has incorrect data
PH04	The TP telegrams are programmed with incorrect data
PH04	ACSES data is not updated and the system reacts to old data
PH05	On-board enforces unsafe Limit of Movement Authority from Wayside
PH05	Initial WIU message shows go aspect but signal is latter canceled by ASC after communication failure
PH05	Operating staff to check DSI before switch and operator per rule book.
PH05	Existing ATC moves a switch under a train or as a train approaches.
PH06	Inadequate maintenance procedures
PH06	Incorrect foundations or structural design
PH06	Incorrect maintenance
PH06	Material with electrical potential accessible to passengers in public area.
PH06	Highway Crossing failure not reported
PH06	Radiating devices accessible to passengers in public area
PH07	Driver fails to obey red signal or ATC fails to stop train from entering mainline.
PH07	System fails to enforce a PTS stop on entry to ASC from ABS.
PH08	Vandalism
PH09	Radiating devices accessible to passengers in public area
PH11	Underrated cables, incorrect materials selection etc.

7 Functional Safety Requirements

The preliminary hazard analysis highlights several safety requirements that have to be taken into account during the PTC system life cycle.

7.1 Function Classification

The preliminary hazard analysis table leads to the following classification of LIRR / MNR PTC functions in term of severity:

Table 15: Function Classification

Function involved	Severity
Braking Curve Compensation.	I
MAS Enforcement	I
PSR Enforcement	I
TSR Enforcement	I
Location Determination	I
Front of train Offset by Direction	I
Wheel Diameters	I

Train Types	I
ACSES Display	I
ACSES II equipment shall shielded to minimize radiation exposure	II
Exiting ACSES II Territory	I
Yard and Siding Entry Protection	I
Stop and Release TSR	I
Roadway Worker Protection	I
Shadowed TSR	I
East Side Access Entry	I
Turnback Function	I
Manual Block System Territory	I
Departure Test	I
Data Radio Transmission	I

7.2 Safety Requirement

All ACSES II safety requirements developed from the PHA tables as well as the methods used to mitigate the hazard will be logged in the Hazard Log (“Identification of proposed hazard mitigation”).

The methods used to mitigate the hazard will specify how the safety requirement must be taken into account by the LIRR / MNR PTC system, and/or by Operating Procedures. This requirement list will be incorporated into the SLR. The SLR will identify safety requirements with a Safety Flag that will be reviewed by Safety Engineering. Please refer to the Requirements Management Plan [10] on how the RTM will be generated from this condition.





8 Conclusion

The LIRR / MNR PTC System Preliminary Hazard Analysis (PHA) has identified the potential high-level hazards in the operation of the PTC System.

Some of the identified primary hazards were lower level hazards (belonging to subsystem level hazard analysis) i.e. due to the way of working, subsystem safety analysis have been handled by different organization, thus, these lower level hazards were recorded within the PHA hazard table (especially from PHA 52 to PHA 72). However, not all the primary hazards were break down further to lower level hazards.

In Section 5.1 the Accident Types A01 to A11 were presented. In Section 5.3 the Primary Hazards were presented.

In Section 6, the Preliminary analysis of the Primary Hazards was presented, which identified the hazard contributors (Causes). These Primary Hazards will be further decomposed in the Project Hazard Log these identified hazards will form the basis of the start of the SHA.

In Section 7 , the Safety requirements are identified. These requirements are listed in Table 16.

The PHA table shows that the identified hazards have been mitigated by appropriate safety requirements. The hazards defined in the PHA will be tracked to full system requirements and test evidence form the project hazard log. Requirements in the project hazard log that correspond to the PHA can be tracked through the source attribute ID in the project hazard log.

Several PHA's have been documented with final risk assessments as IC which is unacceptable because the final mitigation is operating procedures to be agreed with the railroad. The acceptability of these operating procedures to protect these hazards can only be determined once the procedures are agreed.

Long Island Rail Road
ACSES II
Operating & Maintenance Manual (O&MM)

Docket Number FRA-2010-0031

Date: March, 2019

Rev 1.0

Submitted in fulfillment of 49 CFR Part 236, Subpart I, §236.1015, et.al.

REVISION HISTORY

Date	Revision	Description	Author
Jan 31, 2019	0.1	Initial Draft Creation	W. Alston
Feb 2019	0.2	Updates based on LIRR inputs	AECOM
March 29, 2019	1.0	Updates based on LIRR inputs	AECOM

Table of Contents

1 Introduction 1-1

1.1 Executive Summary 1-1
1.2 Scope 1-1
1.3 LIRR Operation Overview 1-2
1.4 ACSES II System Overview 1-4
1.4.1 Description of LIRR Territory 1-5
1.4.2 LIRR Operational Statistics 1-6
1.5 Document Overview 1-10
1.6 LIRR System-Level O&MM Submission History 1-12
1.7 Update of This Document 1-12
1.8 Acronyms and Definitions 1-12
1.9 Reference Documents 1-1

2 LIRR PTC System Implementation [§236.1005(a), §236.1005(f), §236.1015(d)] 2-1

2.1 LIRR Operating Environment 2-1
2.2 Information Required For PTCDP Under §236.1013(a) 2-2
2.2.1 Incorporate PTCDP by Reference 2-3
2.2.2 Final Human Factors Assessment 2-3
2.3 LIRR PTC System Implementation 2-3
2.3.1 LIRR PTC Implementation Plan (PTCIP) 2-3
2.3.2 LIRR-Specific PTC System Functions Implementation, If Any 2-4
2.4 PTC Architecture and Support for Interoperability 2-5
2.4.1 Office Subsystem 2-7
2.4.2 Onboard Subsystem 2-12
2.4.3 Wayside Subsystem 2-17
2.4.4 Roadway Worker Protection System (RWPS) 2-21
2.4.5 Support for Interoperability 2-22
2.5 System Users 2-23
2.5.1 Train Dispatchers 2-23
2.5.2 Chief Train Dispatchers or Train Dispatcher Supervisory Personnel 2-23
2.5.3 Train Engineers 2-24
2.5.4 Signal Installers and Maintainers 2-25
2.5.5 Maintenance of Equipment Personnel 2-25
2.5.6 Maintenance of Way Personnel 2-26
2.5.7 Department of Program Management Track 2-26
2.5.8 Maintenance Roles and Responsibilities 2-27
2.5.9 New Rolling Stock and Infrastructure changes 2-28
2.5.10 FRACAS 2-28

3 LIRR Maintenance Concept 3-1

3.1 Training 3-1
3.2 Configuration Management 3-5

4 LIRR ACSES II PTC System Level Troubleshooting 4-6

5 Procedures, Test Equipment, And Operations And Maintenance Manual [§236.1015(d)(7) and §236.1039, Appendix C (b)(7)] 5-1

5.1 Operations and Maintenance Procedures and Documentation 5-1
5.1.1 Test and Maintenance Equipment 5-1

5.1.2 Data Storage and retrieval (DMS and NMS) 5-3
5.2 O&MM Document Access and Control 5-4
5.3 Change Control of O&MM Documents 5-4

6 Warnings and Warning Labels [§236.1015(d)(8)] 6-1

6.1 Warnings Documented in Operations & Maintenance Manuals 6-1
6.2 Warning Labels 6-1

7 Safety Critical Components 7-1

8 Appendix A : Maintenance of Equipment (MoE) 8-2

8.1 Primary Hardware Components and Interfaces 8-2
8.1.1 Onboard Maintenance Manuals 8-4
8.2 Periodic Maintenance and Testing 8-4
8.2.1 Periodic Tests 8-4
8.3 Troubleshooting and Issue Resolution 8-5
8.3.1 General Steps and Tools 8-5
8.3.2 Remote and Bench Diagnostics Options 8-6
8.3.3 Onboard Personnel Responsibilities 8-6

9 Appendix B : Signals 9-7

9.1 Wayside - Signals 9-7
9.1.1 ACSES Wayside Hardware Components and Interfaces 9-7
9.1.2 Periodic Maintenance and Testing 9-8
9.1.3 Troubleshooting and Issue Resolution 9-9
9.2 Office - Signals 9-9
9.2.1 ACSES Office Hardware Components and Interfaces 9-9
9.2.2 Periodic Maintenance 9-11
9.2.3 Troubleshooting and Issue Resolution 9-12
9.3 RWPS – Signals 9-12
9.3.1 RWPS Hardware Components and Interfaces 9-12
9.3.2 Periodic Maintenance 9-14
9.3.3 Troubleshooting and Issue Resolution 9-15
9.4 SDMF 9-15
9.4.1 ACSES SDMF Hardware Components and Interfaces 9-15
9.4.2 SDMF Personnel Responsibilities 9-16
9.4.3 Periodic Maintenance 9-17

10 Appendix C : Communication 10-1

10.1 Wayside Communications 10-1
10.1.1 ACSES Wayside Hardware Components and Interfaces 10-1
10.1.2 Periodic Maintenance and Testing 10-2
10.1.3 Troubleshooting and Issue Resolution 10-3
10.2 Office Communications 10-4
10.2.1 ACSES Office Hardware Components and Interfaces 10-4

11 Appendix D. Maintaining ACSES Database 11-5

12 Appendix E. Maintenance Scenarios 12-1

List of Tables

TABLE 1-1: ABS AND CMB TERRITORIES ON LIRR 1-6
TABLE 1-2: TABULATION OF ROLLING STOCK TO EQUIP WITH ACSES 1-7
TABLE 1-3: 49 CFR PART 236, SUBPART I CROSS-REFERENCE TO O&MM 1-11
TABLE 1-4: SYSTEM-LEVEL O&MM SUBMISSION HISTORY 1-12
TABLE 1-5: ACRONYM LIST 1-12
TABLE 1-6: DEFINITION LIST 1-16
TABLE 1-7: REFERENCE DOCUMENTS 1-1
TABLE 2-1: PTC MAINTENANCE ROLES AND RESPONSIBILITIES 2-27
TABLE 2-2: ACSES CHANGES FOR MODIFIED INFRASTRUCTURE 2-28
TABLE 3-1: LIRR PTC TRAINING COURSES 3-2
TABLE 5-1: PTC MAINTENANCE TOOLS AND FUNCTIONS 5-1
TABLE 5-2: MAINTENANCE TOOLS FOR PTC SUBSYSTEMS 5-3
TABLE 6-1: ADDITIONAL WARNINGS IN OPERATION AND MAINTENANCE MANUAL 6-1
TABLE 6-2: ADDITIONAL WARNING LABELS ON EQUIPMENT 6-1
TABLE 7-1: PTC SAFETY CRITICAL COMPONENTS 7-1
TABLE 8-1: ONBOARD ACSES EQUIPMENT 8-3
TABLE 8-2: ONBOARD MAINTENANCE MANUALS 8-4
TABLE 8-3 : ONBOARD ACSES EQUIPMENT DEPARTURE TEST PROCEDURES 8-5
TABLE 9-1: ACSES WAYSIDE EQUIPMENT LIST 9-7
TABLE 9-2: WAYSIDE MAINTENANCE MANUALS 9-8
TABLE 9-3: OFFICE HARDWARE COMPONENTS 9-9
TABLE 9-4: OFFICE SUBSYSTEM MAINTENANCE MANUALS 9-10
TABLE 9-5: RWPS HARDWARE COMPONENTS 9-13
TABLE 9-6: RWPS SUBSYSTEM MAINTENANCE MANUALS 9-14
TABLE 9-7: SDMF COMPONENTS 9-15
TABLE 9-8: SDMF MAINTENANCE MANUALS 9-16
TABLE 9-9: SDMF PERSONNEL RESPONSIBILITIES 9-16
TABLE 10-1: WAYSIDE COMMUNICATIONS COMPONENTS 10-1
TABLE 10-2: COMMUNICATIONS MANUALS 10-2

List of Figures

FIGURE 1-1: INTRODUCTORY OVERVIEW OF ASCES II 1-4
FIGURE 1-2: MAP OF LIRR TERRITORY SHOWING SIGNALING TYPES IN PLACE PRIOR TO ADDING PTC 1-8
FIGURE 1-3: MAP OF LIRR TERRITORY AND 11 BRANCHES 1-9
FIGURE 2-1: ACSES SYSTEM BLOCK DIAGRAM LEVEL 0 2-1
FIGURE 2-2: OFFICE SUBSYSTEM CONTEXT DIAGRAM 2-2
FIGURE 2-3: ONBOARD SUBSYSTEM CONTEXT DIAGRAM 2-3
FIGURE 2-4: WAYSIDE SUBSYSTEM CONTEXT DIAGRAM 2-4
FIGURE 2-5: COMMUNICATION SUBSYSTEM CONTEXT DIAGRAM 2-5
FIGURE 2-6: ACSES II PTC BLOCK DIAGRAM FOR ABS TERRITORY 2-6
FIGURE 2-7: ACSES II PTC BLOCK DIAGRAM FOR CMB TERRITORY 2-6
FIGURE 2-3: FRACAS PROCESS MAP 2-29
FIGURE 4-1: LIRR ASCES TROUBLESHOOTING FLOW CHART 4-6
FIGURE 4-2: LIRR ASCES II PTC SYSTEM TROUBLESHOOTING TOP LEVEL 4-8
FIGURE 5-1: MAXIMO WORKFLOW PROCESS 5-4
FIGURE 12-1: EN ROUTE FAILURE RESPONSE SEQUENCE DIAGRAM 12-5

1 Introduction

1.1 Executive Summary

This document is the Long Island Rail Road (LIRR) System-Level Operating and Maintenance Manual (O&MM) for the LIRR deployment of the Advanced Civil Speed Enforcement System (ACSES II), which is designed as a vital overlay PTC system as defined in 49CFR §236.1015 (e)(2).

The LIRR is implementing PTC using the Type Approved ACSES II system (FRA-TA-2010-001) as a vital overlay to its vital cab signaling with Automatic Train Control (ATC) signaling, and on lines without cab signaling, as a vital overlay to its Part 236 compliant non-cab-signaled Automatic Block Signaling (ABS), its non-cab-signaled Controlled Manual Block (CMB) signaling (as Type Approved in the LIRR PTC Development Plan (PTCDP)). The Type Approved ACSES II system added to both ASC and Non-ASC territory is modified to add functionality suitable to the complexity of the LIRR operation

The purpose of the maintenance concepts document is to provide a summary overview of the ACSES maintenance functions in order for Long Island Rail Road (LIRR) to establish how its maintenance staff maintains the ACSES PTC equipment by department and individual areas.

Overall goals for LIRR PTC O&MM include:

- Defining the maintenance elements of the ACSES system.
- Allocating maintenance responsibilities to affected LIRR departments.
- Compliance with FRA regulations and LIRR Engineering and MoE Departmental Standards.
- Integration of the ACSES maintenance elements into the existing practices and intervals to the extent practical.

1.2 Scope

This O&MM provides an overview of the elements for maintenance of the four main ACSES subsystems and their interfaces to each other and to existing LIRR signaling, communications, and onboard systems:

- Onboard
- Wayside
- Communications
- Office (including RWPS)

The document also gives an overview to the post-installation periodic maintenance, troubleshooting, and system modification to reflect changes in the LIRR infrastructure of the ACSES system components. It covers organization and configuration management Maintenance manuals and training programs are included by reference. The document does not include original installation checkout and site performance testing being undertaken as part of the LIRR PTC Program under direction of the PTC System Integrator.

The document does not include the existing LIRR maintenance processes and procedures for existing systems including the signaling, communications, and onboard systems ACSES interfaces to. It also does not include the Maximo activities of MoE which is incorporating ACSES onboard systems.

The following departments are allocated ACSES PTC maintenance responsibilities:

1. Maintenance of Equipment (M of E)
    a. Shop Electricians
    b. Equipment Engineering
    c. Central Control
2. Engineering
    a. Communications (including CNOC)
    b. Signals (including Signal Trouble desk)

For each PTC subsystem covered in this System-Level O&MM, the following information is addressed as appropriate to the LIRR maintenance philosophy for PTC system components:

1. Installation – All equipment is installed per supplier directions and drawings.
2. Maintenance – Maintenance is performed to the LRU level on a swap-out basis.
3. Repairs – Repairs, as necessary are performed by the supplier for the warranty period and the foreseeable future under contract using internal documentation.
4. Modifications – Modifications needed for safe operation are performed by the supplier using internal documentation.
5. Inspection – Inspection are performed by trained LIRR staff in the field. Inspections of unit assemblies and segments are performed by the supplier in the factory.
6. Testing – Testing of LRUs and subassemblies is performed by the supplier. System testing and regression functional/safety testing is performed as per the Master Test Strategy, as shown in the Appendix to the PTCSP.

In summary, this O&MM covers the installation, use, and basic troubleshooting of the LIRR ACSES II PTC system for the purpose of isolating failed equipment so that it can be exchanged with proper functioning equipment on a swap-out basis. This System-Level O&MM is intended to provide an over-arching view of the existing Operations and Maintenance Manuals pertinent to the ACSES II System, but not act as a replacement for the subsystem level operations manuals supplied by the SI and the individual subsystem suppliers. Refer to **Figure 1-1** for a general block diagram of the PTC system.

1.3 LIRR Operation Overview

The LIRR service territory includes the following types of FRA-compliant vital signaling:

- Cab signaling with Automatic Train Control (referred to as Automatic Speed Control [ASC]). This territory has both cab signal with wayside intermediate signals and cab signaling without intermediate wayside signals. LIRR's primary underlying signal system is a vital ATC system operated through distributed supervisory control using a series of Master Dispatching Towers.

- Non-cab signaled Automatic Block Signal (ABS) signaling with wayside signals-only. This territory has continuous vital track circuit and hand operated switch indication control of all signal aspects.
- Non-cab signaled Controlled Manual Block (CMB) signaling with continuous vital track circuit and hand-operated switch indication control of Manual Block Signal aspects.
- Non-signaled segment between Ronkonkoma and Greenport, where operations within the proposed Mainline Track Exclusion Addendum (MTEA).
- Limited Operations Exception (LOE) limits are currently conducted under LIRR's Manual Block Signal System rules.

LIRR trains are operated by a one-person crew in the cab of locomotives, MU units, and cab cars. The train conductor is physically located in the passenger coaches of the trains. As outlined in 49CFR §236 Appendix C, vital overlay PTC systems must show that the PTC system fulfills the safety assurance principles which includes:

- System Safety under Normal Operating Conditions;
- System Safety under Failures;
- Closed-Loop Principle;
- Safety Assurance Concepts;
- Human Factors Engineering Principle;
- System Safety under External Influences; and,
- System Safety after Modification.

The ACSES II PTC System has specific segments which provide vital functions, as listed below:

1. Onboard Segment – Vital;
2. Wayside Segment – Vital;
3. Transponders – Vital data processed by Vital Onboard Reader Device; and,
4. Safety TSR Server (STS) Segment – Vital.

These segments are specifically described and their contributions to preventing the hazards stated in the FRA regulation §236.1005 (previously outlined in section 1.1) are identified as part of the Hazard Analysis. The LIRR ACSES II PTC system also includes subsystems which are not required to perform vital functions, and as such can be considered non-vital. These are listed below:

5. Office System (other than STS);
6. Onboard Aspect Display Unit (display and input functions);
7. Communications Segment; and
8. RWPS.

1.4 ACSES II System Overview

The LIRR Railroad PTC System is based on the Amtrak Advanced Civil Speed Enforcement System (ACSES), and consists of a wayside Cab Signaling System (CSS) with a vehicle-installed Automatic Train Control (ATC) system supplemented with a vital microprocessor-based ACSES system providing several enforcement functions as required for PTC.

The ACSES II PTC System provides for enforcement of Permanent Speed Restrictions (PSR), Temporary Speed Restrictions (TSR), enforcement of Positive Train Stop under Stop Signal aspects at interlocking Home Signal (HS) locations, Positive Train Stop enforcement at malfunctioning grade crossings, and protection against train incursion into track work zones. An introductory overview of the ACSES II system is presented below.

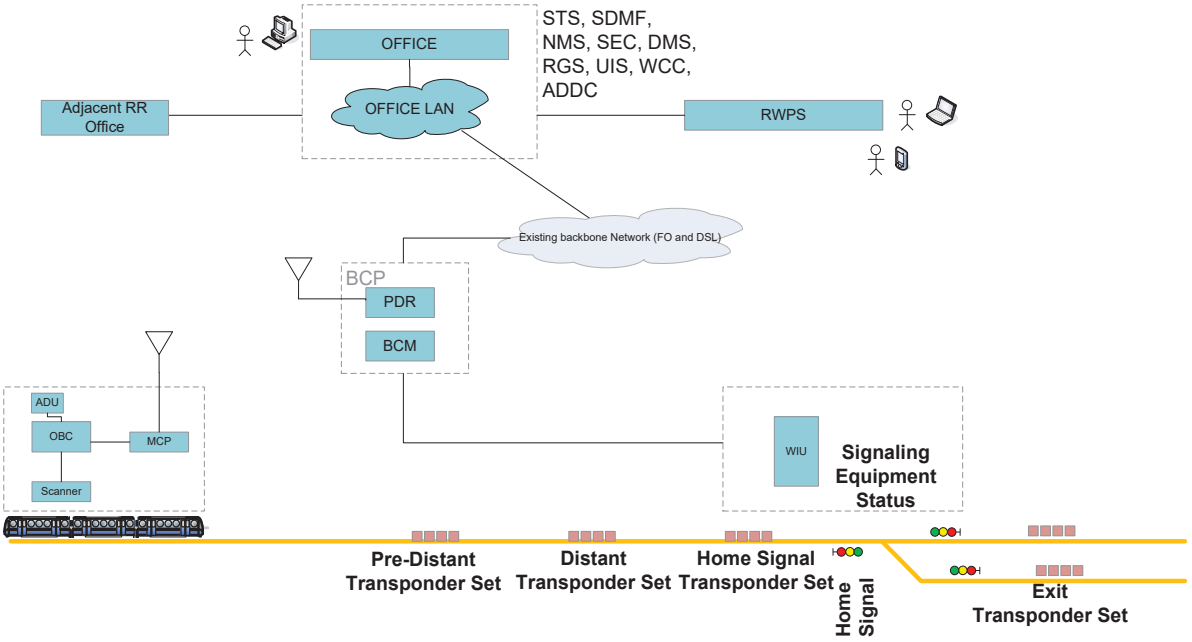


Figure 1-1: Introductory Overview of ASCES II

The ACSES II PTC System is a distance-based positioning system, which establishes incremental vehicle position (as well as other data) from track-mounted transponder sets as the vehicle-mounted scanner antenna passes over them. In between transponder sets, the vehicle positioning is ascertained by counting speed pulses from the speed sensor. Any accumulated distance error is reset when the train encounters the next transponder set. As well, wheel slip/slide compensation errors are also adjusted en route. The PTC System uses the vehicle positioning information to calculate safe braking curves, train speed, and distance travelled with a high level of accuracy.

The ACSES II PTC System, along with all PTC systems required to be installed under 49 CFR Part 236 Subpart I, fulfills the requirements established by §236.1005(a) as it has been designed to:

1. Reliably and functionally prevent:
   a. Train-to-train collisions.

b. Overspeed derailments, including derailments related to railroad civil engineering speed restrictions, slow orders, and excessive speeds over switches and through turnouts.

c. Incursions into established work zone limits without first receiving appropriate authority and verification from the dispatcher or roadway worker in charge, as applicable and in accordance with Part 214.

d. Movement of a train through a main line switch in the improper position, as further described in paragraph (e) of 49 CFR Part 236, Subpart I, §236.1005.

2. Include safety-critical integration of all authorities and indications of a wayside or cab signal system, or other similar appliance, method, device, or system of equivalent safety, in a manner by which the PTC system provides associated warning and enforcement to the extent, and except as, described and justified in the present PTC Safety Plan or in the associated Type Approval FRA-TA-2010-001 (dated May 27, 2010).

3. Provide an appropriate warning or enforcement when:

a. A derail or switch protecting access to the main line required by 49 CFR Part 236, Subpart I, §236.1007, or otherwise provided for in the applicable PTCSP, is not in its derailing or protecting position, respectively;

b. A mandatory directive is issued associated with a highway-rail grade crossing warning system malfunction as required by §§234.105, 234.106, or 234.107;

c. An after-arrival mandatory directive has been issued and the train or trains to be waited on has not yet passed the location of the receiving train;

d. Any movable bridge within the route ahead is not in a position to allow permissive indication for a train movement pursuant to §236.312; such as for the Wreck Lead Bridge, and

e. A hazard detector integrated into the PTC system that is required by§236.1005(c), or otherwise provided for in this applicable PTCSP, detects an unsafe condition or transmits an alarm.

4. Limit the speed of passenger and freight trains in CMB territory to 59 miles per hour in areas without broken rail detection or equivalent safeguards.

1.4.1 Description of LIRR Territory

The LIRR includes the following types of FRA compliant signaling as covered by the PTCSP and as illustrated on the map in **Figure 1-2**:

- Cab signaling with Automatic Train Control (referred to as Automatic Speed Control [ASC]). This territory has both cab signal with wayside intermediate signals and cab signaling without intermediate wayside signals.
- Non-cab signaled Automatic Block Signal (ABS) signaling with wayside signals-only. This territory has continuous vital track circuit and hand operated switch indication control of all signal aspects.

- Non-cab signaled Controlled Manual Block (CMB) signaling with continuous vital track circuit and hand operated switch indication control of Manual Block Signal aspects.

1.4.2 LIRR Operational Statistics

The Long Island Rail Road system has eleven (11) passenger branches as shown on the map in **Figure 1-3**.

1. Port Washington Branch
2. Oyster Bay Branch
3. Port Jefferson Branch
4. Ronkonkoma Branch
5. Montauk Branch
6. Babylon Branch
7. West Hempstead Branch
8. Hempstead Branch
9. Long Beach Branch
10. Far Rockaway Branch
11. City Terminal Zone

The Railroad's non-cab-signaled ABS and CMB wayside signal system territories are located on the following line segments and branches, as shown on Error! Reference source not found.:





Figure 1-2: MAP OF LIRR TERRITORY SHOWING SIGNALING TYPES IN PLACE PRIOR TO ADDING PTC



Figure 1-3: Map of LIRR Territory and 11 Branches

1.5 Document Overview

This document consists of seven (7) main sections and multiple appendices containing documents that are referenced by the various main sections to support the analysis herein. The Appendices provide additional explanatory information required in order to fully demonstrate the LIRR PTC System's repair, maintenance, service, and operation.

As noted in a prior section, the ACSES II PTC System has specific segments which provide vital functions, as listed below:

1. Onboard Segment – Vital;
2. Wayside Segment – Vital;
3. Transponders – Vital data processed by Vital Onboard Reader Device; and,
4. Safety TSR Server (STS) Segment – Vital.

These segments are specifically described and their contributions to preventing the hazards stated in the FRA regulation §236.1005 (previously outlined in section 1.1) are identified as part of the Hazard Analysis. The LIRR ACSES II PTC system also includes subsystems which are not required to perform vital functions, and as such can be considered non-vital. These are listed below:

5. Office System (other than STS);
6. Onboard Aspect Display Unit (display and input functions);
7. Communications Segment; and
8. RWPS.

As the correlation between this O&MM document and the clauses in 49 CFR Part 236, Subpart I is not always one-to-one, a cross-reference between the applicable Subpart I requirement and the O&MM Section or subsection is provided in **Table 1-3** below.

Any change(s) to the ACSES II PTC system, or its PTCIP, or PTCSP (this document) will only be made if LIRR files an RFA with the FRA to obtain authorization for the change(s), and then satisfactorily completes the changes.

Table 1-3: 49 CFR Part 236, Subpart I Cross-Reference to O&MM

Regulatory Reference	Summary of Regulatory Requirements	Description of Regulatory Requirement	PTCSP Section/Chapter Reference
§236.1015(d)(7)	*Test procedures for equipment installs, repair, operations, etc…*	*A complete description of the specific procedures and test equipment necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the PTC system on the railroad and establish safety-critical hazards are appropriately mitigated. These procedures, including calibration requirements, shall be consistent with or explain deviations from the equipment manufacturer's recommendations.*	***Section 15***
§236.1015(d)(8)	*Additional Warnings*	*A complete description of each warning to be placed in the Operations and Maintenance Manual identified in §236.919, and of all warning labels required to be placed on equipment as necessary to ensure safety.*	***Section 16***
§236.1039(c)	*Operations and maintenance manual for hardware and software handling*	*Hardware software and firmware revisions must be documented …according to the railroad's configuration management control plan and any additional …measures specified in the PTCDP and PTCSP*	***Section 15***
§236.1039(d)	*Operations and Maintenance Manual (O&MM) for safety critical components*	*Safety critical components …handled… in accordance with the procedures specified in the PTCDP and PTCSP*	***Section 15***

1.6 LIRR System-Level O&MM Submission History

Table 1-4 provides the submission history of the PTCSP by LIRR to the FRA. The LIRR PTCSP has been developed using input and insight from a variety of industry-standard sources and with input from FRA. As is typical, draft material has been shared with FRA to expedite discussion and final PTCSP review. All changes resulting from the resolution of comments on prior drafts to the FRA have been incorporated in this version of the PTCSP.

Table 1-4: System-Level O&MM Submission History

Submittal #	Date	Document Name	Version #
1	03/29/19	Long Island Rail Road (LIRR) System-Level Operation and Maintenance Manual (O&MM)	LIRR 1.0

1.7 Update of This Document

This O&MM will be updated only in accordance with the LIRR Configuration Management Plan.

1.8 Acronyms and Definitions

This section, via **Table 1-5** and **Table 1-6**, includes definitions of all terms, abbreviations, and acronyms used to properly interpret the PTCSP, and any associated documents, such as this one. The general dictionary of terms and acronyms for PTC is found in project document ID (PMD) 3035624.

Table 1-5: Acronym List

Acronym	Meaning
2oo3	2 out of 3
AAR	Association of American Railroads
ABS	Automatic Block Signaling
ACSES	Advanced Civil Speed Enforcement System
ADDC	Active Directory Domain Controller
ADU	ACSES II Display Unit
AIU	ATC Interface Unit
APT	ACSES II Programming Tool
APTA	American Public Transit Association
AREMA	American Railway Engineering and Maintenance-of-Way Association
ASB	Absolute Stop Bypass
ASC	Automatic Speed Control
ATC	Automatic Train Control
ATCS	Advanced Train Control System
BCM	Base Communications Manager

Table 1-5: Acronym List

Acronym	Meaning
BCP	Base Communication Package
BRCM	Base Radio Communications Manager
CCB	Change Control Board
CIL	Certifiable Items List
CDR	Conceptual Design Review
CDRL	Contract Delivery Requirements List
CFR	Code of Federal Regulations
CI	Configuration Item
CIL	Certifiable Items List
CLS	Clear Line Speed
CM	Configuration Management
CMB	Controlled Manual Block
CMP	Configuration Management Plan
CMS	Configuration Management System
COTS	Commercial Off The Shelf
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CSS	Cab Signal System
CTC	Centralized Traffic Control
CTV	Decoding Module
DC&G	Displays Conventions and Guidelines
DMS	Data and Maintenance System
DOORS	Dynamic Object-Oriented Requirements System
DS	Distant Signal (transponder)
DSI	Distant Switch Indicator
DT	Development Test
EF	Enhanced Functionality
EMU	Electric Multiple Unit
EN	European Norm
ESA	East Side Access
FDB	Fixed Database
FDR	Final Design Review
FFT	Functional Fault Tree
FMECA	Failure Mode, Effects, and Criticality Analysis
FPT	Functional Performance Test
FRA	Federal Railroad Administration
FRACAS	Failure Reporting And Corrective Action System
FRM	Failure Report Matrix
FTA	Federal Transit Administration
FTA	Fault Tree Analysis

Table 1-5: Acronym List

Acronym	Meaning
GBN	Ground Based Network
HF	Human Factor
HFA	Human Factor Analysis
HL	Hazard Log
HMI	Human Machine Interface
HRI	Hazard Risk Index
HS	Home Signal
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IHA	Interface Hazard Analysis
I/O	Input Output
ISR	Interlocking Status Requests
IP	Internet Protocol
JCC	Jamaica Central Control
LAN	Local Area Network
LIRR	Long Island Rail Road
LOE	Limited Operations Exception
LoMA	Limit of Movement Authority
MAS	Maximum Authorized Speed
MBS	Manual Block System
MCM	Mobile Communications Manager
MHz	Megahertz
MNR	Metro North Railroad
MP	Manual Part
MPH	Miles Per Hour
MoE	Maintenance of Equipment
MoW	Maintenance of Wayside
MTA	Metropolitan Transportation Authority
MTBF	Mean Time Between Failure
MTEA	Mainline Track Exclusion Addendum
MTTF	Mean Time To Failure
MTTHE	Mean Time To Hazardous Event
MTTR	Mean Time To Repair
N/A	Not Applicable
NEC	Northeast Corridor
NMS	Network Management System
NPI	Notice of Product Intent
NS	Network Server
NYAR	New York and Atlantic Railroad
OHA	Operational Hazard Analysis

Table 1-5: Acronym List

Acronym	Meaning
OBC	Onboard Computer
OC	Optical Carrier
OT	Operational Test
PDR	PTC Data Radio
PDS	Pre-Distant Signal (Transponder)
PHA	Preliminary Hazard Analysis
PIH	Poison by Inhalation Hazard
PLG	Product Line Guardian
PM	Project Management
PMT	Program Management Team
PrDR	Preliminary Design Review
PSP	Product Safety Plan
PSR	Permanent Speed Restriction
PTC	Positive Train Control
PTE	Passenger Terminal Exception
PTCDP	Positive Train Control Development Plan
PTCIP	Positive Train Control Implementation Plan
PTCSP	Positive Train Control Safety Plan
PTCPVL	Positive Train Control Product Vendor List
PTS	Positive Train Stop
PTSO	Positive Train Stop Override
PVI	Product Version Information
QA	Quality Assurance
RAM	Reliability, Availability, and Maintainability
RAMS	Reliability, Availability, Maintainability, and Safety
RFA	Request For Amendment
RFP	Request For Proposal
RGC	Road Grade Crossing
ROD	Rules of the Operating Department
ROP	Rules of the Operating Department
ROW	Right-of-Way
RTM	Requirement Traceability Matrix
RWPS	Roadway Worker Protection System
SAC	Safety Assurance Concepts
SCIL	Safety Critical Items List
SDC	Software and Database Custodian
SDMF	Software and Data Maintenance Facility
SHA	System Hazard Analysis
SI	Systems Integrator
SIL	Safety Integrity Level

Table 1-5: Acronym List

Acronym	Meaning
SLR	System Level Requirement
SMS	Safety Management System
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SOP	Standard Operating Procedures
SQL	Structured Query Language
SRPB	Stop Release Push Button
SSCB	System Safety Certification Board
SSHA	Subsystem Hazard Analysis
SSLR	Subsystem Level Requirement
SSP	System Safety Program
STS	Safety TSR Server
T&E	Test and Evaluation
TA	Type Approved Functionality
TAV	Type Approval Variance (from PTCDP)
TDMA	Time Division Multiple Access
TIH	Toxic Inhalation Hazard
TM	Type Modified Functionality
TP	Transponder
TRM	Radio Transmission Module
TSR	Temporary Speed Restriction
TT&TO	Timetable and Train Order
TTSI	Timetable Special Instruction
UCS	Central Sequencing Unit
UIS	User Interface Server
USB	Universal Serial Bus
U.S.C.	United States Code
V&V	Verification and Validation
VSL	Vital Signal Logic
WCC	Wayside Communication Controller
WIU	Wayside Interface Unit
WOS	Work Order System

Table 1-6: Definition List

Term	Definition
Class I Railroad	A railroad which in the last year for which revenues were reported exceeded the threshold established under regulations of the Surface Transportation Board (49 CFR part 1201.1-1 (2008)).

Table 1-6: Definition List

Term	Definition
Closed Loop Principle	System design adhering to the closed loop principle requires that all conditions necessary for the existence of any permissive state or action be verified to be present before the permissive state or action can be initiated. Likewise, the requisite conditions shall be verified to be continuously present for the permissive state or action to be maintained. This is in contrast to allowing a permissive state or action to be initiated or maintained in the absence of detected failures. In addition, closed loop design requires that failure to perform a logical operation, or absence of a logical input, output or decision shall not cause an unsafe condition, i.e. system safety does not depend upon the occurrence of an action or logical decision.
Fail-Safe	A design philosophy applied to safety-critical systems such that the results of hardware failures or the effect of software error either shall prohibit the system from assuming or maintaining an unsafe state or shall cause the system to assume a state known to be safe. (IEEE-1483)
Fault Tree Analysis (FTA)	A structured analysis method used to comprehensively identify faults and combinations of faults of software and hardware components as they relate to a hazard using diagrammatic techniques.
Hazard	An existing or potential condition that can result in an accident.
Hazardous Event	An occurrence that creates a hazard. A hazardous event is one which is likely to lead directly or indirectly to a hazard occurring, e.g., if the accident is train collision, the hazard may be a false clear signal and one of the hazardous events may be a track circuit relay stuck in an energized position.
Host Railroad	A railroad that has effective operating control over a segment of track.
Interoperability	The ability of a controlling locomotive to communicate with and respond to the PTC railroad's PTC system, including uninterrupted movements over property boundaries.
Limited Operations Exception	A Limited Operations Exception (LOE) is an identification of territory complying with the requirements of 49 CFR 236.1019(c)(1), describing tracks which are excluded from the requirement for a PTC system where scheduled rail passenger service is provided, and which must be included in the Mainline Track Exclusion Addendum contained in a railroad's PTC Implementation Plan (PTCIP). For any such track, an exception will only be valid when it is identified in an MTEA that is part of an FRA approved PTCIP. LIRR's MTEA-LOEs are provided in Section 13 its PTCIP.

Table 1-6: Definition List

Term	Definition
Mainline	Except as excepted pursuant to §236.1019 or where all trains are limited to restricted speed, a segment or route of railroad tracks, including controlled sidings: of a Class I railroad, as documented in current timetables filed by the Class I railroad with the FRA under § 217.7, over which 5,000,000 or more gross tons of railroad traffic is transported annually, as reported on the traffic density map required to be filed with the Surface Transportation Board; or Used for regularly scheduled intercity or commuter passenger service, as defined in 49 U.S.C. § 24102, or both.
Mainline Track Exclusion Addendum	The document further described in §236.1019.
Mean Time Between Hazardous Event (MTBHE)	The average or expected time of operation of a subsystem or component between occurrences of a hazardous event.
Mean Time to Hazardous Event (MTTHE)	The average or expected time that a subsystem or component will operate prior to the occurrence of a hazardous event.
Mitigation	Method or technique used to reduce the risk of a hazard.
Non-Safety Related Classification	A classification of a product that has no safety implications.
NPI	Notice of Product Intent as further described in §236.1013.
Operating Hazard Analysis (OHA)	An analysis of the potential hazards at human-machine interfaces involved in the operation, testing, and servicing of the system.
Passenger Terminal Exception	Per PTCIP Section 13.1, 49 CFR 236.1019(b) for the passenger-train-only trackage – maximum authorized speed is not greater than 20-MPH, the maximum speed is enforced by the PTC system, interlocking rules are in effect, and no freight-train operations are permitted.
PIH	Materials poisonous by inhalation, as defined in §§ 171.8, 173.115, and 173.132.
Preliminary Hazard Analysis (PHA)	An analysis performed on the potential hazards identified in the PHL, to provide an initial risk assessment of the hazards, and to identify requisite controls and follow-on actions.
Product	A train control system, subsystem, or component. Or An element of the physical or system architecture, specification tree, or system breakdown structure that is a subordinate element to the system or subsystem and which is wholly documented in a separate way, and considered as a terminal branch of the specification tree.

Table 1-6: Definition List

Term	Definition
Project Hazard Log (PHL)	An analysis that determines how system operation and failure modes can affect the safety of the system and its subsystems. Note: Specifically, the PHL examines all subsystem interfaces and interfaces with other systems for: 1. Compliance with safety criteria called out in the applicable system/subsystem requirements documents. 2. Possible combinations of independent or dependent failures that can cause hazards to the system or personnel. Failures of controls and safety devices should be considered. 3. How normal operations of systems and subsystems can degrade the safety of the system. 4. How design changes to system, subsystems, or interfaces, logic, and software can create new hazards to equipment and personnel.
PTC	Positive Train Control as further described in §236.1005.
PTC Railroad	Each Class I railroad and each entity providing regularly scheduled intercity or commuter rail passenger transportation required to implement and operate a PTC system.
PTC System Certification	Certification as required under 49 U.S.C. § 20157 and further described in §§236.1009 and 236.1015.
PTCDP	PTC Development Plan as further described in §236.1013.
PTCIP	PTC Implementation Plan as required under 49 U.S.C. 20157 and further described in §236.1011.
PTCSP	PTC Safety Plan as required under 49 U.S.C. § 20157 and further described in §236.1015.
PTVPVL	PTC Product Vendor List as further described in §236.1023.
Qualitative Evidence of Safety	The evidence provided by the application of the safety assurance methodology, often stated in terms of a Mean Time To Hazardous Events (MTTHE) or Mean Time Between Hazardous Events (MTBHE), that hazards are eliminated or controlled to an acceptable level. The norms for acceptability are usually based upon MIL-STD-882C **Error! Reference source not found.**, or similar documents.
Request For Amendment	A request for an amendment of a plan or system made by a PTC railroad in accordance with §236.1021.
Review	The assessment of a work product's content to verify adherence to defined standards, guidelines, specifications and procedures.
Risk	An expression combining the probability of the accident occurring with the severity of the consequences of the accident, used to rank hazards.

Table 1-6: Definition List

Term	Definition
Risk Assessment	The process of determining the amount of risk associated with use of the product under all intended and anticipated operating conditions. Risk assessment techniques for any product may include qualitative, semi-quantitative and quantitative approaches.
Safety Critical	Safety-critical, as applied to a function, a system, or any portion thereof, means the correct performance of which is essential to safety of personnel or equipment, or both; or the incorrect performance of which could cause a hazardous condition, or allow a hazardous condition which was intended to be prevented by the function or system to exist. A term applied to a system or function, the correct performance of which is critical to safety of personnel and/or equipment; also a term applied to a system or function, the incorrect performance of which may result in an unacceptable risk of a hazard.
Safety Life Cycle	The additional series of activities carried out in conjunction with the system life cycle for safety related systems.
Safety Validation	A structured and managed set of activities, including analysis and test, which show that the system, as specified and implemented, performs the intended functions and that those functions result in overall safe operation. *Validation* answers the question, "Did we build the right system?" (IEEE-1483)
Safety Verification	A structured and managed set of activities, including analysis and test, which show that the system, including its subsystems, interfaces and components, as designed and implemented, meets the allocated system safety goals and requirements. *Verification* answers the question, "Did we build the system right?" (IEEE-1483)
Safety-Critical Classification	A classification of products that have at least one hazard that can lead directly to an accident.
Safety-Related Classification	A classification of products which do not lead directly to an accident but which may significantly increase the overall risk of an accident.
Segment of Track	Any part of the railroad where a train operates. May also refer to specific "Branches" of the LIRR Territory, e.g., Montauk, Far Rockaway, et.al. The terms segment and branch is used interchangeably in this PTCSP.
Self-Revealing Component Failures	Component failures whose effects on system operation are immediately and clearly apparent to a properly trained person.
Subsystem Hazard Analysis (SSHA)	An analysis that looks at each subsystem or component and identifies hazards associated with operating or failure modes and is especially intended to determine how operation or failure of components affects the overall safety of the system.
System	A signal or train control system that includes all subsystems and components thereof, as the context requires.

Table 1-6: Definition List

Term	Definition
Tenant Railroad	A railroad, other than a host railroad, operating on track upon which a PTC system is required.
Track Segment	Segment of track
Vital	A function, system, subsystem, or device configured and applied in a safety-critical system such that the failure of the function, system, subsystem, or device to operate as intended shall not result in an unsafe state.
Vital Circuit	Any circuit and its elements, the function of which affects the safety of train operations. A vital circuit is one for which analysis and testing has proven that the circuit is fail-safe or that the probability of a single point failure resulting in an unsafe condition is 10 to the minus 9th power.
Vital Function	A function in a safety-critical system that is required to be implemented in a fail-safe manner. Note: Vital functions are a subset of safety-critical functions. (IEEE-1483)
Vital Software	Software that can directly or indirectly contribute to the occurrence of an unsafe state; vital software shall not result in an unsafe state under any failure. Software for which analysis and testing has proven that the software is fail-safe or that the probability of a single point failure resulting in an unsafe condition is 10 to the minus 9th power.

1.9 Reference Documents

This section provides a complete list of all the documents and other sources used in the preparation of or referenced in the PTCSP.

Table 1-7: Reference Documents

Reference Number	Document Name	Identification Number
1.	Configuration Management Plan	CDRL 2-13, 2-15, 2-17
2.	LIRR PTC Configuration Management Plan	DEL 0093
3.	Maintenance Plan	CDRL 2-110
4.	Maintenance Manuals	CDRL 2-36
5.	Maintainability Demonstration Test Plan (MDTP)	CDRL 2-143
6.	SDMF Design Document	CDRL 2-30
7.	Maintenance Database	CDRL 2-112
8.	Office Subsystem Description Document	CDRL 6-001 / 3035843
9.	Communications Subsystem Description Document	CDRL 7-001 / 3035865
10.	Onboard Subsystem Description Document	CDRL 5-001 / 3035902
11.	RWPS Subsystem Description Document	CDRL 2-201 / 3035851
12.	Railroad Operating Procedures	
13.	ACSES II Maintenance Plan	CDRL 2-110
14.	ACSES II Master Training Plan	CDRL 2-114
15.	Long Island Rail Road PTC Implementation Plan, latest approved edition	LIRR document
16.	LIRR PTC Security Management Plan	LIRR document

2 LIRR PTC System Implementation [§236.1005(a), §236.1005(f), §236.1015(d)]

Reference §236.1005(a): *Requirements for Positive Train Control systems and*

Reference §236.1015(d): *A PTCSP shall include the same information required for a PTCDP under §236.1013(a).*

Long Island Rail Road (LIRR) is implementing supplemental Positive Train Control (PTC) capabilities to their existing train control and signaling systems, as mandated by the Rail Safety Improvement Act of 2008. Advance Civil Speed Enforcement System (ACSES II), as a vital system overlay, is used to provide PTC capabilities to the following existing Railroad FRA compliant vital train control and signaling systems:

- Cab Signal System (CSS) with Automatic Train Control (ATC) (the combination of which is referred to as Automatic Speed Control [ASC] on the LIRR)
- Automatic Block Signaling (ABS) without cab signaling
- Controlled Manual Block (CMB) without cab signaling
- Manual Block System (MBS)

Note: Some MBS to include limited ACSES functionality (Temporary Speed Restrictions (TSR) and Permanent Speed Restrictions (PSR).

The Railroad's ACSES II System is compliant with all applicable FRA regulations including 49 CFR 236 subparts (inclusive of subpart I), standard practices, and equipment of LIRR. It incorporates the latest technologies; and provides for ACSES II interoperability with North East Corridor (NEC) ACSES II implementations.

(TSR) and Permanent Speed Restriction (PSR))

The ACSES II system provides protection from overspeed derailments through enforcement of MAS, PSRs and TSRs. This functionality is identical to, with no variance from, the "Type Approved" ACSES II PTC System in ASC territory, as described in the separate companion PTCSP. Maximum Authorized Speed for all of the LIRR ABS and CMB territories addressed in this PTCSP is currently 65 MPH or less (Passenger) and 45 MPH or less (Freight).

The following Sections provide additional details about the LIRR incorporation of ACSES II as defined in the referenced Type Approval into its existing operating environment and railroad infrastructure. In addition, Appendix 6-1 provides the detailed LIRR PTC System Description document and related addendums for specific LIRR PTC functions.

2.1 LIRR Operating Environment

Reference §236.1013(a)(3): *An operational concepts document, including a list with complete descriptions of all functions which the PTC system will perform to enhance or preserve safety;*

Reference §236.1013(d)(15): *A complete description of how the PTC system will enforce authorities and signal indications, unless already completely provided for in the PTCDP.*

LIRR PTC Operational Concepts Document is included in the approved PTCDP, as Attachment 1 in that document. The LIRR PTCDP for Non-Cab Territory is found in Appendix 5-1 to the PTCSP.

The LIRR PTC Operational Concepts Document includes the following:

- A complete description of how the PTC system enforces authorities and signal indications.
- A prioritized service restoration and mitigation plan and a description of the necessary security measures for the system.
- A description of any deviation in operational requirements for en route failures as specified under 49 CFR §236.1029.
- An emergency and planned maintenance temporary rerouting plan indicating how operations on the subject PTC system can take advantage of the benefits provided under 49 CFR §236.1005(g) through (k);

The LIRR PTC Operational Concepts Document contains a complete description of the way for the ACSES II to enforce authorities and signal indications in the proposed operation areas, which include ASC cab signaling, non-ASC ABS and CMB, and non-signaled MBS territories. In the ASC cab signaled territory, it is the same as Type Approved ACSES II; in non-cab signaled ABS and CMB territory, ACSES II enforces civil speed limits and Positive Train Stop (PTS) for all home, CMB and automatic wayside signals; in MBS territory, the operation is via MTEA-LOE with ACSES II enforced speed limits (including a 0 MPH TSR implemented by train type for enforcement of freight-passenger temporal separation).

A tenant railroad, freight service provider NYAR, operates in ASC cab signal territory, non-cab signaled ABS and CMB territory, and also in the MBS territory (operating temporally separated from LIRR revenue passenger trains in accordance with a MTEA-LOE, as described in LIRR PTCIP Section 13.14). Another tenant railroad, Amtrak, operates only over a short section of ASC cab signaled territory. Both of these tenant railroads have PTC-equipped all such trains with the same ACSES II functions and interfaces, which are fully compatible with LIRR's PTC system.

2.2 Information Required For PTCDP Under §236.1013(a)

The Amtrak ACSES II system, whose Type Approval FRA-TA-2010-001 (dated May 27, 2010) is on file at the FRA, has been referenced by LIRR in its PTCIP, in addition to issuing a PTCDP document for the use of ACSES II in non-cab-signal territory. Where the ACSES II PTC System does not duplicate the specific components and architecture described in the FRA Type Approval for ACSES II, FRA Type Approval Variance Documents covering all deviations from the specific ACSES II Type Approval (based on the changed or updated PTC function, design, or performance, including accommodation of interoperability) have been created and submitted to the FRA.

All details necessitated as per FRA 49 CFR §236.1013(a) are provided in the above mentioned documents, as referenced in the PTCSP and included in Appendix 5-1 and Appendix 5-2 to the PTCSP.

2.2.1 Incorporate PTCDP by Reference

For LIRR's ACSES II Implementation on ASC territories, the existing ACSES II Type Approval is incorporated by reference. For LIRR's ACSES II Implementation on ABS and CMB territory, the ACSES II Type Approval FRA-TA-2013-04 is incorporated by reference in Appendix 5-1 and Appendix 5-2 to the PTCSP.

2.2.2 Final Human Factors Assessment

Pursuant to 49 CFR §236.1015(d), a final human factors analysis is provided in **Section 7** of the PTCSP and in Appendix 7-1 to the PTCSP.

2.3 LIRR PTC System Implementation

2.3.1 LIRR PTC Implementation Plan (PTCIP)

The FRA approved Long Island Rail Road PTC Implementation Plan is referenced in this PTCSP Error! Reference source not found.. The PTCIP includes a Preliminary Hazard Analysis (PHA) for the planned Main line Track Exception Addendum (MTEA), specifically the PTE and LOE, including LOE in the MBS from Ronkonkoma to Greenport.

The document:

- Describes the functional requirements that the proposed system meets.
- Describes how the railroad intends to comply with 49 CFR Part 236 requirements.
- Defines how the railroad provides for interoperability between the LIRR and all tenant railroads.
- Describes how the PTC system is being implemented to address areas of greater risk to the public and railroad employees before areas of lesser risk, by evaluating multiple risk factors.
- Defines the sequence, schedule, and decision basis for the line segments being equipped, including the risk factors by line segment.
- Identifies the rolling stock being equipped with the PTC technology.
- Identifies the number of wayside devices required for each line segment and the schedule to complete the installations by December 31, 2018.
- Identifies which track segments the railroad designates as main line and non-main line track.
- Identifies and describes the railroad's basis for determining that the risk-based prioritization in Section 6 above is not practical.
- Contains the MTEAs as defined by §236.1019.

2.3.2 LIRR-Specific PTC System Functions Implementation, If Any

The following subsections describe LIRR's specific application of the ACSES II in fulfillment of 49 CFR 236 Subpart I §236.1015(d) requirement to include §236.1013(a) information.

ACSES II is a system that increases the safety of the railroad by providing situational awareness of potential unsafe train operations and limits train operations into unsafe situations. ACSES II warns the onboard crew about predicted violation of signal indications, speed limits, and monitored switch alignments, and applies a penalty brake to preempt or mitigate violation by a locomotive of its non-compliance with speed limits, signal indications or misaligned switches.

In the LIRR application, ACSES II consists of six primary subsystem segments:

- Office segment
- Onboard segment
- Wayside segment
- Communications segment
- RWPS Segment
- Transponder Segment

ACSES II is a vital overlay to the existing LIRR cab signal system. In a small portion of the LIRR territory, ACSES II is a vital overlay to the existing ABS without cab signal and CMB without cab signal. The PTC system provides for the safe train control and operation with the following protections:

1. Against train-to-train collisions.
2. Against overspeed derailments.
3. Against incursions into established work-zone limits.
4. Against switch not properly aligned.

To achieve the above protection goals, the ACSES II system provides a set of primary safety-critical functions using the configuration of equipment, databases, and I/O, which make up the LIRR PTC system. The primary functions of the ACSES II system are:

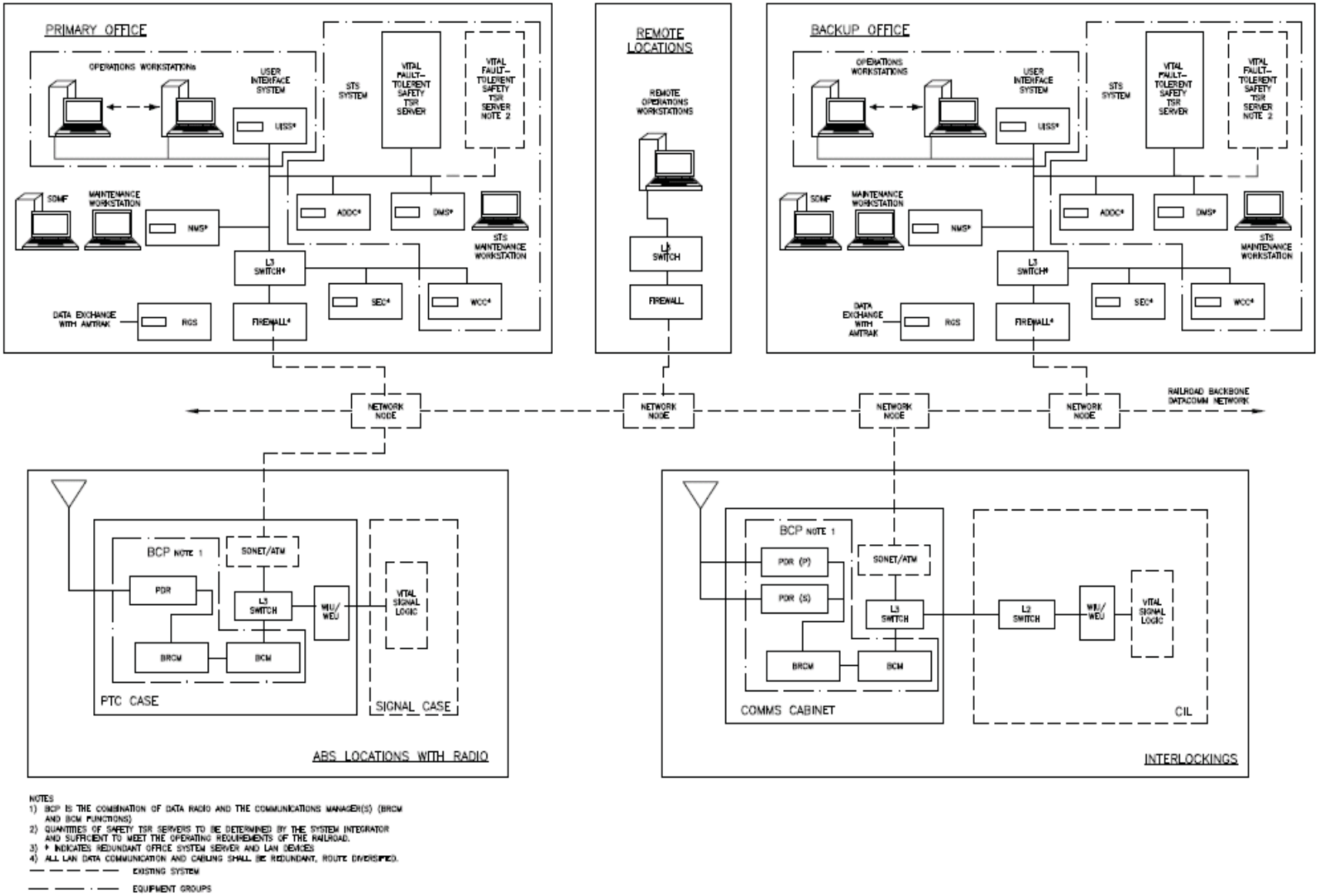
1. Enforcement of Permanent Speed Restrictions (PSR).
2. Enforcement of passenger and freight TSRs received through the data radio network.
3. Enforcement of PTS at HS's displaying a Stop aspect.
4. Release or override of the PTS (PTS Override or PTSO) for either HS not displaying a Stop aspect when cab signal is inoperative or the interlocking signal status allows the train to go.
5. Enforcement of a civil speed received by radio based on switch alignment at interlocking. This speed corresponds to the diverging or crossover civil speed (Interlocking PSR).
6. Route dependent speed enforcement based on selected exit track (Route Dependent PSR).

7. Utilizing the communications network to report and record ACSES II specific maintenance messages from all ACSES II systems to the Office Data and Maintenance System (D&MS).

2.4 PTC Architecture and Support for Interoperability

As defined in the PTCIP [15], the LIRR PTC system consists of existing three types of signaling systems and MTEA operation in one dark territory (a.k.a. LOE) supplemented by a vital microprocessor based ACSES II overlay that implements the previously-described modifications to the Type Approved ACSES II PTC system. As the existing signaling systems are compliant with 49 CFR Part 236 subparts A-H, details of the existing signaling systems are not part of the PTC system and are omitted. The new ACSES II is added as a vital overlay onto this existing signaling system with the planned hardware or software configuration modification as indicated in LIRR PTCIP [15]. The LIRR PTCIP has described all configurations of ACSES II overlay on the several different LIRR territory types, being: ASC, ABS without cab signaling, CMB, and non-signaled territory (MBS).

The ACSES II architecture is the same throughout LIRR territory regardless of the type of signaling system underlying the PTC. The set of safety-critical functions described in **Section 7** ACSES II Subsystem Functions are performed by the ACSES II system to the maximum extent possible for each type of territory. The ACSES II system architecture is described in the following **Figure 2-1** Through **Figure 2-7** which include both cab signal operation under ASC and non-cab-signal operation known as ABS and CMB. These figures are followed by typical subsystem configuration drawings. Detailed description of each system component is found in the ACSES II System Design Specifications, supplemented by the LIRR PTCDP, included in Appendix 5-1, PTC Systems Integrator Specification MNR & LIRR Positive Train Control, Volume 2 – Systems Integrator Specifications, and several LIRR Subsystem Specifications. All such documents are available on request by the FRA from the project office. Throughout this section of the PTCSP, the terminology “crucial” is used in association with component parts of the ACSES II System. This terminology means that the item is necessary for ACSES II to function, but the terminology has no relationship to the safety, i.e., vitality of the item in question.



NOTES
1) BCP IS THE COMBINATION OF DATA RADIO AND THE COMMUNICATIONS MANAGER(S) (BRCM AND BCM FUNCTIONS)
2) QUANTITIES OF SAFETY TSR SERVERS TO BE DETERMINED BY THE SYSTEM INTEGRATOR AND SUFFICIENT TO MEET THE OPERATING REQUIREMENTS OF THE RAILROAD.
3) * INDICATES REDUNDANT OFFICE SYSTEM SERVER AND LAN DEVICES
4) ALL LAN DATA COMMUNICATION AND CABLING SHALL BE REDUNDANT, ROUTE DIVERSIFIED.

EXISTING SYSTEM

EQUIPMENT GROUPS

Figure 2-1: ACSES System Block Diagram Level 0

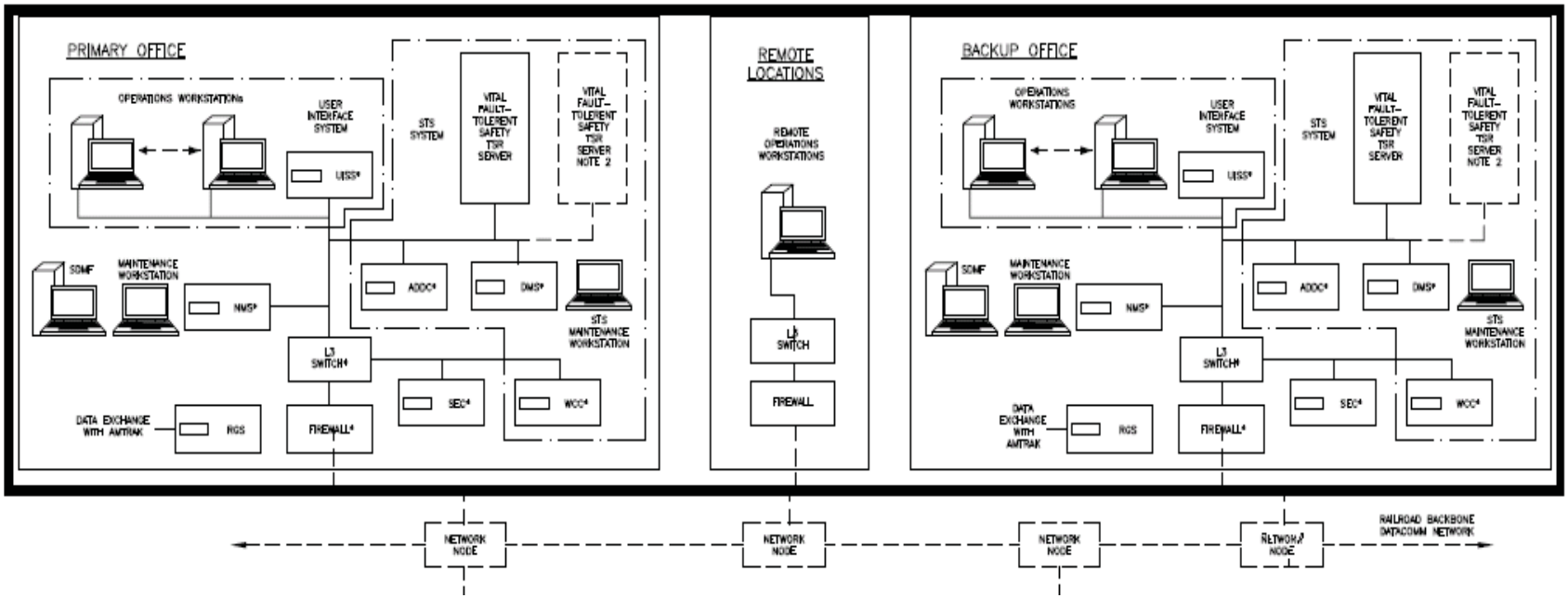


Figure 2-2: Office Subsystem Context Diagram

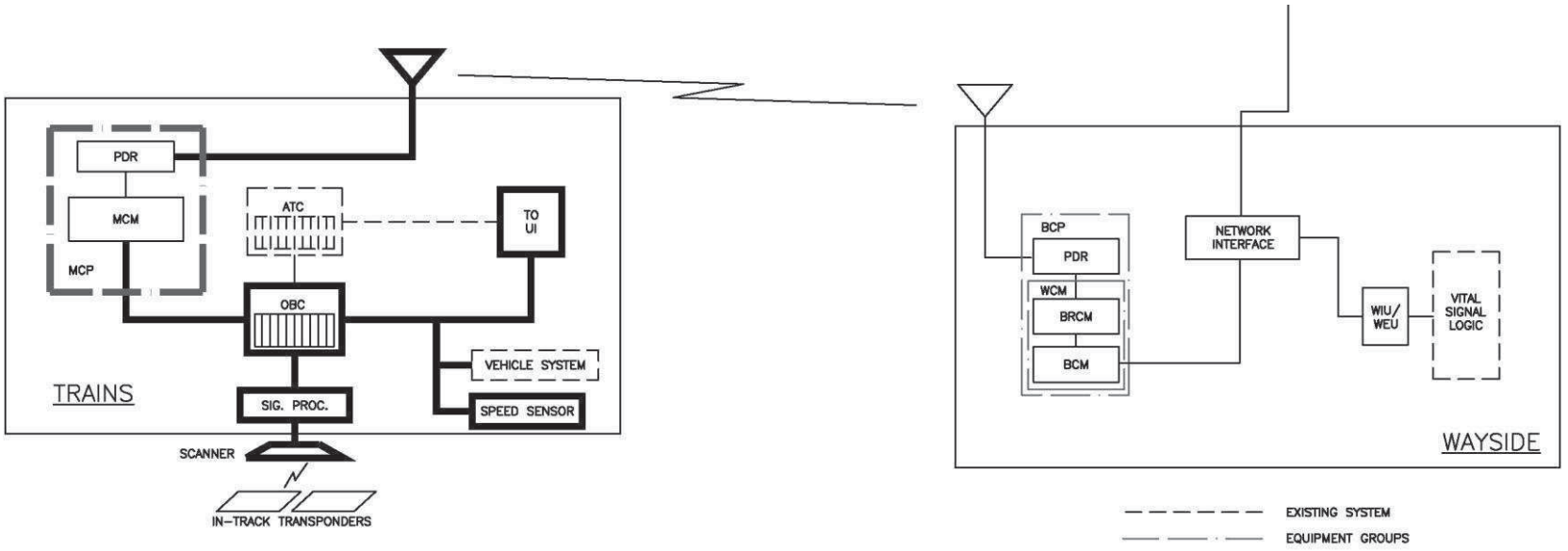


Figure 2-3: Onboard Subsystem Context Diagram

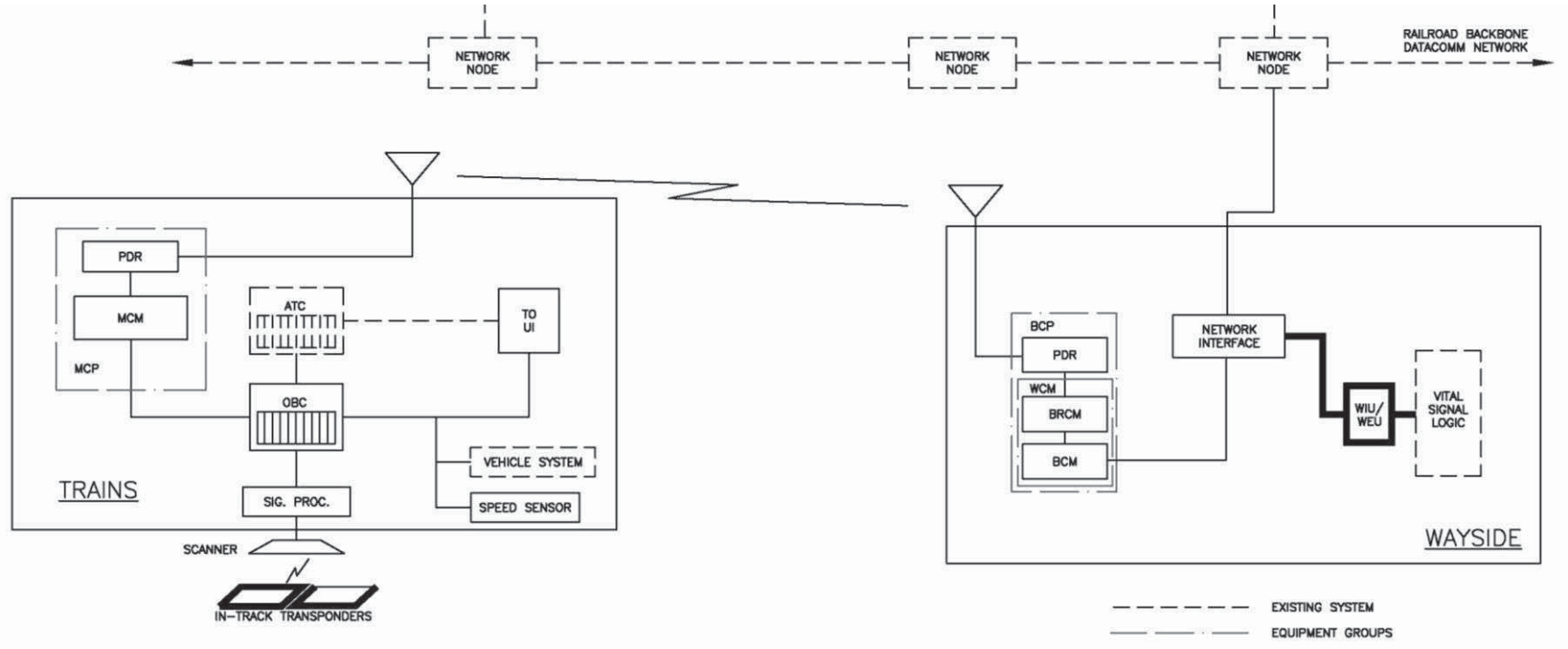


Figure 2-4: Wayside Subsystem Context Diagram

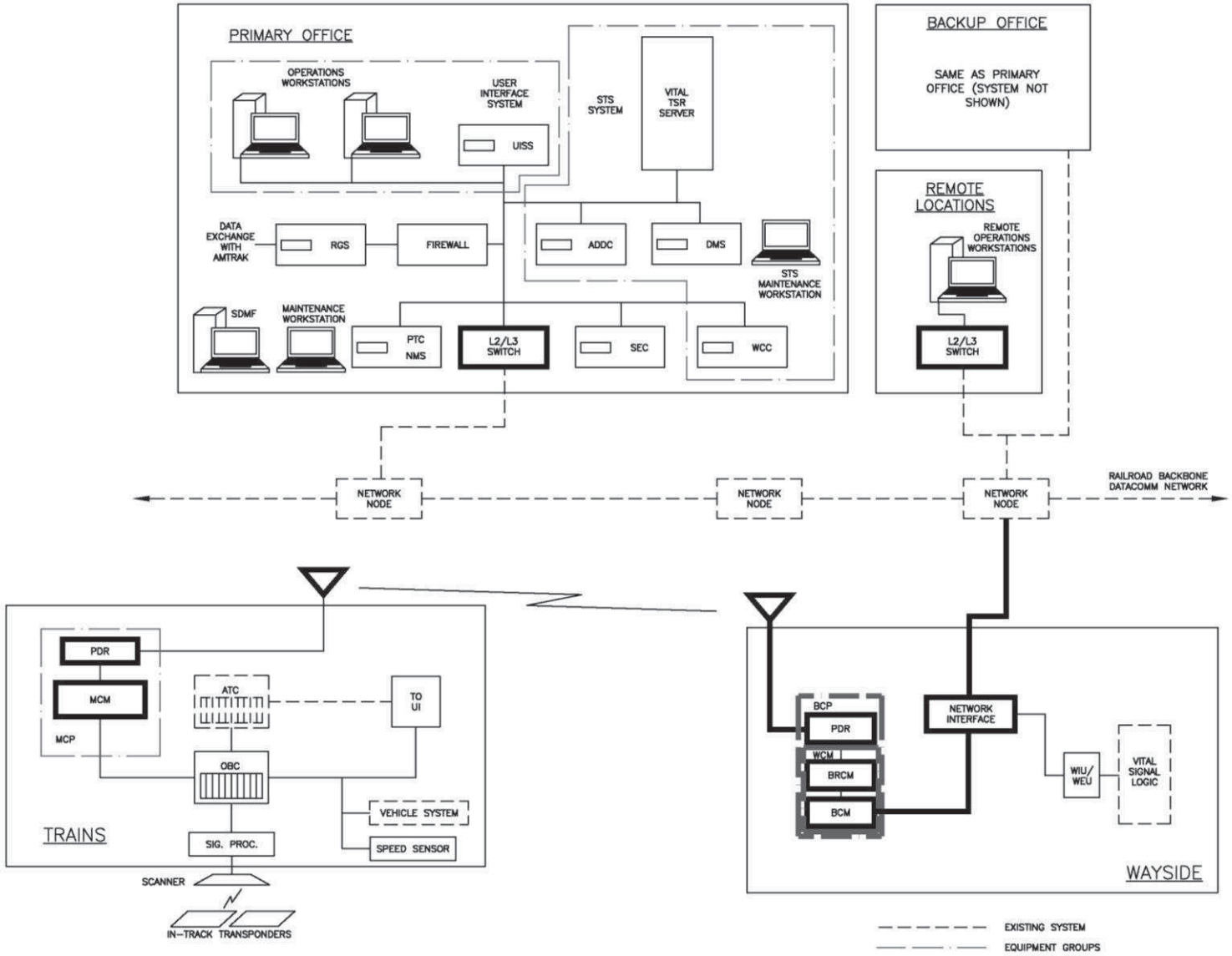


Figure 2-5: Communication Subsystem Context Diagram

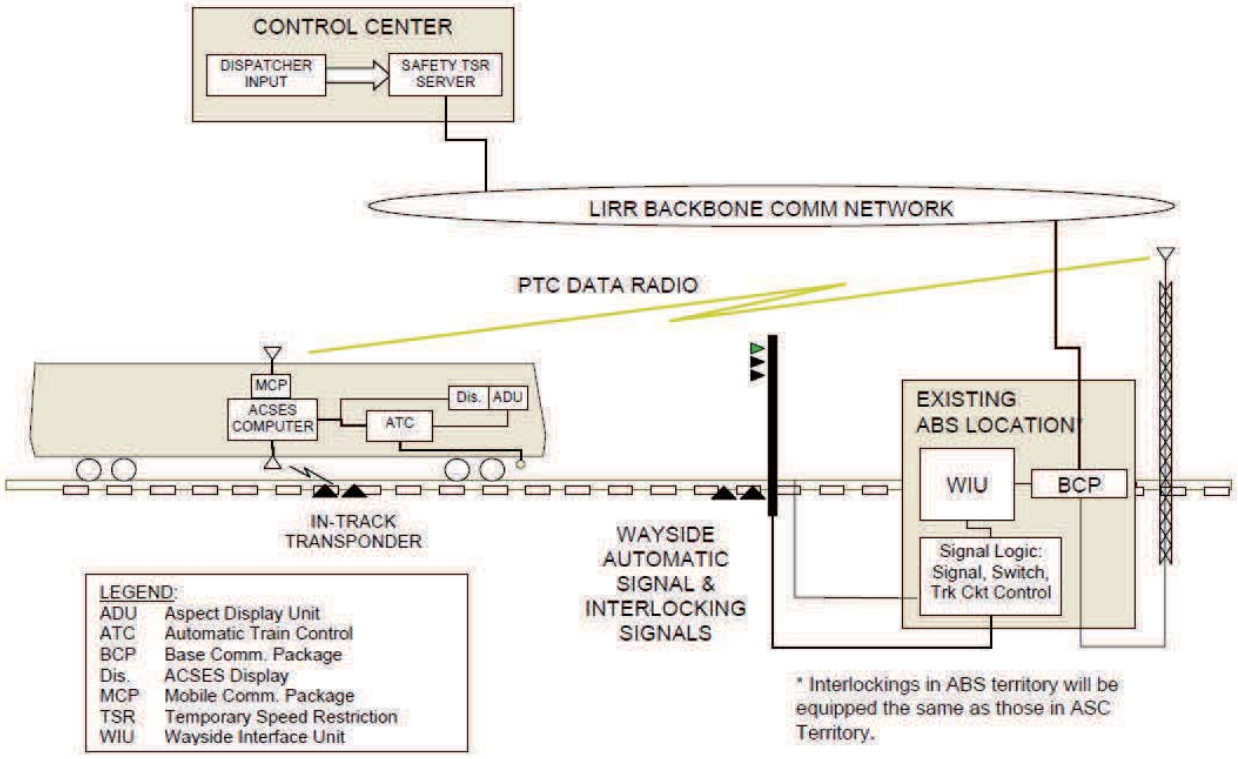


Figure 2-6: ACSES II PTC Block Diagram for ABS Territory

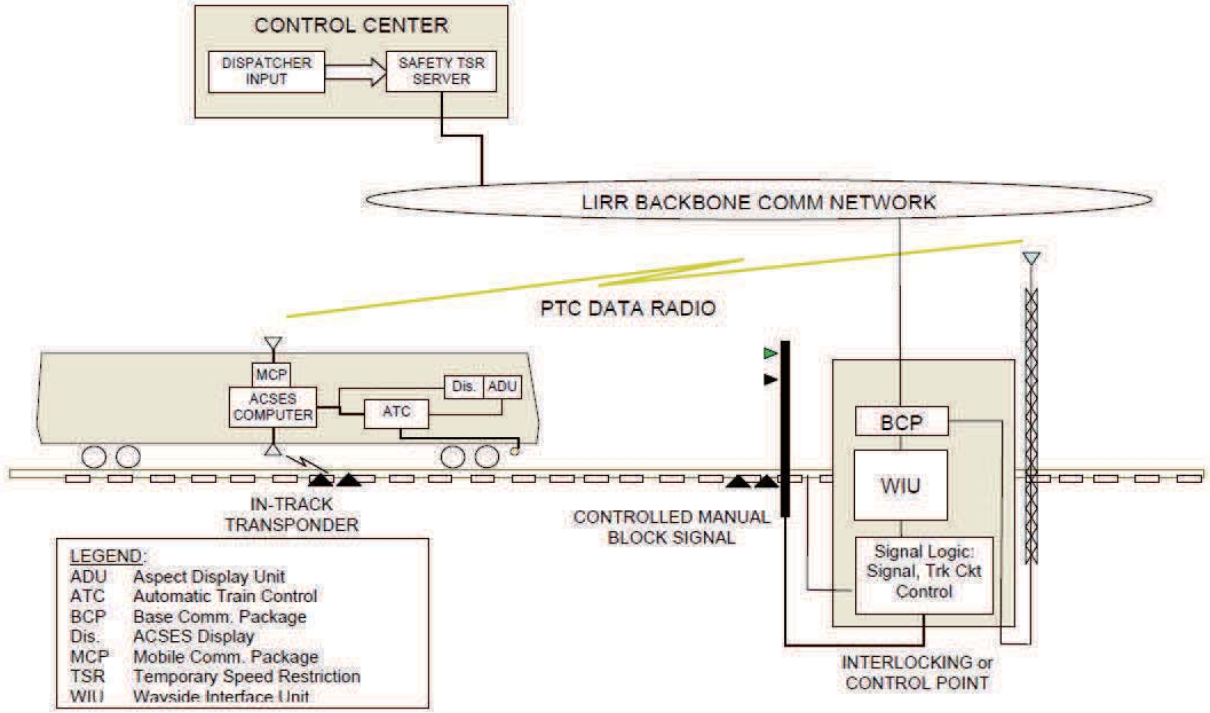


Figure 2-7: ACSES II PTC Block Diagram for CMB Territory

Figure 2-3 depicts the basic configuration of ACSES II system implemented for LIRR PTC.

1. ACSES II Ground Network includes the office and communications components depicted in
2. **Figure *2-5***. The primary role of the office is TSR generation and management. Communications subsystem provides interface between the office, wayside, and the ACSES II onboard subsystems.
    a. Office equipment includes safety-critical and non-safety related components.
    b. Communications equipment includes BCM, BRCM, PTC Data Radio (PDR), and various L2/3 Switches located at the wayside.
2. WIUs provide interface between the existing Vital Signal Logic and ACSES II BCP. Refer to **Figure 2-4** for detail.
3. ACSES II onboard equipment performs the enforcement of TSRs, PSR, PTS, and provides Train Engineer speed display. Onboard subsystem includes OBC, MCM, ADU, location determination, and scanner equipment for communications with Transponders. Refer to **Figure 2-3** for detail.
4. Transponders installed along the tracks.

ACSES II subsystems, working independently and as an integrated whole, support the objectives and functions described above. The specific functions performed by each ACSES II subsystem are described below.

2.4.1 Office Subsystem

Two Office locations are identified within the LIRR properties. The primary Office is located in the Jamaica JCC 4th Floor Computer Room building while the Backup Office is located in the Hill Side facility. In addition, 9 Control Towers are equipped with PTC Office workstations.

The office locations are connected to the existing LIRR Data communication Network through the SONET/ATM network equipment in the basement facilities at the Jamaica JCC building and to the SONET/ATM network equipment at the Hill Side facilities.

The PTC Office Subsystem interfaces with the Wayside Subsystem, the RWPS and to External Railroads through dedicated redundant communication circuits.

2.4.1.1 Safety TSR Server

The Safety TSR Server (STS) provides the Railroad with all the functionality required to validate, schedule, and transmit Temporary Speed Restrictions. The STS is a safety-critical component of the ACSES II office subsystem. The STS receives requests from the User Interface System (UIS) which are initiated by the Train Dispatchers and Rail Traffic Controllers. The STS vitally stores the TSRs, applies appropriate gradient data and transmits the TSRs to trains upon request from the OBC. The STS supplies all of the TSRs a train could encounter in its current radio coverage area along with the next two TSR Blocks in the direction of travel.

The TSR Server Vitally Schedules approved TSRs for automatic activation at a future effective time/date and/or deletion of a TSR at a future expiration time/date per information provided

when establishing the TSR. The TSR database is forwarded to the UIS on an as needed basis so that non vital sorting, reports and event notifications can be handled at the UIS level.

The TSRs are compiled from data entered by Railroad authorized users on dedicated UIS workstations located in the Railroad control center and other remote Railroad designated locations. These TSRs are then sent to the TSR Server for validation, approval and activation. All TSR data generated through UIS are managed by the STS. The STS also manages TSR-specific critical data stored in the STS fixed database that consists of the system layout to allow the validation of TSRs and proper management of the Trains TSR lists.

The STS is responsible for the accuracy and validation of the TSR requests. Integrity of the TSR data is ensured through implementation of the ACSES II "SELECT – CHECK – EXECUTE" process designed to minimize user input errors that could lead to unsafe operation of equipment.

The STS servers are located in both in the Primary Office in Jamaica JCC 4th floor and the Backup Office. Redundant STS servers are installed in each location in order to match the specified RAM numbers. The Bombardier EBILock R4 platform has been selected to implement the STS functionality.

The STS' primary interfaces (via the Office LAN) are as follows:

- UIS for reception of new or modification TSR requests from an authorized user and sending of current TSR status,
- WCC for the purpose of receiving TSR requests from the OBC and returning TSR requests to the OBC.

The STS functions include:

- TSR Generation and Management which includes maintaining lists of active and inactive TSRs, creating duplicate TSRs at boundaries, and adding and deleting TSRs from lists.
- Interface with Work Order System (WOS) includes sending and receiving messages for TSR addition/deletion following the "SELECT-CHECK-EXECUTE" process.
- Responding to TSR requests from trains based on train location (BCP zone), three-zone look ahead including possible diverging routes, and TSR duplicates at line boundaries.
- Interfacing with boundary STS, both internal to LIRR and external, to provide TSR updates at/near line boundaries.
- Executive program and fixed database version checks at startup and verification across all three processors that versions are identical and processor-unique version is correctly loaded. STS does not run unless correctly verified.

2.4.1.2 Data and Maintenance System

The Data & Maintenance System (DMS) is a crucial component of the ACSES II office subsystem. The primary function of the DMS subsystem is to provide data storage to other subsystems that produce data. This data includes operational data created by operators through user interface forms, events generated by various subsystems, and all the ACSES messages. LIRR PTC has a database centric specification where all ACSES message information is stored

in a Highly Available Relational Database Management System (RDBMS) for subsequent Event Review and Reporting. Therefore, availability and reliability of the central RDBMS is of paramount importance while designing the DMS subsystem. User interface to the DMS is through the Maintenance workstations.

DMS are installed in both in the Primary and the Backup Office. The DMS is based on redundant COTS servers. The primary interfaces (via the Office LAN) are as follows:

- WCC for the purpose of receiving ACSES II messaging for archival purposes
- NMS for the purpose of generating SNMP information and receiving Network logging events required for data collection in the DMS.
- Maintenance Workstation for the purpose of user interface to a maintainer.

The primary DMS functions include:

- Record every transmission occurring on the PTC office Local Area Network (LAN) between the STS, UIS, WCC, Network Management System (NMS), WIU, and OBC.
- Redundant DMS servers host Structured Query Language (SQL) databases for logging and reporting of transmission data.
- Manage and interrogate the SQL databases.
- Generate Simple Network Management Protocol (SNMP) alarms and maintenance information on the operational status of the ACSES II Office subsystem.

2.4.1.3 Network Management System

The Network Management System (NMS) is a set of hardware and software tools that allow for the supervision of individual components in a network. The NMS is a crucial Commercial Off-The-Shelf (COTS) system of the ACSES II office subsystem.

The primary functions of the NMS include:

- Network device discovery – This includes the identification of various devices that are part of the network based on their IP address. Devices can be discovered using either Simple Network Management Protocol (SNMP) or Internet Control Message Protocol (ICMP). The device along with its properties is added to the database upon discovery.
- Network device monitoring – Devices added to the database are monitored to determine their health, inter-connectivity and network performance. This can determine if the devices and the connections between them are functioning as expected and if there are any repairs or replacement necessary.
- Network performance analysis – Various parameters that track overall network performance such as bandwidth utilization, packet-loss, latency and uptime of network components such as routers and switches are recorded for analysis. This is done using SNMP. Monitoring network traffic may also indicate an imminent attack if, for instance there is a sudden spike in traffic passing through a firewall.
- Notifications - Any and all alerts pertaining to specific network scenarios can be configured to be sent to an administrator in various ways. This includes calling, instant messaging or e-mail.

The user interface to the NMS is through the Maintenance workstations. Also, the NMS has an interface to the Office LAN. The NMS is installed both in the Primary and the Backup Office. Redundant COTS servers are used to implement the NMS functionality.

The NMS' primary interfaces (via the Office LAN and GBN) are as follows:

- Networked Devices for the purpose of monitoring status.
- DMS for the purpose of receiving SNMP information based on events generated in the system and sending event data for recording as needed.
- Maintenance Workstation for the purpose of user interface to a maintainer.

Additional NMS functions include:

- Poll the ACSES II equipment.
- Collect, manage, and report ACSES II equipment status.
- Provide logging of all maintenance and status data received as well as provide statistics and status reports.
- Monitor the health of all ACSES II equipment servers
- Monitor and provide manual control of the A/B switch position
- Monitor and provide manual control of wayside Radio Transfer Switches
- Generate SNMP alarms and maintenance information on the operational status of the ACSES II office subsystem.

2.4.1.4 Wayside Communications Controller

The WCC is a crucial component of the ACSES II office subsystem. The WCC is the data entry point for communication between field equipment over data networks to the central office. The main functionality of WCC is to route TSR requests from locomotives to the STS and return the TSR list. All field communications such as ISR messages are forwarded to WCC for archived purpose. It maintains the routing information from all BCMs thus it is a central location to assist BCM for route resolutions.

The WCC is installed both in the Primary and the Backup Office. Redundant COTS servers are used to implement the WCC functionality. The WCC' primary interfaces are as follows:

- BCM for the purpose of receiving TSR requests from the train and routing them to the STS as well as receiving TSR responses from the STS and routing them to the originating BCM.
- STS for the purpose of receiving TSR requests from the OBC and transmitting the TSR response from the STS to the requesting train.
- DMS for the purpose of logging all ACSES data message traffic between the OBC and WIU and between the OBC and the STS.

The WCC functions include:

- Process all ACSES II messages and perform addressing and routing of all messages between ACSES II Office (STS, DMS) and Wayside and Onboard equipment (BCP, WIU, OBC).

- Maintain a table of all trains currently communicating including entries for each train comprised of the train address, location (BCP number), Received Signal Strength Indicator reported by each BCP, and the time the entry has been in the list.
- Centralize ACSES II messaging and overlapping BCP coverage to assure that duplicate messages are not sent to the train.

2.4.1.5 Communications/Network Security

LIRR PTC ACSES II system ensures that communications channels are adequately protected. Protections ensure the continued confidentiality, integrity, availability and non-repudiation of all sensitive communications.

LIRR PTC ACSES II has implemented Hash Message Authentication Code (HMAC) cryptographic algorithm to provide the necessary authentication, and to elect NOT to apply message confidentiality. This approach satisfies all of the mandatory requirements levied by the Federal Railroad Administration (FRA) and the railroads for cryptographic security in accordance with FRA 236.1033 specification for communication and security requirements which is split into two parts. Subparts (a) through (d) describe the requirements for cryptographic message integrity for all wireless communications for PTC systems. Subparts (e) through (g) describe the requirements for cryptographic message confidentiality.

The BCM provides an encrypted communications pathway for ACSES traffic between the train and the WCC in the Office Network. The BCM also provides a communication pathway for ACSES traffic between the train and WIUs and provides HMAC authentication for messages with its designated WIUs. HMAC encoding and decoding for messages to and from the Office Network is handled by the WCC. The Key manager (WCC) also handles encryption key management. In order to provide integrity and authentication of messages that are sent (either over the air or via a wired connection) an HMAC cryptographic algorithm has been deployed. Data is hashed using a SHA-2 algorithm (SHA2 is approved by NIST as strong hashing functions), and messages are verified/authenticated using HMAC (hash-based message authentication)

Network security is ensured by a redundant pair of firewalls (one active, one standby) deployed before both of the PCC and BCC office networks to control traffic to and from the Ground-based Network (GBN). These pairs of firewalls also control Wayside-to-Office and Office-to-Wayside traffic. Office devices, such as workstations and servers, are protected from external attacks by the network firewalls, but they are also individually monitored and protected from virus and malware exploits.

2.4.1.5.1 Key Management

As described in the Security Management Plan [16], the Key Management mechanisms must address the secure transmission of the keys from key management server to the equipment (BCRM, MCM, WCC) requiring them.

The Signals Group is responsible for the generation and distribution of the keys to MoE and Comms groups responsible for their installation.

The installation mechanism is performed using one of the following ways :

- For the MCM, “local” installation – a maintainer (MoE representative) directly connects

the MCM to a maintenance laptop, and installs the new certificate. This can be done in the shop or at the time of the installation of the MCM. Certificates for the BCM will be managed by Comms, and it can be done remotely.

- Remote" installation – a maintainer/administrator remotely establishes a secure connection to the security component and installs the new certificate(s). This process can be performed automatically, for both MCM and BCM.

Keys must be renewed on a regular basis (limited life-time), when needed (equipment being replaced) of if a key is suspected to be compromised. The COMMs group will be responsible for the revocation of the MCM keys.

Keys must be exchanged with Amtrak to ensure seamless operation between railroads.

2.4.1.6 User Interface System Server

The User Interface System Server (UIS) is a crucial component of the ACSES II office subsystem. The primary function of the UIS is to allow authorized users to request and manage TSRs. The UIS sends a TSR request to the STS and facilitate the user interactions of the "SELECT – CHECK – EXECUTE" scheme for approving TSRs. The UIS also provides alarms and events associated with TSRs. Redundant UIS servers are located at the Railroad's Primary and Backup Control Centers. The operator interface to the UIS is through the UIS workstation.

The UIS is based on redundant COTS servers. The UIS' primary interfaces (via the Office LAN) are as follows:

- UIS workstations for the purpose of user interface with the UIS system.
- STS for the purpose of requesting or modifying TSRs and for requesting current TSR reporting.
- RWPS for the purpose of receiving TSR requests (worker protection) from the RWPS system

The UIS functions include:

- Gate and enforce user access and rights to the UIS.
- Authenticate user information and grant functional rights within the UIS based on user privilege.
- Interface with the Fax Server to support faxing TSR forms and lists to LIRR personnel.

2.4.2 Onboard Subsystem

Reference to §236.1006*: Each train operating on PTC track shall be controlled by equipped locomotive in accordance with the PTCSP provisions.*

The onboard subsystem is formed by both the ACSES II Onboard equipment and the Communications equipment. The ACSES II Onboard equipment is functionally overlaid on top of the existing ATC Cab Signaling equipment. The Onboard Subsystem interfaces with the Wayside Subsystem and the existing Train equipment. In this section a description of each of the main components of vehicle subsystem is provided.

2.4.2.1 Onboard Computer

The OBC is a safety-critical component of the ACSES II onboard subsystem. The ACSES II Onboard Subsystem (OBC) is based on FRA type approved ACSES II functionality as defined by the Federal Railroad Administration (FRA) Type Approval letter, FRA- TA-2010-001. The ACSES II Onboard Subsystem provides for safe operation of trains by enforcing the following high level functions:

- Speed Restrictions (MAS, PSR and TSR)
- Positive Train Stop at Home Signals displaying a Stop Signal. The OBC is vitally implemented to protect the train by utilizing information from the transponders.

The main interfaces to the OBC are:

- Transponders via the Scanner for reception of information to facilitate advanced speed enforcement, positive train stop and position determination
- ADU – for the purpose of displaying information to the train engineer
- MCM – for the purpose of transmitting and receiving information to the wayside from the train (ISR, TSR and Maintenance Data)
- Train Interfaces such as the train engineer (ACK, Cut-out, Alarms, Cab Key), the braking system, deceleration and speed sensing.

The primary OBC functions include:

- Support all LIRR train types (M7, M3, C3/DE/DM, E10/15/20, and future M9).
- Calculate Alert & Braking Profile for all train types.
- Calculate over-speed Alert & Braking Profiles.
- Determine ACSES II MODE 1 & 2 operation as well as ACSES II Cut-In & Cut-Out conditions.
- Perform construction zone transition.
- Detect reverse movements and trailing.
- Provide trailing unit location retention.
- Detect direction of movement and establishes ACSES II direction of travel.
- Determine front of train by direction.
- Monitor cab signal and detect ATC cab signal Cut-Out.
- Send stop request to ATC.
- Interface with the braking system and speed sensors.
- Monitor and interface with MCM.
- Send train location and distance to approaching signal to MCM.
- Provide scanner antenna control.
- Interface with the vehicle power supply.
- Monitor radio and detect missed radio messages/timeout.
- Detect partial or missing transponder sets.

- Detect linking transponders.
- Decode and store transponder messages.
- Perform transponder milepost conversion.
- Request, decode and store TSR data from STS.
- Request, decode and store interlocking status.
- Request interlocking status on power up.
- Send onboard maintenance messages to DMS.
- Receive DMS acknowledgment.
- Provide speed processing function and detect speed threshold.
- Provide wheel wear compensation function.
- Identify and detect target speed.
- Perform PTS.
- Prevent train type routing to East Side Access (ESA) to avoid tunnel collision.
- Provide penalty request forestall.
- Determine and detect over-speed points.
- Detect downgrade speed change.
- Determine train speed under alert curve and train speed hitting alert curve.
- Allow speed increase after restriction zone ends.
- Provide penalty brake running release.
- Provide Stop signal enforcement.
- Handles “C” signals (Clear Block).
- Enforce interlocking and route dependent PSRs.
- Enforce TSR.
- Provide Stop and Release enforcement of 5MPH TSR.
- Enforce Maximum Authorized Speed (MAS) on ATC failure.
- Enforce single and nested interlocking PTS.
- Manage onboard communications processor messages.
- Provide Pre-Distant Signal (PDS) Read ID of approaching BCP and PDS Read ID of next BCP in direction of travel.
- Provide PDS Read of distance to stop signal.
- Detect train past Stop signal.
- Provide brake assurance determination.
- Provide route management and handle route not available conditions.
- Provide slip/slide compensation.

2.4.2.2 Mobile Communications Manager

The MCM is a crucial component of the ACSES II onboard subsystem. The MCM facilitates the mobile side of the transfer of ACSES II messages between the ACSES II OBC and the ACSES II wayside network. The MCM utilizes the data radio link provided by the 220 MHz radio system. The MCM is responsible for managing the transfer of data to and from all onboard radios (220 MHz PDR, Cellular, Wi-Fi, and 900MHz) and the Onboard Computer (OBC). The MCM supports a TCP/IP Ethernet interface to the OBC and all onboard radios.

The MCM utilizes a Radio Configuration File (RCF) database to reference the radio parameters which allow the MCM, upon receipt of a message from the OBC, to establish communications with an approaching BCP. The purpose of the RCF is to allow dynamic adjustment of the data radio operating frequency and signal power of the onboard PDR as the train moves into the coverage area of a BCP. The MCM is installed in a non-redundant configuration.

The main interfaces for the MCM are:

- Ethernet connection to the ACSES II OBC for the purpose of managing ISR, TSR and Train Maintenance messages from the OBC to the wayside and managing ISR and TSR responses from the wayside to the OBC.
- Ethernet connection to the 220 MHz PTC data radio (PDR), Wi-Fi or Cellular connections for the purpose of transmitting/receiving information between the MCM and the wayside.

The MCM functions include:

- Handle radio messaging between OBC and ACSES II office subsystem.
- Handle radio messaging between OBC and ACSES II wayside subsystem.
- Manage TDMA scheme.
- Manage mobile radio power.

2.4.2.3 Scanner Antenna Interface

The scanner antenna is a crucial component of the ACSES II onboard subsystem. The CTV Box contains the analog RF electronics necessary to scan/read wayside transponders. It utilizes the scanner antenna to power and read transponders and supplies transponder data to the cardfile electronics within the ACSES sub-system. It is a rugged cast aluminum assembly designed for under-body mounting on the vehicle.

The CTV electronics serve as a 27.115 MHz transmitter and a 4.5 MHz receiver. Low-pass filtering on the 27.115 MHz output eliminates unwanted interference from harmonics of the 27.115 MHz signal. The receiver portion performs AM demodulation on the incoming signal and supplies the demodulated data bit stream to the card file electronics. This antenna is designed for use with the transponder sub-system employed by the ACSES equipment. It is used to transmit RF power to wayside transponders and subsequently receive RF data from a responding transponder.

The Scanner Antenna system functions include:

- Energizes the passive transponders laid on the tracks as it passes over them.

- Receives messages from transponders and transmits them to the OBC.

2.4.2.4 ACSES II and ATC Aspect Display Unit Interface

The Aspect Display Unit (ADU) interface is a crucial component of the ACSES II onboard subsystem. The ADU is the train engineers' primary interface to the ATC and PTC systems. The ADU functions as an ATC signal aspect display and displays ACSES related information. The speed limits from both the ATC and ACSES II systems are shown on the ADU. The ADU is powered continuously from both the ATC and ACSES II OBC subsystems and operates regardless of whether or not the cab is activated. If the cab is not activated, the ADU is powered but is darkened and is not actively updated. During normal operation, the device independently communicates with and is commanded by both the ATC and ACSES II systems. In cases where a non-Siemens ATC is installed, an AIU is used to communicate ATC information with the ADU.

For married pair trains, an ADU is installed in each end.

The ADU interface is not standard across all vehicle types. As a result, the interface requirements associated with the existing ATC unit vary with vehicle type.

The ADU functions include:

- Displays Civil Speed and Maximum Authorized Speed (MAS)
- Provides Visual and Audible Alert Curve Violation Displays.
- Allows Audible Alarm acknowledgments.
- Displays ACSES II Status.
- Displays TSR Data Status as available or not.
- Displays "STOP" Target.
- Provides Test Inputs and Display.

2.4.2.5 Speed Sensor Interface

The speed sensor interface is a crucial component of the ACSES II onboard subsystem. Its main function is to convert speed sensor outputs to wheel rotation, and deduce train speed from wheel rotation.

2.4.2.6 Decelerometer

The Decelerometer is a safety-critical, microcontroller-based device whose primary function is to provide grade-compensated deceleration. The Decelerometer data is used by the OBC to implement slip/slide compensation and brake assurance.

2.4.2.7 Configuration Memory Module

The configuration memory module is a vital microcontroller-based device. This processor uses non-volatile memory to store configuration information for a particular vehicle.

2.4.2.8 Cab Controls

Following controls are available:

- Cab active: this control signal indicates to the OBC cardfile which cab is in control.
- ACK switch/ACK foot pedal used by the train operator to acknowledge an alarm, as required by the OBC
- Absolute Stop Bypass push-button: this control signal indicates to the OBC cardfile to override the train stop under a PTS condition.
- ACSES departure test key-switch: this control signal indicates to the OBC cardfile to actuate the departure test.
- Forward/Reverse: these control signals indicate to the OBC cardfile the intended direction of movement for the train.

2.4.2.9 Alarm (Sonalert)

The alarm provides audible warning to the train operator. To sound the alarm, the OBC cardfile provides an alarm control signal over a discrete interface to the cab in control.

2.4.2.10 ACSES II Departure Test

ACSES II onboard systems are verified prior to trains departing their terminals. This Departure Test verification is in addition to verifications currently performed for the existing LIRR ASC system and LIRR's maintenance procedures.

The ACSES II Departure Test provides a check list of verifications and tests to confirm that a train can safely go in service.

Should the ACSES II Departure Test identify a failure or malfunction, the train is not put in service on the PTC territory until the failure is corrected. The failure is reported to the Mechanical Department for repair.

2.4.3 Wayside Subsystem

This section provides a description of each of the main components of the Wayside subsystem. The Wayside subsystem comprised the WIUs, the Transponders and the Wayside Radio and Network equipment. The Wayside Subsystem interfaces with the Office Subsystem and the Vehicle Subsystem and to External Railroads through WIU connected to LIRR reading the status of the External Railroad signal system status in the boundary areas.

2.4.3.1 Wayside Interface Unit

The WIU is a safety-critical component of the ACSES II wayside subsystem. The WIU is connected to vital relay contacts and/or a vital processor in the CIL in order to monitor switch position(s) and signal status at an interlocking. Using the state of the inputs that are connected to it, the WIU then responds to Interlocking Status Requests (ISRs) generated by the ACSES II OBC equipped trains approaching the CIL. The non-redundant WIU to be used on this project is

the Siemens VIU-20E. The VIU 20E manual is contained in CDRL 4-17, WIU Hardware Design Description, which is available to FRA on request.

The primary interfaces of the WIU are:

- Switches and signals through wired connection to either vital relays or vital processor outputs;
- Approaching trains' OBC, via the Base Communication Manager (BCM), to receive ISR requests from the OBC and to provide ISR response messages with the respective Interlocking status.

The WIU functions include:

- Reading the real time status of all interlocking signals (better than stop and Clear Block Signal) and all interlocked switch positions (normal or reverse). Reference to §236.1005(e)(3):
- Transmitting interlocking route status messages to trains via data radio.
- Providing information regarding the interlocking exit track of routes.
- Providing civil speeds for an established route.
- Providing distance from the HS to the diverging switch.
- Providing distance from the facing point of the diverging switch to the trailing point of the switch on the exit track.
- Providing a list of the tracks the train will cross during its move through the interlocking.
- Providing LoMA information.

2.4.3.2 Passive Transponders

The transponders are a safety-critical component of the ACSES II wayside subsystem. The Transponders provide vital data from the Wayside to the OBC in order to ensure the OBC has knowledge of its current location in the system and advance information in front of the train. The Transponder subsystem is detailed within the Transponder Subsystem Description Document.

The Transponders are installed along the centerline of the gauge between the rails. Transponders are installed in groups of 2 to 4 transponders. A minimum of two per set is necessary for travel direction determination. The Transponders selected for this application are the Bombardier JGA29001/6. No additional power supply or connection to the wayside interface unit is necessary.

The main interfaces of the transponders are:

- Transponder to OBC for the purpose of transmitting current location, PSR information and approaching interlocking information (PTS target and ATCS address for radio communication)
- Transponder to Tenant OBC – The transponder must be interoperable with tenant vehicles running on the Railroad. Therefore, all transponder messages are standardized for all trains operating on the system.

There is no interface necessary with the existing Interlocking System or Cab Signaling System.

The Transponder functions include:

- Storing track topographic data, signal, and communications information.
- "Broadcasting" the stored information upon being energized by the trains passing over them.
- Providing the actual distance to the beginning of the next permanent speed restriction(s), or speed change.
- Providing the target speed of all restrictions between this transponder set and the next transponder set.
- Providing all speed upgrades between this transponder set and the next in the direction of train travel.
- Providing the worst-case grade over the distance to the next transponder in the direction of train travel.
- Providing Transponder type, location, and track number.
- Providing the actual distance to the next transponder location and necessary sync and check bytes to transmit a vital, failsafe message.
- Providing the distance to the next Interlocking Home Signal.
- Providing the radio channel assignment for communications between the wayside BCP and the onboard MCP.

2.4.3.3 Base Communications Package

The BCP is a crucial component of the ACSES II wayside subsystem. The BCP functions and modules include:

- BCM with WIU and office subsystem interfaces.
- BRCM with PTC data radio interface.
- PTC data radio.

The main functionality of BCM is to manage routing information for the wayside location in order to interface with Office Subsystem for communication with the vehicles for TSR information and to interface with local WIUs or adjacent WIUs to the vehicles for ISR information.

For LIRR, the BCM is located within the Radio cases and connected to the L3 switch. The BCM has the following primary interfaces:

- WCC for the purposes of transmitting TSR information between the BCM and STS, transmitting ACSES messages to the DMS for archival.
- BRCM for the purpose of managing the PDR communications with the MCM
- WIU for the purpose of transmitting the ISR request and response data between the OBC and the WIU.
- Adjacent BCM for nested interlocking scenarios

The BRCM manages communications between 220 MHz PTC Data Radios (PDR) on the wayside and 220 MHz PDRs on vehicles. One BRCM can manage up to six 220 MHz PDRs and supports communications with multiple vehicles by TDMA time slot assignments. The TDMA

slot approach is based on a six second epoch, with eight time slots available per second (125 ms per slot). The BRCM obtains clocking information from GPS or from IEEE 1588 to provide time synchronization among locomotives for proper time slot assignments. It communicates with the PTC Data Radios using STFP protocol to set up the radio in proper communication frequency and power. It communicates with the MCM on locomotives using RCP protocol for time slot assignments and time slot releasing. It transports the ATCS messages for ISR, TSR, and Maintenance Alarm to and from BCM to support the information requested by MCMs.

For LIRR, the BRCM is located within the Radio Cases and is connected to the L3 switch. The BRCM has the following primary interfaces:

- BCM for the purpose of routing messages
- PTC 220 MHz Radio for the purpose of radio time slot management
- MCM via the 220 MHz Data Radio for the purpose transmitting ACSES II messages between the train and the wayside.

The 220-MHz PTC Data Radio is an electronic device that transmits radio frequency (RF) signals modulated (encoded) with a data stream based on a predefined format. The Data Radio also demodulates received RF signals to recover a similar of data stream transmitted by an identical Data Radio at a remote location. The Data Radio forms the link between wayside and mobile PTC digital systems and the 220-MHz radio spectrum. The same type of radio is used for on-board and wayside installations. The device selected for this application is the GE MDS TD220MAX.

The Data Radio requires an external nominal 12 VDC power source. For LIRR, the Data Radio is located in the Radio Case and connected to the L3 switch. Other Radios to be used during Pilot Testing is the WIFI and the Cellular radios.

The Primary interfaces for the 220-MHz Data Radio are:

- BRCM for the purpose of time slot management and routing of data from the Wayside to the Train.
- MCM for the purpose of time slot management and routing of data from the Vehicle to the Wayside.

The ACSES II Data Communications design is structured around spectrum in the 217 to 223 MHz range required to provide interoperability among the railroads on the Northeast Corridor.

The PTC Data Radio system is fundamentally an intermittent system in which trains initiate communications with wayside base radios (part of the BCP) based on train location along the railroad. Communication is minimally initiated when trains are in approach to interlockings after passing “PDS points’. Communications is terminated once a train passes the interlocking Home Signal. For LIRR, in addition to communications in approach to interlockings, data radio communications is nearly continuous as trains re-request communications with BCPs as they exit interlockings and maintain communications until the next PDS point in the direction of travel.

- The PTC Data Radio system utilizes a TDMA transmission scheme managed by communications managers that were developed by the SI. ACSES II Ground Based Networks utilize LIRR existing Fiber Backbone Networks and “last mile” connectivity to the office and wayside locations

- Data Radio System:
  - Mobile and Base software-defined digital Data Radio (expected to be the same radio for mobile and base). Mobiles are located on rolling stock; Bases are located at wayside locations in communications cases and huts.
  - Base Radio Communications Managers (BRCM) located in communications cases and huts on LIRR and in Signal CILs on MNR.
  - Mobile Communications Managers (MCM) located in rolling stock
  - Mobile antennas mounted on the roof of rolling stock
  - Mobile in-line filter located in rolling stock
  - Base antenna located at wayside BCP sites
  - Base in-line filters located in Wayside systems
  - Layer 2 and Layer 3 switch/routers
  - Ancillary devices such GPS and other time source devices, redundant transfer switch, base antenna power monitor system, power supplies, grounding devices.
- Ground Based Network
  - Multilayer L2 and L3 switches located in the offices; signal CILs and communications cases and huts.
  - Base Communications Manager located in communications huts and cases on LIRR and in signal CILs on MNR.
  - Ancillary connection and network devices.

2.4.4 Roadway Worker Protection System (RWPS)

Two RWPS Office locations are identified within the LIRR properties. The primary Office is located in the Jamaica JCC building while the Backup Office is located in Hillside. The office locations are connected to the existing LIRR Ground Based Network (GNB) through the ATM SONET network equipment in JCC and the Backup Office location. As part of the RWPS Office subsystem, Remote Location Workstations are installed in locations to be confirmed by LIRR.

The RWPS Office Subsystem interfaces with the Office Subsystem through the RGS and with external Internet Services Providers to provide connectivity to the EIC terminals. This section provides a description of each of the main components of the RWPS subsystem.

2.4.4.1 RWPS Office

The scope of the RWPS system is to protect Roadway Workers through Temporary Speed Restrictions (TSR). The EIC terminals (Truck-mount, Handheld and EIC workstations) provide the EIC the ability to request application and removal of Temporary Speed Restrictions (TSR) using EIC terminals and receive a list of active TSR from the Office system.

RWPS system consists of RWPS Servers, RWPS Workstation, EIC Terminals, RWPS DMS, RWPS NMS, RWPS ADDC, and RWPS Security Server. EIC's are designated as Primary or Secondary RWPS terminal users. The Primary EIC defines the limits of TSR and requests TSR to be implemented through the ACSES II system. The Secondary EIC (with Primary EIC's approval) can be attached to or released from an existing TSR. When there are no secondary

EICs attached remaining on to the TSR, the Primary EIC is able to request the work zone TSR to be deleted from ACSES II system.

One hot-standby redundant pair of RWPS servers is located at the primary control center (PCC) and another pair at the backup control center (BCC). The RWPS interfaces to L3 switches that are connected to firewalls which eventually interface to the Cellular, Private Wi-Fi and Public Wi-Fi networks. Also, connection to the Amtrak Network and Office LAN is via the RGS.

The primary interfaces of the RWPS are:

- ACSES II Office (via the RGS) for the purpose of communicating TSR requests and receiving TSR information.
- EIC Terminals for the purpose of EIC interface to the system
- RWPS Workstations for the purpose of interfacing to the RWPS system.

2.4.4.2 EIC Terminals

The EIC terminals are hosted on truck mounted terminals, handheld devices and wayside installed workstations throughout the system. The truck mounted terminals and handheld devices connect to the RWPS office through Wi-Fi and Cellular connections. The EIC Workstations connect to the RWPS office through the Railroad GBN.

The primary functions available on the EIC terminals are:

- View active TSRs list,
- Request to add and remove a Work Zone TSR,
- Manage Secondary EICs requests to be attached or removed from an existing TSR.
- Manage Primary EIC status from one authorized EIC to another authorized EIC.

2.4.5 Support for Interoperability

The PTC architecture that supports interoperability can be grouped into five (5) categories, which are:

- **Temporal Separation**: In the region between Ronkonkoma and Greenport, where Moving Block Rules are used, Fixed Access Time Windows are used to separate Passenger and Freight trains.
- **Boundary Transition**: Fixed and known locations for boundaries between territories enable tenant trains to transition into a host railroad's territory, and return back from host territory seamlessly.
- **Software and Message Version Compatibility**: All trains entering LIRR territory are equipped with ACSES II.
- **Interoperability Verification**: Amtrak and NYAR trains entering the LIRR PTC territories are equipped with compatible ACSES II systems, as determined by ACSES II system design, implementation, verification, and testing.
- **Interchangeability**: As with Interoperability Verification, Amtrak and NYAR trains entering the LIRR PTC territories are equipped with compatible ACSES II systems, as

determined by ACSES II system design, implementation, verification, and testing.

2.5 System Users

The following personnel interact with the PTC system:

- Train Dispatchers
- Chief Train Dispatchers or Train Dispatcher Supervisory Personnel
- Train Engineers
- Signal Installers and Maintainers
- Maintenance of Equipment (MoE) personnel
- Maintenance of Way (MoW) personnel led by Employee In Charge (EIC)

2.5.1 Train Dispatchers

Train Dispatchers interact with the PTC system for the purpose of defining, applying, and removing TSRs and MoW Work Limits through dedicated PTC computerized user interface workstations located at LIRR's Jamaica Central Control (JCC) and the Movement Bureau at the Jamaica Station Building.

When necessary, Train Dispatchers grant permission for Train Engineers to activate the PTSO per the operating rules.

The TSR user interface is of the same basic methodology as for creating track warrants; namely, it is form-based executed via the Work Order System user interface. The track foreman/Employee-In-Charge (EIC) requesting a TSR or MoW Work Limits enters the requested protections on a prescribed form, which is retained until the request is deleted (prior to being approved) or until the protection is cancelled. Only variable information, such as milepost limits, time limits, non-standard flag placement, speed limit (for TSRs), whether a Stop is required at the entry point (Work Limits) or not, the name of the EIC and other instructions, needs to be entered. Fixed wording is part of the form.

The dispatchers select the protection form (either Form V or Form W) in the Work Order System and enter the variable data provided by the track foreman. The TSR system verifies that all the requisite fields for the form selected have been entered and provides appropriate range checking. If the data as entered is acceptable, the TSR system assigns a TSR or Maintenance Work Package (MWP) number (which the train dispatchers pass to the track foreman/EIC) and passes the information over to the chief train dispatcher or designated supervisory personnel for the check and execute phase.

2.5.2 Chief Train Dispatchers or Train Dispatcher Supervisory Personnel

The Chief Train Dispatcher is required to verify that the TSR and/or MoW Work Limit data has been correctly entered before the TSR system activates or deactivates each restriction. When the train dispatcher has finished the data entry and the TSR system has accepted it, the TSR system displays the data to the assigned train dispatcher supervisor for verification.

The process is similar to read back of a track warrant. The supervisor tabs to each field in turn and read the data to the track foreman/EIC. When the track foreman/EIC accepts the read-back

as correct, the supervisor approves the restriction (execute) and provide the time to the track foreman/EIC.

The long-standing process of read/read-back and OK (execute) is well established and well understood within the railroad industry.

2.5.3 Train Engineers

Train Engineers interact with the PTC system to operate trains in accordance with the speed enforcement functionality of LIRR's PTC system.

Train Engineer information display devices include:

- Civil Speed.
- ACSES II system status lights.
- Audible indication if Alert Profile violation is detected. ACSES II generates an alert braking profile that is 3 MPH above the optimum braking speed of the train to meet speed restriction and protect stop targets.
- "No data" indicator light, which is lit yellow when the onboard system has no TP information. This is lit when the system is first initialized until a TP is read; when a train reverses direction until a first TP is read; or when a train does not read a TP at an expected location (based on the distance traveled from the last TP) until a new TP is read. Operation under no transponder data condition is defined by operating rule and procedure.
- "No TSR data" indicator light that is lit when the onboard system enters a block for which no TSR dataset has been successfully received. If a block has no active TSRs, a null dataset is sent to suppress the indicator light.

Train Engineer input to onboard PTC systems includes:

- Acknowledgement of audible Alert Profile Violation alarm.
- Activation of PTSO feature, permitting a train to go by a controlled signal at Stop with dispatcher permission.
- ACSES II cut-out switch.

Train Engineer Overspeed Information and Braking:

- If and when the train reaches a non-suppressed Alert Profile, an alarm is sounded and displayed to the Train Engineer and the speed limit of the restriction is displayed digitally. The Train Engineer is required to acknowledge the alarm to silence it, and operate the train within the Braking Profile (safety envelope).
- If and when the train reaches a non-suppressed Brake Profile, an immediate penalty-brake application is initiated by ACSES II. The train is safely stopped before reaching the Stop Signal (or overlap stop point) if the Train Engineer does not operate the train within the ACSES II Brake Profile. If the Train Engineer applies the brakes to get the train under the ACSES II Braking Profile, the ACSES II enforced braking is released.

2.5.4 Signal Installers and Maintainers

Signal personnel interacts with the wayside PTC equipment during installation, routine inspections, in response to failure reports, following changes in track topology, and following track renewal.

During installation, signal personnel wired WIUs with existing Vital Signal Logic (VSL) using wiring diagrams and installation instructions as prepared by the SI and approved by LIRR. The model number and serial number of each piece of installed equipment together with the software version identification information deployed on each piece is recorded into portable computers for entering into the Configuration Management System (CMS).

The LIRR has obtained system components for trouble-free installation. The techniques include:

- Delivery of fully loaded components (no need for on-site assembly).
- Keyed connectors that cannot be plugged into wrong interfaces.
- Fully labeled components with the labeling matching the installation drawings.
- Fully labeled cabling, pre-harnessed where practicable.

The SI designed and delivered all post-installation test procedures for LIRR together with needed test tools. A full suite of tests were performed following installation at each site. The tests followed formal test procedures (as were approved by LIRR in advance of installation) and the results were logged and appended to the final test plan.

Signal personnel installed and encoded TPs during initial system installation, following changes in track topology, and following track renewal when TPs may have been removed. Techniques and tools already established for Type approved ACSES II were used for placement of TPs and for ensuring correct encoding of the code plugs (if used), and for ensuring that the correct code plug is installed in the correct TP. The after-installation test was performed by signal personnel different from those responsible for the placement and encoding.

Following a report of a malfunction, the signal maintainer must troubleshoot the problem. For maintenance purposes, the signal maintainer undertakes board level replacement rather than component level replacement. Therefore, the field system has the capability to perform periodic self-checks at the board level and report failures to the DMS. The LIRR maintenance document specifies the maintenance logistics, such as for a maintainer to carry the needed replacement parts and post-installation test tools.

The component and individual boards have operational state indicators, so that a signal maintainer can determine which component or board has failed. The design ensures that it is not possible to insert a wrong board into a slot and have the component become operational.

2.5.5 Maintenance of Equipment Personnel

MoE Personnel interacts with the onboard PTC equipment including, but not limited to vital OBC, TP scanner, ADU, data radio and ATC to diagnose problems, and maintain, repair, replace, modify and upgrade onboard PTC equipment.

During installation, MoE personnel installed the TP scanner, the interface with the brake system, and an ACSES II data radio system using wiring diagrams and installation instructions as contained in the O&M Manuals. The model number and serial number of each piece of installed

equipment together with the deployed software identification information was recorded into portable computers for entering into the CMS.

Similar to the field components, the onboard components are designed for trouble-free installation. The techniques include:

- Delivery of fully loaded components (no on-site assembly required).
- Keyed connectors that cannot be plugged into wrong interfaces.
- Fully labeled components with the labeling matching the installation drawings.
- Installation-ready wiring harnesses.

A full suite of tests was performed following installation at each site. The tests followed formal test procedures and the results were logged and appended to the final test plan.

Following a report of a malfunction, the MoE must troubleshoot the problem. For maintenance purposes, the MoE undertakes board level replacement rather than component level replacement. Therefore, the field system has the capability to perform periodic self-checks at the board level.

The component and individual boards have operational state indicators, so that the MoE can determine which component or board has failed. The design of the system components ensures that it is not possible to insert a wrong board into a slot and have the component become operational.

There is a departure test each day before releasing a train for service. The MoE requests the departure test by pressing a button on cab user interface. The departure test does not allow the onboard system to be activated until:

- The onboard system has performed hardware, software and memory self-checks successfully.
- The system has activated the brakes.
- The acknowledgement button electrical contact has been made.
- The system has read a test TP.
- The radio has received a reply message in response to a test transmission to a shop radio.

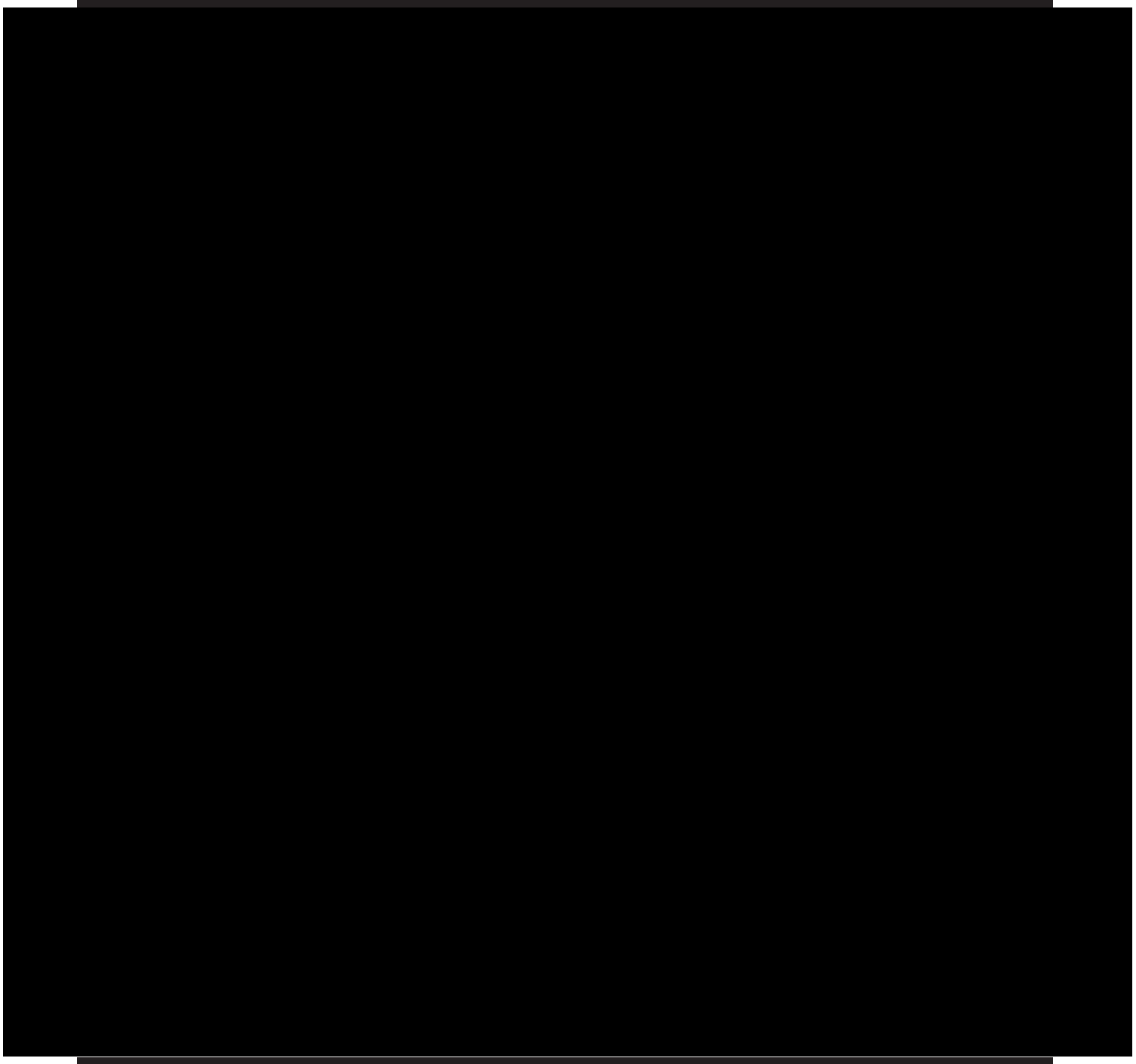
In the departure test, the role of the MoE is limited to initiating the test, pressing the acknowledge button and observing whether the test was successful or not, requiring no special HMI treatment but only adequate training as identified in Section 14.

2.5.6 Maintenance of Way Personnel

MoW Personnel interacts with wayside PTC system equipment including vital WIUs, signal system interfaces, TPs, BCP, and GBN system to diagnose problems and maintain, repair, replace, modify (including safety-critical topographic data programmed into TPs) and upgrade wayside PTC equipment.

2.5.7 Department of Program Management Track

The Department of Program Management Track is responsible for all scheduled service interruptions. Therefore they are the designated office responsible for issues relating to scheduled service interruptions, as required by:







3.2 Configuration Management

Configuration Management (CM) of the ACSES hardware and software is critical to the safe and proper operation of the system. The LIRR System Integrator (SI) is developing and testing the system under a LIRR-approved CM Plan [2]. For post commissioning, LIRR is developing its own CM program suitable for operation and maintenance phase of the system life-cycle.

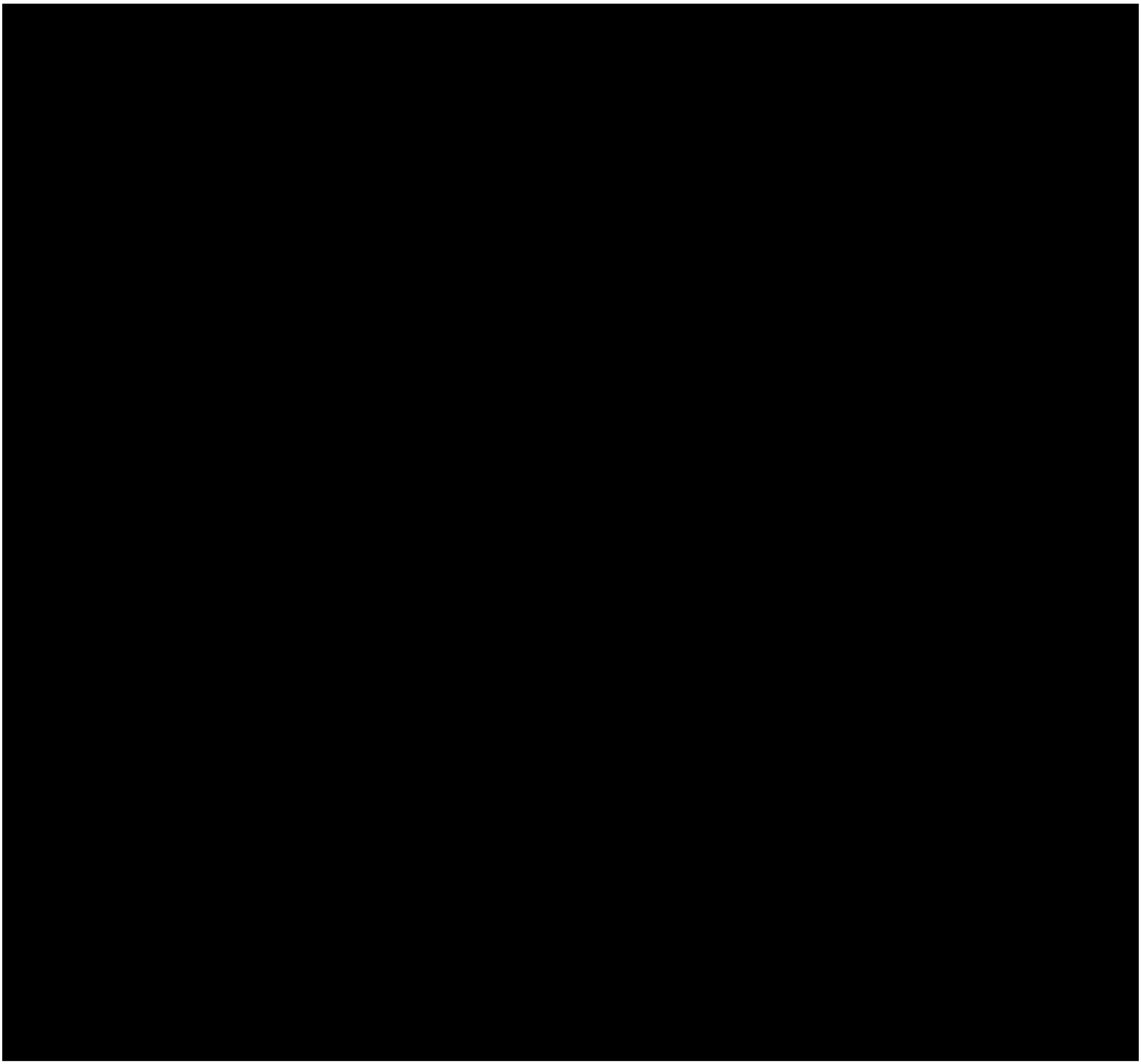
The ACSES system includes a Software Development Maintenance Facility (SDMF) serving as:

- Repository for all of the applications for Configuration Management,
- Repository for controlled versions of ACSES software applications includes tools necessary for the maintenance and modification of the system,
- ACSES inventory control system (Maximo),
- All ACSES system documentation.

Maximo is used to both generate the work-order to update the baselines and record the new baseline revision levels once the updates have been made.

4 LIRR ACSES II PTC System Level Troubleshooting

Figure 4-2 shows an initial troubleshooting flow chart which may help diagnose PTC system problems that occur on the LIRR rail lines. This diagram is not intended to be all-encompassing, but can direct attention to the appropriate segment of the PTC system for further diagnosis. As ACSES II is a complex system, experience with certain problems and their correction will lead LIRR to update, add to, or modify this flowchart for optimum usefulness.





5 Procedures, Test Equipment, And Operations And Maintenance Manual [§236.1015(d)(7) and §236.1039, Appendix C (b)(7)]

Reference §236.1015(d)(7): *A complete description of the specific procedures and test equipment necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the PTC system on the railroad and establish safety-critical hazards are appropriately mitigated. These procedures, including calibration requirements, shall be consistent with or explain deviations from the equipment manufacturer's recommendations.*

Reference §236.1015(d)(8): *A complete description of any additional warning to be placed in the Operations and Maintenance Manual in the same manner specified in §236.919 and all warning labels to be placed on equipment as necessary to ensure safety.*

Reference §236.1039: *Operations and Maintenance Manuals.*

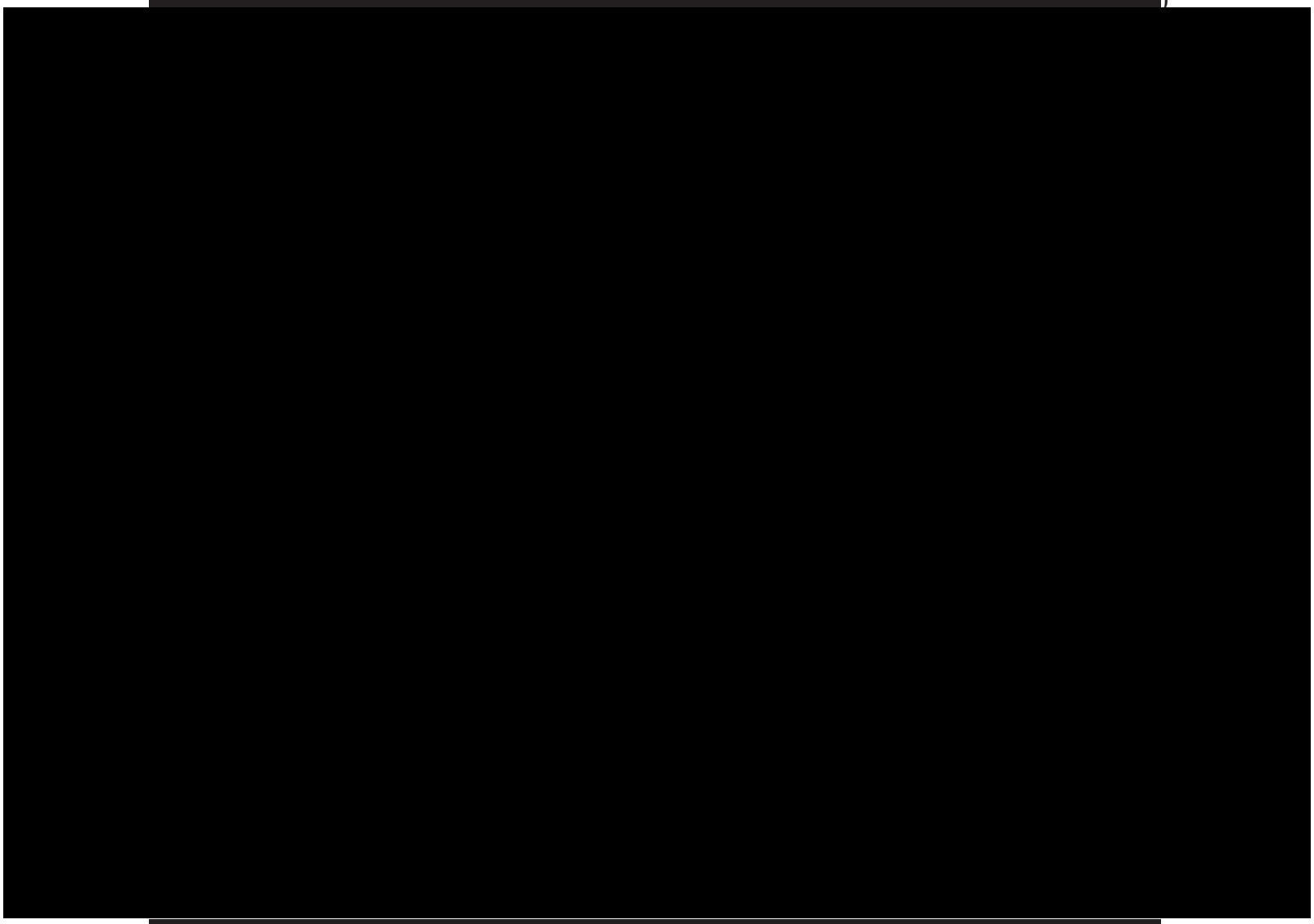
5.1 Operations and Maintenance Procedures and Documentation

The latest LIRR approved SDMF User's Manual (CDRL 2-033) is placed in Appendix 20 of the LIRR PTCSP. The latest LIRR approved Warning and Warning Labels overview Document is shown in Appendix 16 of the LIRR PTCSP.

5.1.1 Test and Maintenance Equipment

As noted in Appendix 15-2 to the PTCSP, which is reserved, other than the common contingent of meters and hand tools required for making physical and electrical adjustments to electronic equipment, the only tools required for troubleshooting and maintenance of the PTC systems are software based. PTC maintenance is supported through a set of tools managed under SDMF.

[redacted]



The Radio Frequency Manager is an application that accesses the health of the Communications Managers: BCM, MCM, and WCC and their controlled devices such as PTC 220 MHz radios (PDR).

Maximo is an application in the SDMF that maintains inventory and manages work orders. The Maximo in the SDMF is the focus of maintenance activity for the ACSES wayside and office components. The exiting MoE Maximo continues to be the focus of maintenance for the ACSES onboard components.



5.2 O&MM Document Access and Control

The latest LIRR approved Operations Manuals (CDRL 2-032) are shown in **Section 15** of the PTCSP. The latest LIRR approved Maintenance Manuals (CDRL 2-034) are shown in **Section 15** of the PTCSP.

The Operating and Maintenance Manuals are kept at the specific LIRR location identified in **Section 15** of the PTCSP.

5.3 Change Control of O&MM Documents

Change control of O&M Documents, as with all documents for use with the LIRR ACSES II system, is covered by the LIRR PTC Configuration Management Plan, as shown in Appendix 17 of the LIRR PTCSP.

6 Warnings and Warning Labels [§236.1015(d)(8)]

Reference §236.1015(d)(8): *A complete description of any additional warning to be placed in the Operations and Maintenance Manual in the same manner specified in §236.919 and all warning labels to be placed on equipment as necessary to ensure safety.*

The supplier of the ACSES II PTC system has included warnings in the LIRR ACSES II System Operation and Maintenance Manual as per Appendix 15-1 to the PTCSP on electrical and mechanical drawings and has applied labels to equipment. Warnings, cautions, and warning labels are also covered under the ACSES II Type Approval.

LIRR has reviewed all electrical and mechanical drawings, maintenance manuals and hardware, and has determined that appropriate and sufficient warnings, cautions, and labels are in place in accordance with the documentation supplied by the SI and its other vendors.

6.1 Warnings Documented in Operations & Maintenance Manuals

The System Integrator has not created additional warnings for the Operation and Maintenance Manual.

Table 6-1: Additional Warnings in Operation and Maintenance Manual

Warning	Description
None	N/A

6.2 Warning Labels

The System Integrator has not created additional warning labels.

Table 6-2: Additional Warning Labels on Equipment

Equipment	Warning Label	Description
N/A	None	N/A

7 Safety Critical Components

The following table identifies the PTC systems'safety critical hardware, software, firmware and other equipment as per following requirement *"(d) Safety-critical components, including spare equipment, must be positively identified, handled, replaced, and repaired in accordance with the procedures specified in the PTCDP and PTCSP."*:



The onboard PTC data radio (PDR) is serviced by communications maintenance personnel. The MoE performs onboard troubleshooting and report any failure/faults of the onboard PDRs to the Communications department. MoE removes defective radios from rolling stock and replace with a radio furnished by Communications. Communications Group performs detailed troubleshooting, repair, and replacement of all onboard PDRs.

8.1.1 Onboard Maintenance Manuals

In support of onboard asset maintenance, below are a series of manuals that define the appropriate instructions and procedures:



8.2 Periodic Maintenance and Testing

This section discusses the tasks associated with required periodic maintenance of all onboard equipment and lists the required maintenance intervals for each task.

8.2.1 Periodic Tests

Due to the safety-critical nature of functions and components within the onboard subsystem, the subsystem must receive a periodic inspection and checkout, and formal inspection and test documents must be prepared and signed-off once the inspection is completed.

Departure Test: The OBC equipment receives a Departure Test every 24 hours in accordance with the CFR Title 49, Part 236.587 requirements. The daily departure test is initiated by an engineer or qualified MoE personnel and checks for functional integrity of the equipment and its vehicle interfaces. The departure test steps and expected results are described in the following

PTC contract documents; the documents listed contain additional tests performed during installation and periodic maintenance as well



8.3 Troubleshooting and Issue Resolution

This section discusses the types of troubleshooting activities that may be required to resolve issues seen with the Onboard equipment. Further Information can be found in the LIRR ACSES OBC Service Manuals.

LIRR has acquired a good understanding of OBC and Undercar troubleshooting steps given the installation work performed to-date on both the M7 and DE/DM. Examples of issues that have been troubleshot and resolved to-date include:

1) Wiring issues with noisy/intermittent carbody spare wires on M7
2) Suspected interactions between ATC and ACSES equipment causing intermittent flip test failures on the M7 ATC packages
3) Defective component troubleshooting and change out as encountered during installation checkout.

8.3.1 General Steps and Tools

In general, the types of issues seen to-date are troubleshot and resolved using similar techniques as those used for the ATC system. Electricians perform the following in various combinations:

1) Review wiring schematics to ensure understanding of wiring and components involved

2) Plug in PTE to interrogate (physical and logical) onboard component. Review signals and system responses using ACSESView application (PTE)
3) Review voltage levels for key signals using the OBC breakout panel
4) If no wiring or obvious component issues are found, attempt to swap suspected component with known good component to see if this resolves the issue.

8.3.2 Remote and Bench Diagnostics Options

The MTA PTC contract includes provision for the following diagnostics/troubleshooting equipment:

1) Portable Test Equipment (PTE): For OBC/Undercar, this is the ACSESView application
2) Bench Test Equipment (BTE): allows for board-level diagnostics and troubleshooting within the OBC cardfile, and possibly other OBC LRUs
3) Remote Diagnostics Interface:
    a. Dedicated workstations are part of the ACSES system for logging into the ACSESView of the OBC on trains operating along the ROW. The connectivity is cellular connection between the workstation and the selected train. One train at a time can be diagnosed remotely.
    b. An RF Manager resident in the ACSES Office subsystem and access by MoE provides data analysis of the onboard MCP equipment.
4) A transponder simulator is part of ACSES. The transponder simulator is provided to test and analyze the train to transponder communication in the shop without having to move the train under test.

8.3.3 Onboard Personnel Responsibilities

The following are the preliminary personnel responsibilities for troubleshooting and resolution of various types of issues:

1) M of E Shops: Troubleshooting of all OBC, Undercar, Rooftop Antenna, and MCP issues, and replacement of wiring/LRU components as deemed necessary.
2) M of E Engineering: Additional troubleshooting of complex issues; management of software and configuration baseline updates on all components.
3) M of E Central Control/204: Initial troubleshooting using Remote Diagnostics Interface
4) Communications: Troubleshooting and resolution of issues within MCP LRUs (once the LRU has been removed from the vehicle).

9 Appendix B : Signals

9.1 Wayside - Signals

This section discusses various aspects of maintaining Wayside and Office ACSES equipment. Content is included for all types of equipment installed along the wayside including Communications Dept. and signal Department equipment.

9.1.1 ACSES Wayside Hardware Components and Interfaces

The following are the primary hardware components and interfaces of the wayside subsystem. Note that some components maybe considered below the LRU-level for troubleshooting or replacement purposes – see Section 9.1.3 for additional details.



9.1.1.1 Wayside Maintenance Manuals

The ACSES II subsystems maintenance manuals are developed and provided by the SI's manuals and training group. These maintenance manuals are used to perform preventative maintenance and testing tasks required for the ACSES II Wayside equipment. Maintenance and safety procedures for each task are identified and provided to all maintenance personnel. These procedures are documented in the Maintenance Plan (CDRL 2-110) and the Maintenance Manual (CDRL 2-036) for each ACSES II Wayside Subsystem as listed below:

[redacted]

9.1.2 Periodic Maintenance and Testing

This section discusses the tasks associated with the required periodic maintenance and testing of all ACSES II wayside equipment, and lists the required maintenance intervals for each task. It also includes a list of ACSES II Wayside Subsystem Maintenance Manuals that are used for the periodic maintenance and testing tasks. Periodic maintenance can be broken down into two functions:

1) Preventative Maintenance
2) Periodic (FRA) Testing

9.1.2.1 Installation Testing

LIRR has performed the installation and installation testing under direction of the PTC System Integrator. The Installation tests are a set of test cases referred to as the Site Installation Tests (CDRL 2-089-207). These same test procedures are followed whenever new equipment installations are implemented.

9.1.2.2 Periodic Test

Due to the safety-critical nature of functions and components within the ACSES II Wayside subsystem, the subsystem must receive a periodic inspection and checkout, and formal inspection and test documents must be prepared and signed-off once the inspection is completed. The periodic testing consists of the following:

1) Transponder visual Inspection and mounting conducted periodically.

9.1.2.3 Preventative Maintenance

The Preventative Maintenance tasks are outlined in the ACSES II Maintenance Plan (CDRL 2-110), and are detailed in the ACSES II Wayside Subsystem Maintenance Manuals (CDRL 2-036).

9.1.3 Troubleshooting and Issue Resolution

This section discusses the types of troubleshooting activities that may be required to resolve issues seen with the wayside equipment.

9.1.3.1 ACSES Lab and Test Equipment

The MTA PTC contract includes provision an ACSES Lab equipped to provide testing of ACSES equipment and system modifications.
The following diagnostics/troubleshooting equipment:

1) Portable Test Equipment (PTE)
2) Remote Diagnostics Interface via the NMS.

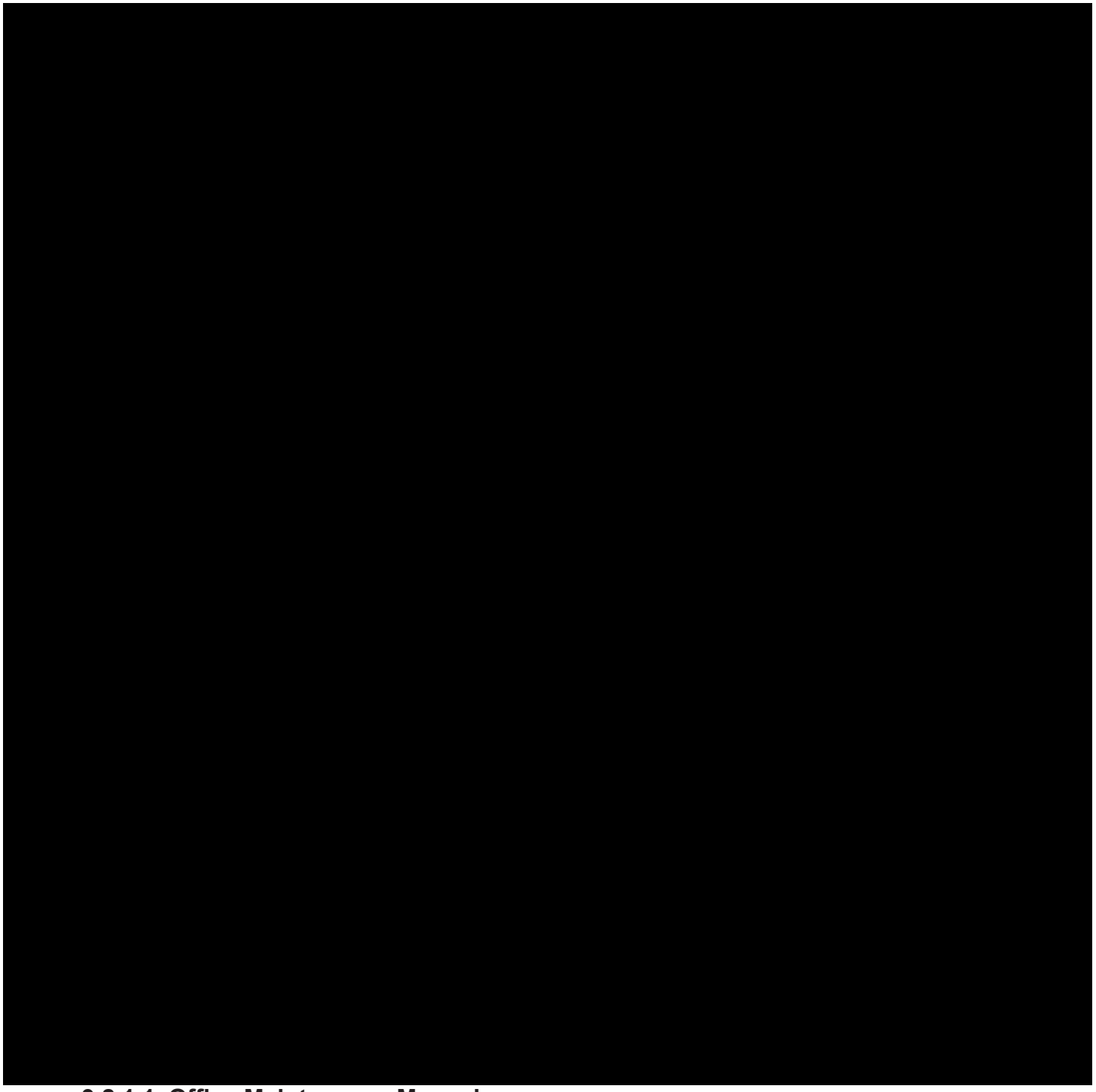
9.2 Office - Signals

This section discusses various aspects of maintaining Office ACSES equipment. Content is included for all types of equipment installed in the Primary and Backup Control centers.

9.2.1 ACSES Office Hardware Components and Interfaces

The following are the primary hardware components and interfaces that are included in office subsystem. Note that some components maybe considered below the LRU-level for troubleshooting or replacement purposes – see Section 8.3 for additional details.





9.2.1.1 Office Maintenance Manuals

In support of Office asset maintenance, below are a series of manuals that define the appropriate instructions and procedures:





9.2.2 Periodic Maintenance

This section discusses the tasks associated with required periodic maintenance of all Office systems and equipment and lists the required maintenance intervals for each task.

9.2.2.1 Installation Testing

There are various tests performed on the Office equipment as it is installed:

1. Cabinet-Level Tests
2. Network Integration Tests

9.2.2.2 Cabinet-Level Tests

This cabinet-level test procedure verifies proper hardware integration of the PTC cabinets, ensuring that the build is correct. Testing verification includes grounding, power, and cabling: short-circuit, power-up, connectivity, and basic communication. Where necessary, the signals and interconnections are verified with a meter, scope and/or other applicable instrument, including test software where needed. Each cabinet installed in the LIRR BCC was tested individually, and test results recorded and documented.

9.2.2.3 Network Integration Tests

This test verifies the proper connection, settings, and operation of the PTC hardware and software configuration. Connectivity, redundancy, and failover scenarios are tested from the perspective of the network devices. This test demonstrates that:

- The network is properly connected
- Spanning-tree is rooted in the correct network devices
- The network re-converges quickly following a switch link failure

- Failover between redundant firewalls works properly
- The overall system is capable of handling large volumes of data at a time

9.2.2.4 Periodic Maintenance

The Office subsystem is comprised of COTS equipment, data & databases, and software applications.

- Periodic Maintenance of all COTS equipment is scheduled and performed as recommended by the COTS vendor material. This maintenance is scheduled through the SDMF Maximo.
- Software, data, and databases do not generally require periodic maintenance. Revisions necessary to support changes to the operation, territory, or to revise software to address any issues are made in accordance with the appropriate Maintenance Manual using the SDMF through the configuration management processes.

9.2.3 Troubleshooting and Issue Resolution

This section discusses the types of troubleshooting activities that may be required to resolve issues seen with the Office equipment.

9.2.3.1 Example Issues

The Office subsystem is a configuration of processor based systems interconnected through the Office Network. All equipment monitors connectivity status which is recorded, and issues are reported through the NMS. As an example, if a UIS Server in the Primary Control Center loses connectivity either to an interface or suffers a failure, the redundant server in the Primary Control Center takes over as the active server or a failover to the Backup Control Center occurs. There are alarms generated to operating and maintenance personnel through the workstations and the NMS including specific information on what occurred. Troubleshooting may require reviewing data on messaging or other status logged prior to, during, or after the issue which would be available through the DMS and/or NMS.

9.2.3.2 Diagnostics

All office workstations and servers report operating status as Networked Elements to the NMS via SNMP. Additionally, the STS and UIS components perform built-in test (BIT) diagnostics to verify proper operation and data integrity. Upon detection of any noted failures, the errors are logged via reporting messages to the NMS/DMS and the faulty system is marked as failed.

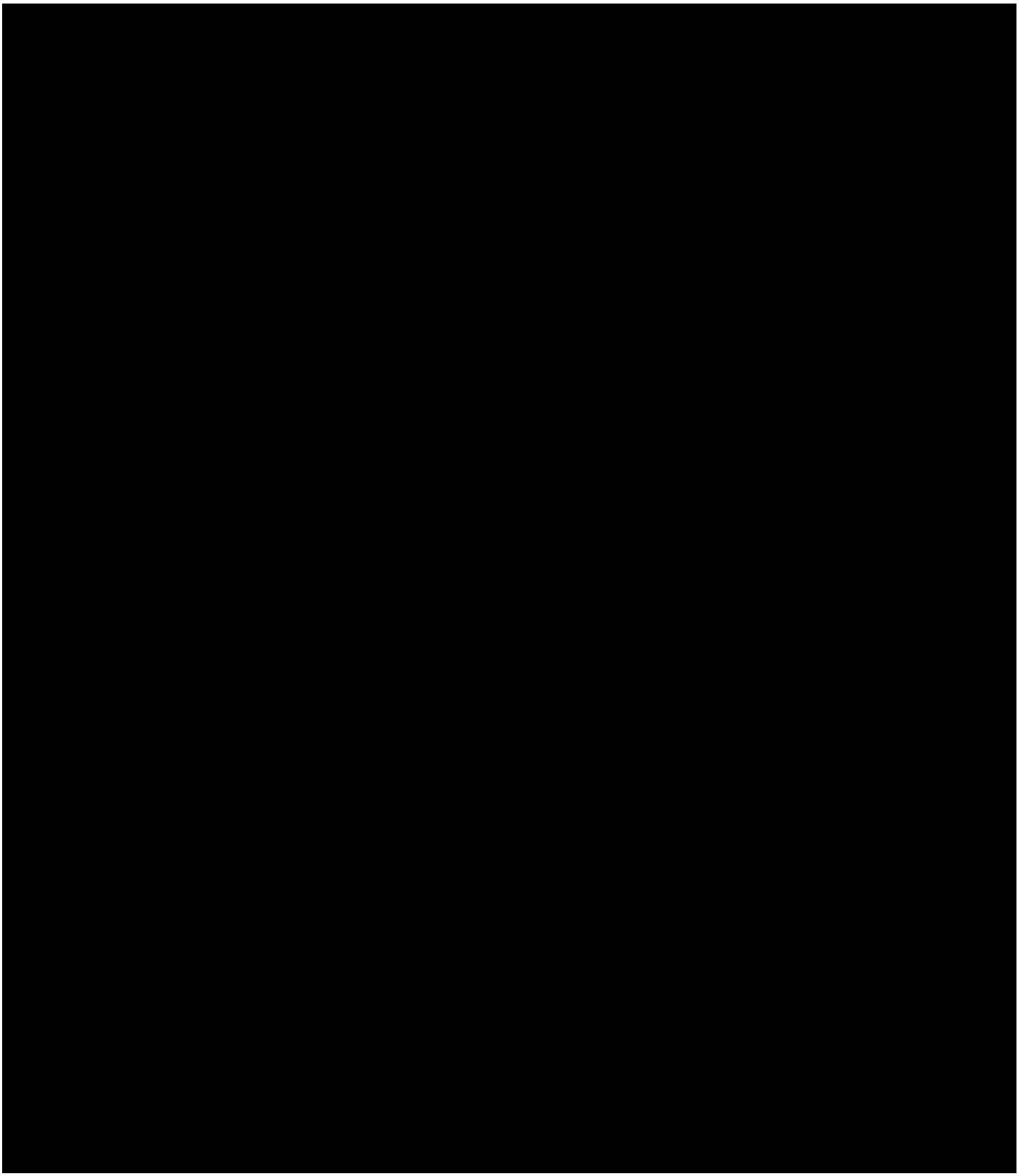
9.3 RWPS – Signals

This section discusses various aspects of maintaining the RWPS equipment.

9.3.1 RWPS Hardware Components and Interfaces

The following are the primary hardware components and interfaces that are included in the RWPS subsystem. Note that some components maybe considered below the LRU-level for

troubleshooting or replacement purposes – see Section 9.3 for additional details.



9.3.1.1 RWPS Maintenance Manuals

In support of the RWPS asset maintenance, below are a series of manuals that define the appropriate instructions and procedures:

[redacted]

9.3.2 Periodic Maintenance

This section discusses the tasks associated with required periodic maintenance of all Office systems and equipment and lists the required maintenance intervals for each task.

9.3.2.1 Installation Testing

There are various tests performed on the RWPS equipment as it is installed:

1. Cabinet-Level Tests
2. Network Integration Tests

9.3.2.2 Cabinet-Level Tests

This cabinet-level test procedure verifies proper hardware integration of the PTC cabinets, ensuring that the build is correct. Testing verification includes grounding, power, and cabling: short-circuit, power-up, connectivity, and basic communication. Where necessary, the signals and interconnections are verified with a meter, scope and/or other applicable instrument, including test software where needed.

9.3.2.3 Network Integration Tests

This test verifies the proper connection, settings, and operation of the PTC hardware and software configuration. Connectivity, redundancy, and failover scenarios are tested from the perspective of the network devices. This test demonstrates that:

- The network is properly connected
- Spanning-tree is rooted in the correct network devices
- The network re-converges quickly following a switch link failure
- Failover between redundant firewalls works properly
- The overall system is capable of handling large volumes of data at a time

9.3.2.4 Periodic Maintenance

The RWPS subsystem is comprised of COTS equipment, data & databases, and software applications.

- Periodic Maintenance of all COTS equipment is scheduled and performed as recommended by the COTS vendor material. This maintenance is scheduled through the SDMF Maximo.
- Software, data, and databases do not generally require periodic maintenance. Revisions necessary to support changes to the operation, territory, or to revise software to address any issues are made in accordance with the appropriate Maintenance Manual using the SDMF through the configuration management processes.

9.3.3 Troubleshooting and Issue Resolution

This section discusses the types of troubleshooting activities that may be required to resolve issues seen with the Office equipment.

9.3.3.1 Example Issues

The RWPS subsystem is a configuration of processor based systems interconnected through the Office Network. All equipment monitors connectivity status which is recorded, and issues are reported through the NMS. There are alarms generated to operating and maintenance personnel through the workstations and the NMS including specific information on what occurred. Troubleshooting may require reviewing data on messaging or other status logged prior to, during, or after the issue which would be available through the DMS and/or NMS.

9.3.3.2 Diagnostics

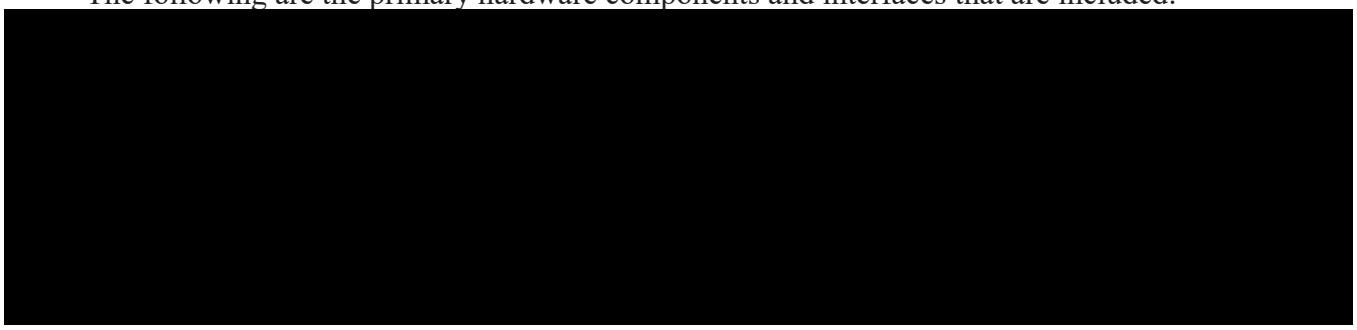
All RWPS workstations and servers report operating status as Networked Elements to the NMS via SNMP. Upon detection of any noted failures, the errors are logged via reporting messages to the NMS/DMS and the faulty system is marked as failed.

9.4 SDMF

This section discusses various aspects of maintaining SDMF ACSES equipment.

9.4.1 ACSES SDMF Hardware Components and Interfaces

The following are the primary hardware components and interfaces that are included:





9.4.1.1 SDMF Maintenance Manuals

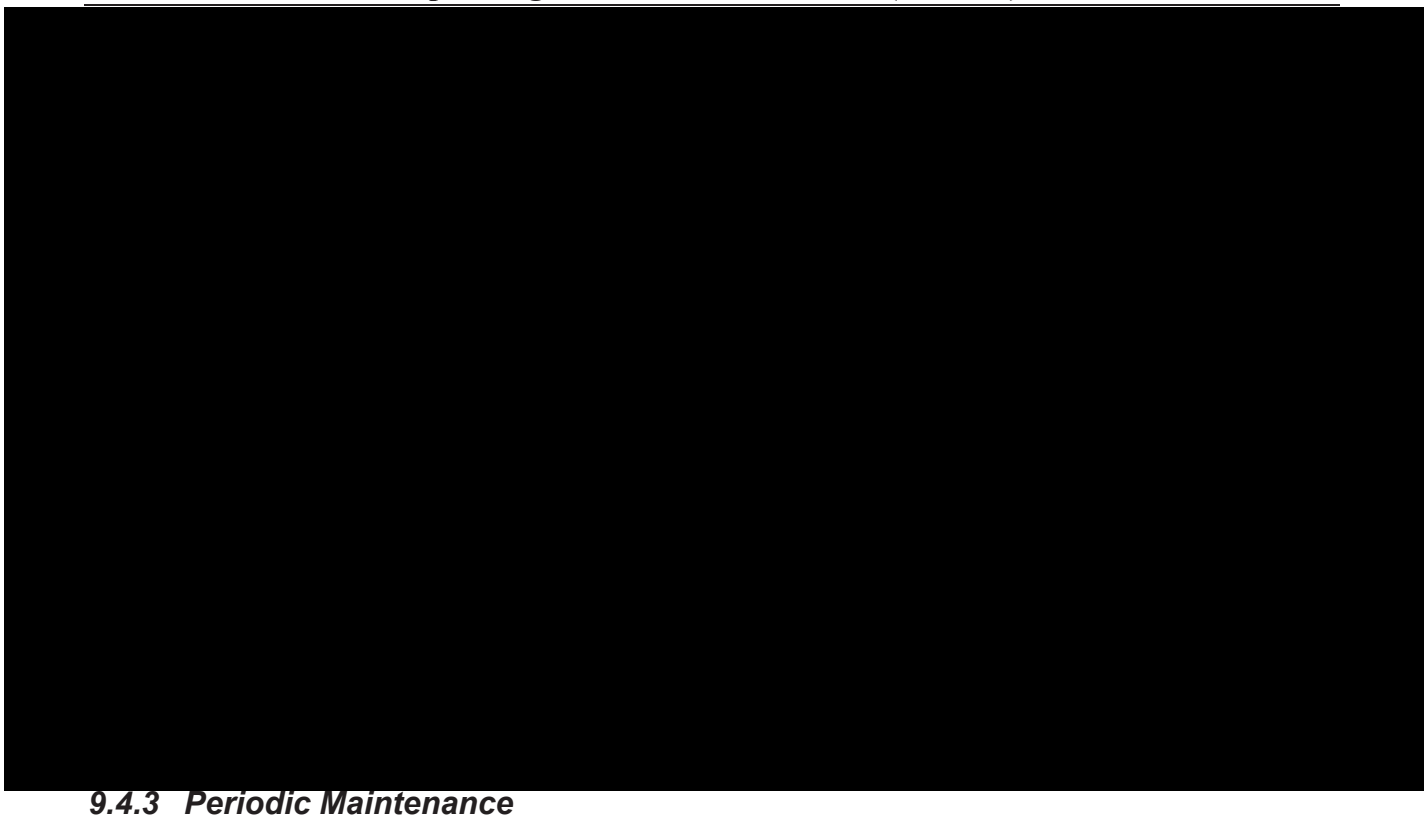
In support of SDMF asset maintenance, there are a series of manuals that define the appropriate instructions and procedures.



9.4.2 SDMF Personnel Responsibilities

The following are the preliminary personnel responsibilities for troubleshooting and resolution of various types of issues.





9.4.3 Periodic Maintenance

The SDMF subsystem is comprised of COTS equipment, data & databases, and software applications.

1. Periodic Maintenance of all COTS equipment is scheduled and performed as recommended by the COTS vendor material. This maintenance is scheduled through the SDMF Maximo.
2. Software, data, and databases do not generally require periodic maintenance. Revisions necessary to support changes to the operation, territory, or to revise software to address any issues are made in accordance with the appropriate Maintenance Manual using the SDMF through the configuration management processes.

10 Appendix C : Communication

Major ACSES communications components maintained the communications department includes:

- BCPs including C-Cases, antennas, and antenna structures
- Network interfaces
- Onboard PTC radios
- Wayside cellular and WiFi equipment
- Office Wayside Communications controller

10.1 Wayside Communications

10.1.1 ACSES Wayside Hardware Components and Interfaces

The following are the primary hardware components and interfaces that are included communication subsystem. Note that some components maybe considered below the LRU-level



[redacted]

10.1.1.1 Communications Maintenance Manuals

In support of Communications asset maintenance, below are a series of manuals that define the appropriate instructions and procedures:

[redacted]

10.1.2 Periodic Maintenance and Testing

This section discusses the tasks associated with required periodic maintenance of all communications equipment and lists the required maintenance intervals for each task.

Under the scope of Maintenance, the key equipment to be supported under this topic are the following:

- L2 and L3 RuggedCom network switches
- Workstation network switches
- Cisco Routers
- Cisco Firewalls
- Cisco Firewall DMZ Zone
- LIRR Optical network(GBN)
- Power supply and UPS
- Batteries

10.1.2.1 Periodic Test

The maintenance performed shall consist of scheduled preventive maintenance, using the manufacturers' suggested preventive maintenance schedules and recommendations.

Components that measurably degrade like batteries should be tested and evaluated by the NMS. Periodic floating current monitoring with a current clamp shall be performed according to battery manufacturer’s recommendation. Battery replacement shall be performed based upon scheduled battery testing results. Reporting of scheduled tests and component and circuit status monitoring should be reported live through telemetry.

10.1.2.2 Preventive Maintenance

Preventive maintenance shall be performed on a schedule consistent with the period as defined in the Preventive Maintenance schedule. Scheduled system inspection and test results shall be maintained and archived in the SDMF and problem items identified and resolved. System

Inspection results and resolutions shall be submitted to the LIRR Support Manager for review and approval. The Support staff shall report infrastructure deficiencies identified during preventive maintenance. Maintenance task includes but not limited to cleaning system equipment, visual checks, tests to verify functional capability and system software upgrades.

10.1.3 Troubleshooting and Issue Resolution

This section discusses activities that may be required to troubleshoot and diagnose various wayside Communication equipment related issues like failure to the BCP, Network and Wayside Antenna's.

The BCM performs the primary communication management functions within the BCP. These functions include, but are not limited to, ACSES message routing, communication network monitoring, PDR Failover, timeslot allocation, and diagnostics. The primary troubleshooting can start by utilizing the Simple Network Management Protocol (SNMP) traps and pinging messages monitored by the Network Management System (NMS).

The Primary Control Center (PCC) and Backup Control Center (BCC) in the office are equipped with a workstation that shows the health of the switches, links, etc. This information can be used during diagnostics and troubleshooting of wayside components. NMS also displays the monitoring BCP Components and links to the network switches. The status of the BCP components can be monitored and automatically alarms in the event of a failure.

CDRL 2-119-209 - Wayside Subsystem Communication identifies Wayside Diagnostics and Troubleshooting, Installing and Configuring Communication Base Communication Manager (BCM) software, PTC Data Radio (PDR) Integration and Replacement Process, Wayside GPS Receiver Replacement Process, Wayside RF Filters and Power Amplifiers Replacement Process. This document also explains C-Case Component Testing Techniques for various failovers.

10.1.3.1 Example Issues

The Various issues that could come up are failure to secondary PDR when Primary radio fails, failure to Dummy Load when VSWR triggers Alarms, Trigger NetGuardian RTU Alarm conditions and RTU Responses, and many more. These troubleshooting, replacement and verification techniques are explained in detail in CDRL 2-119-209 DRAFT (Still in development) (Wayside Subsystem Communication) document for Wayside Communication issues.

10.1.3.2 General Steps and Tools

Corrective maintenance identified by the PTC Support staff shall be performed in timely manner as prioritized by their severity. The support staff shall report to their duty site or remotely log in (if in a network of software support role) within (2) two hours of notification, perform corrective maintenance using procedures identified in the Maintenance Manual.

The Network Management System (NMS) is primarily used by LIRR COMMs and Signals group for maintenance related tasks. NMS monitors the health of the entire PTC communication network, generates alerts and displays information on maintainers' workstation. It monitors the

health of all ACSES II networked devices and interfaces and manages maintenance related alarms.

10.1.3.3 Corrective Maintenance Actions

The support staff shall respond to system failures according to their severity – critical failure and non-critical failure. The response team shall follow the corrective maintenance action plans as identified in the maintenance plan. The action plan shall define the process of assessing the failure class, data collection during troubleshooting and its interpretation and estimated scope and time for restoration. An appropriate response based up on this assessment may be initiating a complete or partial bypass of the PTC system to mitigate service delays, sending out communications to operating groups and the public, etc.

10.2 Office Communications

10.2.1 ACSES Office Hardware Components and Interfaces

The following are the primary hardware components and interfaces that are included in office subsystem. Note that some components maybe considered below the LRU-level for troubleshooting or replacement purposes – see Section 8.3 for additional details.



11 Appendix D. Maintaining ACSES Database

Appendix B describes the process of maintaining the ACSES Database (s). The table below is intended to cross reference each system element under maintenance and its related database(s).

END OF DOCUMENT

Long Island Rail Road
PTC Safety Plan – Warnings and Labels

Docket Number: FRA-2010-0031

DRAFT ONLY

Revision Date: 10-Dec-18

Revision Number: 0.1

Submitted in fulfillment of 49 CFR Part 236, Subpart I, §236.1015, et.al.

REVISION HISTORY

Revision	Date	Description of Changes	Author
0.0	06-Dec-18	Initial Document Draft	W. Alston
0.1	10-Dec-18	Updated Draft to Include: TOC; Revision Field; Title Page; Introduction	W. Alston

Table of Contents

Section Subject Page

Contents

1 Introduction 1

2 Warnings & Labels – WIU Installation and Instruction Manual 2

2.1 Format 2

2.2 Examples – Warnings – WIU 2

2.3 Examples – Cautions – WIU 3

3 Warnings & Labels – Transponder User/Maintenance Manual 5

3.1 Format 5

3.2 Examples – Warnings – Transponder 5

3.3 Examples – Cautions – Transponder 6

List of Figures

Figure 1 – Warning Format – WIU Installation Manual 2
Figure 2 – Example Warnings – WIU Installation Manual 3
Figure 3 – Example Cautions – WIU Installation Manual 4
Figure 4 – Warning Format – Transponder User Manual 5
Figure 5 – Example Warnings – WIU Installation Manual 6
Figure 6 – Example Cautions – Transponder User Manual 6

1 Introduction

This document provides examples of the warnings and warning labels that are used in the User Manuals for the ASCES II System. While this document does not contain every single warning listed in the documents of interest, it does provide examples of the major types of warnings. Documents of interest include:

- Wayside Interface Unit (WIU) Installation and Instruction Manual (Appendix 15-1-2);
- Transponder User/Maintenance Manual (Appendix 15-1-3); and,
- ACSES Onboard Computer (OBC) Service Manual (Appendix 15-1-4).

Each of these manuals is found in full format in the Appendix of the LIRR PTCSP.

2 Warnings & Labels – WIU Installation and Instruction Manual

2.1 Format

Throughout the WIU Installation Manual, notes, cautions, and warnings are frequently used to direct the reader's attention to specific information. These notes, cautions, and warnings have the format shown below.

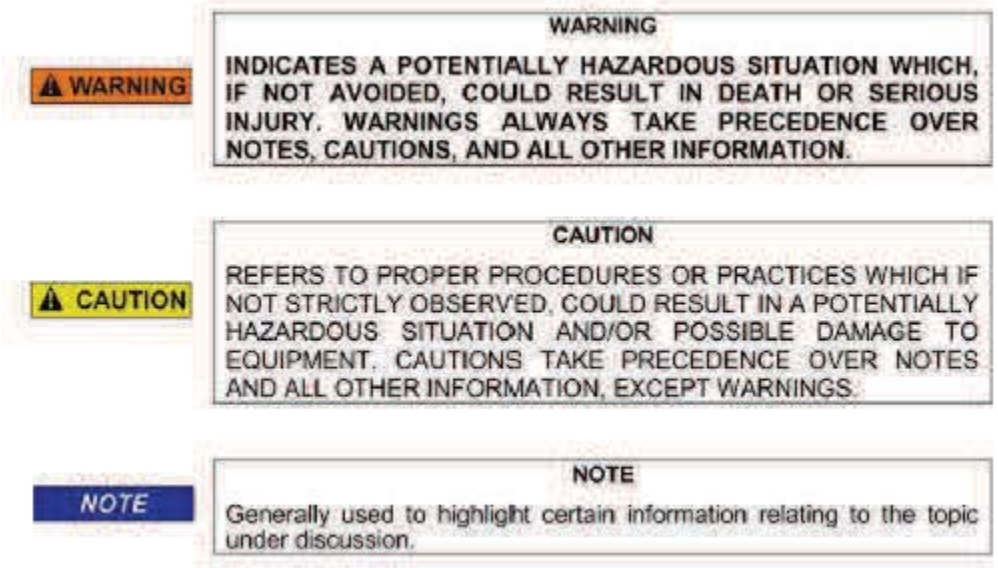
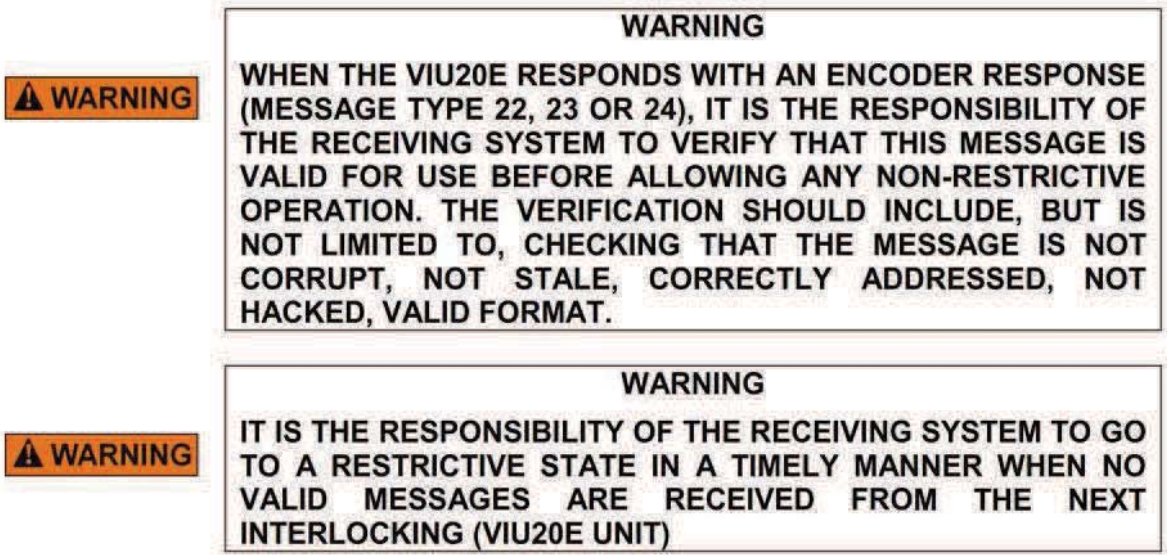


Figure 1 – Warning Format – WIU Installation Manual

2.2 Examples – Warnings – WIU

Warnings provide information with the potential to prevent serious injury to the user.



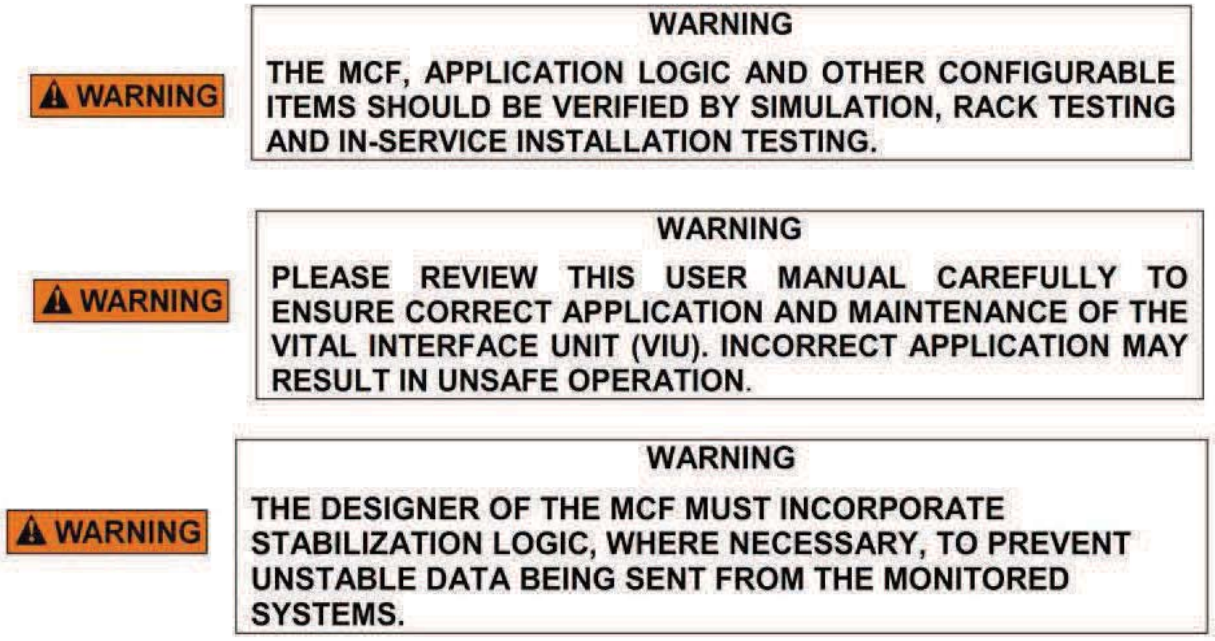
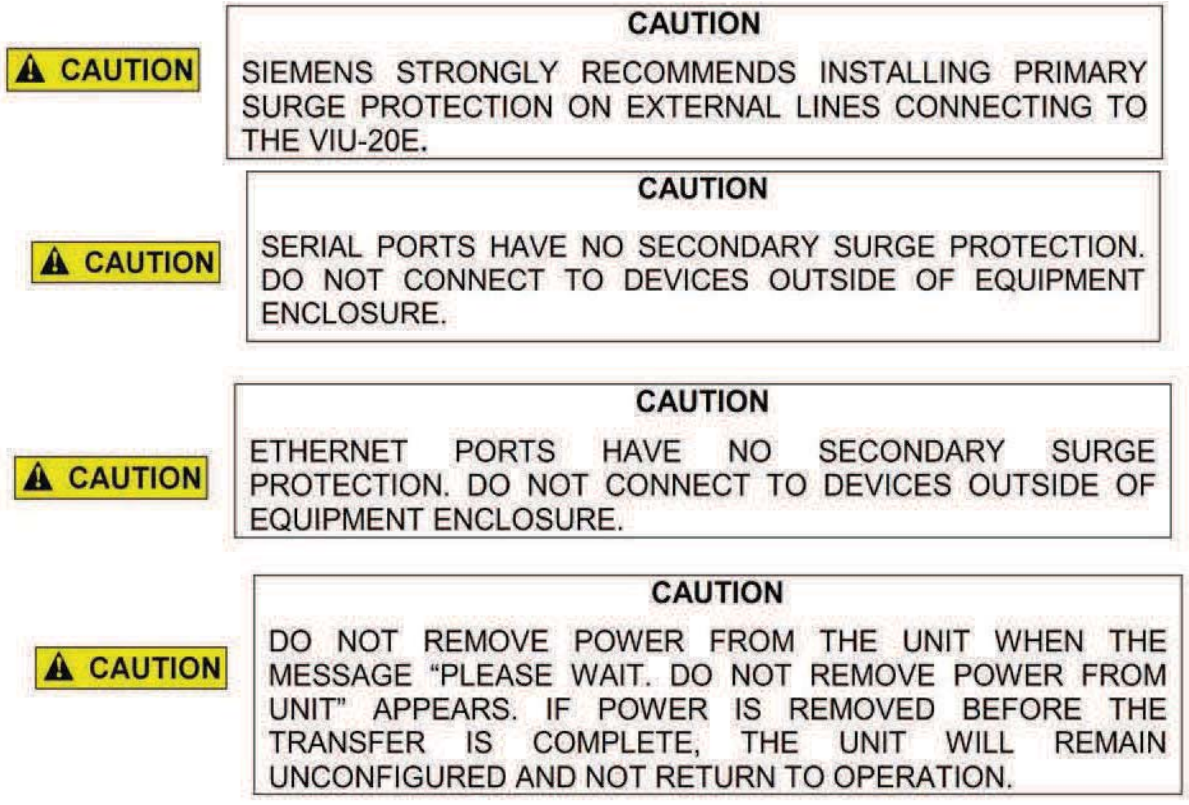


Figure 2 – Example Warnings – WIU Installation Manual

2.3 Examples – Cautions – WIU

Cautions provide information with the potential to prevent damage to the equipment.



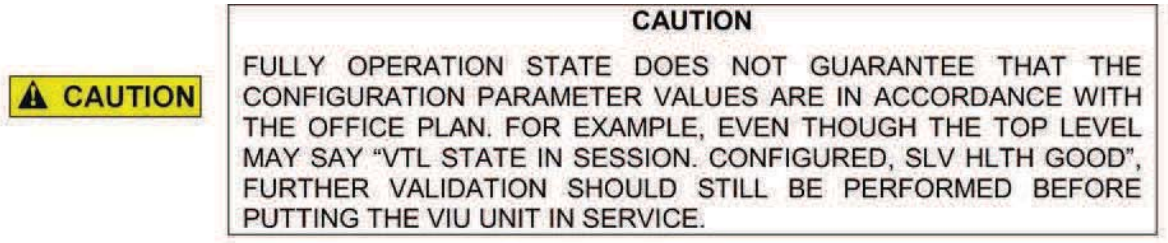


Figure 3 – Example Cautions – WIU Installation Manual

3 Warnings & Labels – Transponder User/Maintenance Manual

3.1 Format

Throughout the Transponder User Manual, warnings, cautions, and notes are used to highlight potentially hazardous situations, critical operating or maintenance procedures, and important facts. Warnings and cautions state the hazard, potential consequences, and result. Those warnings, cautions, and notes are presented as follows:

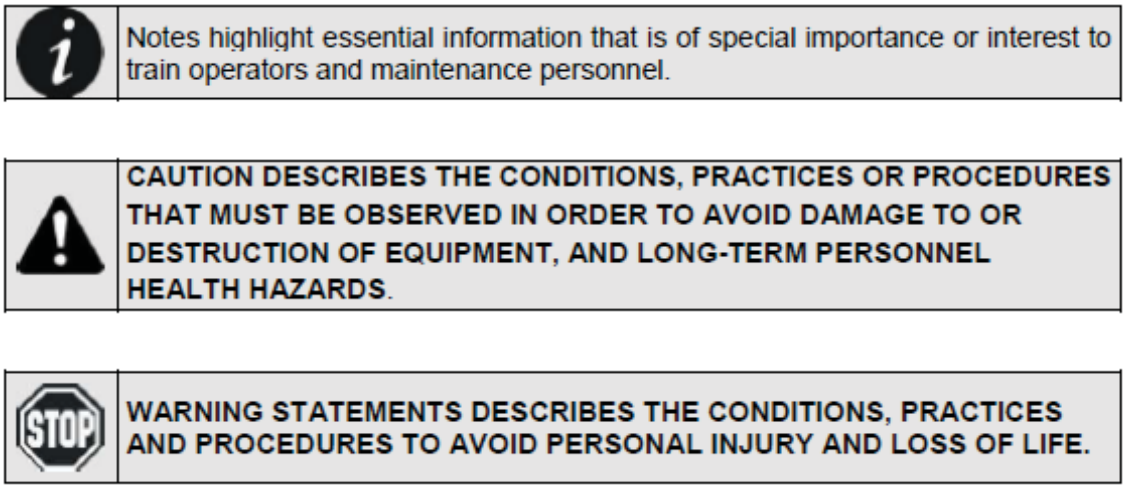
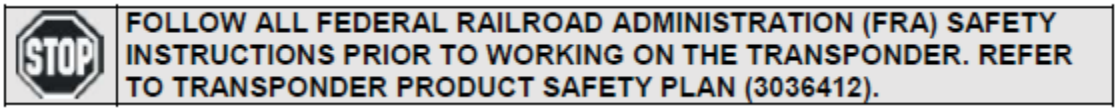


Figure 4 – Warning Format – Transponder User Manual

3.2 Examples – Warnings – Transponder



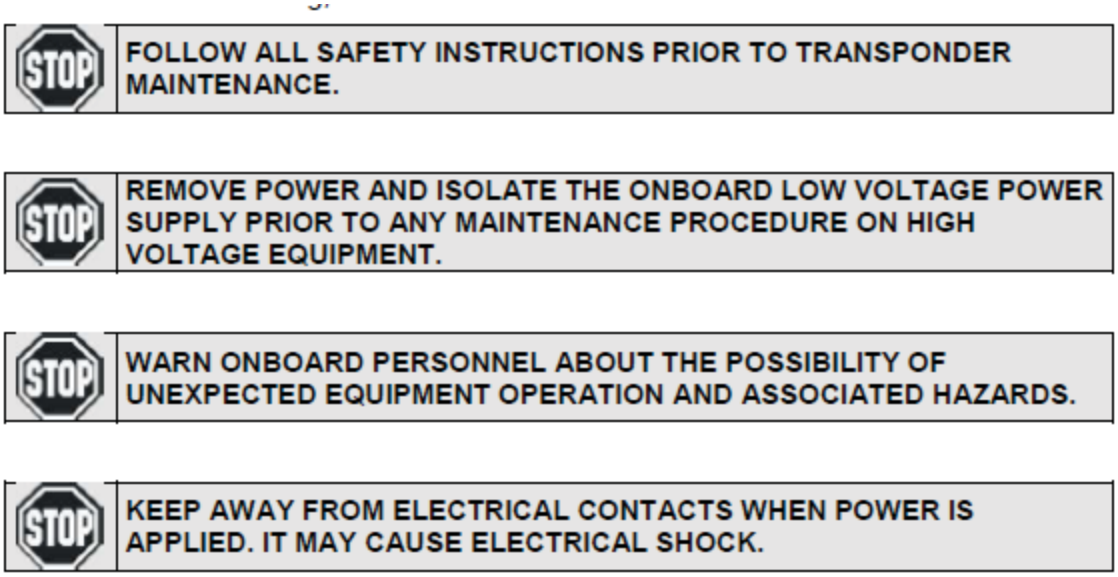


Figure 5 – Example Warnings – WIU Installation Manual

3.3 Examples – Cautions – Transponder

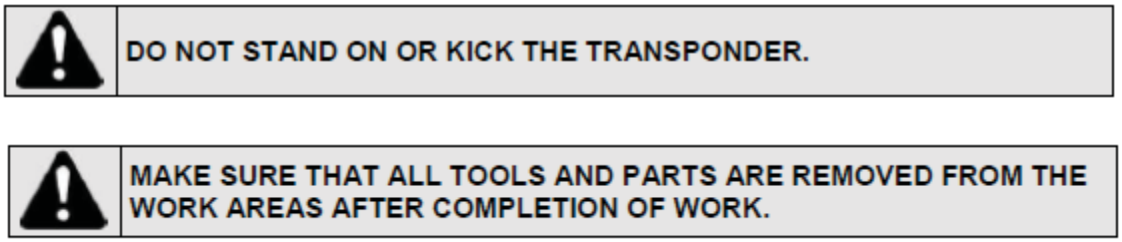


Figure 6 – Example Cautions – Transponder User Manual

Metropolitan Transportation Authority
Long Island Rail Road / Metro-North Railroad
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712/29544

RWPS Subsystem Design Description
CDRL 2-201

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Design	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Smitha Kumar RWPS S/W Lead	Smitha.k	2018-04-23
Verified:	Emily Macklin System Engineer	Emily Macklin	2018-04-23
Approved:	Balamurugan Thangaraj Project Engineer	T. Bn	2018-04-23
SI Quality Process Review:	JL Bright for Bon Provenzano BT Quality Assurance Group	JL Bright	2018.04.25 12:16:12 -04'00'
BT/SRA Review:	Rick Galloway Chief Engineer		2018.04.25 12:00:29 -04'00'
BT/SRA Review:	NA Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2018, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2018 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3035851

Effective Date:	Revision:	Language:
2018-04-23	_C	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2014-03-07	First issue
_A	2014-07-14	Incorporated CDR Comments
_B	2014-10-16	Updated L2 Drawings, Added RWPS Redundancy
_B.1	2017-12-01	Rewritten the content based on the ConOps and recent discussions
_B.2	2018-01-19	Addresed Review comments provided for _B.1
_C	2018-04-23	Addresed Review comments provided for _B.2 Removed RWPS NMS and altered content to accommodate Office NMS monitoring RWPS subsystem Addressed internal review comments Added Void/Undelete TSR Below section that were included as part of original white paper in which different approaches were compared is been removed • Section 2.9.4: Requirement Compliance • Section 3: System Hierarchy is being removed. This is covered as part of the Requirements Management Plan. • Section 6: Network Traffic Analysis • Section 7: Application level Traffic Analysis • Section 8: Pros and cons is being removed as we are not weighing two different approaches

Table of Contents

Section	Subject	Page
1	**Executive Summary**	5
1.1	**Reference Documents**	5
1.2	**Glossary**	5
2	**RWPS Design Approach – Per Vol 2 part I Specification**	6
2.1	**Purpose**	6
2.2	**Architecture**	6
2.3	**RWPS to Office Interfaces**	8
2.4	**Functions**	9
2.4.1	TSR Management	10
2.4.1.1	Request TSR List	10
2.4.1.2	Request TSR request	11
2.4.1.3	Annul/Cancel TSR request	13
2.4.1.4	Void TSR request	15
2.4.1.5	Undelete TSR request	16
2.4.2	EIC Access Assignment	18
2.4.2.1	Attach Secondary EIC to TSR	19
2.4.2.2	Attach Secondary EIC to TSR by Primary EIC	21
2.4.2.3	Remove Secondary EIC from TSR	23
2.4.2.4	Remove Secondary EIC from TSR by Primary EIC	25
2.4.2.5	Transfer Ownership	27
2.4.2.6	Super user Functions	29
2.4.2.6.1	Requesting for Secondary EIC removal	29
2.4.2.6.2	Transfer Ownership	30
2.4.2.6.3	Annul/Cancel TSR	32
2.5	**User Roles and Responsibilities**	34
2.6	**Design Assumptions**	35
2.7	**Hardware Design Details**	36
2.8	**Cyber Security for EIC Devices Communication**	36
2.9	**Software Design Details**	37
2.9.1	Security	37
2.9.2	Safety	37
2.9.3	Redundancy	37
3	**Functional Description**	37
4	**RAM Analysis**	38

List of Figures

Figure 1: Approach - Per Vol 2 part I Specification 7
Figure 2: RWPS to Office Interfaces 8
Figure 3: TSR List 10
Figure 4: Request TSR 12
Figure 5: Annul/Cancel TSR 14
Figure 6: Void TSR 16
Figure 7: Undelete TSR 17
Figure 8: Attach Secondary EIC to TSR 19
Figure 9: Attach Secondary EIC to TSR by Primary EIC 21
Figure 10: Remove Secondary EIC from TSR 23
Figure 11: Remove Secondary EIC from TSR by Primary EIC 25
Figure 12: Ownership Transfer 27
Figure 13: Super user Secondary EIC removal 29
Figure 14: Superuser Transfer Ownership 31
Figure 15: Superuser Annul/Cancel TSR 33

List of Tables

Table 1: Reference Documents 5
Table 2: RWPS Prediction 40

1 Executive Summary

The Roadway Worker Protection System provides protection to the Employees-In-Charge (EIC) by providing functionality for the Roadway workers/Employee in Charge (EIC) to implement manage and report speed restrictions to protect work zones on the Right-of-Way (ROW).

This document describes the design approach of the RWPS system as per contract.

Note: In document the terms RWIC (Roadway worker-In-Charge) and EIC (Employee-In-Charge) are used interchangeably.

1.1 Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624
[2]	RWPS Message Description Document	3051894

Table 1: Reference Documents

1.2 Glossary

Please refer to the Dictionary of Terms and Acronyms [1].

2 RWPS Design Approach – Per Vol 2 part I Specification

The architecture for this approach is per contract to deliver separate RWPS subsystem that resides outside of Office Subsystem network.

2.1 Purpose

The purpose of RWPS system is to protect Roadway Worker through Temporary Speed Restriction (TSR). The RWPS system will provide the ability to Roadway Worker in Charge(RWIC)/Employee in Charge(EIC) to create and manage TSR's. Below is the list of high-level features of RWPS

- TSR Management
- EIC Access Assignments
- Alerts and Alarms
- Admin functions – Function Assignment, Configuration settings

2.2 Architecture

The Figure 1 shows the basic architecture of the RWPS and Office Subsystem at the Primary Control Center. The RWPS within the Backup Control Center is a replica of the RWPS within the Primary Control Center.

The RWPS and Office Subsystem is configured as an independent network entity. The RWPS subsystem communicates directly to the ACSES Office subsystem, it does not communicate with adjacent Railroad servers nor any other ACSES subsystem (inclusive of the OBC) directly.

The ACSES II RWPS subsystem consists of the following high-level components:

- Workstations for all user access to the RWPS system. Workstations are installed in several locations including the primary and backup office locations and remote EIC locations.
- Redundant RWPS Servers for managing all RWPS terminals, EIC terminals and operator commands into the RWPS system.
- RWPS Security Server (RWPS SEC) for managing all security software installed on the RWPS system.
- Redundant RWPS Data and Maintenance System (RWPS DMS) servers for logging data and managing the data logs for all RWPS subsystems, including messages from the EIC to the RWPS and feedback from the ACSES II Office system to EIC terminals.
- Redundant Office Network Management System (Office NMS) servers for monitoring all networked RWPS devices including RWPS subsystem servers.
- Redundant RWPS Active Directory Domain Controller (RWPS ADDC) servers for managing all authorized users of the RWPS system.
- Firewalls for providing protection to the RWPS network and remote EIC terminals.
- Backup RWPS Office system for providing disaster recovery if the primary office exhibits a catastrophic failure.
- Switches for routing messages on the RWPS network.
- Wi-Fi access point for filling coverage gaps of Third Party cellular coverage.
- EIC Terminals – including handhelds, truck mount and wayside terminals.

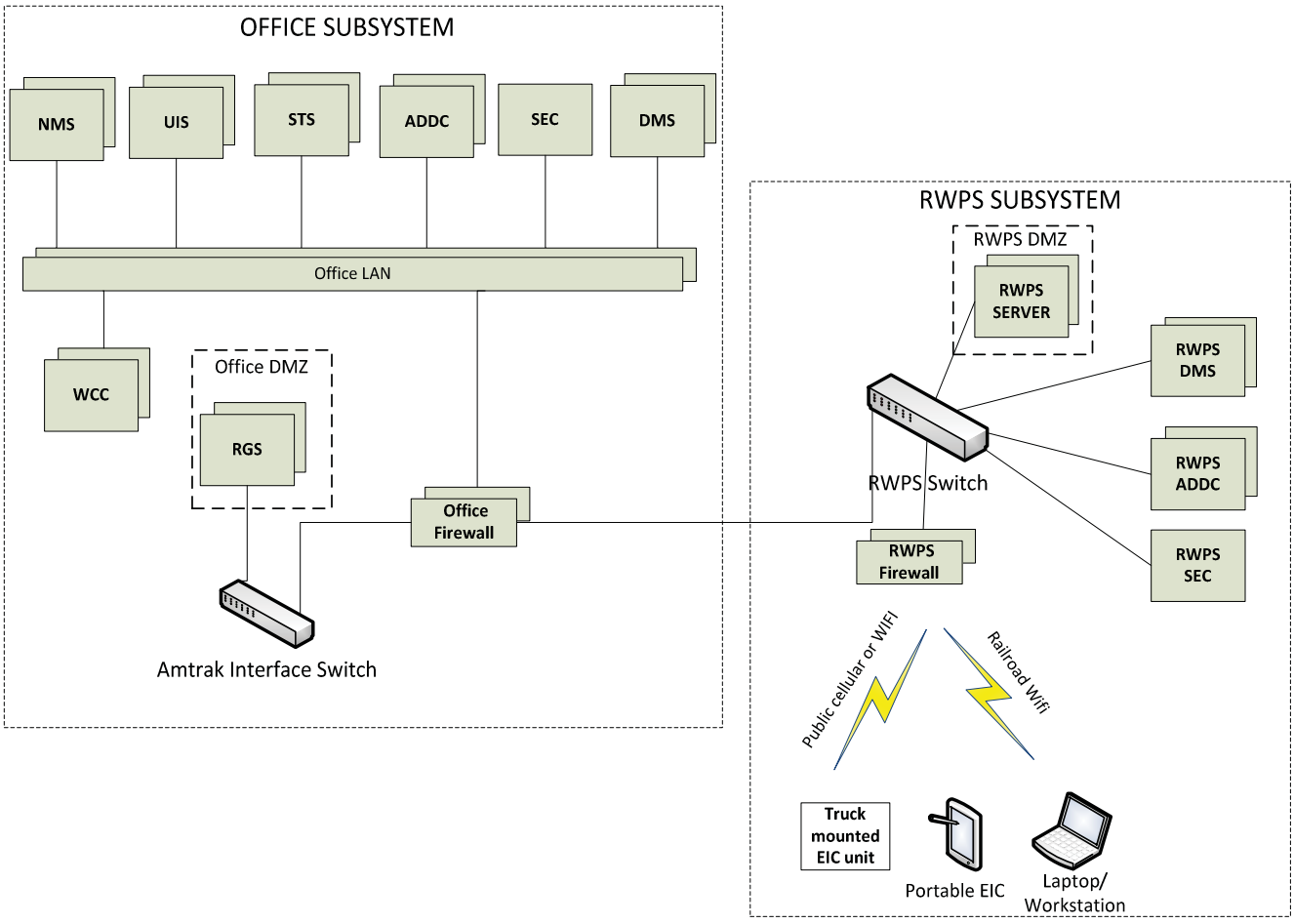


Figure 1: Approach - Per Vol 2 part I Specification

Note: All the redundant components are shown with the shadow boxes. In the above architecture diagram only, SEC component is not redundant.

2.3 RWPS to Office Interfaces

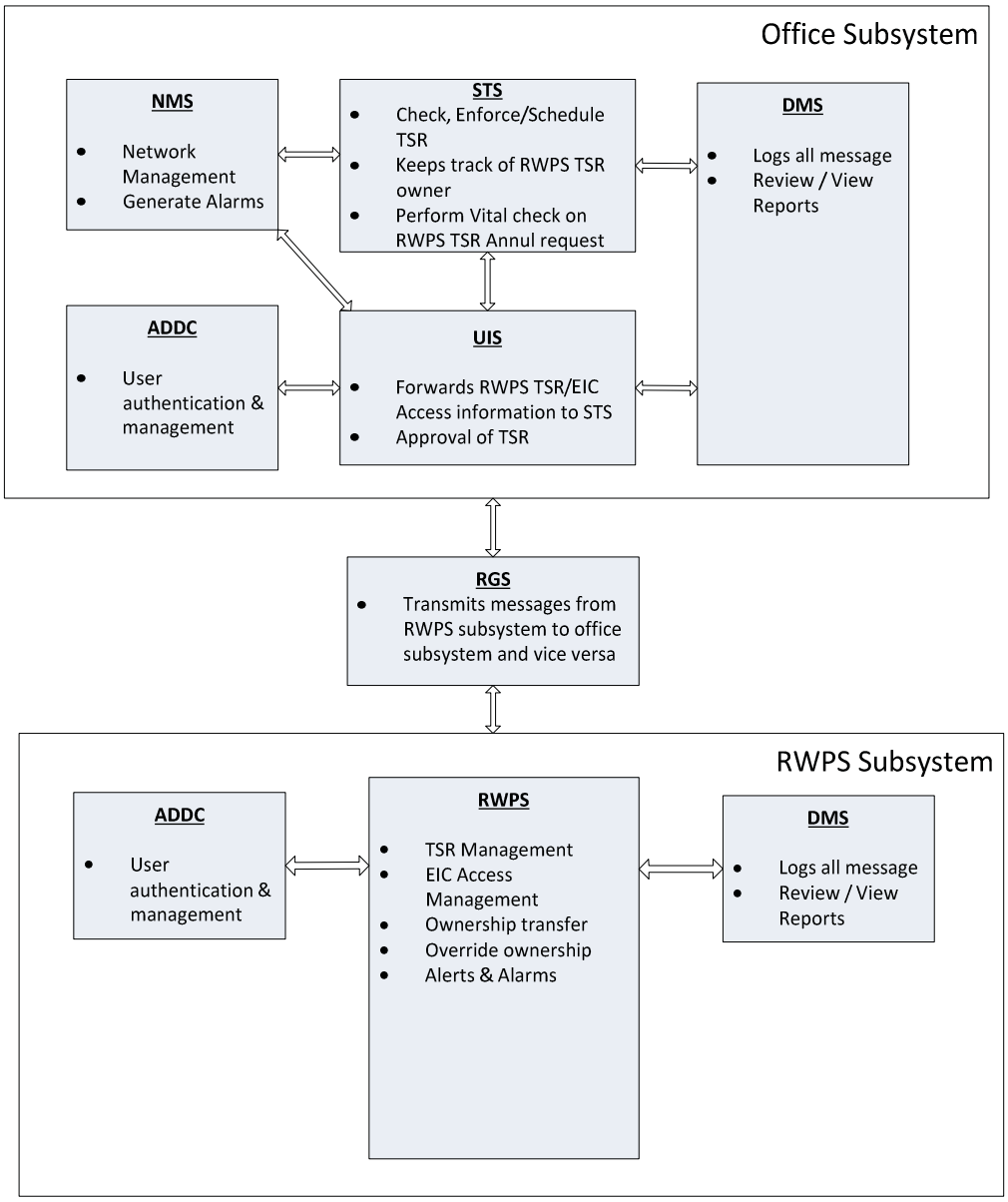


Figure 2: RWPS to Office Interfaces

The above diagram explains the component specific features w.r.t RWPS functionalities and interaction with other components.

RWPS Subsystem

- RWPS Server: The RWPS server is responsible for TSR management, EIC Access assignment, alerts & Alarms and providing system admin functionalities.
- ADDC: The RWPS ADDC is responsible for user authentication and management. RWPS server communicates with RWPS ADDC to validate users.

- DMS: The RWPS DMS is responsible for logging data and managing the data logs.

Office Subsystem

- UIS: The UIS is responsible for forwarding TSR/EIC access messages to STS. UIS Approver has the capability to approve RWPS TSR's, once TSR has been checked by STS.
- STS: The STS will check/enforce the RWPS TSR's. Also, STS will do a vital check on Annul TSR request by storing primary owner information.
- DMS: The office DMS is responsible for logging data and managing the data logs
- NMS: The office NMS is responsible for monitoring all networked Office and RWPS devices including office and RWPS subsystem servers.
    - Monitoring all networked Office and RWPS devices is through ping and SNMP polls. Office NMS will directly communicate to the devices for the monitoring
    - Monitoring Office server applications is through ACSES heartbeat messages. NMS will log the data to Office DMS
    - Monitoring RWPS server applications is through ACSES heartbeat messages and these messages are routed through RGS. NMS will log the data to Office DMS. Since the heartbeat messages should go through RGS from RWPS subsystem to Office subsystem, the delay in heartbeat is slight higher i.e. 1 or 2secs instead of 500ms. The heartbeat delay is configurable and by default the delay is 1sec.
    - NMS will write all the data to Office SQL server

The RWPS server communicates with the UIS server through the RGS.

Note: Refer RWPS MDD [2] for message details between components.

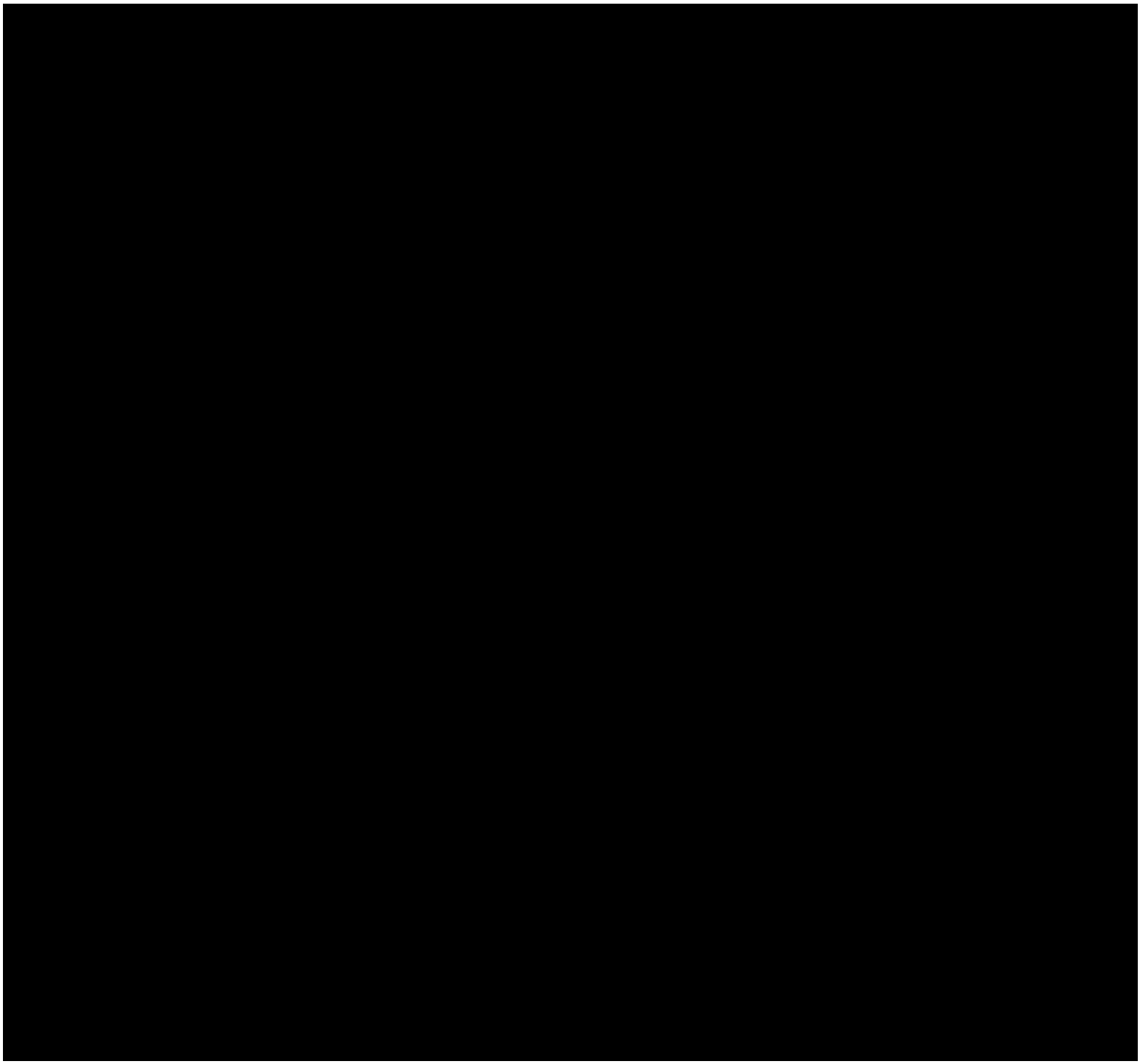
2.4 Functions

RWPS system provide EIC's to perform below major functionalities

1. TSR Management
    - Request TSR List
    - Create TSR request
    - Annul/Cancel TSR request
2. EIC Access Assignment
    - Attach Secondary EIC to TSR
    - Attach Secondary EIC to TSR by Primary EIC
    - Remove Secondary EIC from TSR
    - Remove Secondary EIC from TSR by Primary EIC
    - Transfer Ownership
    - Super user functions
        - Secondary EIC removal (Act as secondary EIC in case of unavailability of secondary EIC)
        - Ownership Transfer (Act as primary EIC in case of unavailability of primary EIC)

- Annul/Cancel TSR (Act as primary EIC in case of unavailability of primary EIC)

For all the functions listed EIC's is required to confirm the request prior to processing. Sequence diagram for each function are captured below







2.6 Design Assumptions

- Overlapping of TSR's are supported between UIS and RWPS
- 1500 TSR's will be the maximum number of TSR's that the PTC system supports
- Attaching/Removing Secondary EIC from the TSR can be performed only on Enforced/Scheduled TSRs
- During the Attachment of Secondary EIC's to TSR, the user who initiates the request will set the work limits.

  Example: If Primary EIC is attaching secondary EIC, then primary EIC will set the work limits. If Secondary EIC is requesting for attachment, then secondary EIC will set the work limits.

- Primary EIC can attach 'N' secondary EIC's for the same work limit. There will 'N' requests created for 'N' users and these requests are processed and tracked separately.
- System Administrator can configure 'Maximum number of Secondary EIC's' that can be attached to a single TSR
  - The default value for 'Maximum number of Secondary EIC's' is 10
  - The 'Maximum number of Secondary EIC's' that can be attached to a single TSR is 50
- Primary EIC can remove 'N' secondary EIC's at the same time. There will 'N' requests created for 'N' users and these requests are processed and racked separately.
- RWPS subsystem will support only line boundary TSRs. Once line boundary TSRs are created each TSR is managed individually. There are no grouping of TSRs supported
- RWPS subsystem does not support Predefined TSRs
- TSR ID generation is part of RWPS sub system. Since RWPS System can generate unique TSR ID, there would be no need for two components to generate ID and confirm. This will add more hops to TSR workflow.

  Every TSR has STS generated ID and UIS/RWPS generated ID respectively. UIS/RWPS generated TSR ID is only used to keep track in UIS/RWPS respectively. The TSR List data is in sync between UIS and RWPS, by using this UIS/RWPS generated TSR ID. User can identify the source of the TSR by looking at the ID. If ID starting with 1 then TSR is originated from UIS. If ID starting with 2 then TSR is originated from RWPS.

2.7 Hardware Design Details

The EIC handheld terminals are connected to RWPS servers located in control centers (PCC and BCC) through cellular, private/public Wi-Fi, or Railroad's ground-based network.

Field EIC Portable Terminal devices are comprised of:

- EIC Portable Handheld devices:
  - Smartphone minimum 5.5-inch resolution
  - Tablet minimum 10-inch resolution
- Truck mounted units / Wayside-located units mounted at interlocking's and designated stations
  - Windows Workstation



2.9 Software Design Details

2.9.1 Security

RWPS SEC along with the firewalls and switches provides Virus protection, Malware protection, intrusion detection, and denial of service protection and alerts. The Architecture and Description for RWPS Security Subsystem is similar same as that of to the Office Security, however it is configured for RWPS.

2.9.2 Safety

Additional verification considered in the system by having STS verify the origination of the TSR request. When UIS sends TSR request originated from RWPS to STS it will include additional information in the message regarding the request origination, so that STS can verify the origination when the removal of the TSR is requested.

This is to make sure the removal of TSR that the RWPS requested is originated from RWPS user not from UIS user and STS will verify that the user who has created the TSR is the one removing it.

Message details is updated to include this additional field in the messaging between UIS and STS.

Note: This needs to be discussed with the Safety team and this is not Part of the specification.

2.9.3 Redundancy

The RWPS subsystem is replicated in both the PCC and BCC. The RWPS, DMS, NMS, ADDC are redundant within a Control Center and across Control centers, where there is only one Security server per Control Center.

The RWPS servers acts as master within RWPS subsystem and communicates across control center. The RWPS Servers is configured to monitor the health of DMS servers located in the same control center to determine the switchover condition. The PCC active RWPS Servers exchange health check with BCC active RWPS server. Fail to receive health check triggers the non-controlling RWPS to become controlling.

The controlling and active RWPS servers exchange messages to office servers through RGS.

The SQL server used by the RWPS servers and DMS are configured with always on cluster across control center. The data replication is taken care automatically by the SQL server configuration and only one server node is available to read/write for the applications.

The four ADDC servers are configured to be active node in both control centers. The availability of single ADDC server provides the user authentication function and user account management. The ADDC changes are replicated to all other ADDC servers automatically.

3 Functional Description

The following are the list of primary functions of the RWPS.

- **EICs logon/logoff authentication:** ADDC server authenticates the EIC that login/logoff to an EIC Terminal by means of user name and password. All user attempts to logon/logoff, EIC Terminal ID, and current user position data is sent to DMS for all requests.
  The RWPS applies a timeout to all users by locking the application. Time out period is configurable by the System Administrator. Default Timeout period is set to 10mins.
- **TSR List Display:** The RWPS will communicate to UIS for the active TSR list when EIC requests for TSR list.
- **ADD TSR:** The authorized Primary EIC is able to create TSR via the EIC terminal. The TSR will go through the Select-Check Execute process for implementation.
- **Annul/Cancel TSR**: The Primary EIC has the capability to Annul/Cancel the TSR via EIC Terminal if there are no secondary EICs attached to the TSR.
- **Attach/Remove secondary EICs to the existing TSR**: Authorized Employee(s) has the capability to be included or removed in an existing TSR as a secondary EIC via their EIC Terminal. The process will require approval from the Primary EIC.
- **Transfer the work zone ownership to another primary EIC or secondary EIC**
- **A special functionality to Superuser to Annul/Cancel the TSRs:** Authorized superusers is provided capability to Annul/Cancel the TSRs initiated by an EIC in case of unavailability of the EIC.
- **Data Validation:** All data received by the RWPS Server (and other equipment) is validated against the RWPS database. The Validation criteria is to verify data correctness and to check that all mandatory data are filled.
- **Alerts and Alarms**
- **Data Monitoring and Logging:** All activity, including all data messaging and communication with EIC Terminals and the components is logged, and time stamped within the DMS.
- **Data Security**
- **RWPS Database of Railroad**: The RWPS has complete database of Railroad topology generated through the ACSES II SDMF. All drawings and software files is stored and maintained on the SDMF within Rational Team Concert. When an update to a RWPS takes place, the source files will first be retrieved from the SDMF.

4 RAM Analysis

Logistics savings related to the reduction of equipment can be found Table 2: below.

Metropolitan Transportation Authority
Long Island Rail Road / Metro-North Railroad
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712/29544

RWPS System Safety Concept Description
CDRL 2-124-06

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Aaron Graham Safety Engineer	Aaron Graham	2017.12.11 13:31:41 -05'00'
Verified:	Jason Weighley Safety Engineer	Jason W Weighley	2017.12.11 15:13:15 -05'00'
Approved:	Anthony DeFrancisco Project Director	Anthony S	12/11/17
SI Quality Process Review:	Bon Provenzano BT Quality Assurance Group	Bon Provenzano	2017.12.11
BT/SRA Review:	NA Title		
BT/SRA Review:	NA Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2017, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2017 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3036417

Effective Date:	Revision:	Language:
2017-12-11	_C	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2014-03-18	First issue
_A	2014-08-27	Updated disclaimer on signature page
_B	2015-07-30	Updated according to PDR comments from the customer.
_B.1	2017-11-17	Updated for FDR
_B.2	2017-12-05	Updated per RR comments, SI-RVW 0212
_C	2017-12-11	Updated for document release

Table of Contents

Section	Subject	Page
1	Executive Summary	5
2	Introduction	5
2.1	Compliance Matrix	6
2.2	References	10
2.3	Glossary	11
3	RWPS Description	11
3.1	Vital Enforcement of Operating Modes	12
3.2	Radio Transmission of Vital Data	13
3.3	Dependency on Database Data	13
3.4	Dependency on Existing Railway Vital Train Control Systems	13
3.5	Component Description	13
3.5.1	RWPS ADDC	13
3.5.1.1	Vital Processing Equipment	13
3.5.1.2	Fail Safe Response to Failures of Safety Critical Equipment	13
3.5.2	RWPS Security Server	13
3.5.2.1	Vital Processing Equipment	13
3.5.2.2	Fail Safe Response to Failures of Safety Critical Equipment	13
3.5.3	RWPS NMS	14
3.5.3.1	Vital Processing Equipment	14
3.5.3.2	Fail Safe Response to Failures of Safety Critical Equipment	14
3.5.4	RWPS Server	14
3.5.4.1	Vital Processing Equipment	14
3.5.4.2	Fail Safe Response to Failures of Safety Critical Equipment	14
3.5.5	RWPS Workstation	14
3.5.5.1	Vital Processing Equipment	14
3.5.5.2	Fail Safe Response to Failures of Safety Critical Equipment	14
3.5.6	Employee In Charge Terminal	14
3.5.6.1	Vital Processing Equipment	15
3.5.6.2	Fail Safe Response to Failures of Safety Critical Equipment	15
3.5.7	Data Management System (DMS)	15
3.5.7.1	Vital Processing Equipment	15
3.5.7.2	Fail Safe Response to Failures of Safety Critical Equipment	15
3.5.8	Local Area Network (LAN)	15
3.5.8.1	Vital Processing Equipment	15
3.5.8.2	Fail Safe Response to Failures of Safety Critical Equipment	16
3.5.9	De-militarized Zone (DMZ)	16
3.5.9.1	Vital Processing Equipment	16
3.5.9.2	Fail Safe Response to Failures of Safety Critical Equipment	16
3.5.9.3	Vital Processing Equipment	16

3.5.9.4 Fail Safe Response to Failures of Safety Critical Equipment 16
3.5.10 RWPS Firewall 16
3.5.10.1 Vital Processing Equipment 16
3.5.10.2 Fail Safe Response to Failures of Safety Critical Equipment 16
3.6 Methods used to protect Databases 17
4 Conclusion 17

List of Tables

Table 1: Compliance Matrix 6
Table 2: Reference Documents 10
Table 3: Acronyms Specific to this Document 11
Table 4: SIL Allocation 12

1 Executive Summary

The RWPS Subsystem performs the functions of sending TSR requests and lists to and from the EIC terminals and workstations. This functionality is implemented through its interface to the Office subsystem. The PHA [R1] looked at this functionality and the failures of the interfaces and determined that the functionality performed by the RWPS did not require mitigations from the RWPS.

2 Introduction

This document describes the safety concepts and techniques to be applied to the design of the RWPS, RWPS Interfaces and RWPS Data. The document will detail each component of the RWPS and its interfaces and data and need to apply safety concepts to each component, interface or data. Since the PHA [R1] has only defined the RWPS Database as a safety critical (SIL 4) element within the RWPS subsystem, the interface analysis will examine the external interfaces only and any security issues with internal interfaces.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part 1	12.10.1.1	A.	Description The ACSES II Subsystem suppliers shall submit a System Safety Concepts Document, CDRL 2-124. This document shall describe the ACSES II Subsystem suppliers application of the system level concepts which assure ACSES II System safety, specifically: fail-safe design (hardware and software) approaches used in the implementation of processor-based safety-critical equipment; operational safeguards; and methods of ensuring safety-critical data integrity. ACSES II vital functions must be implemented using concepts, which can be verified as being both correct and sufficiently robust to mitigate the hazards of the system.	All
Vol 2 Part 1	12.10.1.1	B.	The safety concepts for processor-based system shall be in accordance with FRA 49 CFR 236 Subpart I, Appendix C and the IEEE Standard for verification of Vital Functions in Processor-Based Systems 1483-2000.	3.5.1.2

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part 1	12.10.1.1	C.	The System Safety Concepts Document shall explain the safety design approach and underlying principles at the system level and at the safety-critical subsystem level. The System Safety Concepts Document shall define the design methodologies upon which the implementation of the requirements will be based, consistent with the stated concepts. Safety concepts which address the following topics shall be discussed, as a minimum, in the System Safety Concepts Document:	All
Vol 2 Part 1	12.10.1.1	C.	1. Dependence on the existing vital train control system, such as interlocking indications, cab signal system;	3.4
Vol 2 Part 1	12.10.1.1	C.	2. Dependence on the accuracy of stored information in databases, such as Track Topography Data supplied by the Railroad. This discussion shall describe how databases and associated data which affect safe system performance will be determined to correctly and completely represent the physical status of the ACSES II System and applicable parameters of the existing subway system.	3.3

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part 1	12.10.1.1	C.	3. Methods used to protect the vital contents of databases from corruption in their development, programming, and installation in the ACSES II equipment. All safety critical databases, their functions and data parameters, shall be identified.	3.3
Vol 2 Part 1	12.10.1.1	C.	4. Radio transmission of vital data, including any error detection/correction schemes, between wayside/train, train/train, and wayside/wayside. The safety assurance of data transmitted on the radio frequency data link shall be discussed in detail, identifying the necessary calculations and testing to demonstrate that the level of vital error detection and data integrity is sufficient to achieve an adequate level of safety.	3.2

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part 1	12.10.1.1	C.	a. The need or absence of need for vital design, specific safety analysis, test, and/or operating/maintenance procedures to achieve safety of the data communications link shall be discussed. The quantifiable measures to be applied to the protection shall be identified (e.g., vital protection for “n” bits in error). The margin of protection against environmental effects and electromagnetic interference shall be projected for later validation.	3, 3.1
Vol 2 Part 1	12.10.1.1	C.	5. Vital processor-based equipment performing safety-critical functions.	N/A
Vol 2 Part 1	12.10.1.1	C.	6. Fail-safe hardware providing vital inputs to ACSES II or execution of ACSES II outputs.	N/A
Vol 2 Part 1	12.10.1.1	C.	7. Vital enforcement of ACSES II operating modes, and fail-safe response to failures of safety-critical ACSES II equipment.	3.1

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part 1	12.10.1.1	C.	8. Dependence on partitioning of the system into vital subsystems, vital interfaces, and subsystems which are non-vital, and the rationale for determining vital and non-vital subsystems. Based on the partitioning of functions, those subsystems performing vital functions, thus requiring fail-safe implementation shall require detailed safety analysis.	3.5

.

2.2 References

Table 2: Reference Documents

Id.	Title	Ref.
[R1]	Preliminary Hazard Analysis CDRL 2-127-06	3035821
[R2]	Dictionary of Terms and Acronyms	3035624
[R3]	RWPS Subsystem Design Description CDRL 2-201	3035851
[R4]	Railway Applications – Communication, signaling and processing systems – Safety related electronic systems for signaling	EN-50129
[R5]	Railway Applications – Communications, Signaling and Processing Systems – Software for railway control and protection systems	EN-50128
[R6]	System Vulnerability Assessment CDRL 2-137	3035840
[R7]	FRA –Safety Assurance criteria and processes	49 CFR 236, APP C
[R8]	IEEE standard for Verification of Vital Functions in Processor-Base Systems used in Rail Transit Control	IEEE STD 1483-2000
[R9]	System Safety Software V&V Plan, CDRL 2-11	3035711
[R10]	RWPS Product Safety Plan CDRL 2-123-06	3036415
[R11]	Office Subsystem Safety Concept Description CDRL 2-124-02	3036410
[R12]	Human Factor Analysis CDRL 2-025	3035722
[R13]	Office Subsystem Design Description, CDRL 6-1 and 6-2	3035943 3035944

Id.	Title	Ref.
[R14]	RWPS Database Verification Report MNR DCRL 2-133-16	3043888
	RWPS Database Verification Report LIRR CDRL 2-133-26	3043889

2.3 Glossary

Acronyms only related to this document are listed below in Table 3. For additional Terms and acronyms, please refer to the Dictionary of Terms and Acronyms, [R2].

Table 3: Acronyms Specific to this Document

Acronym	Definition
ADDC	Active Directory Domain Controller
COTS	Commercial Off-the-Shelf
DMS	Data Management System
DMZ	De-Militarized Zone
EIC	Employee In Charge
NMS	Network Management System
RWPS	Roadway Worker Protection Subsystem
STS	Safety TSR Server
TSR	Temporary Speed Restriction
UIS	User Interface System

3 RWPS Description

The RWPS is fully defined in the RWPS Subsystem Design Description [R3]. RWPS consists of the following components: RWPS ADDC, RWPS Security Server (SEC), RWPS NMS, RWPS Server, RWPS Workstation, DMS, LAN, DMZ, Employee In Charge (EIC) Terminal, and the RWPS Firewall. Several versions of the Employee In charge terminal will be developed from a truck based solution, portable terminal and wayside terminal each with the same functionality.



The allocation of components listed above are to be confirmed by future analysis. The RWPS system allows track maintenance personnel to request temporary speed restrictions. It provides the qualified EIC along the Right-of-Way (ROW) that are responsible for work within the clearance envelope of the mainline to request TSR application, modification, and removal. A detailed functional description is described in the RWPS Subsystem Design Description [R3].

Aside from the RWPS database, the functions and components of RWPS are not Safety Critical, and this system safety concept will describe the safety functions and features of the system that allow the RWPS to be a non-safety critical subsystem. So, the scope of this document is limited on identifying the safety concept and its requirements and techniques to be applied to the design to ensure safety.

3.1 Vital Enforcement of Operating Modes

The RWPS Subsystem does not enforce any PTC Operating modes and only allow track maintenance personal to request temporary speed restrictions.

3.2 Radio Transmission of Vital Data

All data transmitted is between non-vital Subsystems. A security analysis of authenticating EIC terminal that connect over the public internet via public Wi-Fi and cellular services will be performed. EIC Terminal to RWPS server will be protected by a VPN with proper encryption and authentication protocols. This analysis will be described in detailed in the System Vulnerability Assessment [R6].

3.3 Dependency on Database Data

Common Track/MAP database for the safety critical data between the exchange to UIS and STS. The RWPS/EIC must compare its database version with the STS database version to ensure they are the same. The EIC Track/MAP database will be downloaded from the RWPS server at login. The maximum login time of an EIC will be 24 hours, forcing an update of checked download. Should a static check being performed by the RWPS fail, then the RWPS must ignore all future TSR requests to be sent to UIS and TSR List Responses to EIC Terminals.

3.4 Dependency on Existing Railway Vital Train Control Systems

No dependency on any components to existing vital train control systems exists.

3.5 Component Description

3.5.1 RWPS ADDC

Authenticates and defines the roles of users on the system. Not a safety critical function.

3.5.1.1 Vital Processing Equipment

Not applicable.

3.5.1.2 Fail Safe Response to Failures of Safety Critical Equipment

Not applicable.

3.5.2 RWPS Security Server

COTS Server with COTS Security Software that manages application software and monitors network traffic to detect and respond to security threats. The Hardware and software used for this application are not vital.

3.5.2.1 Vital Processing Equipment

Not applicable.

3.5.2.2 Fail Safe Response to Failures of Safety Critical Equipment

Not applicable.

3.5.3 RWPS NMS

Stores and collects network packets and polls network equipment for alarms and events to be indicated for maintenance. Not a safety critical function.

3.5.3.1 Vital Processing Equipment

Not applicable.

3.5.3.2 Fail Safe Response to Failures of Safety Critical Equipment

Not applicable.

3.5.4 RWPS Server

COTS Hardware with specialized software that allows the Employee in charge terminals to request TSRs from the UIS. The TSR list will be passed through the UIS along with the CRC, so that the CRC can ensure the TSR list is not corrupted while being sent to the RWPS server. The RWPS will compare the TSR list ID every 500 ms, and any mismatch will be corrected by reloading the TSR list. Even without any mismatches, an updated TSR list is requested and sent to the UIS and RWPS databases periodically (Time TBD) in order to reload the TSR list.

3.5.4.1 Vital Processing Equipment

Not applicable.

3.5.4.2 Fail Safe Response to Failures of Safety Critical Equipment

Not applicable.

3.5.5 RWPS Workstation

COTS Hardware with specialized software that allows the Employee in charge terminals to request TSRs from the UIS. The workstation shall be designed as per requirement in Vol. 6, Sec. 6.6.2.4. The human factor activities will be described in detail in the Human Factor Analysis [R12]

3.5.5.1 Vital Processing Equipment

Not applicable.

3.5.5.2 Fail Safe Response to Failures of Safety Critical Equipment

Not applicable.

3.5.6 Employee In Charge Terminal

Hardware and software that will allow authorized employees to request TSR's from remote locations. There are 3 types of terminals being used and they are as follows:

1. EIC Portable Terminals.

2. EIC Wayside Terminals
3. EIC Truck Mounted Terminals

The three (3) types shall be in accordance to the requirement specification Vol.2.14.5.3.6

TSR approval will still be via UIS and STS. Select – Check – Execute will mitigates any failures of the EIC equipment. The STS shall confirm that a remove request for a TSR was generated from the primary EIC assigned to that TSR. Modification of the TSR with a Primary EIC assigned must also be from the Primary EIC. Changing of the assignment from Secondary to Primary and adding Secondary EIC does not require STS approval or tracking. Protected data from the RWPS server is sent to the EIC terminal using an HTTP checksum (which runs TCP/IP in the background) to detect any corruption of data. Any EIC terminals communicating by cellular service or Wi-Fi is protected via VPN encryption AES 256. EIC database will be downloaded from RWPS server at login. To ensure that the EIC database is up to date, the EIC must be logged out after 24 hours.

3.5.6.1 Vital Processing Equipment

Data storage functions are safety critical. Suspected failures in data storage is protected by COTS hardware and daily reboot/reloads. COTS hardware is not safety-critical.

3.5.6.2 Fail Safe Response to Failures of Safety Critical Equipment

Not applicable.

3.5.7 Data Management System (DMS)

As the data control center solution, the DMS shall be designed in accordance to Vol.6, Sec.6.2.4. Redundant pairs will be installed in the PCC and BCC RWPS Office.

3.5.7.1 Vital Processing Equipment

Not applicable.

3.5.7.2 Fail Safe Response to Failures of Safety Critical Equipment

Not applicable.

3.5.8 Local Area Network (LAN)

The Networks provides a secure, highly available, reliable and autonomous LAN to interconnect the elements of the RWPS Office to ACSES UIS, Railroad Fiber Backbone Network and to commercial wireless services. The necessary firewalls and switches will assure security of the interfaces.

3.5.8.1 Vital Processing Equipment

Not applicable.

3.5.8.2 Fail Safe Response to Failures of Safety Critical Equipment

Not applicable.

3.5.9 De-militarized Zone (DMZ)

This component provides security for interfaces between the EIC terminal and RWPS servers. This interface will be implemented through public Wi-Fi, internet and cellular networks. To provide proper security and protection of the data over this interface engineering will implement a VPN with encryption that assures data protection and authentication of equipment connecting to the server.

3.5.9.1 Vital Processing Equipment

Not applicable.

3.5.9.2 Fail Safe Response to Failures of Safety Critical Equipment

To provide proper security and protection of the data over this interface engineering will implement a VPN with encryption that assures data protection and authentication of equipment connecting to the server.

3.5.9.3 Vital Processing Equipment

Not applicable.

3.5.9.4 Fail Safe Response to Failures of Safety Critical Equipment

Not applicable.

3.5.10 RWPS Firewall

This component provides protection to the RWPS network and remote EIC terminals. Though RWPS firewalls are enabled with Internet, security wise all servers are protected because none of the servers are hosted in the Internet. Only RWPS application servers (like local LAN) has been given to EIC user once he/she connected in VPN. Everything else is blocked.

3.5.10.1 Vital Processing Equipment

Not applicable.

3.5.10.2 Fail Safe Response to Failures of Safety Critical Equipment

Not applicable.

3.6 Methods used to protect Databases

The methods being used to protect the vital contents of the databases from corruption in their development, programming, and installation in the ACSES II equipment will be detailed in the RWPS Database Verification Report [R14]. A CRC must be added to the Track/MAP Database to confirm that the data stored is not corrupted. The evidence of the results from the verification and validation methods performed will also be released in the RWPS Database Verification Report [R14].

4 Conclusion

The RWPS SSCD presents the basis, in accordance to the FRA-Safety Assurance criteria and processes [R7], IEEE Standard for Verification of Vital Functions in Processor-Based Systems [R8], CENELEC Standards EN 50129 [R4] and EN 50128 [R5] for demonstrating a convincing and a comprehensive argument for the Safety of the LIRR/MNR PTC Project.

Metropolitan Transportation Authority
Long Island Rail Road / Metro-North Railroad
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712/29544

RWPS Subsystem
Operating Hazard Analysis
CDRL 2-130-06

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Report	Project	Released

Prepared:	Aaron Graham System Safety Engineer	Aaron Graham	2018.04.23 14:13:17 -04'00'
Verified:	Jason Weighley System Safety Engineer	Jason W Weighley	2018.04.23 16:16:20 -04'00'
Approved:	Anthony DeFrancisco Project Director	Anthony DeFrancisco	4/24/18
SI Quality Process Review:	Bon Provenzano BT Quality Assurance Group	M. Bon	2018.04.24 13:27:38 -04'00'
BT/SRA Review:	NA		
BT/SRA Review:	NA Title		
	Name / Title, Group	**Signature**	**Date**

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2018, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2018 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3037424

Effective Date:	Revision:	Language:
2018-04-23	_A	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2015-09-24	First issue
__.1	2018-03-15	Updated per RR comments
__.2	2018-03-28	Updated per RR comments
__.3	2018-04-13	Updated per RR comments
__.4	2018-04-20	Updated per RR comments
_A	2018-04-23	Updated for release

Table of Contents

Section	Subject	Page
1	Executive Summary	5
2	Introduction	5
2.1	Objective	7
2.2	Scope	7
2.3	Compliance Matrix	8
2.4	Reference Documents	10
2.5	Glossary	13
2.6	Document Updates	14
2.7	RWPS Subsystem Overview	14
3	OHA Activity	14
3.1	Methodology	14
3.2	People who interact with the RWPS Subsystem	15
3.3	The Hazard Risk Index	16
3.4	Hazard Tracking	16
4	RWPS Subsystem OHA Table	17
4.1	Summary of Interfaces	18
4.2	Operating Scenarios Considered	19
4.3	OHA Table	20
4.4	Operating/Safety Requirements	28
5	Conclusion	30

List of Figures

Figure 1: RWPS Subsystem OHA Process Context 6
Figure 2: RWPS OHA Method 15

List of Tables

Table 1: Required Input Documents 6
Table 2: Compliance Matrix 8

Table 3: Reference Documents 10
Table 4: Terms Specific to this Document 13
Table 5: Acronyms Specific to this Document 13
Table 6: RWPS OHA Table Column Headings and Description 17
Table 7 : RWPS Subsystem OHA table 20
Table 8:Operating/Safety Requirements 28

1 Executive Summary

This document records the RWPS Subsystem Operating Hazard Analysis (OHA) of the LIRR and MNR PTC systems. This analysis of the interactions between the RWPS subsystem and people in the course of RWPS operation, installation, maintenance, includes operation under degraded modes and failure conditions. It defines procedures to develop the operational and\or maintenance manual documents to operate the PTC system on the right of way. The analysis evaluates the severity and frequency and identifies the causes of hazardous events in order to develop safety mitigation. These identified safety mitigations are translated into design, safety operations and/or maintenance manual requirements, as necessary to achieve acceptable final risk. The identification of OHA hazards extend the preliminary and system level hazard analysis of hazards resulting from subsystem design, procedure design, or human errors.

Preliminarily, the OHA suggests procedural mitigations. When safety analyses are complete, they also identify human interaction. When manuals are produced they will be reviewed to close previously determined mitigations, as well as to identify new hazards.

All identified hazards will be maintained in the System Hazard Log [10] for tracking and proper closure.

2 Introduction

As described in the RWPS Subsystem Product Safety Plan [1], the Operating Hazard Analysis (OHA) is an analysis of the potential hazards at human-machine interfaces involved in the operation, maintenance, and installation of the PTC System of the LIRR/MNR projects. This OHA is mainly focused on at the RWPS subsystem level operating hazard analysis. Once all the subsystem OHAs are finalized and approved, all the OHAs including the system level OHA [6] will be incorporated into the system level master hazard log [10]. This RWPS OHA is developed in accordance with guidance derived from MIL-STD-882C [13] for the execution of Operating and Support Hazard Analysis.

As cited in the System SPSP [3] Section 6.4.3.7, each subsystem will produce its own Operation Hazard Analysis that will analyze human operation interfaces, rules, processes, installation procedures, maintenance procedures, and external data that are relied upon to mitigate certain subsystem hazards.

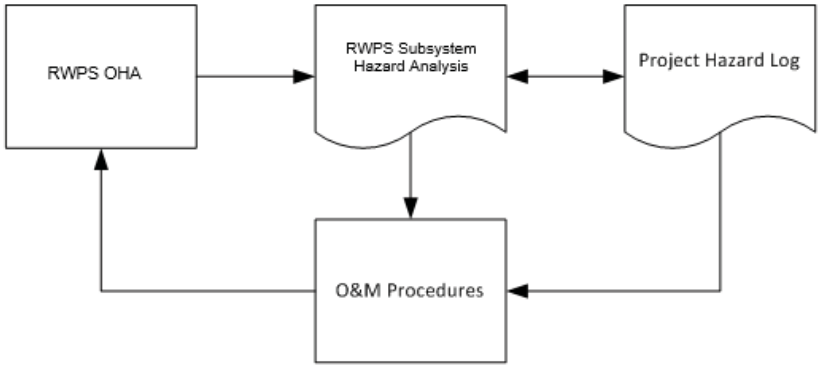


Figure 1: RWPS Subsystem OHA Process Context

Figure 1 represents the context of the RWPS Subsystem OHA. For the wider context of the system hazard analysis flow, see Figure 8 in the system SPSP [3].

Table 1: Required Input Documents

Safety Document	Required Inputs from Project	Comments
RWPS Operating Hazard Analysis	System Operating Hazard Analysis [6] RWPS Preliminary Hazard Analysis [7] RWPS Subsystem Design Description [5] System Operating Context Description (SyOCD) By Railroads [14] LIRR Operating Procedures (Rule Book) [14] Final Human Factors Analysis [12] NORAC Rule Book [15] Proposed, Modify, and/or new rules and procedures	Iteration: prelim OHA suggests procedural mitigations. When safety analyses are complete, they also identify human interaction When manuals are produced they will be reviewed to close previously determined mitigations as well as to identify new hazards.

Failures due to outside influences that cannot be detected and/or controlled by the PTC system such as earthquake, fire, flood, evacuation, or terrorist acts are out of the scope of this analysis, as stated in the System PHA [4].

2.1 Objective

The purpose of the RWPS Subsystem Operating Hazard Analysis (OHA) is to identify and analyze hazards associated with personnel and procedures during application, installation and testing, operation, and maintenance of the RWPS Subsystem. Mitigations are not limited to procedural corrective or preventative measures, and may include design changes when required. The OHA is conducted on all tasks and human actions (Section 3.2), including acts of omission and commission, by persons interacting with the subsystem, and assembling of the subsystem. The primary purpose of the OHA is to establish and document the fact that all hazards related to human interaction with the RWPS subsystem have been effectively mitigated.

Another outcome of the OHA is a set of recommendations for corrective or preventive measures to be taken to minimize the possibility that any human error or procedure will result in injury or system damage.

These measures include recommendations for:

- Hazards inherent in system level operating and support activities;
- Changes needed in functional or design requirements for subsystem hardware/software, facilities, tooling, or support/test equipment to eliminate or control hazards or reduce associated risks;
- Warnings, cautions, and special emergency procedures, including those necessitated by failure of a computer software-controlled operation, to produce the expected and required safe result or indication;
- Requirements for storage, transportation, maintenance, and disposal of hazardous materials;
- Requirements for safety training and personnel certification;

Following completion of this RWPS OHA, the System Safety Engineer is responsible for ensuring that all identified hazards (and associated recommendations for corrective or preventive measures) are included in the Hazard Log [10]. Hazard tracking and control, including tracing through to the appropriate system level requirements is in accordance with the SPSP [3] section 6.2.4.

2.2 Scope

This Subsystem OHA will identify and assess hazards associated with Human-Machine Interfaces of the RWPS subsystem. This activity is prescribed by the OHA requirements of the System SPSP [3] Section 6.4.3.7.

Operation and support activities include:

- Normal operation;
- Failure management and recovery;
- Installation, preventative and corrective maintenances;

As cited in SPSP [3] Section 6.4.3.7, each subsystem will produce its own Operation Hazard Analysis that will analyze human operation interfaces, rules, processes, installation procedures, maintenance procedures, and external data that are relied upon to mitigate certain subsystem hazards.

Failures due to outside influences that cannot be detected and/or controlled by the PTC system such as earthquake, fire, flood, evacuation, or terrorist acts are out of scope of this analysis, as stated in the PHA [4].

2.3 Compliance Matrix

Table 2: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol.2	12.10.5 A to C	Operating Hazard Analysis	An Operating Hazard Analysis (OHA), CDRL 2-130, shall be performed to analyze the interface between humans and the ACSES II System, including all systems and subsystem.	Section 2
		A.	The SI shall include operating rules and procedures applicable to the service delivery using the ACSES II System. Mitigation shall include identification of new or modified operating rules and procedures. The writing of the actual rule modifications and/or new procedures is not required.	Section 4.2, 4.4
		B.	Operations performed by the Train Engineer, maintenance staff, or other the Railroad personnel shall be considered, as well as system support and maintenance activities which have an impact on ACSES II safety assurance. The purpose of the OHA is to identify those specific procedural requirements that protect passengers and/or personnel from hazards.	Section 3.2, OHA Table (applicable records)

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
		C.	The Operating Hazard Analysis shall be performed and documented on all ACSES II System and Subsystems. The OHA identifies and evaluates hazards associated with operation and maintenance of the system. It shall consider the system configuration, the system state, phase of activity, environment, support equipment and all other factors that could affect operational and support safety. The OHA shall address, as applicable:	Table 7, Table 8, Section 4.2
			1. Facilities, support equipment, training and certification related to safety operations and maintenance;	Table 7
			2. Activities, which occur under hazardous conditions, time periods, and the actions necessary to minimize risks;	OHA Table
			3. Changes in functional or design requirements needed to eliminate or control hazards or reduce associated risks;	Sec. 4
			4. Requirements for safety devices and equipment;	OHA Table

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
			5. Warnings, cautions, and special emergency procedures;	OHA Table
			6. Requirements for packaging, handling, transportation, maintenance, and disposal of any hazardous materials;	N/A
			7. Requirements for safety training and personnel certification;	OHA Table Table 8
			8. Effects of commercial equipment, both hardware and software, across the interface with other components or subsystems;	OHA Table
			9. Potentially hazardous system states under operator control (hardware/software).	OHA Table

2.4 Reference Documents

Table 3: Reference Documents

Reference Number	Document Name	Identification Number
[1]	RWPS Product Safety Plan CDRL 2-123-06	3036415
[2]	Dictionary of Terms and Acronyms	3035624
[3]	Systems Product Safety Plan (SPSP) CDRL 2-123-20	3035815

Reference Number	Document Name	Identification Number
	System Product Safety Plan (SPSP) CDRL 2-123-10	3036467
[4]	Systems Preliminary Hazard Analysis CDRL 2-127	3035821
[5]	RWPS Subsystem Description Document CDRL 2-201	3035851
[6]	System Level Operating Hazard Analysis CDRL 2-130-20 CDRL 2-130-10	3035826 3043906
[7]	RWPS Subsystem Preliminary Hazard Analysis CDRL 2-127-06	3036416
[8]	RWPS Subsystem Hazard Analysis CDRL 2-128-06	3037401
[9]	RWPS Interface Hazard Analysis CDRL 2-131-06	3037436
[10]	System Project Hazard Log CDRL 2-126-20 System Project Hazard Log CDRL 2-126-10	3035819 3043891
[11]	System Level Requirements	3036443
[12]	Human Factors Analysis, CDRL 2-025-20 Human Factors Analysis CDRL 2-125-10	3035722 3052704
[13]	MIL-STD-882_C	
[14]	LIRR/MNR Contract 1712 Positive Train Control Volume 2 – PTC Systems Integrator Specification	Rev 1.0 Part 1 & Part 2
[15]	NORAC Rules Book	
[16]	Lesson Plan: Course 16 - ACSES II RWPS User Training Program (MNR) CDRL 2-116-116	3037871
[17]	Lesson Plan: Course 17 - ACSES II RWPS Maintenance Training Program (MNR) CDRL 2-116-117	3037872
[18]	Lesson Plan: Course 16 - ACSES II RWPS User Training Program (LIRR) CDRL 2-116-216	3037888

Reference Number	Document Name	Identification Number
[19]	Lesson Plan: Course 17 - ACSES II RWPS Maintenance Training Program (LIRR) CDRL 2-116-217	3037889
[20]	Instructor's Guide: Course 16 - ACSES II RWPS User Training Program (MNR) CDRL 2-118-116	3037905
[21]	Instructor's Guide: Course 17 - ACSES II RWPS Maintenance Training Program (MNR) CDRL 2-118-117	3037906
[22]	Instructor's Guide: Course 16 - ACSES II RWPS User Training Program (LIRR) CDRL 2-118-216	3037922
[23]	Instructor's Guide: Course 17 - ACSES II RWPS Maintenance Training Program (LIRR) CDRL 2-118-217	3037923
[24]	Participant's Guide: Course 16 - ACSES II RWPS User Training Program (MNR) CDRL 2-119-116	3037939
[25]	Participant's Guide: Course 17 - ACSES II RWPS Maintenance Training Program (MNR) CDRL 2-119-117	3037940
[26]	Participant's Guide: Course 16 - ACSES II RWPS User Training Program (LIRR) CDRL 2-119-216	3037956
[27]	Participant's Guide: Course 17 - ACSES II RWPS Maintenance Training Program (LIRR) CDRL 2-119-217	3037957
[28]	Electronic Training Materials: Course 16 - ACSES II RWPS User Training Program (MNR) CDRL 2-120-116	3037973
[29]	Electronic Training Materials: Course 17 - ACSES II RWPS Maintenance Training Program (MNR) CDRL 2-120-117	3037974
[30]	Electronic Training Materials: Course 16 - ACSES II RWPS User Training Program (LIRR) CDRL 2-120-217	3037990

Reference Number	Document Name	Identification Number
[31]	Electronic Training Materials: Course 17 - ACSES II RWPS Maintenance Training Program (LIRR) CDRL 2-120-217	3037991
[32]	Training Aids: Course 16 - ACSES II RWPS User Training Program (MNR) CDRL 2-122-116	3038007
[33]	Training Aids: Course 17 - ACSES II RWPS Maintenance Training Program (MNR) CDRL 2-122-117	3038008
[34]	Training Aids: Course 16 - ACSES II RWPS User Training Program (LIRR) CDRL 2-122-216	3038024
[35]	Training Aids: Course 17 - ACSES II RWPS Maintenance Training Program (LIRR) CDRL 2-122-217	3038025

2.5 Glossary

Please refer to the Dictionary of Terms and Acronyms [2]. Terms and acronyms only related to this document are listed below in Table 3 and Table 4 respectively.

Table 4: Terms Specific to this Document

Term	Definition
Operation	Series of functions and tasks that are involved in a single process.

Table 5: Acronyms Specific to this Document

Acronym	Definition
OHA	Operating Hazard Analysis
PSP	Product Safety Plan
PHA	Preliminary Hazard Analysis
DSP	Dispatcher
EIC	Employee In Charge

2.6 Document Updates

This Operating Hazard Analysis is a living document and will be reviewed and updated as necessary throughout the LIRR project development lifecycle. Circumstances requiring an update to the OHA would include, for example, significant changes to the project functions, architecture, or design. Any update to this OHA will be produced, verified and approved by the System Safety Engineer.

2.7 RWPS Subsystem Overview

Please refer to RWPS Subsystem Description Document [5].

3 OHA Activity

Top Level Hazards considered:

- Collision
- Derailment
- Staff Injury or Death
- Property Damage
- Security Breach

3.1 Methodology

The identification of hazards extend the preliminary and system level hazard analysis to analyze interactions between the RWPS subsystem and people. Information from source documents is referenced for traceability, and is not duplicated to prevent inconsistencies in documentation as the project matures.

The methods used in this OHA to identify hazards are:

- Analysis of operations and support scenarios from the operators' perspective to identify hazards;
- Assess identified hazards on a per Operating Scenarios basis and populate the OHA Table;
- Review of other documentation:
    1. Review of System Level Requirements Specification [11] for requirements allocated for the RWPS Safety Analysis and for verification;
    2. Review of hazards in the Subsystem PHA [7] and SSHA [8] that are mitigated by operating and support activities.

The hazards are assessed in accordance with the hazard risk assessment and acceptance criteria as defined in the SPSP [3].

The mitigations are recommended in accordance with the safety criteria as defined in the SPSP [3].

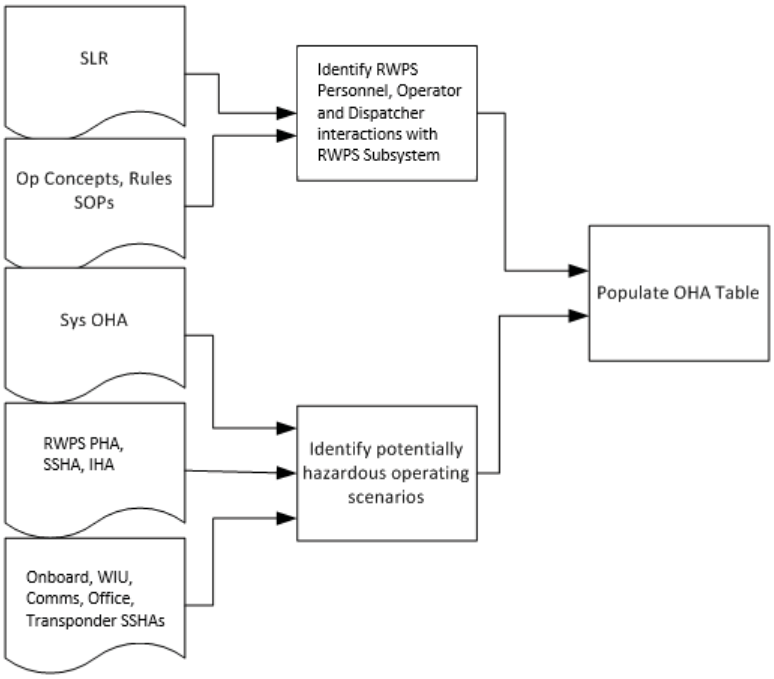


Figure 2: RWPS OHA Method

3.2 People who interact with the RWPS Subsystem

The following people are identified as personnel who involve in the operation of the PTC system. These roles are further explained in the Human Factor Analysis [12] and the RWPS SDD [5]:

- **Employee In Charge(EIC):** Roadway worker that is responsible for requesting TSR's and providing status of TSR's for a specific section of the system that has Roadway workers present.

- **Dispatcher (DSP):** The DSP manages and monitors the PTC system operation strictly following operating procedures. The PTC system will normally operate without the DSP's intervention in ACSES II Control Mode. During abnormal, failure or emergency scenarios, the DSP may be required to intervene to ensure the safety of the PTC system (MNR refers to this role as RTC).

- **Maintenance Staff:** The Maintenance staff performs planned preventive maintenance activities and corrective maintenance activities to restore the PTC system operation from a failure condition. The maintenance activities are governed by maintenance procedures which contain cautions and warnings to ensure safety.

- **Chief Dispatcher (CDSP):** The CDSP manages the requests and duties of the DSP by strictly following operating procedures. The PTC system will normally operate without the CDSP's intervention in ACSES II Control Mode. During abnormal, failure or emergency scenarios, the CDSP may be required to intervene to ensure the safety of the PTC system.

- **Operations Supervisor (OS):** The OS manages the operations of the EIC's. The PTC system will normally operate without the OS's intervention in ACSES II Control Mode. During abnormal, failure or emergency scenarios, the OS may be required to intervene to ensure the safety of the PTC system.

- **System Administrator:** The System Administrators are responsible for managing RWPS configuration, user management, group policies, Database backup and recovery, system configurable parameters adjustment, and report templates creation

- **System Maintainer:** The System maintainers are responsible for maintenance of the RWPS and monitor device failure alarms and alerts to plan for maintenance activities

3.3 The Hazard Risk Index

Please refer to CDRL 2-123-10 System Product Safety Plan [3] section 7.5.

3.4 Hazard Tracking

All hazards identified in the subsystem OHA that have critical or catastrophic severity will be entered into the System Hazard Log [10][7], so that they can be tracked through resolution and can reviewed for appropriate action. Some OHA subsystem level hazards may replace more general Subsystem PHA [7][8] and SSHA [8] resolutions, and the PHA [7] or SHA [8] item will be closed. Hazards will have reference made to the Subsystem OHA (this document) item in the System Hazard Log [10].

From SysOHA hazard tracking: All hazards identified in the OHA for which mitigating risk reduction was required to achieve an acceptable safety level (risk index value below the safety target identified in section 6.5 of the SPSP [3]) will be entered into the Hazard Log [10], so that they can be tracked through resolution and regularly reviewed for appropriate action.

4 RWPS Subsystem OHA Table

Hazard-related information in the OHA worksheet is organized in a table format, consistent with those defined in the Subsystem's PSP [1] for the PHA [7][4], and SSHA [8][7]. The detail of the Subsystem OHA results table is presented in

OHA Table. A brief description of each column headings in the table is provided in the Table 6 below:

Table 6: RWPS OHA Table Column Headings and Description

Heading	Description
RWPS_OHA ID	This unique ID reference number assigned to an individual hazard for the RWPS. This reference is provided for cross-referencing and traceability for the specific hazard, its cause, and potential resolutions. RWPS_OHA_xx
OHA ID	This unique ID reference number assigned to an individual hazard for the system level hazards. This reference is provided for cross-referencing and traceability for the specific hazard, its cause, and potential resolutions.
Reference ID	Reference as to the source of the Hazard. PHA or System OHA.
Operating Scenario	A specific manual, procedure, or description which is utilized as part of the maintenance, operation, or installation step which could contribute to a hazard condition. (e.g. Train Entry from Depot/Yard/siding/Mainline Track Exception).
Operating Description	The type of human interaction with the Product, such as maintenance, train engineer in control, etc.
Hazard Description	A hazard summary provides a description of the specific potential hazards that can be precipitated by the faults identified.
Potential Cause(s)	A potential cause of the hazard identified in the Hazard Description.
Hazard Effects	The potential effects on person(s) and/or system equipment should the hazard occur.
Initial Hazard Severity (I,II,III,IV)	The Severity of a hazard before the safety requirement has been implemented and mitigated the associated hazard.
Initial Hazard Probability (A-E)	The likelihood of a hazard occurring before the safety requirement has mitigated the associated hazard.

Heading	Description
Type	The type of human interface analyzed, such as Operation, Maintenance, Installation.
Operating/Safety Requirements	This requirement is in the form of an operating or maintenance procedure that will eliminate or control the Hazard.
Operating/Safety Requirements ID	Each operating requirement is assigned a unique ID Operating requirements originating from the System OHA are numbered, OHA-xx. Operating requirements originating from the RWPS OHA are numbered RW-OR-xx., or RW-SR-xx for RWPS.
Post Mitigation Hazard Severity (I,II,III,IV)	The Severity of a hazard after the safety requirement has been implemented and mitigated the associated hazard.
Post-Mitigation Hazard Probability (A-E)	The likelihood of a hazard occurring after the safety requirement has mitigated the associated hazard.
Subsystem Interface	The subsystem responsible for carrying out the safety requirement execution.
Closure References	A reference to the document(s) where specific system/subsystem safety requirement(s) for the LIRR/MNR implementation are located. In some cases, these documents may not yet be published or available, and a new safety-critical requirement is generated in the OHA to be addressed in the document(s).
Comments	Any miscellaneous comments associated with the hazard's management.

4.1 Summary of Interfaces

Below is a list of interfaces that relate to the RWPS Subsystem. These interfaces can be examined more in-depth in the RWPS IHA [9]:

External Interfaces:

a. EIC to EIC Terminal.
b. RWPS to Office (RGS)
c. Office(RGS) to RWPS
d. RWPS BCC to RWPS BCC
e. Programming RWPS
f. Programming EIC
g. Superuser to Workstation
h. System Admin Configuring RWPS
i. System Admin User Management
System Admin Database Recovery

Internal Interfaces:

a. RWPS to EIC Handheld
b. EIC Handheld to RWPS
c. RWPS to EIC Workstation
d. EIC Workstation to RWPS
e. RWPS to NMS
f. RWPS to DMS
g. RWPS to ADDC
h. NMS to NMS
i. RWPS to RWPS
j. NMS to EIC Handheld
k. NMS to EIC Workstation

4.2 Operating Scenarios Considered

Alarm Generation and Response

Installation and Maintenance

Operation of Electrical Equipment

Security Breach

STS Cold-start

TSR Management

Superuser Overrides

Primary to Secondary EIC Transfers

Ensuring all Secondary EIC Clear

Making sure Worksite is Clear

4.3 OHA Table

Table 7 : RWPS Subsystem OHA

RWPS_OHA ID	OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Cause(s)	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	Operating/Safety Requirements ID	Post-Mitigation Hazard Severity (I,II,III,IV)	Post-Mitigation Hazard Probability (A-E)	Subsystem Interface	Closure References	Comments
RWPS_OHA_01		PHA-49 (System)	Electrocution	Maintenance of Electrical Equipment	The maintenance or testing operator mistakenly connects to high power sources.	Maintenance Personnel oversight; Inadequate training/qualification	Staff injury or death	I	C	Maintenance	RW_OR_01	I	D	Wayside/ Office/Onboard		
RWPS_OHA_02			Entry of TSR Data	EIC enters TSR Data	Train does not receive correct TSR and enters roadway worker protection area	EIC Terminal User interface is not up to Human Factor Engineering Standard or best practice	Staff injury or death	I	C	Operation	RW_OR_02 RW_OR_20	I	D	Office		
RWPS_OHA_03*																Moved to IHA

RWPS_OHA ID	OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Cause(s)	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	Operating/Safety Requirements ID	Post-Mitigation Hazard Severity (I,II,III,IV)	Post-Mitigation Hazard Probability (A-E)	Subsystem Interface	Closure References	Comments
RWPS_OHA_04			Remove TSR	EIC Requests to Remove TSR	TSR Removed with Secondary EIC in area	RWPS failure allows TSR Removal when Secondary EIC still in area.	Staff injury or death	I	C	Operation	RW_OR_04 RW_OR_14 RW_OR_22	I	D			
RWPS_OHA_05			Get TSR List	EIC requests TSR List	EIC Terminal shows TSR where no TSR is enforced	RWPS Failure indicates TSR where none exists	Staff injury or death	I	C	Operation	RW_OR_05 RI_SR_19 RI_SR_14 RW_SR_16	I	D			
RWPS_OHA_06			Get TSR List	EIC requests TSR List	EIC Terminal shows TSR where no TSR is enforced	EIC Terminal Failure indicates TSR where none exists	Staff injury or death	I	C	Operation	RW_OR_05 RI_SR_19 RW_OR_06	I	D			

RWPS_OHA ID	OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Cause(s)	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	Operating/Safety Requirements ID	Post-Mitigation Hazard Severity (I,II,III,IV)	Post-Mitigation Hazard Probability (A-E)	Subsystem Interface	Closure References	Comments
RWPS_OHA_07			Superuser Override	TSR Remove Override	TSR Removed with EIC in area	Supervisor performs TSR Override with EIC still in area	Staff injury or death	I	C	Operation	RW_OR_07 RI_SR_22 RW_OR_09 RW_OR_10	I	D			
RWPS_OHA_08			Entry of TSR Data	EIC enters TSR Data	TSR Request not received by RWPS	Loss of communication between EIC terminal and RWPS.	Staff injury or death	I	C	Operation	RI_SR_09 RW_OR_29 RW_OR_18 RW_OR_19	I	D	RWPS		

RWPS_OHA ID	OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Cause(s)	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	Operating/Safety Requirements ID	Post-Mitigation Hazard Severity (I,II,III,IV)	Post-Mitigation Hazard Probability (A-E)	Subsystem Interface	Closure References	Comments
RWPS_OHA_09			STS Cold Start	EIC enter Railway and TSR is removed	EIC Terminal shows TSR where no TSR is enforce	STS Cold Start	Staff injury or death	I	C	Operation	RW_OR_29 RW_OR_15 RW_OR_26 RW_OR_27 RW_OR_28	I	D	Office		
RWPS_OHA_10			Security Breach	Secondary EIC removal request	Secondary EIC removed without authorization	Unauthorized person requests removal of Secondary EIC	Staff injury or death	I	C	Operation	RW_OR_04 RW_OR_12 RW_OR_17	I	E	RWPS		

RWPS_OHA ID	OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Cause(s)	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	Operating/Safety Requirements ID	Post-Mitigation Hazard Severity (I,II,III,IV)	Post-Mitigation Hazard Probability (A-E)	Subsystem Interface	Closure References	Comments
RWPS_OHA_11			Primary to Secondary EIC Transfer	Primary to Secondary EIC Transfer	Primary EIC Removed from TSR without Ack	Superuser override of Primary EIC transfer	Staff injury or death	I	C	Operation	RW_OR_16 RW_OR_04	I	E	RWPS		
RWPS_OHA_12			Ensuring all Secondary EIC Clear	Primary EIC requests removal of TSR	TSR removed with Secondary EIC in area	Primary EIC requests removal with Secondary EIC attached	Staff injury or death	I	C	Operation	RW_OR_04 RW_OR_11 RW_OR_12 RW_OR_02	I	E	RWPS		
RWPS_OHA_13			RWPS Executable and Config Data	Installation of Executable Files/Data	TSR Request with incorrect data	System Administrator loads incorrect data or Executable	Staff Injury or Death	i	C	Operation	RW_OR_02 RW_OR_13	I	E	RWPS		

RWPS_OHA ID	OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Cause(s)	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	Operating/Safety Requirements ID	Post-Mitigation Hazard Severity (I,II,III,IV)	Post-Mitigation Hazard Probability (A-E)	Subsystem Interface	Closure References	Comments
RWPS_OHA_14			EIC Handheld Executable and Config Data	Installation of Executable Files/Data	TSR Request with incorrect data	Executable or data with incorrect data loaded	Staff Injury or Death	I	C	Operation	RW_OR_02 RW_OR_13	I	E	EIC Handheld		
RWPS_OHA_15			EIC Workstation Executable and Config Data	Installation of Executable Files/Data	TSR Request with incorrect data	Executable or data with incorrect data loaded	Staff Injury or Death	I	C	Operation	RW_OR_02 RW_OR_13	I	E	EIC Workstation		
RWPS_OHA_16			RWPS User Management	Unauthorized user allowed to access system	Unauthorized users removes TSR	System Admin authorizes users for access who should not have access	Staff Injury or Death	I	C	Operation	RW_OR_21 RW_OR_02	I	D			
RWPS_OHA_17			RWPS Database Recovery	RWPS Static database installation / configuration	TSR request sent to UIS/STS at incorrect location or speed	Incorrect static database prevents checks that RWPS could perform to reject requests	Staff Injury or Death	I	C	Operation	RW_OR_20 RW_OR_02	I	D			

RWPS_OHA ID	OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Cause(s)	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	Operating/Safety Requirements ID	Post-Mitigation Hazard Severity (I,II,III,IV)	Post-Mitigation Hazard Probability (A-E)	Subsystem Interface	Closure References	Comments
RWPS_OHA_18			RWPS Data Configuration	RWPS Data Configuration change	Parameters changed to unacceptable values	Adjustment of default Train speed set to high	Train speed through a TSR	I	B	Operation	RW_OR_21	I	D			
RWPS_OHA_19			Setting Work Limits	Primary makes secondary EIC request and sets work limits	Work Limits not extended for Secondary EIC	Primary sets work limits to restrictive	Staff Injury or Death	I	C		RW_OR_23	I	D			
RWPS_OHA_20			Setting Work Limits	Secondary makes attachment request and sets work limits	Work Limits extend beyond TSR	Secondary sets work limits beyond TSR locations	Staff Injury or Death	I	C		RW_OR_24 RW_OR_25	I	E			
RWPS_OHA_21			Installing Executables and Data Configuration Files for RWPS	RWPS Data Configuration Installation	Error in TSR Indication to EIC.	Executable Corruption	Staff struck by train	I	B		RI_SR_24 RI_SR_27 RW_SR_10	I	D			
RWPS_OHA_22			Installing Executables and Data Configuration files for EIC	RWPS Data Configuration Installation	Error in TSR indication to EIC.	EIC Terminal executes incorrect executable.	Staff struck by train	I	B		RI_SR_25 RW_SR_10	I	D			

RWPS_OHA ID	OHA ID	Reference ID	Operating Scenario	Operating Description	Hazard Description	Potential Cause(s)	Hazard Effects	Initial Hazard Severity (I,II,III,IV)	Initial Hazard Prob. (A-E)	Type	Operating/Safety Requirements ID	Post-Mitigation Hazard Severity (I,II,III,IV)	Post-Mitigation Hazard Probability (A-E)	Subsystem Interface	Closure References	Comments
RWPS_OHA_23			UIS Cold Start	TSR removed while Secondary EIC still in place.	TSR removed while Secondary EIC still in place.	UIS Cold Start	Staff struck by train	I	B		RW_OR_30 RW_OR_31	I	C			

5 Conclusion

The RWPS OHA was performed by identifying potential hazards which may result if a human does not adhere to procedures for operation, maintenance, or installation, and analyzing their effects based on system design behavior and identified operating requirements. As a result of conducting the OHA, it has been shown that all LIRR/MNR operation and support activities involving a human interface have been addressed with operating requirements such that their successful execution results in risk levels which are acceptable to the LIRR/MNR customer.

Hazards that also require design for mitigation are identified by referencing the hazard analysis ID in the Ref ID column.

Metropolitan Transportation Authority
Long Island Rail Road / Metro-North Railroad
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Number: 1712/29544

RWPS Preliminary Hazard Analysis
CDRL 2-127-06

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	PM	Report	Project	Released

Prepared:	Aaron Graham Safety Engineer	Aaron Graham	2018.03.08 16:24:56 -05'00'
Verified:	Jason Weighley Safety Engineer	Jason W Weighley	2018.03.08 16:51:51 -05'00'
Approved:	Anthony DeFrancisco Project Director		3/12/18
SI Quality Process Review:	Bon Provenzano BT Quality Assurance Group		2018.03.09
BT/SRA Review:	N/A Title		
BT/SRA Review:	N/A Title		
	Name / Title, Group	**Signature**	**Date**

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2018, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2018 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3036416

Effective Date:	Revision:	Language:
2018-03-08	_D	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2014-03-13	First issue
_A	2014-08-27	Updated disclaimer on signature page
_B	2015-09-25	Submitted for PDR
_B.1	2017-12-12	Updated for FDR
_B.2	2018-01-12	Updated per RR comments
_B.3	2018-01-24	Updated per RR comments
_C	2018-01-30	Updated for document release
_D	2018-03-08	Updated Template, no changes to content of Document

Table of Contents

Section	Subject	Page
1	Executive Summary	4
2	Introduction	4
2.1	Objective	4
2.2	Scope	4
2.3	Compliance Matrix	5
2.4	Reference Documents	11
2.5	Glossary	13
3	Subsystem Overview	14
4	Methodology	15
4.1	Risk Assessment Classification Frame Work	16
5	Hazard Assessment & PHA Result Table	19
5.1	Hazard Analysis Table	21
5.2	Hazard Analysis Results	30
6	Safety Requirements	30
7	Conclusion	32

List of Tables

Table 1: Compliance Matrix 5
Table 2: Reference Documents 11
Table 3: Terms Specific to this Document 13
Table 4: Acronyms Specific to this Document 14
Table 5: SIL Allocation 14
Table 6: Hazard Severity Classifications 17
Table 7: Hazard Probability Classifications 17
Table 8: Hazard Risk Assessment Matrix 18
Table 9: Hazard Risk Index 18
Table 10: Hazard Table Column Definition/Description 20
Table 11: LIRR / MNR Hazard Analysis 22
Table 12: Summary of Identified Hazards 30
Table 13: Safety Requirements 30

1 Executive Summary

This document records the RWPS Preliminary Hazard Analysis of the LIRR / MNR PTC system. This analysis forms the initial safety demonstration document for the RWPS Subsystem; its purpose is to identify the potential hazardous events that can occur as a result of operating the RWPS Subsystem.

The analysis evaluates the severity and identifies the causes of hazardous events in order to develop safety requirements. These identified hazards will be further broken down and analyzed in greater detail in the RWPS Subsystem Hazard Analysis to assess their compliance with the Safety requirements.

2 Introduction

2.1 Objective

This PHA is undertaken in order to identify hazards related to the design and operation of the RWPS Subsystem as part of the LIRR/MNR PTC system. This is to aid the derivation and verification of the PTC system safety requirements.

This document provides an initial list of hazards, which require tracking mitigation resolution during the PTC system design and development. The PHA is the foundation for further system and subsystem level hazard analyses. Hazards that pertain to the management of TSRs are already covered under the Office PHA [12].

2.2 Scope

The objective of this analysis does not include:

- Tenant railroad equipment except for ensuring interoperability.
- External equipment located outside of the RWPS Subsystem boundary;
- Environmental conditions exceeding the specifications;
- Catastrophic natural events (lightning, flooding, earthquake, etc.); and
- Other external factors, such as, vandalism, fire, smoke, gas-build, electrification, rolling stock and construction.

2.3 Compliance Matrix

Table 1: Compliance Matrix

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Requirement Summary (2)	Document Section Reference
1	Contract 1712 Vol 2	Vol 2 PART I rev1.01- Section 12.10.2	A. The SI shall perform and document a Preliminary Hazard Analysis (PHA) [CDRL 2-127], starting with the ACSES II hazards defined in the Type Approved ACSES II PHL, identifying the system hazards, conditions that could result in the hazard, and the mitigation strategy for protecting and maintaining the safety of the ACSES II System.			Section 5
2	Contract 1712 Vol 2	Vol 2 PART I rev1.01- Section 12.10.2	B. The PHA shall be performed in general conformance to MIL-STD-882C including the following:	1. Hazard severity and probability for each hazard and the level achieved after mitigation;		Section 4 [*PHA regarding mitigation will identify Potential mitigation]*
3	Contract 1712 Vol 2	Vol 2 PART I rev1.01- Section 12.10.2		2. Safety provisions and alternatives needed to eliminate the hazards or reduce their associated risk to a level acceptable to the Engineer;		Section 5

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Requirement Summary (2)	Document Section Reference
						[*PHA will identify System (high) level potential mitigations with regard to Safety order of precedence as identified in Mil-Std-882C to achieve a Risk level as defined in the Safety Plan Risk Acceptability matrix.*]
4	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		3. The following as minimum shall be considered in the hazard analysis:	a. ACSES II Subsystems and components;	Section 4 *[PHA will be done at to System (high) level and will not go into subsystem and component details. Each subsystem will generate a separate PHA that will go to sufficient detail.*]

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Requirement Summary (2)	Document Section Reference
5	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			b. Hazardous components;	*Covered by the Subsystem PHAs: [9], [10], [11], [12], [13]*
6	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			c. Safety related interfaces;	Section 4
7	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			d. Operating environments, including vehicles, track beds, wayside rooms and huts, control centers, and other required ACSES II installation sites.	Section 4
8	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			e. Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures;	Section 4
9	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			f. Human interface;	Section 4
10	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			g. Safety concepts and dependencies;	Section 4

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Requirement Summary (2)	Document Section Reference
11	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			h. Operations and Maintenance procedures;	Section 4
12	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			i. Training and emergency preparedness;	Section 5.1. *The Subsystem PHA's will address Subsystem and component issues*
13	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2			j. Safety related equipment, safeguards, and possible alternate approaches (e.g., system redundancy; fail safe design considerations using hardware or software controls);	Section 4

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Requirement Summary (2)	Document Section Reference
14	Contract 1712 Vol 2	Vol 2 PART I rev1.01- Section 12.10.2			k. Malfunctions to the system, subsystems, or software. Each malfunction shall be specified, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and/or design changes developed.	Section 4
15	Contract 1712 Vol 2	Vol 2 PART I rev1.01- Section 12.10.2	C. Functional failure analysis shall be derived from the Preliminary Hazard Analysis (PHA) and subsequent Hazard Analyses, including subsystem HA's. Hardware items on this list as applicable. This analysis looks at software's relationship to hardware.			Please see documents: [14] [15] [16] [17]

Item #	Specification Volume	Specification Section	Requirement Title	Requirement Summary (1)	Requirement Summary (2)	Document Section Reference
16	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2	D. A Preliminary Hazard Report shall be furnished as part of the PHA by the SI including for each hazard the following:	1. Hazard Description;		Section 5
17	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		2. Safety Requirement(s), with reference to the RTM (Section 6.6);		Section 5
18	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		3. Hazard Cause;		Section 5
19	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		4. Hazard Control;		Section 5
20	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		5. Hazard Detection Method;		Section 5
21	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		6. Safety Verification Method (analysis, test, demonstration, or inspections), with reference to Subsystem Test Plan (Section 10.4.1);		Section 5
22	Contract 1712 Vol 2	Vol 2 PART I rev1.01-Section 12.10.2		7. Status		Section 5

2.4 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	PDM 3035624
[2]	RWPS Subsystem Description Document CDRL 6-1	PDM 3035851
[3]	MIL-STD-822C	
[4]	System Product Safety Plan LIRR CDRL 2-123-20 System Product Safety Plan MNR CDRL 2-123-10	PDM 3035815 PDM 3036437
[5]	RAM Program Plan CDRL 2-139	PDM 3035841
[6]	RWPS Product Safety Plan CDRL 2-123-06	PDM 3036415
[7]	System Preliminary Hazard Analysis CDRL 2-127	PDM 3035821
[8]	RWPS System Safety Concept Description CDRL 2-124-06	PDM 3036417
[9]	Onboard PHA	3036405
[10]	WIU PHA	3036409
[11]	Transponder PHA	3036413
[12]	Office PHA	3035822
[13]	Comms PHA	3036420
[14]	LIRR System IHA	3035828
[15]	MNR System IHA	3043905
[16]	LIRR RWPS IHA	3037436
[17]	MNR RWPS IHA	3037437
[18]	AREMA, Communications and Signals Manual – 2009 Section Parts 16, 17, 21, and 23.	2001
[19]	CENELEC EN50126, Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)	EN50126:1999

Reference Number	Document Name	Identification Number
[20]	CENELEC Standard. Railway Applications – Communication, signaling and processing systems – Safety related electronic systems for signaling.	EN50129:2003

2.5 Glossary

Please refer to the Dictionary of Terms and Acronyms, [1]. Terms and acronyms only related to this document are listed below in Table 3 and Table 4 respectively.

Table 3: Terms Specific to this Document

Term	Definition
Preliminary Hazard Analysis (PHA)	An analysis performed on the potential hazards identified in the PHL, to provide an initial risk assessment of the hazards, and to identify requisite controls and follow-on actions.
Product	A train control system, subsystem, component, or an element of the physical or system architecture, specification tree, or system breakdown structure that is a subordinate element to the system or subsystem and which is wholly documented in a separate way, and considered as a terminal branch of the specification tree.
Qualitative Proof of Safety	Argument provided by the application of the safety assurance methodology that hazards are eliminated or controlled to an acceptable level. The norms for acceptability are usually based upon MIL-STD-882C[3], or similar documents.
Quantitative Proof of Safety	A measure of safety, stated in terms of a Mean Time To Hazardous Events (MTTHE) or Mean Time Between Hazardous Events (MTBHE), usually obtained by mathematical analysis of the safety assurance mechanisms used in the product/system, or by modeling and simulation techniques applied to the hardware and software of the product/system.
Review	The assessment of a work product's content to verify adherence to defined standards, guidelines, specifications and procedures.
Risk	An expression combining the probability of the mishap occurring with the severity of the consequences of the mishap, used to rank hazards.
Risk Assessment	The process of determining the amount of risk associated with use of the product under all intended operating conditions. Intended operating conditions include normal operations, degraded operations, and operation under failure conditions including unintended human error. Risk assessment techniques for any product may include qualitative, semi-quantitative and quantitative approaches.

Term	Definition
Safety-Critical Classification	A classification of products that have at least one hazard that can lead directly to a mishap.
Safety-Related Classification	A classification of products which do not lead directly to a mishap but which may significantly increase the overall risk of a mishap.
Safety Life Cycle	The additional series of activities carried out in conjunction with the system life cycle for safety related systems.
Self-Revealing Component Failures	Component failures whose effects on system operation are immediately and clearly apparent to a properly trained person.
Subsystem Hazard Analysis (SSHA)	An analysis that looks at each subsystem or component and identifies hazards associated with operating modes, failure modes, and human errors and is especially intended to determine how operation or failure of components affects the overall safety of the system.
Subsystem Preliminary Hazard Analysis	The Subsystem PHA is undertaken in order to identify hazards related to the design and operation of the PTC Subsystems identified in the System PHA. This is to aid the derivation and verification of the PTC system safety requirements.

Table 4: Acronyms Specific to this Document

Acronym	Definition
SPSP	System Product Safety Plan
SSHA	Subsystem Hazard Analysis

3 Subsystem Overview

The RWPS system is described by the RWPS Subsystem Design Specification [2], which includes the type of communication used by the PTC ACSES II System. These components include:





4 Methodology

The System PHA [7] identifies the primary hazards inherent with the railway system that are applicable to the RWPS Subsystem. Primary hazards that the ACSES II PTC system must control are identified based in the System PHA [7]. This is described in the RWPS PSP [6].

The PHA determines the RWPS Subsystem's contribution to the primary hazards and defines the role and responsibilities of the RWPS subsystem in the mitigation of each of the primary hazards. The link between the 2 levels of PHA is listed in Table 12. Out of these roles and responsibilities, a set of hazards is deduced. Subsystem hazards are defined as conditions associated with the physical and functional boundaries of the ACSES II system.

This analysis uses a "top-down" deductive approach to systematically and comprehensively identify hazards associated with the ACSES II system design and operation. The primary hazards (top events) are decomposed into contributing lower level hazards (trigger events) associated with the RWPS subsystem functions, equipment and interfaces.

The identification of hazards at the Preliminary level is based on the best available data, including mishap data from similar PTC or advanced train control systems and other lessons learned from similar projects. The analytical process took into considerations the following factors in the identification process of hazards:

a) Hazardous components including the use of toxic or flammable materials;

b) Interfaces between subsystems and the interfaces between the RWPS subsystem and

existing LIRR / MNR System and third parties;

c) Electromagnetic interference;

d) Fire/explosive initiation and propagation;

e) Contributions to hazards by hardware and software elements;

f) Human errors including incorrect inputs and commands to The System;

g) Environmental impacts including shock, vibration, extreme temperatures, noise, electrostatic discharge, lightning;

h) Human factor impacts by operators and maintainers;

i) System malfunctions; and

j) Errors arising from the application of design tools or processes including database errors and performance parameters

The Hazard Risk Assessment used in this Preliminary Risk Assessment complies with the process described in the RWPS Product Safety Plan [6] and the System Product Safety Plan [4].

4.1 Risk Assessment Classification Frame Work

Throughout the product development life-cycle, risk assessment practices are applied to guide the implementation of mitigating actions to control or eliminate each identified hazard such that the risk introduced by each is acceptable. Risk assessment and management is a decision-making process consisting of evaluation and control of the severity and probability of a potentially hazardous event. As hazard analyses are performed, Bombardier will identify hazards that will require resolution through this mechanism.

The classification of severity for hazards will be based on the four categories from MIL-STD-882C [3] and AREMA Section 17.3.5 [18] identified in Table 6,ranging from Category I (Catastrophic) to Category IV (Negligible). The severity classification assigned to each hazard will provide a qualitative indication of the worst-case consequences that could occur if the hazard is not eliminated or controlled.

Probability classifications will be based on the five categories from MIL-STD-882C and AREMA Section 17.3 as shown in Table 7. These range from Category A (Frequent) to Category E (Improbable). The assigned probability will be based on the likelihood that a particular hazard and effect would occur in the planned life expectancy of the product. To assist in assigning the specific categories of probability, Table 7 shows definitions for both a specific individual item (i.e. a specific component of the system), as well as for the fleet or overall inventory of the system. The table also provides the Mean Time Between Events (MTBE) to guide the consistent application to hazards of all severities (even Category IV), it is not appropriate to use Mean Time Between Hazardous Events (MTBHE) in Table 7 as all events may not be truly hazardous in nature and therefore MTBE is used.

Table 6: Hazard Severity Classifications

Description	Category	Definition
Catastrophic (1 Yr.-death)	**I**	Death, system loss, or severe environmental damage.
Critical (21-363 Days)	**II**	Severe injury, severe occupational illness, major system or environmental damage.
Marginal (8-20 Days)	**III**	Minor injury, minor occupational illness, or minor system or environmental damage.
Negligible (0-7 Days)	**IV**	Less than minor injury, occupational illness, or less than minor system or environmental damage.

Table 7: Hazard Probability Classifications

Description	Level	# of accidents # of employees	Specific individual item	Fleet or inventory	Numerical range of failure rate (f/Hr) for fleet/inventory
Frequent	**A**	(> .24)	Likely to occur frequently.	Continuously experienced.	Greater that 10^{-1}
Probable	**B**	(0.16 – 0.24)	Will occur several times in the life of an item.	Will occur frequently.	$\geq 1.39x10^{-3}$ to $\leq 1.0x10^{-1}$
Occasional	**C**	(0.10 – 0.15)	Likely to occur sometime in the life of an item.	Will occur several times.	$\geq 1.14x10^{-5}$ to $\leq 1.39x10^{-3}$
Remote	**D**	(0.02 – 0.09)	Unlikely but possible to occur in the life of an item.	Unlikely but can reasonably be expected to occur.	$\geq 5.12x10^{-7}$ to $\leq 1.14x10^{-5}$
Unlikely	**E**	(<0.01)	So unlikely, it can be assumed occurrence may not be experienced.	Unlikely to occur, but possible.	Less than $5.12x10^{-7}$

The combination of the hazard severity and hazard frequency forms a Hazard Risk Index (HRI). The resulting Hazard Risk Assessment Matrix is obtained from MIL-STD-882C [3] as shown in Table 8 and

Table 9.

The HRI presents the hazard analysis results in a format useful to the decision-maker in determining whether hazards should be eliminated, controlled, or accepted. This provides a logical basis for management decision-making, considering both the severity and probability of any individual hazard in a weighted fashion.

Table 8: Hazard Risk Assessment Matrix

	Catastrophic	Critical	Marginal	Negligible
Frequent	**IA**	**IIA**	**IIIA**	**IVA**
Probable	**IB**	**IIB**	**IIIB**	**IVB**
Occasional	**IC**	**IIC**	**IIIC**	**IVC**
Remote	**ID**	**IID**	**IIID**	**IVD**
Improbable	**IE**	**IIE**	**IIIE**	**IVE**

Table 9: Hazard Risk Index

Hazard Risk Index	Acceptance Criteria
IA, IIA, IIIA, IB, IIB, IC	**Unacceptable**
ID, IIC, IID, IIIB, IIIC	**Undesirable** - Requires solution acceptable to Bombardier Project Manager.
IE, IIE, IIID, IIIE, IVA, IVB	**Acceptable with review -** Requires review.
IVC, IVD, IVE	**Acceptable** - Review not required.

It should also be noted that these hazard classifications are consistent with CENELEC standards ([19], [20]), which define a sixth probability classification and different numerical ranges but similar severity definitions. As long as the definitions are appalled consistently throughout all product safety analyses, the resulting risk assessment will be consistent and sufficiently accurate to guide the development process.

By assigning a Hazard Risk Index (HRI), a determination can be made as to how the hazards should be addressed, in the order of precedence shown below:

1. **Design for Minimum Risk:** Eliminate hazards by safety-critical design. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level through design concept and implementation.
2. **Incorporate Safety Devices:** If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk shall be reduced to a level acceptable through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks of safety devices when applicable.

3. **Provide Warning Devices:** When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, warning devices shall be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems.
4. **Develop Rules, Procedures, and Training:** Where it is impractical to eliminate hazards through design selection or adequately reduce associated risk with safety and warning devices, procedures and training shall be used. Procedures may include the use of personal protective equipment. Such practices shall be evaluated for completeness, clarity, and applicability where necessary to provide adequate safety. Such methods may also include warnings and equipment labeling.
5. **Note:** The use of warnings, cautions, or other written advisory shall not be used as the only risk reduction method for Category I or II severity hazards unless approved. Safety-critical tasks may require personnel proficiency in specific areas; the need for personnel proficiency certification will be identified in the analysis.

Hazard severity, before and after mitigation, provides a measure of the worst credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction. The hazard severity ranking of “AFTER mitigation” takes into account the actual design and architecture of the system (fail-safe design, maintenance procedures, etc.) and uses the following rationale:

- Failures of components related to non-vital systems lead to hazard Category IV when an independent vital subsystem protects them.
- The failure of a safety-related system, dependent on external requirements (e.g. periodic maintenance, periodic adjustments, cycle checking, or daily safety test) will lead to a hazard with a severity Category I.
- A (Vital) fail-safe system will fail into a restrictive mode. The use of a fail-safe system can reduce the probability of the hazard occurrence for the item to an extent where it can be easily assumed that the hazard may not occur. This leads to a hazard probability of Category E.

5 Hazard Assessment & PHA Result Table

The contributors to the primary hazards identified in the System PHA [7] are categorized and summarized in this section. The hazard analysis tables presented in this section include the assessment of applicability of the hazard contributors to the PTC, System operation and support, and exported hazards that are outside of the scope of the PTC system to mitigate. As well, the initial risk assessment, the proposed mitigation requirements, and the residual risk assessment based on the implementation of the mitigations are presented.

The hazards are analyzed and assessed to determine their associated risk. In general, the hazard assessment is performed according to Frequency and Severity of each hazard in the list. The hazard risk is derived according to best available data, problems reported from similar projects and other lessons learned from similar systems.

The analysis and assessment results are presented in table format which contains the following columns:

Table 10: Hazard Table Column Definition/Description

Column Title	Description
ID	A unique identification number is provided per line to simplify hazard location in the tables
Event	List of potential hazardous events that could occur on the LIRR / MNR Right of Way with ACSES II equipped trains or equipment rooms or office locations.
Primary Hazard ID	A unique identification number for the Primary Hazard. See the System Preliminary Hazard Analysis [7].
Status	Status of the Hazard (Open, Mitigated, Verified, Closed)
Hazard Description	Description of the hazard
Potential Cause	Description of the possible causes which might be at the origin of the hazard
Effect	The effect (e.g. hazard consequences) of the hazard on the system.
Initial Risk Assessment	IS – Severity - The severity of the hazard consequences; (Refer to the System Product Safety Plan [4]) IF – Frequency - The frequency of occurrence of the hazard condition; (Refer to the System Product Safety Plan [4])
Final Risk Assessment	FS – Severity - The severity of the hazard consequences; (Refer to the System Product Safety Plan [4]) FF – Frequency - The frequency of occurrence of the hazard condition; (Refer to the System Product Safety Plan [4])
Subsystem(s) / Interface involved	Identification of the subsystem or interfaces that can contribute to the hazardous event: RWPS, Onboard; Wayside; Data Communication System; Office; STS database.

Safety Requirement ID	A unique identification assigned to a Safety Requirement.
Proposed Mitigation	Description of how the Subsystem or components will control the hazard
Hazard Detection Method	Method used to detect the hazard if applicable.
Safety Verification Method	Method(s) used to verify the Hazard has been properly mitigated by the component / system (Analysis, Test, Demonstration, or Inspection)

5.1 Hazard Analysis Table

The Hazard Analysis is presented in Tabular form as per the column Definition/Description given Table 10 above. Refer to Table 11.

Table 11: LIRR / MNR Hazard Analysis

ID	Event	Primary Hazard ID	Status	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Subsystem(s) / Interface Involved	Safety Requirement ID	Hazard Detection Method	Safety Verification Method
RWPS-PHA-01	Staff struck by train	PH04	Open	RWPS indicate TSR where no TSR is being enforced by the office.	Message Failure between UIS and RWPS. RWPS memory Failure.	Collision; Derailment; Staff struck by Train	I	B	I	C	EIC Terminal, RWPS workstation	RW-SR-1 RW-SR-26	Training Review	Inspection of Training Record
RWPS-PHA-02	Staff struck by train	PH04	Open	TSR Requested for incorrect location	RWPS Database provides incorrect location RWPS Equipment sends request for wrong location. EIC enters wrong location	Collision; Derailment; Staff struck by Train	I	B	I	D	EIC Terminal, RWPS workstation	RW-SR-2 RW-SR-10 RW-SR-24 RW-SR-26 RW-SR-28	Training Review	Testing Verification Inspection of Training records

ID	Event	Primary Hazard ID	Status	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Subsystem(s) / Interface Involved	Safety Requirement ID	[redacted]	Hazard Detection Method	Safety Verification Method
RWPS-PHA-03	Staff struck by train	PH04	Open	TSR removed from incorrect location	RWPS Database provides incorrect location RWPS Equipment sends request for wrong location. EIC enters wrong location	Collision; Derailment; Staff struck by Train	I	B	I	D	EIC Terminal, RWPS workstation	RW-SR-2 RW-SR-10 RW-SR-26		Training Review	Testing Verification Inspection of Training records
RWPS-PHA-05	Electrocution	PH06	Open	Person in contact with or near an electrical power source.	Inadequate maintenance procedures	Non-Vehicular death or injury (Staff or Passenger)	I	B	I	E	All s/systems	RW-SR-4		Design Review Training	Inspection Training
RWPS-PHA-06	Fire	PH11	Open	Burns to staff and third parties	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection etc.	Non-Vehicular death or injury (Staff)	III	B	III	D	All s/systems	RW-SR-5 RW-SR-6		Design Review	Analysis, Inspection
RWPS-PHA-07	Fire	PH11	Open	Inhalation damage to staff and third parties	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection, etc.	Non-Vehicular death or injury (Staff)	I	B	I	E	All s/systems	RW-SR-5 RW-SR-6		Design Review	Analysis, Inspection

ID	Event	Primary Hazard ID	Status	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Subsystem(s) / Interface Involved	Safety Requirement ID	Hazard Detection Method	Safety Verification Method
RWPS-PHA-08	Staff struck by train	PH08	Open	TSR improperly removed	Unauthorized access to EIC allows a user to request to remove TSR without authorization.	Collision; Derailment; Staff struck by Train	I	B	I	E	EIC Terminal / RWPS workstation	RW-SR-7 RW-SR-8	Design Review	Test, Inspection
RWPS-PHA-09	Installation / Maintenance Staff Injury	PH10	Open	Design of RWPS created components that injure maintenance or installation staff	Components have heavy weights, sharp edges etc.	Maintenance or installation staff injury	III	B	III	E	All s/systems	RW-SR-9	Design Review	Inspection
RWPS-PHA-10	Staff struck by train	PH04	Open	TSR Requested for incorrect location	Database Generation Error	Collision; Derailment; Staff struck by Train	I	B	I	E	SDMT	RW-SR-11	Design Review	Inspection
RWPS-PHA-11	Staff struck by train	PH04	Open	TSR improperly removed	Invalid user logged in from WiFi or Cellular System	Collision; Derailment; Staff struck by Train	I	B	I	D	RWPS	RW-SR-12	Design Review	Test
RWPS-PHA-12	Staff struck by train	PH04	Open	TSR Requested for incorrect location	EIC Database Failure	Collision; Derailment; Staff struck by Train	I	B	I	D	EIC	RW-SR-13 RW-SR-26	Design Review	Test
RWPS-PHA-13	Staff struck by train	PH04	Open	TSR Requested for incorrect location	RWPS Server Database Version Error	Collision; Derailment; Staff struck by Train	I	B	I	E	Office	RW-SR-14 RW-SR-15	Design Review	Test

ID	Event	Primary Hazard ID	Status	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Subsystem(s) / Interface Involved	Safety Requirement ID	Hazard Detection Method	Safety Verification Method
RWPS_ PHA_14	Staff struck by train	PH04	Open	TSR Requested for incorrect location	RWPS Server Database Version Error		I	B	I	D	RWPS	RW-SR-16 RW-SR-26	Installatio n Check	Inspection
RWPS_ PHA_15	Staff struck by train	PH04	Open	TSR Requested for incorrect location	EIC Terminal has incorrect SW		I	B	I	D	EIC	RW-SR-17	Design Review	Test
RWPS_ PHA_16	Staff struck by train	PH04	Open	TSR improperly removed	Secondary EIC sends remove request for TSR	Collision; Derailment; Staff struck by Train	I	B	I	E	Office	RW-SR-18 RW-SR-19	Design Review	Test

ID	Event	Primary Hazard ID	Status	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Subsystem(s) / Interface Involved	Safety Requirement ID	Hazard Detection Method	Safety Verification Method
RWPS_ PHA_17	Staff struck by train	PH04	Open	TSR Indicated on EIC but not enforced	Loss of communication between EIC and RWPS or RWPS and office	Collision; Derailment; Staff struck by Train	I	B	I	D	RWPS	RW-SR-20 RW-SR-21 RW-SR-22 RW-SR-26	Inspection Design Review Design Review Inspection	Inspection Test Test Inspection
RWPS_ PHA_18	Staff struck by train	PH04	Open	Incorrect TSR Location	Communication failure between STS and RWPS	Collision; Derailment; Staff struck by Train	I	B	I	D	RWPS	RW-SR-23 RW-SR-16 RW-SR-25 RW-SR-26	Design Review Design Review Design Review Training Review	Analysis Test Analysis Inspection

ID	Event	Primary Hazard ID	Status	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Subsystem(s) / Interface Involved	Safety Requirement ID	Hazard Detection Method	Safety Verification Method
RWPS_ PHA_19	Staff struck by train	PH04	Open	Incorrect TSR Location	Loss of communication between RWPS and EIC	Collision; Derailment; Staff struck by Train	I	B	I	D	EIC	RW-SR-21 RW-SR-20	Design Review Training Review	Test Inspection
RWPS_ PHA_20	Staff struck by train	PH04	Open	Incorrect TSR Location	Communication Error between RWPS and EIC	Collision; Derailment; Staff struck by Train	I	B	I	E	Office	RW-SR-20 RW-SR-2	Training Review Analysis	Inspection Analysis
RWPS_ PHA_21	Staff struck by train	PH04	Open	Incorrect TSR Location	Loss of communication between RWPS and UIS	Collision; Derailment; Staff struck by Train	I	B	I	D	EIC	RW-SR-22	Design Review	Test
RWPS_ PHA_22	Staff struck by train	PH04	Open	Incorrect TSR Location	Communication Error between RWPS and UIS	Collision; Derailment; Staff struck by Train	I	B	I	E	Office	RW-SR_20 RW-SR-2	Training Review Design Review	Inspection Test

ID	Event	Primary Hazard ID	Status	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Subsystem(s) / Interface Involved	Safety Requirement ID	Hazard Detection Method	Safety Verification Method
RWPS_ PHA_23	Staff struck by train	PH04	Open	Incorrect TSR Location	EIC Request work zone entry error	Collision; Derailment; Staff struck by Train	I	B	I	E	Office	RW-SR-2	Design Review	Test
RWPS_ PHA_24	Staff struck by train	PH04	Open	Incorrect TSR Location	EIC Remove work zone entry error	Collision; Derailment; Staff struck by Train	I	B	I	E	Office	RW-SR-2	Design Review	Test
RWPS_ PHA_25	Staff struck by train	PH04	Open	Incorrect TSR Location	Primary EIC change request error		I	B	I	E	Office	RW-SR-18	Design Review	Test
RWPS_ PHA_26	Staff struck by train	PH04	Open	TSR removed too early	Primary EIC change request error	Collision; Derailment; Staff struck by Train	I	B	I	E	Office	RW-SR-16 RW-SR-22 RW-SR-26 RW-SR-27	Design Review Training Review	Test Inspection

ID	Event	Primary Hazard ID	Status	Hazard Description	Potential Cause	Effect	IS	IF	FS	FF	Subsystem(s) / Interface Involved	Safety Requirement ID	[redacted]	Hazard Detection Method	Safety Verification Method
RWPS_ PHA_27	Staff struck by train	PH04	Open	TSR requested too late	Primary EIC change request error	Collision; Derailment; Staff struck by Train	I	B	I	E	Office	RW-SR-16 RW-SR-22 RW-SR-26 RW-SR-27		Design Review Training Review	Test Inspection
RWPS_ PHA_28	Staff struck by train	PH04	Open	Incorrect TSR Location	EIC determines work zone location incorrectly	Collision; Derailment; Staff struck by Train	I	B	I	E	Office	RW-SR-2		Design Review	Test
RWPS_ PHA_29	Staff struck by train	PH04	Open		EIC determines that track is available for operations without all workers or work trains removed							RW-SR-27		Training Review	Inspection

5.2 Hazard Analysis Results

The PHA identified the Possible Causes as the contributors to the Primary Hazards and these are listed in Table 12. These will be further decomposed into their contributing events in the SSHA.

Table 12: Summary of Identified Hazards

Primary Hazard ID	Potential Cause
PH04	TSR Displayed where no TSR exists
PH04	TSR requested or removed at wrong location
PH04	TSR removed too early or requested too late
PH06	Inadequate maintenance procedures
PH06	Material with electrical potential accessible to passengers in public area.
PH08	Unauthorized access to EIC allows a user to request to remove TSR without Authorization.
PH10	Components have heavy weights, sharp edges etc.
PH11	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection etc.

6 Safety Requirements

The preliminary hazard analysis generates several safety requirements that have to be taken into account during the RWPS Subsystem life cycle.

All RWPS safety requirements developed from the PHA activity, as well as the methods used to mitigate the hazard will be logged and tracked in the Project Level System Hazard Log (“Identification of proposed hazard mitigation”). Please see the RWPS SPSP for how safety



[redacted]

7 Conclusion

The LIRR / MNR PTC RWPS Preliminary Hazard Analysis (PHA) has identified the potential high-level hazards in the operation of the RWPS Subsystem.

In Section 5, the Preliminary analysis of the Primary Hazards was presented, which identified the hazard contributors (Causes). These Primary Hazards will be further decomposed in the RWPS Subsystem Hazard Analysis (SSHA), these identified hazards will form the basis of the start of the SSHA.

In Section 6 , the Safety requirements are identified. These requirements are listed in Table 13.

Metropolitan Transportation Authority
Long Island Rail Road
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712

RWPS Subsystem Hazard Analysis (SSHA)
CDRL 2-128-26

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Calvin Perine System Safety Engineer	Calvin Perine	2015-09-30
Verified:	Theresa Barbour System Safety Engineer	T. Barbour	2015-09-30
Approved:	Marty Matvey Project Director	M. Matvey	2015-10-01
SI Quality Process Review:	Michael Giometti BT Quality Assurance Group	Michael Giometti	2015-10-02
BT/SRA Review:	NA		
BT/SRA Review:	NA Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2015, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2015 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3037395

Effective Date:	Revision:	Language:
2015-09-30	—	EN

Released
Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2015-09-30	First issue

Table of Contents

Section	Subject	Page
1	Executive Summary	4
2	Introduction	4
2.1	Compliance Matrix	5
2.2	Reference Documents	8
2.3	Glossary	9
2.4	Objective	9
3	Subsystem Overview	10
4	Methodology	10
5	Hazard Assessment & SSHA result table	11
5.1	RWPS Subsystem Hazard Analysis Table	12
5.2	Hazard Analysis Results	19
6	Functional Safety Requirements	19
6.1	Safety Requirement	19
7	Conclusion	20

List of Figures

No table of figures entries found.

List of Tables

Table 1: Compliance Matrix 5
Table 2: Reference Documents 8
Table 3: Terms Specific to this Document 9
Table 4: Acronyms Specific to this Document 9
Table 5: Hazard Table column Definition/Description 11
Table 6: RWPS Sub system Hazard Analysis 13
Table 7: Safety Requirements 19

1 Executive Summary

This document records the Subsystem Hazard Analysis (SSHA) of the RWPS subsystem. This analysis forms the safety demonstration document for the RWPS Subsystem; its purpose is to verify safety compliance and identify hazards associated with the RWPS Subsystem. The main focus of the SSHA is on the faults recognized within the RWPS Subsystem.

The analysis evaluates the severity and verifies the methodology or actions in order to eliminate, minimize or control each hazard. This analysis will recommend an approach for eliminating, controlling, or minimizing hazards identified during this analysis. These mitigations will be traced to verification evidence that consists of Test Procedures or Operating Procedures to ensure the hazard is properly closed.

2 Introduction

This SSHA is undertaken in order to verify hazards that have been identified in the Preliminary Hazard Analysis (PHA) [2], which is related to the design and operation of the RWPS Subsystem as part of the LIRR PTC system.

The SSHA is performed and documented to verify compliance with safety requirements and identify hazards associated with the design. This includes hazards caused by component failure modes, critical human error inputs, and the hazards resulting from functional relationships between equipment compromising the RWPS Subsystem and the entire PTC System.

The document presents a hazard analysis for the RWPS subsystem. The starting point is the definition of all safety critical services for the system. Based on these, the corresponding top level hazards are defined, and analyzed.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol. 2 Part 1	12.10.3 A	A. Subsystem Hazard Analysis (SSHA), CDRL 2-128	SSHA shall be documented to verify safety compliance and identify hazards associated with this Subsystem. As an extension SHL (PHL), the main focus of the SSHA shall be on the faults recognized within this Subsystem.	Sec. 6.0
	12.10.3. B	Methods or actions for eliminating, minimizing, or controlling each hazard, as well as the recommended approach for eliminating, controlling, or minimizing hazard identified during this analysis shall be documented in the SSHA including:	1.) Independent, dependent and simultaneous events or failures and system interactions that could create increased risk.	Sec. 6.1
			2.) Effects of reasonable human errors	Sec. 6.1

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
			3.) Effects on system safety from the functional, interoperable relationships between Subsystems.	Sec. 6.1
			4.) Safety design criteria has been satisfied.	Sec. 6.1
			5.) Analysis that implementation of safety recommendations and corrective actions will not impair or degrade safety performance of hardware or software and will not create additional hazards.	Sec. 6.1

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
			6.) The SSHA is performed and documented to verify compliance with safety requirements and identify hazards associated with the design of subsystems. This includes hazards caused by component failure modes, critical human error inputs, and hazards resulting from functional relationships between equipment compromising each subsystem.	Sec. 6.1
	12.10.3.C	The following issues shall be considered during the performance of a SSHA.	1.) Modes of failure including reasonable human errors, single point and common mode failures, and the effects of failures on subsystem elements.	Sec. 6.1
			2.) Potential contribution of hardware and software controlled events, faults and occurrences.	Sec. 6.1

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
			3.) Satisfaction of all safety design criteria.	Sec. 6.1
			4.) Integrating safety testing into hardware and software testing programs.	Sec. 6.1
			5.) System level hazards attributed to subsystems are controlled.	Sec. 6.1
			6.) Input information from other subsystems that is required to perform the functions of this ACSES II Subsystem in a safe manner.	Sec. 6.1

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Project Hazard Log (PHL)	3035819
[2]	RWPS Preliminary Hazard Analysis (PHA)	3036416
[3]	Dictionary of Terms and Acronyms	3035624
[4]	RWPS Subsystem Description Document	3035851
[5]	System PHA	3035821
[6]	System Product Safety Plan	3035815
[7]	RWPS System Safety Description Concept	3036417
[8]	RWPS Subsystem Interface Hazard Analysis (IHA)	3035828

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms [3]. Terms and acronyms only related to this document are listed below in Table 3.

Table 3: Terms Specific to this Document

Term	Definition
Preliminary Hazard Analysis (PHA)	An analysis performed on the potential hazards identified in the PHL, to provide an initial risk assessment of the hazards, and to identify requisite controls and follow-on actions.
Subsystem Hazard Analysis (SSHA)	An analysis that looks at each subsystem or component and identifies hazards associated with operating or failure modes and is especially intended to determine how operation or failure of components affects the overall safety of the system.
Project Hazard Log (PHL)	Also known as System Hazard Log (SHL), is the record of the system level hazards associated with the development and implementation of the ACSES II system for LIRR.

Table 4: Acronyms Specific to this Document

Acronym	Definition
PHA	Preliminary Hazard Analysis
PHL or SHL	Project Hazard Log
SSHA	Subsystem Hazard Analysis
SSDD	Subsystem Description Document
FTA	Fault Tree Analysis
HA	Hazard Analysis

2.4 Objective

The following issues are considered during the performance of the SSHA:

- Modes of failure including reasonable human errors, single point and common mode failures, and the effects of failure on subsystem elements.

- Potential contribution of hardware and software controlled events, faults and occurrences
- Satisfaction of all safety design criteria.
- Integrating safety testing into hardware and software testing programs.
- System level hazards attributed to subsystems are controlled.
- Input information from other subsystems that is required to perform the functions of this ACSES II Subsystem in a safe manner.

3 Subsystem Overview

Please refer to RWPS Sub-System Description Document (SSDD), [4]

4 Methodology

The SSHA verifies the primary hazards that are applicable to the RWPS Subsystem. Primary hazards that the RWPS subsystem must control are identified based in the RWPS PHA [2].

The methods or actions for eliminating, minimizing, or controlling each hazard, as well as the recommended approach for eliminating, controlling, or minimizing hazard identified during this analysis are documented in the SSHA including:

- Independent, dependent and simultaneous events or failures and system interactions that could create increased risk.
- Effects of reasonable human errors.
- Effects on system safety from the functional, interoperable relationships between Components. Please note that subsystem relationships are addressed in the Project Hazard Log [1].
- Safety design criteria has been satisfied
- Analysis that implementation of safety recommendation and corrective actions will not impair or degrade safety performance of hardware or software and will not create additional hazards.

5 Hazard Assessment & SSHA result table

The contributors to the subsystem preliminary hazards identified in the RWPS PHA [2] are categorized and summarized in this section. The hazard analysis tables presented in this section include the assessment of applicability of the hazard contributors to RWPS, Subsystem operation and support, and hazards that are within the scope of the RWPS subsystem to mitigate. As well, the initial risk assessment, the proposed mitigation requirements, and the residual risk assessment based on the implementation of the mitigations are presented.

The hazards are analyzed and assessed to determine their associated risk. In general, the hazard assessment is performed according to Frequency and Severity of each hazard in the list. The hazard risk is derived according to best available data, problems reported from similar projects and other lessons learned from similar systems.

The analysis and assessment results are presented in table format which contains the following columns:

Table 5: Hazard Table column Definition/Description

Column Title	Description
ID	A unique identification number is provided per line to simplify hazard location in the tables
Reference ID (RWPS_PHA ID & FFT ID)	A unique identification number from the RWPS PHA. See the RWPS Preliminary Hazard Analysis [2]. The link to the fault tree will be updated once the Fault Tree is finalized.
Hazard Description	Description of the sub-system hazard.
Potential Cause	Description of the possible causes which might be at the origin of the hazard.
Effect	The effect (e.g. hazard consequences) of the hazard on the system.
Initial Risk/Hazard Severity	S - The severity of the hazard consequences; (Refer to the System Product Safety Plan [6]) F - The frequency of occurrence of the hazard condition; (Refer to the System Product Safety Plan [6]) R - The risk level associated with the hazard; (Refer to the System Product Safety Plan [6])
Subsystem(s)/ Interface	Identification of the subsystem or interfaces that can contribute to the hazardous event: Onboard; Wayside; Data Communication System & STS database.

Column Title	Description
Type	Type of control measure; can be one or more of design, Operation, Maintenance.
Safety Req.	The safety requirement listed in table 8 of RWPS PHA [2].
Hazard Control	Description of how the Subsystem or components will control the hazard
Residual Risk	The risk that remains after all efforts have been made to mitigate or eliminate risks or danger of an event. S - The severity of the hazard consequences; (Refer to the System Product Safety Plan[6]) F - The frequency of occurrence of the hazard condition; (Refer to the System Product Safety Plan [6])
Subsystem Function involved	ACSES II Subsystem level function description.
Safety Verification	Method(s) used to verify the Hazard has been properly mitigated by the component / system (Analysis, Test, Demonstration, or Inspection)
Comments	General remarks to the subsystem identified hazards.

5.1 RWPS Subsystem Hazard Analysis Table

The Subsystem Hazard Analysis is presented in Tabular form as per column Description given in Table 5 above. Refer to Table 6.

Table 6: RWPS Sub system Hazard Analysis

RWPS_SSHA_ID	Reference ID		Subsystem Hazard Description	Potential Cause	Effect	Initial Risk			Sub-Syst/ I'face	Type	Residual Risk		Subsystem Function involved	Safety Verification Method	Comments
	RWPS_PHA ID SHA ID	FFT ID.				S	F	R			S	F			
RWPS_SSHA_01	RWPS_PHA_01		RWPS indicate TSR where no TSR has been applied. Or RWPS receives an incorrect TSR report from STS.	Message Failure between STS and RWPS. RWPS Failure indicating a TSR where no TSR exists	Staff struck by Train.	I	B	UN	RWPS	Operations	I	E	RWPS Operations	Analysis of Training Material	
RWPS_SSHA_02	RWPS_PHA_02 SYS_IHA_37 RWPS_IHA_04		TSR Requested or removed from incorrect location.	RWPS Database provides incorrect location RWPS Equipment Fails sending request for wrong location. EIC enters wrong location	Staff struck by Train.	I	B	UN	RWPS	Design	I	E	RWPS Data Design	Analysis of Training Material	
RWPS_SSHA_03	RWPS_PHA_03 RWPS_PHA_04		Person in contact with or near an electrical power source.	Material with electrical potential accessible to passengers in public area Inadequate maintenance procedures	Non-Vehicular death or injury (Staff or Passenger).	I	B	UN	RWPS	Design	I	E	RWPS Electrical Design	Analysis of Design	

RWPS_SSHA_ID	Reference ID		Subsystem Hazard Description	Potential Cause	Effect	Initial Risk			Sub-Syst/ I'face	Type	Residual Risk		Subsystem Function involved	Safety Verification Method	Comments
	RWPS_PHA ID SHA ID	FFT ID.				S	F	R			S	F			
RWPS_SSHA_04	RWPS_PHA_05 RWPS_PHA_06		Burns to passengers, crew and third parties Inhalation damage to passengers, crew, and third parties.	Inadequate cooling and ventilation of equipment, underrated cables, incorrect materials selection etc.	Non-Vehicular death or injury (Staff or Passenger)	I	B	UN	RWPS	Design	I	E	RWPS Design	Analysis of Design	
RWPS_SSHA_05	RWPS_PHA_07		TSR improperly removed.	Unauthorized access to EIC Terminal allows a user to request to remove TSR without authorization.	Staff struck by Train	I	B	UN	RWPS	Design	I	E	User Authentication	Analysis of Design	

RWPS_SSHA_ID	Reference ID		Subsystem Hazard Description	Potential Cause	Effect	Initial Risk			Sub-Syst/ I'face	Type	Residual Risk		Subsystem Function involved	Safety Verification Method	Comments
	RWPS_PHA ID SHA ID	FFT ID.				S	F	R			S	F			
RWPS_SSHA_06	RWPS_PHA_08		Design of RWPS created components that injure maintenance or installation staff.	Components have heavy weights, sharp edges etc.	Maintenance or installation staff injury.	III	B	UN	RWPS	Design	III	D	RWPS	FAI inspection	
RWPS_SSHA_07	RWPS_IHA_01		TSR Request from RWPS fails to be set.	Loss of Interface between RWPS and Office.	Staff Struck by Train.	I	B	UN	RWPS / Office	Design	I	D	Add TSR Remove TSR	Test Analysis	

RWPS_SSHA_ID	Reference ID		Subsystem Hazard Description	Potential Cause	Effect	Initial Risk			Sub-Syst/ I'face	Type	Residual Risk		Subsystem Function involved	Safety Verification Method	Comments
	RWPS_PHA ID SHA ID	FFT ID.				S	F	R			S	F			
RWPS_SSHA_08	RWPS_IHA_02		TSR request message from RWPS is corrupted before Office receives.	Incorrect Transfer of Information between RWPS and Office.	Staff Struck by Train	I	B	UN	RWPS/Office	Design	I	E	Add TSR Remove TSR	Analysis	
RWPS_SSHA_09	RWPS_IHA_03 RWPS_IHA_04		TSR Request from EIC fails to be sent.	Loss of Interface between EIC and RWPS.	Overspeed, Train Derailment, Staff Struck by Train.	I	B	UN	EIC to RWPS	Design	I	E	EIC Interface	Test Analysis	
RWPS_SSHA_10	RWPS_IHA_05		Both RWPS servers become controlling. EIC Terminal gets a different list of TSR.	Dual failure of GBN network prevents health check messages.	Staff Struck by Train.	I	B	UN	RWPS / RWPS	Design	I	E	RWPS Healthcheck	Test	

RWPS_SSHA_ID	Reference ID		Subsystem Hazard Description	Potential Cause	Effect	Initial Risk			Sub-Syst/ I'face	Type	Residual Risk		Subsystem Function involved	Safety Verification Method	Comments
	RWPS_PHA ID SHA ID	FFT ID.				S	F	R			S	F			
RWPS_SSHA__11	RWPS_IHA_06		EIC Terminal receives a corrupted message from RWPS and displays the data to the EIC.	Incorrect data transfer from RWPS to EIC Terminal.	Staff struck by Train.	I	B	UN	RWPS / EIC	Design	I	E	RWPS	Analysis of Design	
RWPS_SSHA_12	RWPS_OHA_02		Train does not receive correct TSR and enters roadway worker protection area.	EIC enters incorrect data into TSR Request.	Staff injury or death.	I	B	UN	RWPS	Operation	I	D	RWPS	Analysis of Operating Procedures	
RWPS_SSHA_13	RWPS_OHA_03		A trains fails to receive TSR.	RWPS In each control center become Controlling and only one gets request.	Staff injury or death.	I	B	UN	RWPS	Operation	I	D	RWPS	Analysis of Operating Procedures	

RWPS_SSHA_ID	Reference ID		Subsystem Hazard Description	Potential Cause	Effect	Initial Risk			Sub-Syst/ I'face	Type	Residual Risk		Subsystem Function involved	Safety Verification Method	Comments
	RWPS_PHA ID SHA ID	FFT ID.				S	F	R			S	F			
RWPS_SSHA_14	RWPS_OHA_04		TSR Removed with Secondary EIC in area.	RWPS failure allows TSR Removal when Secondary EIC still in area.	Staff injury or death.	I	B		RWPS	Operation	I	D	RWPS	Analysis of Operating Procedures	
RWPS_SSHA_15	RWPS_OHA_05 RWPS_OHA_06		EIC Terminal shows TSR where no TSR is enforced.	RWPS Failure indicates TSR where none exists	Staff injury or death.	I	B		RWPS	Operation	I	D	RWPS	Analysis of Operating Procedures	
RWPS_SSHA_16	RWPS_OHA_07		TSR Removed with EIC in area.	Supervisor performs TSR Override with EIC still in area.	Staff injury or death.	I	B		RWPS	Operation	I	D	RWPS	Analysis of Operating Procedures	
RWPS_SSHA_17	RWPS_OHA_08		TSR request not received by RWPS.	Loss of communication between EIC Terminal and RWPS.	Staff injury or death.	I	B	UN	RWPS	Operation	I	D	RWPS	Testing. Analysis of Operating Procedures	

5.2 Hazard Analysis Results

The SSHA verified the Causes as the contributors to the Preliminary Hazards. These hazards have been tracked from the RWPS PHA [2] to the System PHA [5] reference ID.

6 Functional Safety Requirements

The preliminary hazard analysis highlights several safety requirements that have to be implemented during the RWPS Sub-System life cycle.

6.1 Safety Requirement

All RWPS safety requirements developed from the PHA tables as well as the methods used to mitigate the hazard will be logged in the Sub-System Hazard Log (“Identification of proposed hazard mitigation”).

The methods used to mitigate the hazard will specify how the safety requirement must be taken into account by the RWPS Sub-System, and/or by Operating Procedures.





7 Conclusion

The LIRR PTC RWPS Subsystem Hazard Analysis (SSHA) captures the potential hazards in the operation of the RWPS Sub-System.

In Section 5, the analysis of the Subsystem Hazards was further analyzed in this document. The result shows that those hazards can be mitigated to a tolerable level and can be considered non-significant or zero effect on the operation of the ACSES II system.

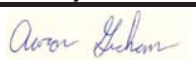
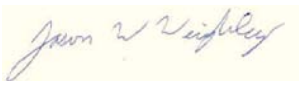
In Section 6 , the Safety requirements are identified. These requirements are listed in Table 7.

Metropolitan Transportation Authority
Long Island Rail Road / Metro-North Railroad
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712/29544

RWPS Interface Hazard Analysis

CDRL 2-131-06

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Aaron Graham System Safety Engineer		Aaron Graham 2019.07.25 15:05:14 -04'00'
Verified:	Jason Weighley System Safety Engineer		Jason W Weighley 2019.07.25 15:31:46 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.07.25 17:12:04 -04'00'
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group		Phil Magloire 2019.07.26 06:38:42 -04'00'
BT/SRA Review:	NA		
BT/SRA Review:	NA Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3037436

Effective Date:	Revision:	Language:
2019-07-25	_C	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2014-10-31	First issue
_A	2015-09-23	Updated for PDR
_A.1	2018-02-27	Updated per RR Comments, also added relevent MNR material to create a common Document.
_A.2	2018-04-12	Updated per RR Comments
_A.3	2018-04-20	Updated per RR Comments
_B	2018-04-25	Updated for release
_C	2019-07-25	Updated in response to PTCSP Comments

Table of Contents

Section	Subject	Page
1	**Executive Summary**	6
2	**Introduction and Scope**	6
2.1	**Compliance Matrix**	6
2.2	**Reference Documents**	8
2.3	**Glossary**	9
2.4	**Methodology**	11
3	**Analysis Prerequisites**	12
3.1	**Subsystem Description**	12
3.2	**General Assumptions and Boundary Conditions**	13
4	**Summary of Interfaces**	14
4.1	**External interfaces**	14
4.1.1	EIC to EIC Terminal	14
4.1.1.1	Physical Attribute	14
4.1.1.2	Functional Attribute	14
4.1.1.3	Information Attribute	15
4.1.2	RWPS to Office (RGS)	15
4.1.2.1	Physical Attribute	15
4.1.2.2	Functional Attribute	15
4.1.2.3	Information Attribute	15
4.1.3	Office (RGS) to RWPS	15
4.1.3.1	Physical Attribute	15
4.1.3.2	Functional Attribute	15
4.1.3.3	Information Attribute	15
4.1.4	RWPS BCC to RWPS BCC	15
4.1.4.1	Physical Attribute	15
4.1.4.2	Functional Attribute	15
4.1.4.3	Information Attribute	15
4.1.5	Installing Executables and Data Configuration Files for RWPS	16
4.1.5.1	Physical Attribute	16
4.1.5.2	Functional Attribute	16
4.1.5.3	Information Attribute	16
4.1.6	Installing Executables and Data Configuration Files for EIC	16
4.1.6.1	Physical Attribute	16
4.1.6.2	Functional Attribute	16
4.1.6.3	Information Attribute	16
4.1.7	Superuser to Operation Superuser Workstation	16
4.1.7.1	Physical Attribute	16
4.1.7.2	Functional Attribute	16
4.1.7.3	Information Attribute	16

4.2 Internal Interfaces 17
4.2.1 RWPS to EIC Handheld 17
4.2.1.1 Physical Attribute 17
4.2.1.2 Functional Attribute 17
4.2.1.3 Information Attribute 17
4.2.2 EIC Handheld to RWPS 17
4.2.2.1 Physical Attribute 17
4.2.2.2 Functional Attribute 17
4.2.2.3 Information Attribute 17
4.2.3 RWPS to EIC Workstation 17
4.2.3.1 Physical Attribute 17
4.2.3.2 Functional Attribute 17
4.2.3.3 Information Attribute 17
4.2.4 EIC Workstation to RWPS 18
4.2.4.1 Physical Attribute 18
4.2.4.2 Functional Attribute 18
4.2.4.3 Information Attribute 18
4.2.5 RWPS to NMS 18
4.2.5.1 Physical Attribute 18
4.2.5.2 Functional Attribute 18
4.2.5.3 Information Attribute 18
4.2.6 RWPS to DMS 18
4.2.6.1 Physical Attribute 18
4.2.6.2 Functional Attribute 18
4.2.6.3 Information Attribute 18
4.2.7 RWPS to ADDC 18
4.2.7.1 Physical Attribute 18
4.2.7.2 Functional Attribute 19
4.2.7.3 Information Attribute 19
4.2.8 NMS to NMS 19
4.2.8.1 Physical Attribute 19
4.2.8.2 Functional Attribute 19
4.2.8.3 Information Attribute 19
4.2.9 NMS to EIC Handheld 19
4.2.9.1 Physical Attribute 19
4.2.9.2 Functional Attribute 19
4.2.9.3 Information Attribute 19
4.2.10 NMS to EIC Workstation 19
4.2.10.1 Physical Attribute 19
4.2.10.2 Functional Attribute 19
4.2.10.3 Information Attribute 19
4.3 IHA Hazard Category 20
4.4 Hazard Log Tracking 20
5 Hazard Description & Result Table 20
5.1 RWPS Interface Hazard Analysis Table 21

6 Safety Requirements 21
7 Conclusion 24
8 Attachment A 24

List of Figures

Figure 1: RWPS Office Interface Diagram 13

List of Tables

Table 1: Compliance Matrix 6
Table 2: Reference Documents 8
Table 3: Terms Specific to this Document 10
Table 4: Acronyms Specific to this Document 10
Table 5: Hazard Table Column Definition/Description 20
Table 6: Safety Requirements 21

1 Executive Summary

This document records the RWPS Interface Hazard Analysis of the LIRR and MNR PTC systems. This analysis forms part of the evidence to support compliance with the safety requirements allocated to the ACSES II RWPS Subsystems.

2 Introduction and Scope

This hazard analysis documents the interface hazard analysis (IHA) performed for the ACSES II RWPS Subsystem. The interfaces for this analysis were determined by review of the RWPS Subsystem Description [2]. This IHA is the hazard analysis performed to serve as one of the inputs to the Project Hazard Log [9].

The ACSES II RWPS Subsystem IHA provides the analysis of all the interfaces associated with the RWPS subsystem for the LIRR and MNR PTC projects. This analysis will also perform an analysis of any maintenance and diagnostic tools that interface to the subsystem. This document will identify each interface, identifying the potential hazards associated with the loss of or incorrect functioning of the interface together with the mitigations in place to maintain the safety of the ACSES II System and Subsystems. The analysis of external interfaces from the RWPS subsystem, are covered in the System Interface Hazard Analysis.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
Vol 2 Part 1	12.10.6 A to C	Interface Hazard Analysis	The Interface Hazard Analysis (IHA), CDRL 2-131, shall be performed by the SI and subsystem supplier and be documented on the ACSES II System and Subsystems.	All

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.6 A	Interface Hazard Analysis	The ACSES II Subsystem IHA provides the analysis of all the interfaces associated with the ACSES II Subsystem. The Interface Hazard Analysis shall identify each interface for the ACSES II Subsystem, identifying the potential hazards associated with the loss of or incorrect functioning of the interface together with the mitigations in place to maintain the safety of the ACSES II System and Subsystems.	Sec. 4.0, 4.1, and 5.1
	12.10.6 B	Interface Hazard Analysis	The SI shall combine the results of the ACSES II Subsystem IHAs into an overall IHA for the ACSES II System. This process is designed to ensure that all hazards associated with the interfaces of the subsystems within the ACSES II System have been identified and adequately addressed and controlled to an acceptable level within the implementation of the ACSES II System for the Project.	Sec. 2.4
	12.10.6 C1	Interface Hazard Analysis	1. Physical, functional, information and all other interface attributes between ACSES II Subsystems.	Sec. 5.1

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
	12.10.6 C2	Interface Hazard Analysis	2. Loss of or incorrect transfer of information between ACSES II Subsystem.	Sec. 5.1
	12.10.6 C3	Interface Hazard Analysis	3. Timing issues associated with the transfer of information.	Sec. 5.1
	12.10.6 C4	Interface Hazard Analysis	4. Redundancy management and assurance of information during redundancy handover.	Sec. 5.1
	12.10.6 C5	Interface Hazard Analysis	5. Required alarm notifications and safe default actions for the interface failures.	Sec. 5.1
	12.10.6 C6	Interface Hazard Analysis	6. Handover of information between wayside to carborne.	Sec. 5.1
	12.10.6 C7	Interface Hazard Analysis	7. Testing of interface subsystems to ensure correct operation of the subsystems and overall system.	Sec. 5.1

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624
[2]	RWPS Sub-System Description Document CDRL 2-201	3035851
[3]	MIL-STD-882C	N/A
[4]	System Product Safety Plan CDRL 2-123-20 System Product Safety Plan CDRL 2-132-10	3035815 3036437
[5]	RAM Program Plan CDRL 2-139	3035841
[6]	RWPS Product Safety Plan CDRL 2-123-06	3036415

Reference Number	Document Name	Identification Number
[7]	System Preliminary Hazard Analysis CDRL 2-127	3035821
[8]	RWPS System Safety Concept Description CDRL 2-124-06	3036417
[9]	Project Hazard Log CDRL 2-126-20 Project Hazard log CDRL 2-126-10	3035819 3043891
[10]	RWPS Interface Control Document CDRL 2-225	3035874
[11]	System Interface Hazard Analysis CDRL 2-131-20 System Interface Hazard Analysis CDRL 2-13-10	3035828 3043905
[12]	AREMA, Communications and Signals Manual – 2009 Section Parts 16, 17, 21, and 23.	Revision 2001
[13]	CENELEC EN50126, Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)	EN50126:1999
[14]	CENELEC Standard. Railway Applications – Communication, signaling and processing systems – Safety related electronic systems for signaling.	EN50129:2003
[15]	RWPS Subsystem Design Description CDRL 2-201	3035851
[16]	RWPS Preliminary Hazard Analysis CDRL 2-127-06	3036416

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in Table 3 and Table 4 respectively.

Table 3: Terms Specific to this Document

Term	Definition
Interface Hazard Analysis (IHA)	An analysis performed on the potential hazards identified between subsystems associated interfaces. To identify hazards that associates with the loss of or incorrect functioning of the interface together with the mitigations in place to maintain the safety of the entire system.
Product	A train control system, subsystem, or component. Or An element of the physical or system architecture, specification tree, or system breakdown structure that is a subordinate element to the system or subsystem and which is wholly documented in a separate way, and considered as a terminal branch of the specification tree.
Review	The assessment of a work product's content to verify adherence to defined standards, guidelines, specifications and procedures.
Risk	An expression combining the probability of the mishap occurring with the severity of the consequences of the mishap, used to rank hazards.
Risk Assessment	The process of determining the amount of risk associated with use of the product under all intended operating conditions and anticipated conditions. Risk assessment techniques for any product may include qualitative, semi-quantitative and quantitative approaches.

Table 4: Acronyms Specific to this Document

Acronym	Definition
SPSP	System Product Safety Plan
SSHA	Subsystem Hazard Analysis
IHA	Interface Hazard Analysis
PHL	Preliminary Hazard List
RGS	Railroad Gateway Server
RWPS	Roadway Worker Protection System
DMS	Data Management System
NMS	Network Management System

Acronym	Definition
ADDC	Active Directory Domain Controller

2.4 Methodology

The analysis will identify the cause and effect of possible independent, dependent and simultaneous failures that could present a hazardous condition. The analysis will also be subjected to design review in order to verify that design modifications do not introduce new hazards or increase the risk from existing hazards.

The RWPS Subsystem IHA will address the following for each interface:

- Physical, functional, information and all other interfaces
- Loss or incorrect transfer of information
- Timing issues associated with the interfaces
- Redundancy management and assurance of information during redundancy handover
- Required alarm notifications and safe default actions for interface failures
- Handover of information between wayside and carborne
- Testing of interfaces to ensure correct operation

The Subsystem Safety Engineer will add the Interface Hazards to the Subsystem Hazard Analysis and were relevant to the Project Hazard Log.

Any new hazards, or more detailed information on previously identified hazards, will be added to the Hazard Log and properly tracked and mitigated.

Safety Document	**Required Inputs from Project**	**Comments**
System Hazard Analysis	1. System Level Requirements Specification (SLR) 2. System Design Description (SDS) 3. System PHA	System PHA is split into System functions and assigned to subsystem by SHA. System Design Description is reviewed, and updated hazards are added to the SHA based on current system design.
Subsystem Hazard Analysis (SSHA)	1. Subsystem Level Requirements Specification (SSLR) 2. Subsystem Design Description	Each subsystem performs its own subsystem hazard analysis as per its subsystem safety plan.

Safety Document	Required Inputs from Project	Comments
	3. System Hazard Analysis 4. Each subsystem Preliminary Hazard Analysis	
Interface Hazard Analysis (IHA) (System and all Subsystem)	1. System Design Specification (SDS) 2. Interface Control Documents 3. PHA (from all the Subsystems) 4. SSHA (of each Subsystems)	This should cover both internal and external interfaces.
Project Hazard Log – (System)	1. Hazard List from PHA, SHA, SSHA; IHA; OHA; FTA. 2. Hazards from all the Subsystem Hazard Analysis.	Each sub system must also track its own hazards in the sub system hazard Analysis. Those hazards which can't be closed at Subsystem level should be exported to System Hazard Log, i.e. Project Hazard Log.

The methodology used to perform the RWPS Subsystem IHA used the following steps:

1. Identification of external and internal sub system interfaces.
2. Identification of all interfaces that are vital.
3. Tabular analysis allowing classifications of the hazards due to interface failures, as well as identification of the measures to be taken for risk reduction.

The hazard analysis was then conducted according to the steps defined in the System Product Safety Plan [4] and the RWPS System Safety Concept Description [8].

3 Analysis Prerequisites

3.1 Subsystem Description

A detail description of the subsystem is given in the RWPS SDD [2].

Figure 1 shows the basic architecture of the RWPS Office Subsystem at the Primary Control Center. The Backup Control Center is a replica of the Primary Control Center. The RWPS along with its EIC Terminals are responsible for managing TSR requests and TSR information associated with Roadway worker protection. The RWPS sends TSR requests and retrieves TSR Status and other messages with the Office subsystem. The ADDC and SEC perform the User Authentication and Security. The DMS provides Data Logging and review. NMS provides for alarm management and maintenance functionality.

The RWPS Interface Control Document [10] describes the structure and content of each interface in detail.

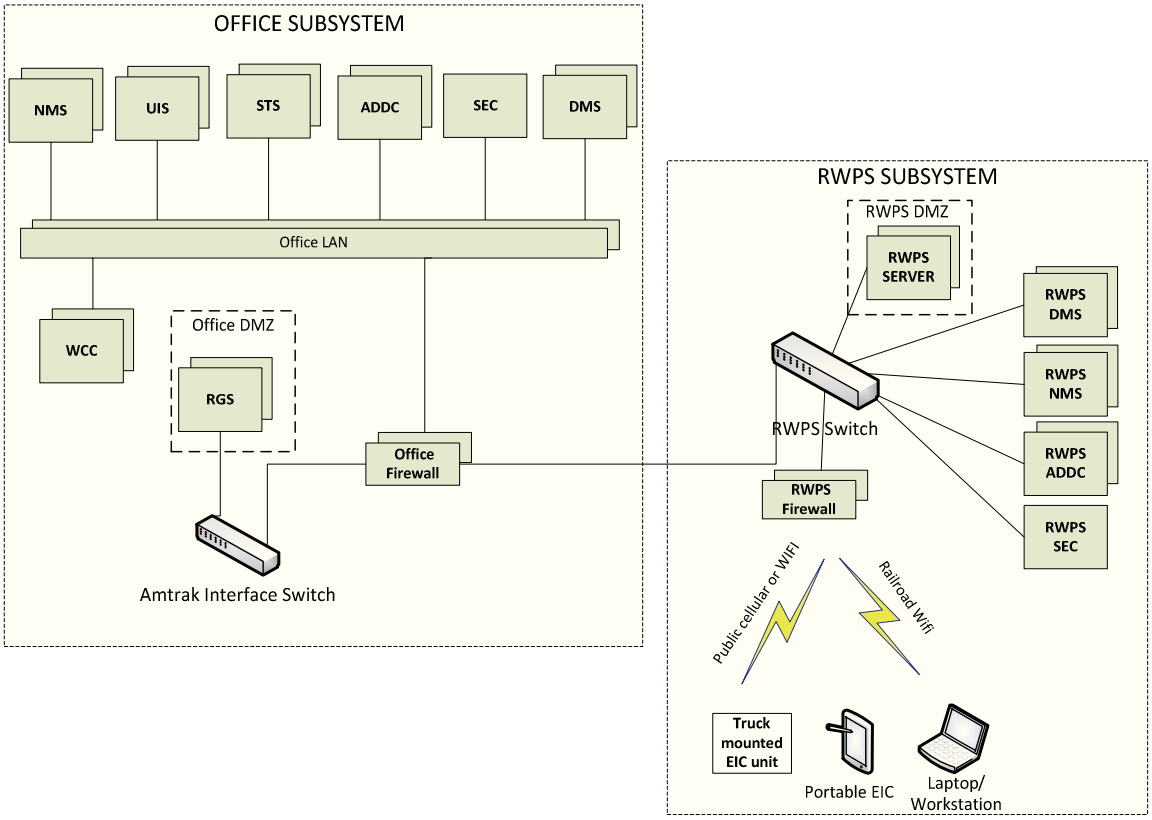


Figure 1: RWPS Office Interface Diagram

3.2 General Assumptions and Boundary Conditions

The following general assumptions and boundary conditions apply to the IHA.

- The analysis covers normal, degraded, and emergency operational modes of the equipment. The equipment is assumed to have been correctly installed, and its function completely verified before it is taken into operation.

4 Summary of Interfaces

The results from this subsystem IHA will be collected and combined with other subsystem IHAs to form an overall IHA for the ACSES II System. This process is designed to ensure that all hazards associated with the interfaces of the subsystems within the ACSES II System have been identified and adequately addressed and controlled to an acceptable level within the implementation of the ACSES II System for the Project.

External Interfaces:

a. EIC to EIC Terminal.
b. RWPS to Office (RGS)
c. Office (RGS) to RWPS
d. RWPS BCC to RWPS BCC
e. Installing Executables and Data Configuration Files for RWPS
f. Installing Executables and Data Configuration Files for EIC
g. Superuser to Workstation

Internal Interfaces:

a. RWPS to EIC Handheld
b. EIC Handheld to RWPS
c. RWPS to EIC Workstation
d. EIC Workstation to RWPS
e. RWPS to NMS
f. RWPS to DMS
g. RWPS to ADDC
h. NMS to NMS
i. RWPS to RWPS
j. NMS to EIC Handheld
k. NMS to EIC Workstation

4.1 External interfaces

4.1.1 EIC to EIC Terminal

4.1.1.1 Physical Attribute

Display indications from the EIC Terminal to the Employee in Charge User.

4.1.1.2 Functional Attribute

List TSR start and stop location and speed for each TSR in the assigned area. Must allow EIC to enter TSR start and stop location, and TSR speed.

4.1.1.3 Information Attribute

Indicate RWPS server connection with this EIC terminal. RWPS to Office communication status.

4.1.2 RWPS to Office (RGS)

4.1.2.1 Physical Attribute

Ethernet interface that utilizes the RGS component.

4.1.2.2 Functional Attribute

Allows RWPS to send TSR requests from EIC terminals to the Office.

4.1.2.3 Information Attribute

Allows RWPS to send alarms on RWPS system status to NMS.

4.1.3 Office (RGS) to RWPS

4.1.3.1 Physical Attribute

Ethernet interface that utilizes the RGS component.

4.1.3.2 Functional Attribute

Allow Office to send active and approved TSR Lists to the RWPS. Office NMS will have the ability to interface to RWPS Server to allow remote reboot of equipment.

4.1.3.3 Information Attribute

Indicate UIS connection to STS.

4.1.4 RWPS BCC to RWPS BCC

4.1.4.1 Physical Attribute

Ethernet interface.

4.1.4.2 Functional Attribute

RWPS TSR request from active to standby.

*Note: UIS sends each RWPS server the TSR list.

4.1.4.3 Information Attribute

Active/controlling status of each RWPS Server.

4.1.5 Installing Executables and Data Configuration Files for RWPS

4.1.5.1 Physical Attribute

USB Interface

4.1.5.2 Functional Attribute

Engineering to confirm that there is an error check on the software load.

4.1.5.3 Information Attribute

Latest MAP Version status to be checked with UIS.

4.1.6 Installing Executables and Data Configuration Files for EIC

4.1.6.1 Physical Attribute

USB

4.1.6.2 Functional Attribute

Engineering to confirm that there is an error check on the software load.

4.1.6.3 Information Attribute

Latest MAP Version status shall be checked with UIS.

4.1.7 Superuser to Operation Superuser Workstation

4.1.7.1 Physical Attribute

Display interface for Superuser.

4.1.7.2 Functional Attribute

Superuser can request override Primary EIC. Superuser can also request Control User release of a ‘not logged on’ Secondary EIC from a TSR. Can act like a Primary EIC to delete an existing EIC TSR. View list of active EICs logged into system

4.1.7.3 Information Attribute

View all applicable alerts. Needs to know loss of Comms at EIC terminals.

4.2 Internal Interfaces

4.2.1 RWPS to EIC Handheld

4.2.1.1 Physical Attribute

Ethernet interface through Cellular/Wi-Fi.

4.2.1.2 Functional Attribute

View active TSR list. Must be able to view Secondary EIC's.

4.2.1.3 Information Attribute

Needs to be able to see communication status of RWPS server. RWPS Server status to be sent to EIC terminals. Must be able to see RWPS connections status to UIS.

4.2.2 EIC Handheld to RWPS

4.2.2.1 Physical Attribute

Ethernet interface through Cellular/Wi-Fi.

4.2.2.2 Functional Attribute

EIC must be able to Request/change/remove TSR.

*__Note:__ If request from EIC Workstation gets lost, it becomes stale data. This is not a safety issue, and can be covered through Select/Check/Execute.

4.2.2.3 Information Attribute

N/A

4.2.3 RWPS to EIC Workstation

4.2.3.1 Physical Attribute

Ethernet interface.

4.2.3.2 Functional Attribute

Must be able to view active TSR list. Must be able to view Secondary EIC's.

4.2.3.3 Information Attribute

Needs to be able to see communication status of RWPS server. RWPS Server status to be sent to EIC workstations. Must be able to see RWPS connections status to UIS.

4.2.4 EIC Workstation to RWPS

4.2.4.1 Physical Attribute

Ethernet interface.

4.2.4.2 Functional Attribute

EIC must be able to Request/change/remove TSR.

*__Note:__ If request from EIC Workstation gets lost, it becomes stale data. This is not a safety issue, and can be covered through Select/Check/Execute.

4.2.4.3 Information Attribute

N/A

4.2.5 RWPS to NMS

4.2.5.1 Physical Attribute

Ethernet interface.

4.2.5.2 Functional Attribute

Active standby/controlling status of RWPS servers.

4.2.5.3 Information Attribute

Office communication status alert. RWPS communication status alert. EIC Terminal status.

4.2.6 RWPS to DMS

4.2.6.1 Physical Attribute

Ethernet interface.

4.2.6.2 Functional Attribute

TSR requests to UIS must be logged.

4.2.6.3 Information Attribute

Loss of comms with DMS.

4.2.7 RWPS to ADDC

4.2.7.1 Physical Attribute

Ethernet interface.

4.2.7.2 Functional Attribute

Authenticate users and provide Role-definition for users (i.e. EIC or Superuser).

4.2.7.3 Information Attribute

Loss of communication to ADDC.

4.2.8 NMS to NMS

4.2.8.1 Physical Attribute

Ethernet interface.

4.2.8.2 Functional Attribute

Network communication and device status (active and controlling).

4.2.8.3 Information Attribute

Loss of communication

4.2.9 NMS to EIC Handheld

4.2.9.1 Physical Attribute

Ethernet interface through Cellular/WIFI.

4.2.9.2 Functional Attribute

Determine whether EIC handheld is out on the network. Is NMS providing device authentication (i.e. WMAC authentication).

4.2.9.3 Information Attribute

Device on network not present.

4.2.10 NMS to EIC Workstation

4.2.10.1 Physical Attribute

Ethernet interface.

4.2.10.2 Functional Attribute

Determine whether EIC workstation is out on the network.

4.2.10.3 Information Attribute

Device on network not present.

4.3 IHA Hazard Category

The risk classification used in the Interface Hazard analysis defined for severity, frequency, and risk assessment follows the frame work set in the System Product Safety Plan [4]. This frame work was derived from AREMA and MIL_STD_882C guidelines.

4.4 Hazard Log Tracking

Every hazard defined in this Interface Hazard Analysis has been entered into the project hazard log and tracked according to the process defined in the System Product Safety Plan [4], and the RWPS Subsystem Product Safety Plan [6]. The mitigations for the interface hazards will also be entered into project hazard log and linked to the appropriate requirement(s) and reported in the Requirement Traceability Matrix.

5 Hazard Description & Result Table

The hazard analysis tables presented in this section include Physical, functional, information and all other interface attributes between the components of the RWPS subsystem and users of the RWPS subsystem.

The hazards are analyzed and assessed to determine their associated risk. In general, the hazard assessment is performed according to Frequency and Severity (explained in Section 4.4) of each hazard in the list. The hazard risk is derived according to best available data, problems reported from similar projects and other lessons learned from similar systems.

The analysis and assessment results are presented in table format which contains the following columns:

Table 5: Hazard Table Column Definition/Description

Column Title	Description
RWPS_IHA ID	A unique identification number for the RWPS IHA. The format of this ID is RWPS_IHA_XX, where *XX* is a unique number.
Assigned Interface	Subsystem Level description of the interface
Detailed interface Description	Specific details of the interface being analyzed.
Hazard Description	Description of the hazard that can be caused by the interface.
Hazard Cause	A person or thing that gives rise to an action, phenomenon, or condition.

Column Title	Description
Hazard Effects	A change that is a result or consequence of an action or other cause.
Hazard Log Reference	Reference ID to or from the hazard log.
Initial Risk Index	Preliminary Risk assessment. Prior to mitigation.
Final Risk Index	Hazard Risk Assessment including mitigation.
Mitigation/Controls/Safeguards	Means that can be employed to prevent the Hazard or detect the hazard.
Remarks	Additional comments

5.1 RWPS Interface Hazard Analysis Table

The Hazard Analysis is presented in Tabular form as per the column Definition/Description given in Table 5 above. Refer to Attachment A.

6 Safety Requirements

All RWPS safety requirements developed from the IHA tables, as well as the methods used to mitigate the hazard, will be logged in the Subsystem Hazard Log. Each entry in this log will be linked to subsystem-specific requirements that implement the mitigation and/or operating mitigations that will be indicated in training manual or operating procedures, The System and RWPS Product Safety Plans ([4],[6]) detail the traceability of the hazards to requirements.

The methods used to mitigate the hazard will specify how the safety requirement must be





7 Conclusion

The LIRR/MNR ACSESS II RWPS Subsystem Interface Hazard Analysis (IHA) have identified the potential interface hazards in the RWPS Subsystem. Mitigations to these hazards have been added to the design to ensure that any possible failures will be detected, and the system will safely respond to these failures. Where these failures warrant additional actions from users, they are captured in safety requirements for process, procedure, and training; and where these failures require other subsystem actions, they are also captured in the Safety Requirements in Table 6. Where these failures warrant additional actions from users or other subsystems these hazards have been added to the Project Hazard Log for proper tracking of the mitigations.

8 Attachment A

RWPS Interface Hazard Analysis Table

RWPS_IHA_ID	Assigned Interface	Detailed interface Description	Subsystem Hazard Description	Hazard Cause	Hazard Effect	Hazard Log Reference	Initial Risk	Final Risk	[redacted]	Safety Requirement ID	Remarks
RWPS_IHA_01	RWPS / Office	Redundant Ethernet Interface via RGS	TSR Request from RWPS fails to be set in the Office Subsystem.	Loss of Interface between RWPS and Office.	Overspeed, Train Derailment, Staff Struck by Train	RWPS HL - 74	IB	ID		RWPS_SR-31 RWPS_SR-32 RWPS_SR-33 RWPS_SR-43 RWPS_SR-44 RWPS_SR-89	
RWPS_IHA_02	RWPS / Office	Redundant Ethernet Interface via RGS	TSR request message from RWPS is corrupted before Office receives.	Incorrect Transfer of Information between RWPS and Office.	Overspeed, Train Derailment, Staff Struck by Train	RWPS HL - 75	IB	ID		RWPS_SR-34 RWPS_SR-45 RWPS_SR-87	
RWPS_IHA_03	RWPS / EIC Handheld	Ethernet interface through Cellular/WIFI	TSR Request from EIC fails to be set in RWPS and in Office.	Loss of RWPS Interface to EIC Handheld.	Overspeed, Train Derailment, Staff Struck by Train.	RWPS HL - 76	IB	ID		RWPS_SR-33 RWPS_SR-35 RWPS_SR-36 RWPS_SR-39 RWPS_SR-81 RWPS_SR-94	
RWPS_IHA_04	RWPS / EIC Handheld	Ethernet interface through Cellular/WIFI	TSR request from EIC Handheld is incorrect.	Deliberate attack causes incorrect transfer of information.	Overspeed, Train Derailment, Staff Struck by Train.	RWPS HL - 77	IB	ID		RWPS_SR-36 RWPS_SR-37 RWPS_SR-38 RWPS_SR-95	
RWPS_IHA_06	RWPS / RWPS	Redundant Ethernet via the RGS in the Office	Both RWPS servers become controlling. TSR Request not sent to Office.	Dual failure of GBN network prevents health check messages.	Staff Struck by Train.	RWPS HL - 78	IB	IE		RWPS_SR-41 RWPS_SR-55 RWPS_SR-81	
RWPS_IHA_07	RWPS / EIC Handheld	Ethernet interface through Cellular/WIFI	EIC Terminal receives a corrupted message from RWPS and displays the data to the EIC.	Deliberate attack causes incorrect data transfer from RWPS to EIC Handheld.	Staff struck by Train.	RWPS HL - 79	IB	ID		RWPS_SR-36 RWPS_SR-38 RWPS_SR-47	
RWPS_IHA_08	RWPS / EIC Workstation	Through the internet	EIC Terminal receives a corrupted message from RWPS and displays the data to the EIC.	Deliberate attack causes incorrect data transfer from RWPS to EIC Workstation.	Staff Struck by Train.	RWPS HL - 80	IB	ID		RWPS_SR-38 RWPS_SR-47 RWPS_SR-48	

RWPS_IHA_09	RWPS / EIC Handheld	Ethernet interface through Cellular/WIFI	TSR request from EIC Handheld is incorrect.	Radio Interference causes incorrect transfer of information.	Overspeed, Train Derailment, Staff Struck by Train.	RWPS HL - 81	IB	ID	[redacted]	WPS_SR-36 WPS_SR-37 WPS_SR-38 WPS_SR-49 WPS_SR-95	
RWPS_IHA_13	RWPS / EIC Workstation	Through the internet	EIC Terminal receives a corrupted message from RWPS and displays the data to the EIC.	Radio Interference causes incorrect transfer from RWPS to EIC Workstation..	Staff Struck by Train.	RWPS HL - 82	IB	ID		WPS_SR-38 WPS_SR-47	
RWPS_IHA_14	Superuser / Operation Superuser Workstation	Display interface for Superuser	TSR removed while work crew on track.	EIC Handheld loss of communication not indicated to staff.	Staff Struck by Train.	RWPS HL - 83	IB	ID		WPS_SR-29 WPS_SR-63	
RWPS_IHA_15	Display Interface for Superuser	Display interface for Superuser	Single user removes TSR without proper checks.	Superuser logged in at UIS and RWPS.	Staff Struck by Train.	RWPS HL - 84	IB	ID		WPS_SR-29 WPS_SR-52	
RWPS_IHA_16	RWPS / NMS	Redundant Ethernet.	Wrong RWPS Server Active and Controlling.	Loss of communication - Remote reset of RWPS not possible.	Staff Struck by Train.	RWPS HL - 85	IB	ID		WPS_SR-33	
RWPS_IHA_17	RWPS / EIC Workstation	Through Internet	TSR request from EIC fails to be set in RWPS and in Office.	Loss of RWPS Interface to EIC Workstation.	Overspeed, Train Derailment, Staff Struck by Train.	RWPS HL - 86	IB	ID		WPS_SR-33 WPS_SR-35 WPS_SR-46 WPS_SR-81 WPS_SR-94	
RWPS_IHA_18	NMS / EIC Handheld	Ethernet interface through Cellular/WIFI	Staff assumed clear when EIC is loss of comm.	Loss of EIC to NMS communication.	Staff Struck by Train.	RWPS HL - 87	IB	ID		WPS_SR-29 WPS_SR-35 WPS_SR-81 WPS_SR-94	
RWPS_IHA_19	Installing Executables and Data Configuration Files for RWPS	USB	Error in TSR Indication to EIC.	Executable Corruption.	Staff Struck by Train.	RWPS HL - 88	IB	ID		WPS_SR-16 WPS_SR-82 WPS_SR-85	Still working on implemetnation of map check with RWPS
RWPS_IHA_20	Installing Executables and Data Configuration files for EIC	USB	Error in TSR Indication to EIC.	EIC Terminal executes incorrect executable.	Staff Struck by Train.	RWPS HL - 89	IB	ID		WPS_SR-16 WPS_SR-83	Still working on implementation of Map Chedk with RWPS
RWPS_IHA_21	EIC / EIC Handheld	Screen	Error in TSR Indication to EIC.	Screen changes TSR Start/Stop location or speed.	Staff Struck by Train.	RWPS HL - 90	IB	ID		WPS_SR-33 WPS_SR-38	
RWPS_IHA_22	EIC / EIC Workstation	Screen	Error in TSR Indication to EIC.	Screen changes TSR Start/Stop location or speed.	Staff Struck by Train.	RWPS HL - 91	IB	ID		WPS_SR-33 WPS_SR-38	

RWPS_IHA_23	Office / RWPS	Redundant Ethernet interface via RGS	TSR list from Office fails to be sent to the RWPS Subsystem.	Loss of Interface between Office and RWPS.	Overspeed, Train Derailment, Staff Struck by Train.	RWPS HL - 92	IB	ID	[redacted]	RWPS_SR-18 RWPS_SR-31 RWPS_SR-32 RWPS_SR-33 RWPS_SR-43 RWPS_SR-44 RWPS_SR-84 RWPS_SR-89	
RWPS_IHA_24	Office / RWPS	Redundant Ethernet Interface via RGS	TSR list from Office is corrupted before RWPS receives.	Incorrect transfer of information between Office and RWPS.	Overspeed, Train Derailment, Staff Struck by Train.	RWPS HL - 93	IB	ID	[redacted]	RWPS_SR-12 RWPS_SR-27 RWPS_SR-88	



Long Island Rail Road
PTC Safety Plan – Safety Analysis of Work Zone Incursion Protection from Human Error

Docket Number: FRA-2010-0031

DRAFT ONLY

Revision Date: 2019-08-15

Revision Number: 0.2

Submitted in fulfillment of 49 CFR Part 236, Subpart I, §236.1015, et.al.

REVISION HISTORY

Revision	Date	Description of Changes	Author
0.1	20-Jul-19	Initial Document Created, based on content from Section 21 of PTCSP Main Body.	W. Alston
0.2	15-Aug-19	Updated references to Attachments from Appendices to match Main Body	W. Alston

Table of Contents

Section Subject Page

Contents

1 Introduction 1

1.1 Functional Description of Work Zone Operations (with RWPS) 1

1.2 Mitigation of Human Errors Potentially Causing a Work Zone Incursion (RWPS-Enhanced) 1

List of Figures

Figure 21-1: Existing Manual Process vs. Process with ASCES and RWPS 2
Figure 21-2: Select-Check-Execute Failure Combined with RWPS… (from System FTA) 3
Figure 21-2: RWPS Subsystem Faults (from System FTA) 4

1 Introduction

This document meets the requirement of describing the safety analysis for protecting a work zone from unsafe incursions due to human error. It is based upon content originally in the LIRR PTCSP Main Body. It also includes pertinent excerpts from related documents, including but not limited to:

- System Fault Tree Analysis (**Attachment O**);
- Risk Assessment (**Attachment K**); and,
- RWPS Operating Hazard Analysis (**Attachment U**).

Each of these documents is included in full format in the Appendix of the LIRR PTCSP.

1.1 Functional Description of Work Zone Operations (with RWPS)

The ACSES II RWPS enhances the protection provided by onboard enforcement of train and engine movements while approaching or occupying work zones that have been conveyed via a track bulletin. In addition to the previous-described functions provided by ACSES II to prevent unauthorized train incursions into the limits of work zones, or unauthorized train movements when operating within the limits of a work zone, two (2) specific additional functions are provided.

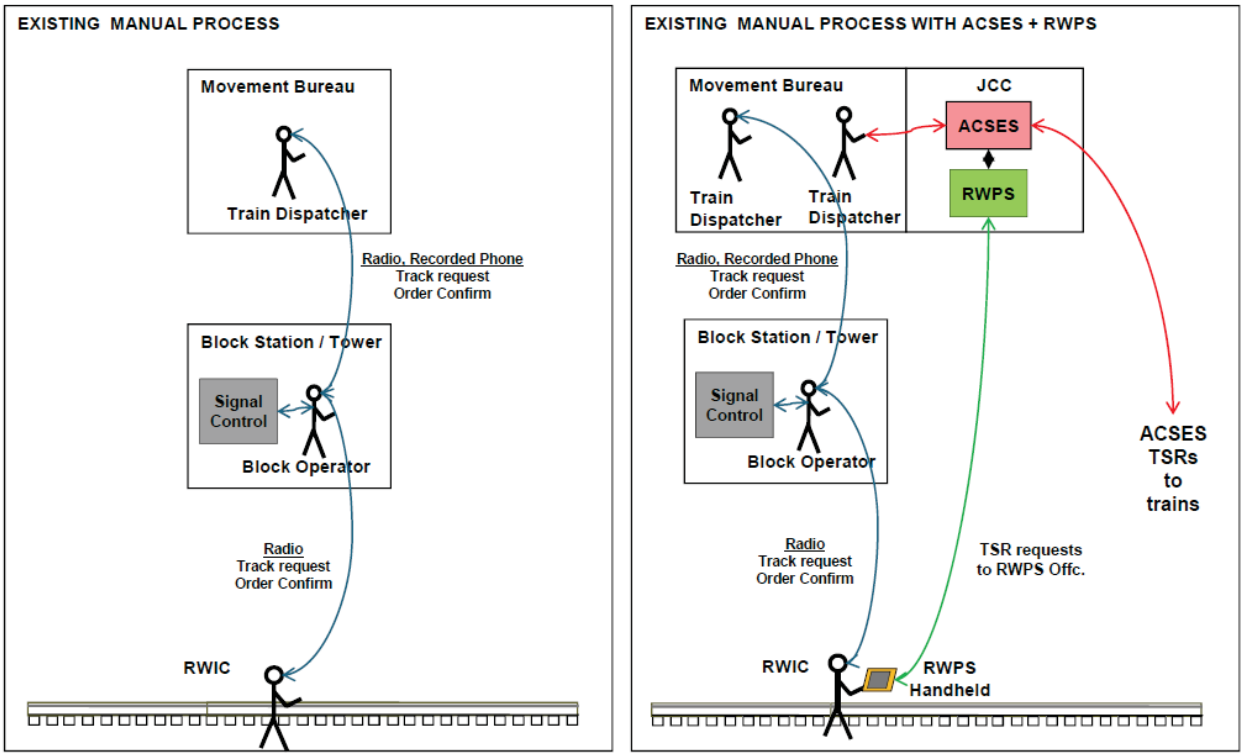
The Onboard System provides enforcement for the limits of the work zone. However, the status of existing TSRs is communicated digitally to the RWPS Handheld, allowing the RWIC to act accordingly. This is the first additional function supplied by the RWPS. As well, the RWPS can be used to establish TSRs, which become part of the list of TSRs enforced by the Onboard. This is the second additional function supplied by the RWPS. Finally, TSRs can be requested for removal via the RWPS, allowing for more real-time maintenance of the TSRs List, based upon Work Zones. However, given the safety impact of erroneously removing a TSR, all such requests must be verified by the STS, which adds an additional later of vital protection. All existing procedural protections for the establishment and/or removal of TSRs are in-place for the use of the RWPS, it simply provides a digital means for communication with the RWIC.

1.2 Mitigation of Human Errors Potentially Causing a Work Zone Incursion (RWPS-Enhanced)

After the incorporation of the RWPS, additional protections will exist. The LIRR EIC RWPS application is not part of the PTC system used onboard, but instead is used to digitize communications between the Roadway-Worker-In-Charge (RWIC), the EIC, and the dispatcher as appropriate. The RWPS is, in fact, another source for TSRs that must be followed by the onboard. This establishing of TSRs is how safety of the on-track staff is maintained and enhanced under PTC.

Figure 1-1 below presents a side-by-side comparison of the processes establishing a protected Work Zone in the "as-is" and planned process with the RWPS.

Figure 1-1: Existing Manual Process vs. Process with ASCES and RWPS



In order to demonstrate and verify that any risk for an unintended incursion into a Work Zone has been mitigated, the Terminal Faults that might be associated with the use and performance of the RWPS were analyzed via the System Level FTA. An excerpt of that fault tree analysis, specific to the RWPS, is provided below. There are three (3) Terminal Events identified for the RWPS, given its three (3) system functions. Those Terminal Events are:

- RWPS Fails to Properly Create a TSR;
- RWPS Erroneously Requests Removal of a TSR; and,
- RWPS Fails to Properly Attach to an Existing TSR.

The intention of the System FTA, as described in **Attachment O**, and the Risk Assessment, as described in **Attachment K**, is to verify that such failures, even from a non-vital system such as the RWPS, do not result in MTTHE that exceeds the project goal. In the cases of both the ATC and ABS/CMB Territories, LIRR mitigates any such errors via a combination of proper usage of the RWPS and several layers of procedural verification, as shown in the excerpts from the System FTA shown below. In the case of the erroneous removal of a TSR, the Office Subsystem mitigates.

Metropolitan Transportation Authority
Long Island Rail Road / Metro-North Railroad
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712/29544

System Vulnerability Assessment
CDRL 2-137

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	ENG	Report	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Jason Weighley Safety Engineer		Jason W Weighley 2019.06.13 08:52:00 -04'00'
Verified:	Francis Tabi Safety Engineer		Francis Tabi 2019.06.13 09:27:08 -04'00'
Approved:	Ranjit Kaur Project Director		Ranjit Kaur 2019.06.13 13:47:46 -04'00'
SI Quality Process Review:	Phil Maglorie BT Quality Assurance Group		Phil Magloire 2019.06.13 13:40:50 -04'00'
BT/SRA Review:	N/A Title		
BT/SRA Review:	N/A Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2019, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2019 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3035840

Effective Date:	Revision:	Language:
2019-06-13	_F	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2014-02-24	First issue
_A	2014-08-27	Updated disclaimer on signature page
_B	2016-01-22	Re-Write
_B1	2016-11-21	Revision based on document quality review by RSC
_B2	2016-12-16	Update as per RR comments. Entire document has been updated
_B3	2017-01-12	Update as per RR comments.
B4	2017-01-24	Update as per RR comments.
_C	2017-02-03	Released for FDR
C1	2017-03-09	Update as per RR comments. Address the following open RR comments: Cmt.No. 5; 11, 32, 43, 64, 65, 67, 68, 69, 70 Added SVAR-43
C2	2017-03-21	As per RR comment, rewrite of SVAR-31.
_D	2017-04-07	Released
E	2017-05-05	Moved Proposed mitgations from Section 5.5 to 6
E1	2018-09-24	Updated based on subsystem security and vlunerability hazards
E2	2019-01-15	Updated based on the RR comments
_F	2019-06-13	Released with Subsystem Inputs

Table of Contents

Section	Subject	Page
1	**Executive Summary**	5
2	**Introduction**	6
2.1	**Purpose**	6
2.2	**SVA Compliance Matrix to the System Specification**	7
2.3	**Scope**	17
2.4	**Reference Documents**	18
2.5	**Glossary**	19
3	**System Description**	20
3.1	**Current Security Conditions**	21
4	**Threat and Vulnerability Process**	22
4.1	**Target or Threat Identification**	25
4.2	**Critical Asset Value Assessment**	25
4.3	**Vulnerability Assessment**	25
4.4	**Consequence and Risk Assessment Classification Frame Work**	26
4.4.1	Severity of Occurrence	26
4.4.2	Likelihood of Occurrence	27
4.4.3	Threat and Vulnerability Acceptance Criteria	29
4.5	**Counter Measure and Mitigation Recommendation**	29
5	**Threat and Vulnerability Analysis**	30
5.1	**Identify System Topology**	30
5.2	**Threat Identification**	34
5.2.1	Identifying the Threat	34
5.3	**Critical Asset Value**	49
5.3.1	Identifying the Critical Assets	49
5.4	**Vulnerability Assessment**	50
5.4.1	Vulnerability due to degradation of the RAM	50
5.5	**Risk Assessment**	51
5.6	**Considering Mitigation Options**	51
6	**Threat and Vulnerability Assessment**	51
6.1	**Subsystem Level Assessment**	55
6.1.1	Office Subsystem Assessment	55
6.1.1.1	Firewall	57
6.1.1.2	Switch	58

6.1.1.3 Router 58
6.1.1.4 Virtual Private Networks (VPN) 58
6.1.2 Wayside 59
6.1.3 Onboard 59
6.1.4 Communication 59
6.1.5 RWPS 59
7 Security and Vulnerability Analysis 60
8 Security Recommendations 61
8.1 Security Principles 61
8.2 Security Checklists 61
Appendix 1. FEDERAL BUREAU OF INVESTIGATION (FBI) TERRORISM VULNERABILITY SELF-ASSESSMENT 62
Appendix 2. secuirty check list 69
9 Attachment A – System Vulnerability Assessment Matrix 82

List of Figures

Figure 4-1: Risk Assessment Process Model 23
Figure 4-2: SVA Process 24
Figure 4-3: Asset/Threat Severity Determination 26
Figure 5-1: ACSES II external subsystems and their Interfaces. 31
Figure 5-2: ACSES II Internal Subsystems and their interfaces 32

List of Tables

Figure 4-1: Risk Assessment Process Model 23
Figure 4-2: SVA Process 24
Figure 4-3: Asset/Threat Severity Determination 26
Figure 5-1: ACSES II external subsystems and their Interfaces. 31
Figure 5-2: ACSES II Internal Subsystems and their interfaces 32

1 Executive Summary

This document is a System Vulnerability Analysis (SVA) on the LIRR/MNR PTC ACSES II Systems provided by Bombardier Transportation to LIRR/MNR Railroad. The SVA focused on identify and characterize the methods of accessing the LIRR/MNR PTC ACSES II system (including network management) to cause harm to the public and\or the LIRR/MNR Railroads. The LIRR/MNR PTC ACSES II System consists of the following critical components:

1. The Office Subsystem,
2. The Wayside Subsystem,
3. The Onboard Subsystem,
4. The Communication Subsystem and
5. The RWPS Subsystem

This document analyzes the ACSES II System Architecture, including internal and external interfaces to determine any vulnerabilities and threats that exist, evaluates their impact, determines the mitigation methods to control the risk if evaluated as not acceptable, implements the mitigation methods in all necessary ACSES II System Design, Process, Operation, Installation and Maintenance and validates their effectiveness of controlling the risk.

2 Introduction

The Transit System architectures face a certain level of risk associated with various threats. These threats may be the result of intentional acts to cause harm to the organization or inadvertent actions or environmental defects. Regardless of the nature of the threat, the Transit Agencies have a responsibility to limit or manage risks from these threats to the extent possible. All Transit agencies are faced with the dilemma of maintaining their Systems versus making them more secure. The complexity of the transit environment dictates the level of security in the organization's operation of the system.

The public transportation industry faces many threats, all of which have the potential for disrupting local communities, causing casualties, and damaging and destroying public and private property. At the LIRR/MNR level, the system architecture will be affected by adversarial threat events ranging as shown below in sequence of the threat actions

1. Perform reconnaissance and gather information.
2. Craft or create attack tools.
3. Deliver/insert/install malicious capabilities.
4. Exploit and compromise.
5. Conduct an attack (i.e., direct/coordinate attack using tools or activities).
6. Achieve results (i.e., cause adverse impacts, obtain information)
7. Maintain a presence or set of capabilities.
8. Coordinate an adversary campaign.

As part of the System Vulnerability Assessment process [8], the system threat and vulnerability assessment has to be conducted to identify critical subsystem and interface, vulnerability to specific threats based on the likelihood of occurrence (probability) and the severity of occurrence (given current security baselines and/or practices), and to develop passive and active counter-measures for addressing prioritized vulnerabilities [7].

The System Vulnerability Analysis (SVA) is designed to identify, eliminate and/or control identified security threats related to the Transit agency's System assets to the lowest practical level. Perceived security is as important to a Transit agency as actual security performance. This SVA presents a detailed assessment of potential safety issues that may be associated with the LIRR/MNR ACSES II System.

2.1 Purpose

A SVA is a comprehensive study of the LIRR/ MNR Systems to identify threats and vulnerabilities of the LIRR/MNR ACSES II System assets and to make recommendations for their elimination or control during all life cycle phases. Combating security issues facing transit agencies today involves integrating changes to administrative policies. New technologies and physical protection of structures all lead to developing a formalized process to identify, eliminate, and control threats and vulnerabilities. The goal is to clarify and systematically assess conditions that make the ACSES II system vulnerable to acts of intrusion or potential violence. A threat and vulnerability resolution process outlines how actual and potential threats will be identified, evaluated and resolved. Proper threat identification, categorization, and data collection are crucial to this process.

2.2 SVA Compliance Matrix to the System Specification

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	SVA Document Section Reference
LIRR/MNR Contract No. 1712, Positive Train Control Volume 2 – PTC Systems Integrator Specification Rev 1.0	9.6	ACSES II System Security	The ACSES II System shall be secured against unauthorized access and attack, inclusive of all communications and networks, processor input devices, user interactions, external networks, other Railroad systems, and all other unauthorized inputs. The SI shall be responsible for the security of the ACSES II System through the design or implementation of security devices sufficient to ensure unauthorized intrusions are detected and denied access, regardless if the risk has been identified within these Specifications. 1. Security requirements shall apply when ACSES II equipment and systems are in revenue service, are out-of-service, or maintenance is being performed. 2. Security measures shall be consistent with industry best practices at the time of design.	6

Specification Volume	Specification Section	Requirement Title	Requirement Summary	SVA Document Section Reference
LIRR/MNR Contract No. 1712, Positive Train Control Volume 2 – PTC Systems Integrator Specification Rev 1.0	9.6	ACSES II System Security	To demonstrate compliance, the SI shall prepare and submit for approval an ACSES II System Vulnerability Assessment, CDRL 2-137, identifying all potential system vulnerabilities; associated risk (including exploit likelihood and consequences); countermeasures applied; and resulting mitigated risk.	6
LIRR/MNR Contract No. 1712, Positive Train Control Volume 2 – PTC Systems Integrator Specification Rev 1.0	9.6	ACSES II System Security	The System Vulnerability Assessment shall be planned and the procedures defined as part of the PSP for Engineer Approval. The report format shall be similar to that of the Hazard Analyses; a representative sample of the proposed report format shall be submitted for approval as part of the PSP.	6

Specification Volume	Specification Section	Requirement Title	Requirement Summary	SVA Document Section Reference
LIRR/MNR Contract No. 1712, Positive Train Control Volume 2 – PTC Systems Integrator Specification Rev 1.0	9.6	ACSES II System Security	Exploits to be considered as part of the System Vulnerability Assessment shall include the following, as appropriate: 1. Vandalism 2. Terrorism 3. Device/user impersonation 4. Dictionary attacks 5. Message modification 6. Session hijacking 7. Buffer overflow 8. Denial of service 9. Jamming (physical layer denial of service) 10. Virus/worm infection 11. Unauthorized software installation 12. Unauthorized root/administrator access 13. Others identified by the Engineer.	5.2.1 5. N/A 6. N/A

Specification Volume	Specification Section	Requirement Title	Requirement Summary	SVA Document Section Reference
LIRR/MNR Contract No. 1712, Positive Train Control Volume 2 – PTC Systems Integrator Specification Rev 1.0	9.6	ACSES II System Security	The SI shall ensure that adequate security measures are implemented as part of each ACSES II Subsystem as appropriate, including the following: 1. Restricting physical access to communication and control system components to all but authorized personnel. 2. Use of access control lists (ACL). 3. Use of device and/or user authentication. 4. Use of encryption. 5. Use of hardware keys in conjunction with passwords/passphrases. 6. Access logs. 7. Intrusion detection/prevention. 8. Antivirus. 9. Proper isolation of security critical system functions from other functions. 10. Application of secure coding practices. 11. Use of secure operating systems.	6

Specification Volume	Specification Section	Requirement Title	Requirement Summary	SVA Document Section Reference
LIRR/MNR Contract No. 1712, Positive Train Control Volume 2 – PTC Systems Integrator Specification Rev 1.0	9.6	ACSES II System Security	Security measures shall be designed and implemented such that their effect on reliability, availability, performance, and basic system operation is minimized.	5.3.1
LIRR/MNR Contract No. 1712, Positive Train Control Volume 2 – PTC Systems Integrator Specification Rev 1.0	9.6	ACSES II System Security	Security events or detected intrusion attempts shall be managed as safety events and reported and tracked through the SSCB as described in Section 6.10.	6
LIRR/MNR Contract No. 1712, Positive Train Control Volume 2 – PTC Systems Integrator Specification Rev 1.0	1.4.8	ACSES II System Security	Throughout these Contract Specifications, references are made to codes and standards which establish qualities and types of workmanship and materials, and which establish methods for testing and reporting on the pertinent characteristics. The SI, unless specified otherwise herein, shall follow the requirements of the applicable standards, recommendations, and regulations, which shall form a part of this Specification	2.4

Specification Volume	Specification Section	Requirement Title	Requirement Summary	SVA Document Section Reference
LIRR/MNR Contract No. 1712, Positive Train Control Volume 2 – PTC Systems Integrator Specification Rev 1.0	12.10.1.4	ACSES II System Security	The SI shall provide the plan, procedures, and forms for performing a System Vulnerability Assessment as part of the PSP. B. The System Vulnerability Assessment shall be performed on each ACSES II Subsystem as well as the overall ACSES II System. The SI shall submit the System Vulnerability Assessment, CDRL 2-137, defining the security vulnerabilities and protective measures to be implemented. The System Vulnerability Assessment shall minimally address those threats and protective measures specified in Section 9.6.	Subsystem level will be done after subsystem level is completed.
LIRR/MNR Contract No. 1712, Positive Train Control Volume 6 – PTC Systems Integrator Specification Rev 1.0	6.4	ACSES II System Security	The SI shall create, document, and maintain a System Security Awareness and security training program in conformance with the latest Railroad Enterprise Technology Physical and Environmental Security Policy.	6

LIRR/MNR Contract No. 1712, Positive Train Control Volume 6 – PTC Systems Integrator Specification Rev 1.0	1.4.7	Access and Security Criteria	A. Security threats come in several forms including unauthorized user access to the system in general, unauthorized user access to system functionality, and introduction of software that disrupts the proper functioning of the system software (commonly referred to as viruses malware). Unauthorized access to the system shall be controlled through several techniques including: 1. Prohibit unauthorized access to user interface equipment and provide external / interface access to the Office Subsystem through firewalls (Railroads to external Railroads ACSES II). 2. Protection from introduction of unauthorized software at user workstations shall be accomplished by removal of all removable media devices (floppy drives and CD drives) from the workstations upon completion of Site Testing (see Section10.4.6). 3. Housing of all processing and data communication equipment, including workstation processors, central network equipment, and servers shall be in secure cabinetry. 4. User and password protection for those personnel authorized to log onto the system. 5. In order to prevent the uncontrolled operation or destruction of the system from viruses, virus protection software will be current and operational at all times on all system processors. 6. ACSES II System functionality assigned to users according to user classifications	5, 6

Specification Volume	Specification Section	Requirement Title	Requirement Summary	SVA Document Section Reference
			and assigned access allocation within the user classification. 7. Vehicle communication and control systems shall be secured against unauthorized access and attack, both from the vehicle itself and from the wayside. Security requirements shall apply when both vehicle and non-vehicle systems are in revenue service and when vehicle and non-vehicle systems are out-of-service for maintenance or storage.	
			B. The SI shall prepare and submit for approval a System Vulnerability Assessment (CDRL 2-137, refer to Section 9.6) identifying all potential system vulnerabilities; associated risk (including exploit likelihood and consequences); countermeasures applied; and resulting mitigated risk. The report format shall be similar to that of a hazard analysis; a representative sample of the proposed report format shall be submitted for approval as part of the Product Safety Plan.	6

Specification Volume	Specification Section	Requirement Title	Requirement Summary	SVA Document Section Reference
			C. The SI shall create, document, and maintain a program of Information Technology (IT) Security Awareness and security training in conformance to the Railroad Enterprise Technology Physical and Environmental Security Policy. Security measures shall include the following, as appropriate: 1. Restricting physical access to communication and control system components to all but authorized personnel. 2. Use of access control lists (ACL). 3. Use of device and/or user authentication. 4. Use of encryption. 5. Use of hardware keys in conjunction with passwords/passphrases. 6. Access logs. 7. Intrusion detection/prevention. 8. Antivirus. 9. Proper isolation of security critical system functions from other functions. 10. Application of secure coding practices. 11. Use of secure operating systems.	5,6
	1.4.7.1	Intrusion Detection and Prevention		The threat and vulnerability analysis related to IDS will be performed in the next revision due to IDS design document has not be finalized.

Specification Volume	Specification Section	Requirement Title	Requirement Summary	SVA Document Section Reference
	1.4.7.2	Malicious Software Protection	A. The SI shall furnish a Commercial-Off-The-Shelf (COTS) Malware Protection software package as part of the ACSES II Systems running on commercial operating systems (such as Windows), with the capability for manual upgrade of virus and malware signatures to prevent interrupted operation or destruction of applications or data from viruses and other malicious software. All user interface systems (terminals and workstations) shall be configured to perform automatic virus scans on incoming files and local hard drives upon access.	5,6

2.3 Scope

The analysis presented in this document is meant to assist LIRR/MNR staff in identifying potential security threats associated with the ACSES II PTC System. The SVA is intended to be a comprehensive list of all security threats potentially occurring on the LIRR/MNR ACSES II PTC System to the extent possible. The analysis focuses primarily on hazards and vulnerabilities of the ACSES II System assets that may result in catastrophic or substantial loss or damage to the system operations and loss of service to passengers.

The LIRR/MNR ACSES II PTC System architecture is defined by its internal/external interfaces to the systems and its subsystems. The Hazards and vulnerabilities identified in this analysis are both general in nature and specifically unique to the LIRR/MNR ACSES II PTC System.

As mentioned above, this SVA focuses on the hazards and vulnerabilities of the PTC ACSES II System assets limited to items within the system design. The ACSES II System asset items are static and, as such, the risk associated with the hazards and vulnerabilities of the system assets is also static. Considering just the assets, network system risk remains constant unless the network system assets change.

However, this is not the entire picture. There is a potential dynamic counterpart to system risk for such things as terrorist intentions, population changes, and onsite hazards such as increasing hazardous material traffic, etc, all of which can change on a daily basis. Such operational hazards and vulnerabilities also play a role to the risk of the system. This analysis will only focus on the static hazards and vulnerabilities and will not address dynamic risks as they are not identifiable in the transit operating context...

This assessment complies with “The Public Transportation System Security and Emergency Preparedness Planning Guide” of the Federal Transit Administration [7] and where the guide as identified does not clearly define the specific steps to perform the analysis, this SVA follows “FEMA 452” [9] and “Threat and Hazard Identification and Risk Assessment Guide-CPG 201”, Department of Homeland Security [10].

2.4 Reference Documents

Documents referenced in this SVA are identified in Table 2 below.

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Security for Industrial Automation and Control Systems	ISA99 SCADA
[2]	Guide to Industrial Control System Security	NIST SP800-82
[3]	Guide for Conducting Risk Assessments	NIST SP800-30
[4]	System Protection Profiling – Industrial Control Systems	NIST IR7176
[5]	Dictionary of Terms and Acronyms	3035624
[6]	Requirements Traceability Matrix	CDRL 2-4
[7]	NIST Guide for Conducting Risk Assessment	U.S. Department of Commerce, NIST Special Publication 800-30 Revision 1
[8]	Network Vulnerability Assessment process	CDRL-2-137
[9]	Risk Assessment – FEMA 452	Jan 2005
[10]	Threat and Hazard Identification and Risk Assessment Guide.	CPG 201, Department of Homeland Security
[11]	System Description Document	3035724
[12]	MIL-STD-882C, System Safety Program Requirements.	19 January 1993 with Notice 1, 19 January 1996
[13]	System Product Safety Plan	3035815 Rev C Sep-04-2015
[14]	Long Island Rail Road PTC Implementation Plan	Note: RR document submitted to FRA
[15]	RWPS Subsystem Design Description	3035851 Rev_B
[16]	Metro-North Railroad PTC Implementation Plan	Note: RR document submitted to FRA
[17]	ACSES System Security Risk Register,	LIRR/MNR PTC design document

Reference Number	Document Name	Identification Number
[18]	System Program Safety Plan,	CDRL 2-123-20
[19]	The Public Transportation System Security and Emergency Preparedness Planning Guide, Federal Transit Administration, January 2003	January 2003

2.5 Glossary

Please refer to the Dictionary of Terms and Acronyms, project document number 3035624 [5].

3 System Description

The LIRR/MNR PTC ACSES II System is described in the System Description Document [11].

Services and Operations:

The details of LIRR/MNR services and operations can be found in the PTCIP documents [14] [16].

The following personnel will interact with or may have access to the LIRR/MNR ACSES II PTC System:

- **Train Dispatchers:**

  Train Dispatchers will interact with the LIRR/MNR PTC ACSES II network system for the purpose of defining, applying, and removing TSRs and MoW Work Limits through dedicated PTC computerized user interface workstations located at LIRR's Jamaica Central Control (JCC) and the Movement Bureau at the Jamaica Station Building.

- **Chief Train Dispatchers or Train Dispatcher Supervisory Personnel:**

  The Chief Train Dispatchers will interact with the LIRR/MNR PTC ACSES II network system with higher security clearance to control the operation of the ACSES II system. The chief Train Dispatchers are responsible to verify and validate all the data entered by the dispatcher.

- **Train Engineers:**

  Train Engineers will not interact with the LIRR/MNR PTC ACSES II network system. However the Train Engineer can have the access to the PTC ACSES II network system via the onboard system located in the locomotive.

- **Signal Installers and Maintainers:**

  Signal personnel will not interact with the LIRR/MNR PTC ACSES II network system. However, installer and maintenance personnel can have the access to the PTC ACSES II network system via wayside PTC equipment during installation or routine inspections.

- **Maintenance of Equipment (MoE) personnel:**

  MoE Personnel will interact with the onboard PTC equipment including, but not limited to vital OBC, TP scanner, ADU, data radio and ATC to diagnose problems, and maintain, repair, replace, modify and upgrade onboard PTC equipment.

MoE personnel will also interact with the remainder of the network equipment, including dispatching subsystem, client devices, all communications and server devices, and PTC office subsystems. The only subsystems not handled is the field- based equipment which is handled by the MoW personnel (see next bullet).

- **Maintenance of Way (MoW) personnel:**

  MoW Personnel will interact with wayside PTC system equipment including vital WIUs, signal system interfaces, TPs, BCP, and GBN system to diagnose problems and maintain, repair, replace, modify (including safety-critical topographic data programmed into TPs) and upgrade wayside PTC equipment. The maintenance of way personnel on a work team are led by an Employee In Charge (EIC).

- **Employee in Charge (EIC):**

  The EIC can directly control the entry of trains into the work zone and restrict the speed of the train through the work zone using the EIC Remote Terminal device as per the system design. If the EIC does not grant authority for the train to enter the work zone, the train is forced to a stop by the PTC system prior to violating the work zone authority limits. If the EIC authorizes entry of the train into the work zone, the EIC may establish a maximum operating speed for the train consistent with the safety of the roadway worker employees.

- **RWPS Supervisor (RWPS):**
  The Operations Supervisor has the capability to perform two unique overrides using the RWPS system device. These overrides can be performed with the concurrence of the Dispatcher/RTC .
  - Change Primary EIC override
  - Release Secondary EIC override.

3.1 Current Security Conditions

The LIRR/MNR PTC ACSES II System (including network) security will be enhanced prior to the full deployment of the PTC ACSES II system to protect against threats to the vulnerabilities of the PTCACSES II System. The ACSES II system security will be analyzed, and tested based on the addition of PTC to the LIRR/MNR Network Management, Office, Communications, wayside, Onboard and RWPS architecture.

4 Threat and Vulnerability Process

Threats and vulnerabilities to the LIRR/MNR commuter transit systems cover a wide array of events, virtually none of which can be totally eliminated while still being able to operate the system. Since no system can be rendered totally secure, once threats and vulnerabilities are identified, their impact on the total system must be assessed to determine whether to accept the risk of a particular threat or danger, or to define the extent to which corrective measures can eliminate or reduce its severity.

Thus, security is a process of risk management, identifying major threats and considering how vulnerable the LIRR/MNR systems might be to the actions they threaten. Threat and vulnerability assessment provides an analytical process to consider the likelihood that a specific threat will endanger the system. It can also identify activities to be performed to reduce risk of threat and mitigate its consequences [7].

Threats are defined as specific activities that will damage the system, its facilities, or it patrons. Threats include any actions which detract from overall security. Vulnerability is defined as the susceptibility of the system to a particular type of security hazard or Threat. Vulnerabilities can be corrected, but risk analysis must be performed to determine which vulnerabilities take the highest priority. Because transit systems cover a vast amount of territory that is often unfenced or otherwise unprotected (rail rights-of-way or bus-ways) all equipment is vulnerable to manmade or natural threats.

As per ”The Public Transportation System Security and Emergency Preparedness Planning Guide” [7], the effective threat and vulnerability assessments typically include five elements as are illustrated graphically in Figure 4-1 below:

1. Target and threat identification;
2. Asset analysis;
3. Vulnerability assessment;
4. Consequence/Risk analysis (scenarios); and
5. Countermeasure / Mitigation recommendation.

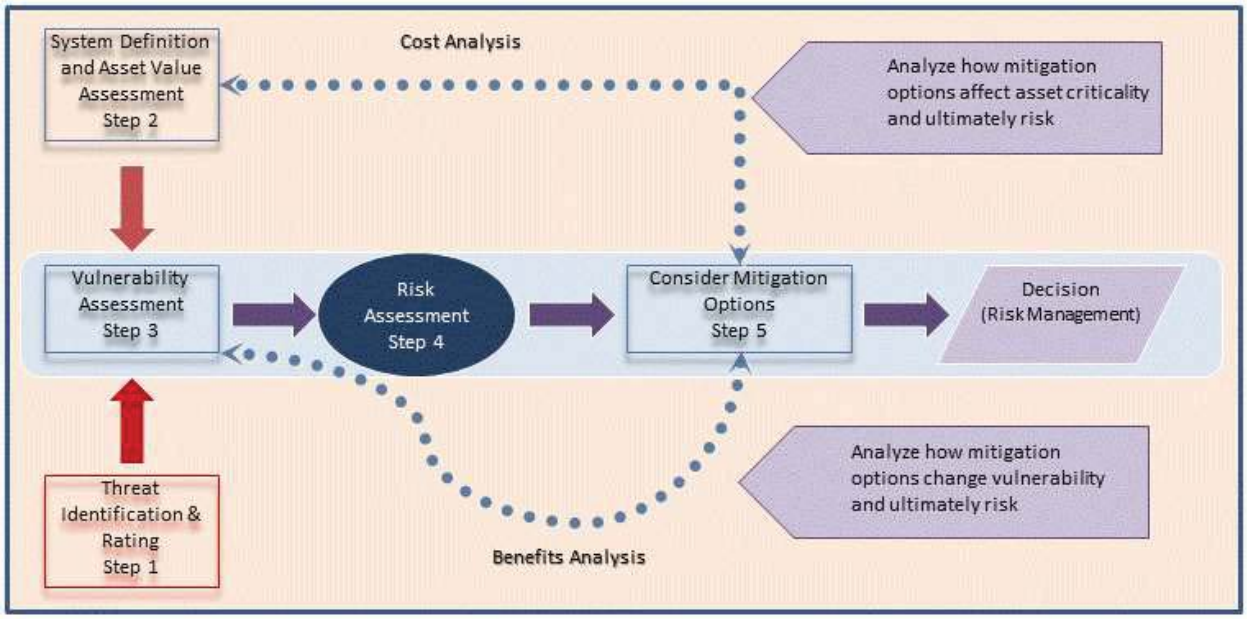


Figure 4-1: Risk Assessment Process Model

Vulnerability is not limited to equipment security and human created items. The LIRR/MNR transit systems must also be analyzed for natural and environmental events such as hurricanes, thunderstorms, flooding etc., to determine the system vulnerability to damage or casualties from such events. Such hazards, not being “threats” as such, will be handled by the Operating Hazard Analysis of the Safety Program as defined in the System Program Safety Plan, CDRL 2-123-20 [18].

However, the overall ACSES II system vulnerability is best controlled by the SVA process presented in Figure 4-2 taken from [7] below.

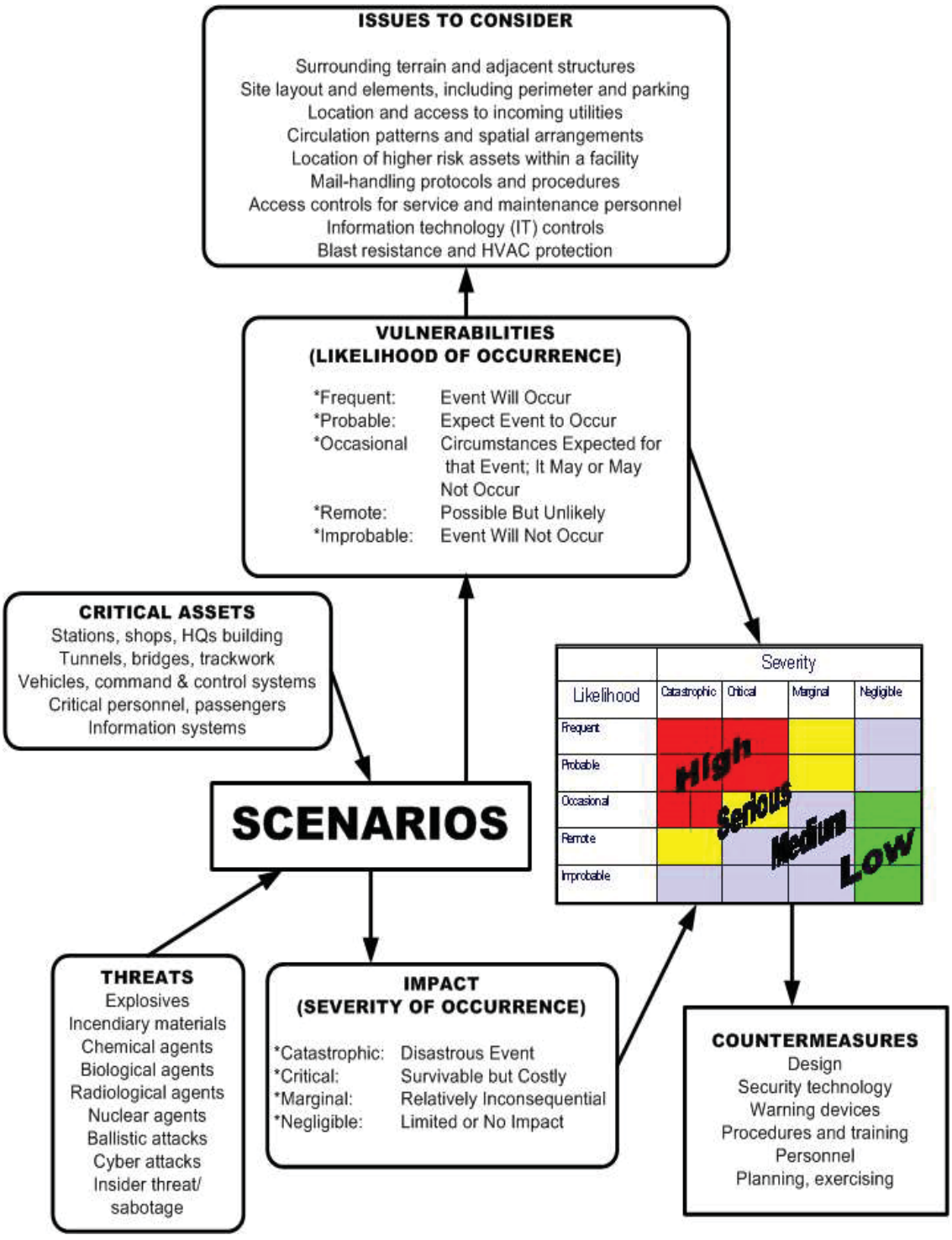


Figure 4-2: SVA Process

4.1 Target or Threat Identification

The first step in the assessment process is to identify threats that are a priority concern to the LIRR/MNR ACSES II PTC System and to rate them by probability and severity. Threat is defined as any indication, circumstance, or event with the potential to cause loss of functionality, halt transit services, or cause damage to an asset. All manmade threats need to be identified. Once threats have been systematically identified, information regarding those threats needs to be collected.

Natural or environmental threats can also be identified, but mitigations are far less precisely defined, as the scope of the threat cannot be easily predicted. These types of “threats” are generally considered as “hazards” and are analyzed in the Operating Hazard Analysis of the project.

4.2 Critical Asset Value Assessment

The second step in the assessment process, as defined by the NIST guideline [7], is to identify the ACSES II system equipment, define the functional characteristics, the people, information, and facilities which interface with the threat target. The asset value assessment process starts by identifying the types of mitigation forming the layers of defense. The next task in this step is identifying the critical assets which are located within the layers of defense. The identification of the core functions and infrastructure of the system is the key element of the value assessment process. By performing this task, the ACSES II architecture and geographical distribution and interdependencies between the system users and its equipment will be analyzed.

4.3 Vulnerability Assessment

The third step in the assessment process is to prepare a vulnerability assessment of the ACSES II assets that can be affected by threats. Vulnerability is the degree to which an asset can be taken advantage of to carry out a threat. This includes vulnerabilities in the design and construction of a facility, in its technological design of systems, and in the way a facility is operated. Vulnerability analysis identifies specific weaknesses with respect to how they may invite threats and permit a threat to be accomplished [7]. A vulnerability assessment is an in-depth analysis of the system architecture its functions, and facility site characteristics to identify weaknesses and determine mitigations or corrective actions that can be designed or implemented to reduce the vulnerabilities. As per The Public Transportation System Security and Emergency Preparedness Planning Guide, Federal Transit Administration [19], FBI Vulnerability self-assessment shall be used to assess the vulnerability of system/infrastructure Appendix 1

4.4 Consequence and Risk Assessment Classification Frame Work

The fourth step in the assessment process is to conduct a system threat and vulnerability assessment. There are number of methods and means to conduct the system risk assessment and can be accomplished in different sequences. However, the assessment methods must, at a minimum, include the following tasks:

a) Preparing the risk assessment matrices,

b) Determining the risk rating, and

c) Prioritizing observations in the network system vulnerability assessment.

This activity has been achieved in this SVA document and is presented in Excel spreadsheet form in Section 6.

The National Institute of Standards and Technology (NIST), [2][3], establishes general guidelines for determining risk. The NIST SP800 [2][3] method uses a severity and probability matrix to illustrate risk. The following sections provide a description how severity and probability (likelihood) described by NIST SP800 standard [2][3] are scaled in the SVA to be equivalent to the hazard risk assessment process presented in the System Product Safety Plan (SPSP) [13][16].

4.4.1 Severity of Occurrence

The combination of threat identification and asset vulnerability assessment shall provide severity of occurrence. The process of combining asset assessment and identified threats is illustrated in Figure 4-3. An asset with a high degree of resistance to threats results in a lower severity of the threat occurrence. Conversely, an asset that is highly vulnerable will have a higher severity of the threat occurrence.

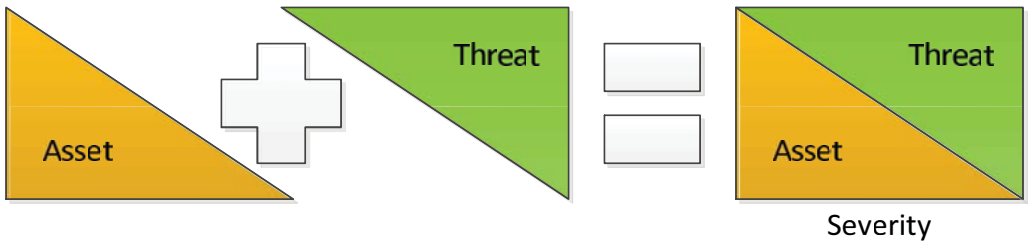


Figure 4-3: Asset/Threat Severity Determination

The severity categories provided by the NIST [2][3] are listed in Table 3 and provide a qualitative indication of the relative severity of the possible consequences of the vulnerable conditions.

Table 3: Threat/Asset Severity Categories

Description (system outage duration)	Category	Definition
Catastrophic	**I**	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
Critical	**II**	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Marginal	**III**	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Negligible	**IV**	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

4.4.2 Likelihood of Occurrence

The vulnerability assessment results shall provide likelihood (probability) of occurrence. The probability levels provided by NIST [2][3] and listed in Table 4 represent a qualitative judgment of the relative likelihood of occurrence of an security incident caused by an uncorrected or uncontrolled vulnerability as a result of a particular event or series of adversarial events. The table provides a qualitative probability category for a particular event occurring within the entire inventory of system equipment or subsystems.

Table 4: Vulnerability Probability Categories

Description	Level	Specific Individual Item	System Impact
Frequent	**A**	Likely to occur frequently. Adversary is almost certain to initiate the threat event. Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year	Continuously experienced.

Description	Level	Specific Individual Item	System Impact
Probable	**B**	Will occur several times in the life of an item. Adversary is highly likely to initiate the threat event. Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.	Will occur frequently.
Occasional	**C**	Likely to occur sometime in the life of an item. Adversary is somewhat likely to initiate the treat event. Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.	Will occur several times.
Remote	**D**	Unlikely but possible to occur in the life of an item. Adversary is unlikely to initiate the threat event. Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.	Unlikely but can reasonably be expected to occur.
Unlikely	**E**	So unlikely, it can be assumed occurrence may not be experienced. Adversary is highly unlikely to initiate the threat event. Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.	Unlikely to occur, but possible.

Together, the threat/asset severity and vulnerability probability properties measure magnitude and set the priority for applying control measures. Threats are then examined, qualified, addressed, and resolved based on the severity of a potential outcome and the probability that such an outcome will occur. The value derived by considering severity and probability is the Risk Index. The resulting index is a measure of the tolerance or intolerance to the threat and is applied in the Risk Assessment Matrix, as shown in
Table 5.

Table 5: Threat and Vulnerability Resolution Matrix

	Catastrophic	Critical	Marginal	Negligible
Frequent	**IA**	**IIA**	**IIIA**	**IVA**
Probable	**IB**	**IIB**	**IIIB**	**IVB**
Occasional	**IC**	**IIC**	**IIIC**	**IVC**
Remote	**ID**	**IID**	**IIID**	**IVD**
Unlikely	**IE**	**IIE**	**IIIE**	**IVE**

4.4.3 Threat and Vulnerability Acceptance Criteria

The Risk Assessment Matrix, as developed originally by NIST [2][3] assists the decision-making process in determining whether a threat & vulnerability condition must be eliminated, controlled, or accepted, in terms of severity and probability. This risk rating process is summarized in Table 6. Furthermore, the rating is used to assess NVA Risk as described in section 4.4.

Table 6: Risk Rating Scale

Hazard Risk Index	Acceptance Criteria
IA, IIA, IIIA, IB, IIB, IC	**Unacceptable**
ID, IIC, IID, IIIB, IIIC	**Undesirable** - Requires solution acceptable to Bombardier Project Manager and to the Safety Assessor.
IE, IIE, IIID, IIIE, IVA, IVB	**Acceptable with review -** Requires review by the Safety Assessor.
IVC, IVD, IVE	**Acceptable** - Review not required.

4.5 Counter Measure and Mitigation Recommendation

The last step of the risk assessment modeling process emphasizes mitigation measures that can reduce the destructive effects against the system in case of a manmade threat. During this step, the mitigations will be examined from effectiveness, acceptability and feasibility point of view with respect to the prevailing implementation conditions. Useful mitigations will be retained and placed in the system safety specifications, while ineffective mitigations will be discarded. Tracking of the Threats and Mitigations will be provided in the Hazard Log.

5 Threat and Vulnerability Analysis

This threat and vulnerability analysis is focused primarily on the Accidental and Structural related threat types. The analysis excluded the environmental related threat types.

The threat and vulnerability analysis of the subsystems are performed at the subsystem level hazard analysis. In the subsystem hazard analysis where the hazards related to security and vulnerability are exported into this document. The exported subsystem related security and vulnerability hazards are captured in excel sheet and attached as an object in end of section 6 below.

5.1 Identify System Topology

In order to identity the significant vulnerabilities of the LIRR/MNR PTC system, the topology of the PTC system must be understood. This includes determining and systematically documenting the baseline system architecture and all of its components

The ACSES II system architecture has been divided into two levels of detail, external subsystems and interfaces and internal subsystems and interfaces of the ACSES II system. The Figure **5-1** and Figure 5-2 present the external and internal subsystems of the ACSES II system. Following sections describes the threats and vulnerabilities associated with each level of the ACSES II system environment.

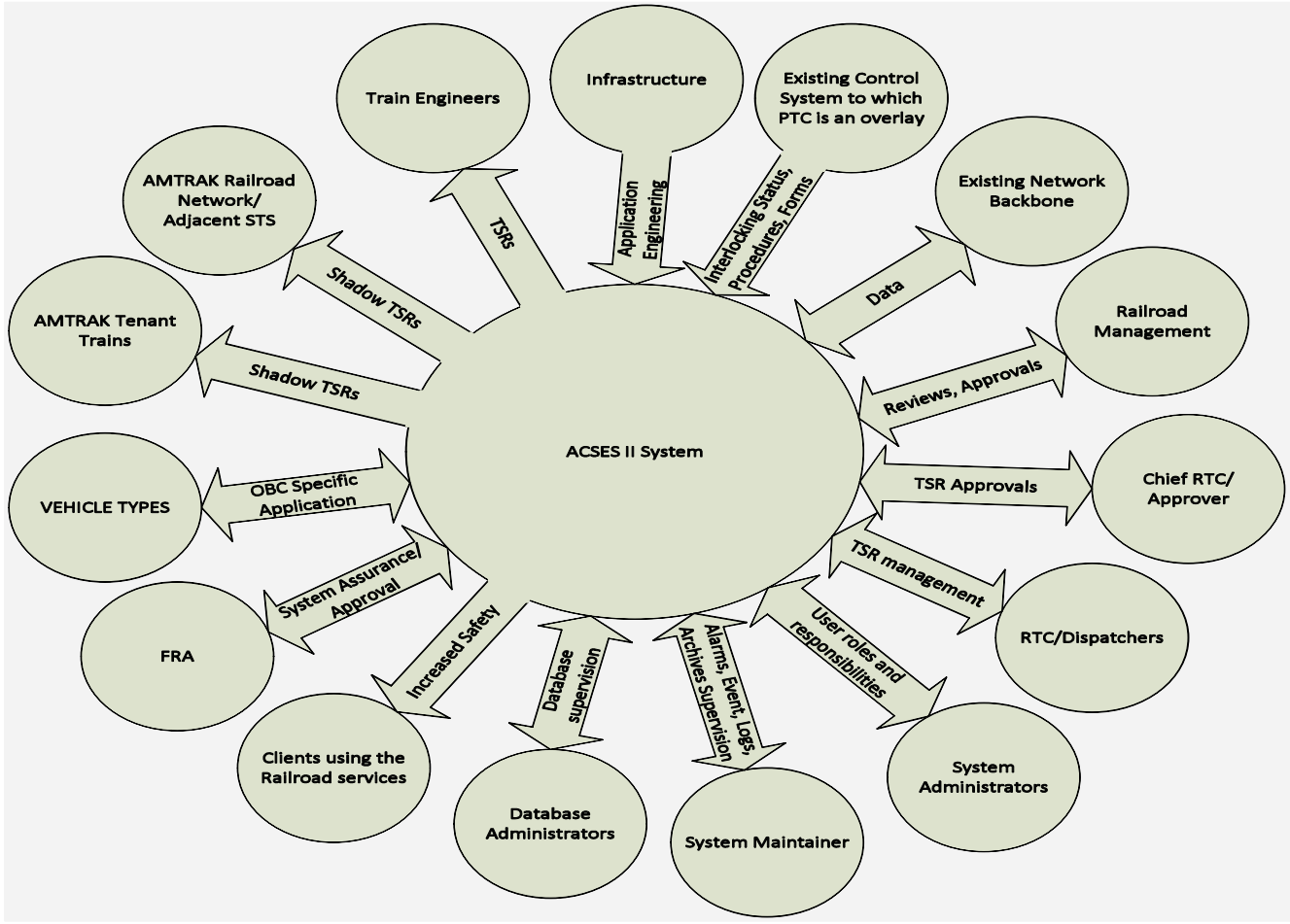


Figure 5-1: ACSES II external subsystems and their Interfaces.

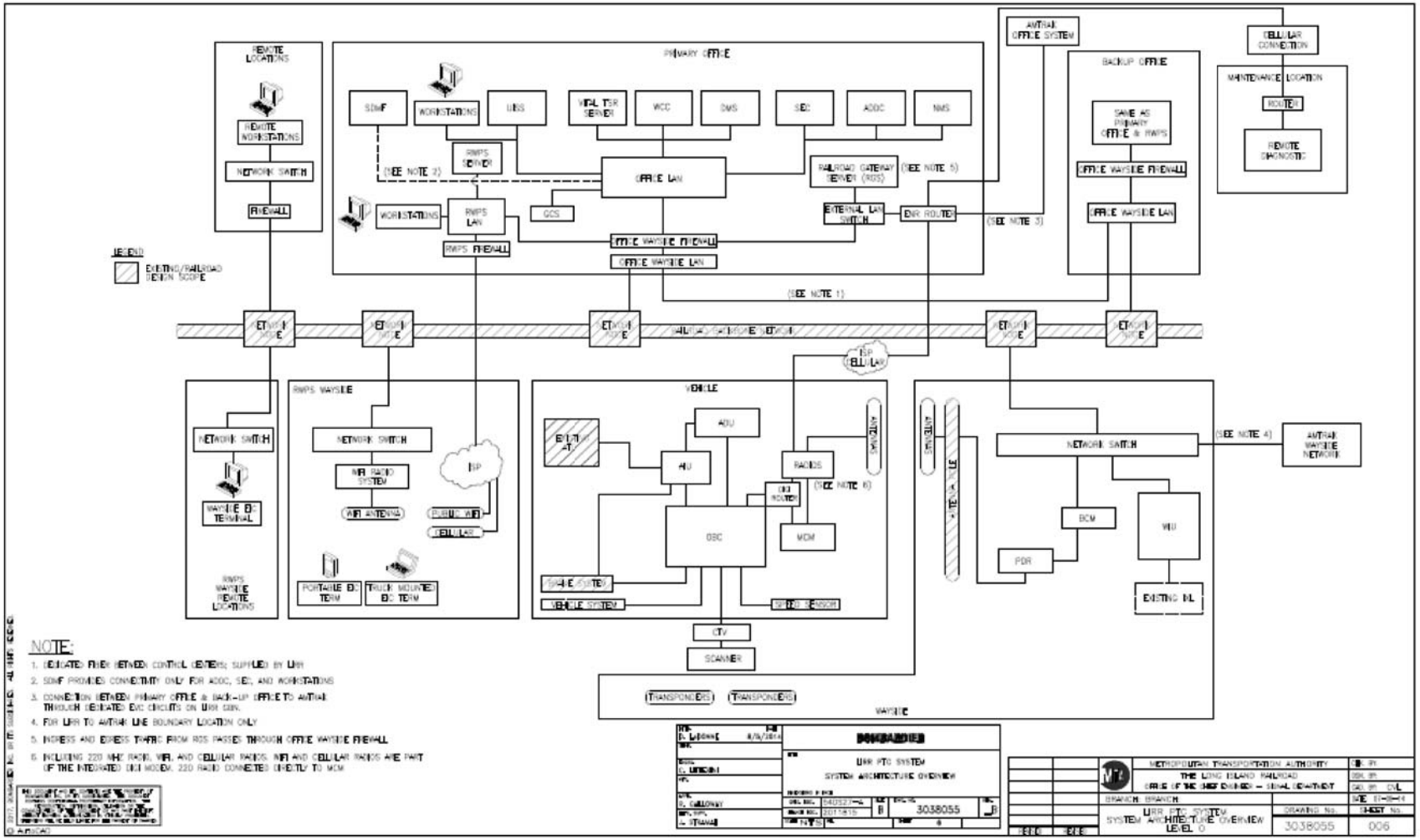


Figure 5-2: ACSES II Internal Subsystems and their interfaces

Based on the external entities presented in Figure **5-1** above the following steps help to accomplished to determine the system-applicable threats:

- Determine the location of the external entities components in the PTC system.
- Determine which internal subsystem(s) components it's interfacing with
- Determine the connectivity between the components in the following modes:
  - Physical – connected by direct interfaces consisting of comms or wired links.
  - Logical – connected only by the transfer of data within a component or segment.
- Determine the tools used by each subsystem for maintenance and support

All the above-mentioned information for internal ACSES II system is presented in detail in the system description document [11]. The Table 7 presents brief description of the external entities to ACSES II System.

Table 7: External ACSES II Entities

External Entities	Location	Subsystem components	Connectivity	Tool
Train Engineers	Vehicle	ADU, AIU	N/A	Procedures
Infrastructure	Guideway	Wayside, Office	Physical	Procedures and Application Engineering Tools
Existing Control System to which PTC is an overlay	Vehicle	Onboard, Office, Wayside and RWPS	Physical and Logical	Laptop, terminal and Hand held devices
Existing network Backbone	Guideway LIRR/MNR Buildings	Communication	Physical and Logical	Laptop, terminal, Hand held devices
RR Management	LIRR/MNR Buildings	Management	N/A	Procedures
Chief RTC/Approver	Guideway Office	Office, Wayside	Physical and Logical	Laptop, terminal, Hand held devices and Procedures
RTC/Dispatchers	Guideway Office	Office, Wayside	Physical and Logical	Laptop, terminal, Hand held devices and Procedures
System Administrators	Office	Office	Physical and Logical	Laptop, terminal, Hand held devices and Procedures
System Maintainer	Office	Office	Physical and Logical	Laptop, terminal, Hand held devices and Procedures
Database Administrators	Office	Office	Physical and Logical	Laptop, terminal and Procedures
Clients using the RR services	N/A	N/A	N/A	Train
FRA	N/A	N/A	N/A	N/A
Vehicle Types	Vehicle	Onboard	Physical	Laptop

External Entities	Location	Subsystem components	Connectivity	Tool
Amtrak Tenant Trains	N/A	N/A	N/A	N/A
Amtrak RR Network/Adjacent STS	Amtrak territory	Office (STS)	Physical	Terminal and procedures

The core challenge of addressing the vulnerabilities of a LIRR/MNR transit system is to recognize the assets which are open to the public. LIRR/MNR operates a system in which public access to many facilities is crucial not only to daily operations but also to the fulfillment of the basic LIRR/MNR mission of transporting people, but it is difficult to secure and protect any area to which the public is allowed open access. The public areas and passenger vehicles of the LIRR/MNR transit systems have complete and unchecked access, but other facilities are restricted to LIRR/MNR employees, contractors, and vendors. Efforts must be made to use the technologies of credentialing and access control to ensure that the sensitive areas of the transit systems are accessible only by those permitted by their essential job function.

The LIRR/MNR system facilities accommodate thousands of daily customers, 24 hours a day / 7 days a week. Customers using transit systems may circulate near restricted areas such as tunnels, control rooms, utility rooms, power supplies, or hazardous-material storage areas. The LIRR/MNR is constantly faced with the challenge of managing the risk posed by the general public to their assets. Each asset has its own level of risk based on its attractiveness as a target, vulnerabilities, accessibility, and criticality to the system. Each component must be characterized to determine susceptibility to security risks. This is shown in the spreadsheet table in Section 6.

5.2 Threat Identification

Threats are defined as specific activities that will damage the system, its facilities, or injure its personnel or patrons. Threats include any actions which detract from overall security. They range from the extreme of terrorist-initiated bombs or hostage-taking to hacks into the LIRR/MNR network system. In order to take over full control of the system, these threats must inject a virus into the network system or similar and shut down the operation. Those responsible for identifying and assessing threats must not only measure the degree of potential danger (criticality/severity), but the chances of that particular danger actually occurring (probability).

5.2.1 Identifying the Threat

The PTC ACSES II Systems threats and hazards are categorized into two major types and that can be the result of natural (non-adversarial threat events) and human-caused (adversarial threat events) incidents.

- The first type is natural hazards and those that result from acts of nature, such as hurricanes, earthquakes, tornadoes etc. These related hazards will be analyzed separately in the Operating Hazard Analysis for the LIRR/MNR PTC ACSES II systems.

- The second type is human-caused incidents, which further categorized into two types, intentional and unintentional human-causes. These two types of incidents are resulting from
    - The intentional actions are bomb threats, terrorist attack, cyber-attack, violence, theft, vandalism, etc. and
    - The unintentional actions are gas outage, water outage, accidental contamination or hazardous materials spills, etc.

The ACSES II System related adversarial threats events and their description are identified in details in Table 8 below. Based on the context of LIRR/MNR ACSES II System, some of the adversarial threats are either duplicate of the other existing threats or is not applicable to the ACSES II System. Those threats are marked as “not applicable” and the ID’d all set to “SVA-Hz-00”. Also, the reason for not applicable are presented in Table 8 below.

A Terrorism threat is not analyzed in this document. A Terrorism Vulnerability Self-Assessment tool developed by the Federal Bureau of Investigation (FBI) is provided in reference [19] for determining an organization’s dynamic risk. The FBI recommends that this tool be used annually by each transit agency, including LIRR/MNR.

Also security recommendation presented in section 8 below should be exercised every six months or yearly by LIRR/MNR to eliminate new or the once were existing and comes to active when update certain License/software/hardware of the system.

Bombardier recommends to LIRR and MNR that they use the FBI Self-Assessment Appendix 1 tool and security check checklist Appendix 2 semi-annually or annually to reduce the dynamic vulnerability in their system.





5.3 Critical Asset Value

The second step in the assessment process is to identify the assets of LIRR/MNR system, area, site, and building that may be affected by a threat. Asset value can be defined as a degree of debilitating impact that would be caused by the incapacity or destruction of an asset. An asset refers to a resource of value requiring protection. It can be tangible (i.e., buildings, facilities, equipment activities, operations, and information) or intangible (i.e., processes or a company's information and reputation).

5.3.1 Identifying the Critical Assets

Based on "The Public Transportation System Security and Emergency Preparedness Planning Guide, Federal Transit Administration" [19], the critical assets of LIRR/MNR transit system are as follows:

- Office.
- Wayside.
- Onboard.
- RWPS.
- Communication
- Network equipment (i.e. Firewall, Switches and routers)

The functional characteristics, the people and the information can be found for all the subsystem in SDD [11]. The subsystems related security and vulnerability analysis are captured in section 6 below.

5.4 Vulnerability Assessment

The third step in the assessment process is to prepare a vulnerability assessment of the LIRR/MNR ACSES II System that can be affected by a threat. A vulnerability assessment is an in-depth analysis of the ACSES II System infrastructure and functions and site characteristics to identify its weaknesses and lack of redundancy, and determine mitigations or corrective actions that can be designed or implemented to reduce the vulnerabilities.

The vulnerability assessment for the LIRR/MNR System identified in conjunction with each threat are analyzed and captured in the SVA Assessment Excel file which is attached in section 6 below.

5.4.1 Vulnerability due to degradation of the RAM

The vulnerabilities due to degradation of the ACSES II system equipment may not pose a real threat to LIRR/MNR railroads. The ACSES II system designed in such a way that a loss of a subsystem input, the system will react in a fail-safe manner. The ACSES II system is such that each vulnerability of the system to RAM issues is accounted for by the design for reliability. This means that the system results from RAM negative effects do not increase the vulnerability of the system to security issues.

For example, if a TP is stolen or damaged, the system will treat it as a missing transponder and the ACSES II system will assume that a speed restriction could have been missed and enforce to MAS per the vehicle configuration or the default speed configured for the onboard, whichever is lower. Until the next transponder set is received, the Onboard no longer displays an enforced speed on the ADU and indicates missing transponder data to the train engineer. The train engineer shall follow the MAS as presented.

Another example would be that when the Onboard fails to receive a valid TSR list for the direction of travel from the office, the ADU displays the ACSES II civil speed restriction (alternating with a double-dash to indicate no TSR), and indicate the absence of TSR data to the train engineer. The train engineer shall follow the TSR list he/she obtained beginning of their train run.

Each ACSES II subsystem vulnerability analysis will describe how the system reacts when there is absence (stolen, missing, not functioning properly, etc. representing RAM negative events) of the subsystem itself.

5.5 Risk Assessment

The fourth step in the assessment process is to prepare a risk assessment for the LIRR/MNR ACSES II System. The risk assessment analyzes the threat events and vulnerability to ascertain the level of risk for each critical subsystem level network (i.e. office, wayside, On-board, RWPS) against each applicable threat. Inherent in this is the likelihood of the threat occurring (probability) and the consequences of the occurrence (Criticality/Severity).

There are a number of methods and means to conduct ACSES II system risk assessment, and the steps can be accomplished in different sequences. However, they all have one common objective, which is to apply a quantitative assessment process that identifies those ACSES II System locations at highest risk and evaluate mitigation measures that can reduce that risk.

The risk assessment has been captured in the SVA Assessment Excel file which is attached in section 6.

5.6 Considering Mitigation Options

The fifth step in SVA is to identify and evaluate various mitigation options that are directly associated with, and responsive to, the major risks identified.

This step emphasizes mitigation measures that can reduce the destructive effects against the ACSES II System where it is vulnerable to threats. During this step, the mitigations will be examined from the point of view of their effectiveness, acceptability, and feasibility with respect to prevailing implementation conditions. In order to identify, select, and implement the most appropriate mitigation measures, general mitigation goals and objectives and the merits of each potential mitigation measure, should be examined

6 Threat and Vulnerability Assessment

The ACSES II System Security and Vulnerability Analysis is recorded in a matrix form and is attached as an object at the end of this section 7. The mitigations for each threat events are somewhat similar throughout the system, regardless of ACSES II System location or function. This analysis mainly focusing on the Threat events identified in the section 5.2 Table 8.

The following terms are appear in the Excel matrix and are defined as follows:

Adversarial Individual	
Outsider	Person unrelated to the LIRR.MNR staff
Insider	Person belonging to LIRR/MNR staff
Trusted Insider	Managerial person belonging to LIRR/MNR staff
Privileged Insider	IT person belonging to LIRR/MNR staff.

Adversarial Organization

Established	A political or other external adversary with no business relationship to LIRR/MNR
Competitor	An adversary who would compete with suppliers to LIRR/MNR or related organizations.
Supplier	An adversary who also supplies materials to LIRR/MNR.

As a result of the assessment, the following conclusions are drawn concerning the LIRR/MNR ACSES II System vulnerability and the most productive mitigations that can be applied. The LIRR/MNR ACSES II System is particularly vulnerable to the following types of threats:

1. Obtain Information using open source discovery of LIRR/MNR organizational information (NVA-Hz-03).
2. Exploit physical access of authorized staff to gain access to LIRR/MNR organizational facilities.(NVA-Hz-16)
3. Conduct wireless jamming attacks. (NVA-Hz-24)
4. Conduct physical attacks on LIRR/MNR organizational facilities. (NVA-Hz-26)
5. Cause disclosure of critical and/or sensitive information by authorized users. (NVA-Hz-30)

The following mitigations provide the most effective reduction in identified threat risk for the LIRR/MNR Railroad PTC ACSES II System. See below for the proposed mitigation. These mitigations must be properly traced to either (1) existing system requirements for the PTC system or (2) New system level security requirements generated for the PTC ACSES II System. The full traceability of this SVA will be captured in the project hazard log and will be closed as per hazard log closure process.





6.1 Subsystem Level Assessment

6.1.1 Office Subsystem Assessment

During the Office Subsystem level hazard analysis, i.e. FMECA, OSHA there are number of security and vulnerability related hazards also identified and recorded in a matrix form. See section 7 . The proposed security and vulnerability mitigations are captured in Table 10 below.

The following terms are appear in the Office subsystem hazard analysis excel matrix and are defined as follows:

Heading	Description
SVA ID	Unique Security reference ID
OFFICE_OHA ID	This unique ID reference number assigned to an individual hazard. This reference is provided for cross-referencing and traceability for the specific hazard, its cause, and potential resolutions. Office_OHA_xx
Operating Scenario	System or subsystem state, phase of activity or environment.
Operating Description	The type of human interaction with the Product, such as transponder antenna usage, onboard system module maintenance, Train Engineer in control, etc.

Heading	Description
Hazard Description	A hazard summary provides a description of the specific potential hazards that can be precipitated by the faults identified.
Potential Cause(s)	A potential cause of the hazard identified in the Hazard Description.
Hazard Effects	The potential effects on person(s) and/or system equipment should the hazard occur.
Initial Risk	The Severity of a hazard before the safety requirement has been implemented and mitigated the associated hazard. The likelihood of a hazard occurring before the safety requirement has mitigated the associated hazard.
Type	The type of human interface analyzed, such as Operation, Maintenance, Installation.
Operating Security Requirements	This requirement is in the form of an operating or maintenance procedure that will eliminate or control the Hazard.
Operating Requirements ID	Each operating requirement is assigned a unique ID. Operating requirements originating from the System OHA are numbered, OHA-xx. Operating requirements originating from the Office OHA are numbered OF-OR-xx. Other existing safety requirements providing mitigation are numbered OF_SR_xx for Office, or RW-SR-xx for RWPS.
Post Risk	The Severity of a hazard after the safety requirement has been implemented and mitigated the associated hazard. The likelihood of a hazard occurring after the safety requirement has mitigated the associated hazard.
Subsystem/Equipment	The subsystem responsible for carrying out the operating requirement execution.
Reference ID	The source of the record.
Comments	Any miscellaneous comments associated with the hazard's management.

As a result of the assessment, the following conclusions are drawn concerning the LIRR/MNR ACSES II office subsystem security and the most productive mitigations that can be applied.

The following mitigations provide the most effective reduction in identified threat risk for the Office subsystem. See Table 10 below for the proposed mitigations and see section 7 for the details analysis. These mitigations must be properly traced to either (1) existing system and/or subsystem level requirements for the PTC system or (2) New system and/or subsystem level security requirements generated for the PTC ACSES II System. The full traceability of this SVA will be captured in the project hazard log and will be closed as per hazard log closure process.





6.1.1.1 Firewall

Firewalls are used to separate networks with differing security requirements; where an organization's internal networks are to be maintained at a more secure level than third-party networks to which it interfaces. Their primary function is to prevent unwanted traffic from entering a secure network, meaning they are usually located at the edge of the logical boundary between systems.

In the case of LIRR/MNR, firewalls are anticipated to be required at the following boundaries:

- Office
- Existing Control System to which PTC is an overlay
- Existing network backbone
- Amtrak Railroad Network

NIST divides firewalls into three basic types; most modern firewalls employ a combination of these to achieve an effective cyber security measure:

- Packet Filters – A Packet Filter examines the header of each packet addressed through the firewall and permits/restricts traffic according to a specific set of rules.

- Stateful Inspection – This filter monitors outgoing connections over a period of type and permits passage of only solicited responses. This prevents malicious packets masquerading as response telegrams from entering the network.

- Proxys – Proxy firewalls build upon the function of stateful inspection with deeper application inspections, in addition to monitoring protocols for known signs of attack. This is achieved by setting up a connection between the client and firewall, which opens a separate connection with the server on behalf of the client.

The firewall technology applied for each of these boundaries may vary, catering for specific interface requirements at that interface. Refer to technical documentation covering each of these interfaces for details of the equipment and interface protocols in effect.

The rules for restriction of traffic across each of the boundaries listed above are subject to a review of the technical requirements for each and makes configuration recommendations for each interface, which should be refined and implemented by subject-matter experts.

The security and vulnerability related hazards has been exported from Office FMECA. The analysis is inlcuded section 7 below.

6.1.1.2 Switch

Switches are used to route messages on the network. The security and vulnerability related hazards has been exported from Office FMECA. The analysis has been included in section 7 below.

6.1.1.3 Router

The routers are used to forward data packets from one router to another router through the networks that constitute an internetwork until it reaches its destination. The security and vulnerability related hazards has been exported from Office FMECA. See section 7 below.

6.1.1.4 Virtual Private Networks (VPN)

A VPN is a virtual network which sits on top of existing physical networks in order to provide a secure mechanism for transmission of data, while also providing sufficient segregation between networks to fulfil cyber security requirements. This is a much more efficient solution than implementing standalone physical networks for each interface, which becomes costly from both a capital and operational expenditure point of view.

The benefit of VPNs is that it provides a traffic isolation effect where access required by some defined services on the physical network can be restricted and segregated from those residing on the primary LIRR/MNR network.

To achieve network segmentation, a range of ports of the physical switch may be enabled and tagged as VLAN ports for areas requiring configuration as such. All services within the VLAN grouping have their connections configured according to the requirements of the Network architecture. The configurable information includes subnet masks, default gateways and IP address ranges; this portion of the document must be reviewed by the relevant subject-matter expert and updated either in the Network architecture.

NIST SP800-125B makes specific recommendations for the implementation of Virtualization of Physical Networks; this standard should be referred to in case of hazard mitigation being required for the VLAN approach proposed.

6.1.2 Wayside

There is no security and Vulnerability related hazards has been exported from WIU subsystem hazard analysis. The WIU uses the same communication network equipment as used in the office subsystem (i.e. switches, firewall, routers, etc.). This equipment related security and vulnerability hazards are identified in section 6.1.1 above.

Also, there is no Security and Vulnerability related hazards has been exported from Transponder subsystem.

6.1.3 Onboard

There is no security and vulnerability related hazards has been exported from Onboard hazard analysis. However, most of the system level security and vulnerabilities analysis would applicable to onboard subsystem and it has been identified in section 7 below.

6.1.4 Communication

The Communication subsystem includes the network and radios to send Temporary speed restriction requests and interlocking status from the wayside to the Onboard subsystem, and diagnostic and performance data on the radios

6.1.5 RWPS

There is no security and vulnerability related hazards has been exported from RWPS hazard analysis. However, most of the system level security and vulnerabilities analysis would applicable to RWPS subsystem and it has been identified in section 7 below.

7 Security and Vulnerability Analysis

See section 9

8 Security Recommendations

Security is essential to maintain the operation of network-based systems and mitigate the risk posed by malicious attacks. There are core security principles that shall be implemented to protect against any security threats or attacks. This section includes the security recommendations for the operational components (e.g. office, communication, wayside, etc.) involved in the LIRR/MNR ACSES II system.

8.1 Security Principles

The principles applied on the LIRR/MNR network in relation to Security and are built on the tenets of Confidentiality, Integrity and Availability:

- Security is at the forefront and part of the culture.
- All reasonable steps shall be employed to avoid malware infections and security breaches.
- Networks/systems shall be protected through segmentation.
- Access and privileges are granted on a ‘needs must’ basis.
- Data shall be protected.
- Software shall be approved and kept up-to-date.
- Configuration shall be known and up-to-date.
- Records and logs shall be kept.
- Users of all types must be trained and competent and Authorized.
- Audit, Asses and test regularly.

8.2 Security Checklists

Refer to Appendix 2 where the checklist items are identified.

APPENDIX 1. FEDERAL BUREAU OF INVESTIGATION (FBI) TERRORISM VULNERABILITY SELF-ASSESSMENT

To complete the assessment, circle the evaluated score on each scale for each question. Then total the scores and enter the total on the last page. Based on the total, use the score guide to assign an overall ranking to the transportation organization.

POTENTIAL TERRORIST INTENTIONS

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Are you aware of any terrorist threat to your organization?
⇒ Are you aware of a history of terrorist activity in your area or your specialty?
⇒ Are you aware of the level of capability of

SPECIFIC TARGETING

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Have you obtained current information from law enforcement or other sources that your organization has been targeted by terrorists?
⇒ What is the reliability of these information sources?
⇒ What is your organization's public visibility?
⇒ Does the nature of your organization's activity lead you to think it may be targeted?
⇒ Are there activities that indicate possible terrorist preparations in your area or specialty?

VISIBILITY OF YOUR FACILITY OR ACTIVITY WITHIN THE COMMUNITY

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Is your organization well known in the community?
⇒ Do you regularly receive media attention?
⇒ Is your organization nationally prominent in your field or industry?
⇒ Are your location and the nature of your activity known generally to the public?

⇒Have you ever had an event or accident with potential health risks that attracted public attention to your facility?

ON-SITE HAZARDS

Low Vulnerability														High Vulnerability					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Are hazardous materials, explosives or other dangerous items on your site?
⇒ Do you store or use biologic or chemical materials that have the potential to be used as a threat or weapon?
⇒ Do you store or use radioactive material at your site?
⇒ Do you have a system to control access to hazardous materials, explosives or any other dangerous materials at your site?
⇒ Can any products stored or used on your site be used as, or in the manufacture of a mass casualty weapon?
⇒ Can any products stored or used on your site cause extensive environmental damage?

POPULATION OF SITE, FACILITY, OR ACTIVITY

Low Vulnerability														High Vulnerability					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Do you have more than 250 people normally present at your site?
⇒ Do you have more than 1,000 people normally present at your site?
⇒ Do you have more than 5,000 people normally present at your site?
⇒ Do you hold events at your site that attracts large crowds?

POTENTIAL FOR MASS CASUALTIES

Low Vulnerability														High Vulnerability					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Do materials stored or used at your site have the potential to create mass casualties on-site?
⇒ Do materials stored or used at your site have the potential to create mass casualties within 1 mile of your site?
⇒ How many people live or work within one mile of your site? 500? 1,000? 2,000? 5,000? More than 5,000?

SECURITY ENVIRONMENT AND OVERALL VULNERABILITY TO AN ATTACK

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Does your organization have effective internal security procedures?
⇒ What is the law enforcement presence in your area?
⇒ What is the hardness, level of blast protection, etc. of your facilities?
⇒ How accessible (security presence, access control, id badges, metal detection buffer zones, fences, etc.) is your facility?
⇒ Are your assets and/or its potential recognized as a symbol?
⇒ What level of public access is necessary for you to function?
⇒ Can you control high-speed vehicle approaches to your facility?
⇒ Do you have access control to your parking area?
⇒ Do you conduct vehicle searches when entering facility grounds or parking areas?
⇒ Do you employ detection/monitoring systems (video surveillance, intrusion detection systems, etc.)?
⇒ Is your parking delivery area adjacent to or near your facility?
⇒ Is your delivery area supervised during hours of normal business?
⇒ Is your delivery area access blocked during hours that your business is closed?
⇒ Do you have an on-site food service facility for employees and visitors?
⇒ Is access to the water supply for your facility protected?
⇒ Is access to the ventilation system for your facility protected?
⇒ Do you have a way to quickly shut down the water supply or ventilation system for your facility?

CRITICAL PRODUCTS OF SERVICES

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ What is the importance of your organization to the community?
⇒ Is your organization critical to the local population, economy or government?
⇒ Is your organization critical to the continuity of basic services?
⇒ Is your organization critical to state or national commerce?
⇒ What would be the social, economic or psychological ramifications of a terrorist attack against your organization?
⇒ What is the nature of your assets: hazardous materials, uniqueness, potential danger to others, etc?
⇒ How long would it take to restore your critical services/functions?

HIGH RISK PERSONNEL

Low Vulnerability	High Vulnerability

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Do you have personnel that are critical to the continuing function of state or local government, basic services, utilities infrastructure, the community, the economy, or of inherent value to your business or agency?
⇒ Do you have personnel that are critical for responding to a terrorist act?
⇒ What would be the effect of a terrorist act against these high-risk personnel?

ORGANIZATION COMMUNICATIONS

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Do you have a mass notification system (public address system, intercoms, alarms)?
⇒ Do you have a secure communications network that can be relied upon during a crisis?
⇒ Do you have a crisis response team?
⇒ Is your crisis response team trained?
⇒ Do you conduct regular exercises?
⇒ Do local/regional emergency responders participate in your exercises?
⇒ Does your Crisis Response Team have its own portable communications system?
⇒ Can your Crisis Response Team communicate directly with emergency responders?
⇒ Do you have an emergency law enforcement notification system including a hot line, panic button or something similar?
⇒ Is your alarm system tied into the local law enforcement department or do you have an alarm service?
⇒ Are your systems tested regularly?

SECURITY AND RESPONSE

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Are your security forces' staffing and training levels adequate?
⇒ Do you have the capability to maintain a security presence in a high threat situation?
⇒ Are additional security personnel available if requested?
⇒ Are there affiliated agency/industry/organization support services available?
⇒ Do you have trained disaster response teams within the organization?
⇒ Do you have necessary specialty detection, monitoring, hazard assessment devices on hand and are they functional?
⇒ Are local/regional law enforcement forces adequate and can they respond rapidly?
⇒ Are local emergency responders familiar with your facility and its contents?
⇒ Do you keep records on who visits your facility and where they go within the facility?

POLICIES, PROCEDURES, AND PLANS

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Do you have a current crisis response/disaster plan?
⇒ Does your plan include the types of crises you are most likely to encounter (e.g., fire, explosion, chemical release)?
⇒ Are your employees familiar with the plan?
⇒ Have you conducted crisis response and disaster drills and were they effective?
⇒ Have you identified the critical functions of your workplace and do you have a plan for continuation of operation during an emergency?

SECURITY EQUIPMENT

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Do you have a security system and is it current technology?
⇒ Do you have an intrusion monitoring motion detector or an alarm system?
⇒ Do your systems have backup if power is cut or fails?
⇒ Do you have security equipment that would detect leaks or ruptures of potentially hazardous materials?

⇒ Do you have personnel protective equipment for your emergency response team appropriate for the hazardous materials at your facility?

⇒ Is such equipment in working order and has it been inspected recently?

COMPUTER SECURITY, CYBER-CRIME, AND CYBER-TERRORISM

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Is your site dependent on information technology including computers and networks to accomplish its daily business activities?
⇒ Is the information stored in your computer systems valuable?
⇒ Do you have back-up power available for your computer systems?
⇒ Do you make back-up copies of your data?
⇒ Is your back-up data securely stored?
⇒ Does your site have computers or networks connected to the Internet?
⇒ Have you experienced problems with computer security incidents, including computer viruses, worms, web-site defacements and/or denial of service attacks in the past?
⇒ Do you have staff in place that are adequately trained and are available to monitor security warnings and take protective measures, including loading system patches?
⇒ Do you have technology security tools in place including firewalls, intrusion detection systems or anti-virus software to protect your computer systems?
⇒ Do you have a computer security policy, plan, and procedure that includes a computer security incident response team?

SUSPICIOUS MAIL AND PACKAGES

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Is the mail for your facility opened in a secured area or an area isolated from the majority of personnel?
⇒ Have the personnel who open mail received training on the recognition of suspicious mail and/or packages?
⇒ Do you have specific procedures on how to handle suspicious mail and/or packages, including possible facility evacuation?
⇒ Do you have a secure and contained location where any unusual or suspect deliveries or mail can be stored until proper authorities can evaluate the suspect items?

TELEPHONE, BOMB, AND OTHER TYPES OF THREATS

Low Vulnerability																			High Vulnerability
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

⇒ Has your staff received training on how to handle bomb and other threat calls?

⇒ Does your staff have a checklist of questions to ask the caller in case of a bomb or other threatening call?
⇒ Does your facility have a plan on how to handle bomb and other threatening calls?
⇒ Does your bomb threat plan include a system whereby your personnel would search your facility to identify suspicious objects to point out to emergency response personnel?
⇒ Does your plan include a decision making process on whether to evacuate the facility?
⇒ Are personnel familiar with the plan? Have evacuation drills been conducted?
⇒ Is your plan coordinated with local law enforcement and the local phone company?

EMPLOYEE HEALTH AND THE POTENTIAL FOR BIO-TERRORISM

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

⇒ Do you have an occupational health safety program in place?
⇒ Do you have a health professional working at your facility?
⇒ Do you have a procedure in place to track the health of each employee and know if more than one employee has the same symptoms?
⇒ Do you monitor the health status of employees on sick status or absent otherwise?
⇒ Are employees encouraged to keep supervisors informed on any unusual health related event or condition?
⇒ Are employees required to report any unusual conditions or substances encountered in the course of their normal duties, including strange substances or odors from packaging or mail?
⇒ Do employees know the proper procedures for emergency operation or shut-off of air handler, air circulating or ventilation systems?
⇒ Do you keep a current list of employees, home addresses and emergency contact information?
⇒ Do you have an emergency notification plan for employees (e.g. calling tree)?

APPENDIX 2. SECUIRTY CHECK LIST

Incident Management & Recovery

- It is the responsibility of all IT staff, contractors or third parties to notify the Security Engineer (SE) or representative of any security breach, unusual behavior, and intelligence of increased or new threats.

- The SE shall review all notifications and decide on immediate actions. This will be:
    - Declare an incident and invoke Incident Management Plans.
    - Refer to the Security Audit Committee (SAC) for further consideration.
    - Decide further Incident Management is not required. This decision shall still be logged with the SAC.
- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions shall be taken in the event of certain occurrences?

- Succession Plan: Describe the flow of responsibility when normal staff are unavailable to perform their duties.

- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.

- Criticality of Service List: List all the services provided and their order of importance.

- The order of recovery in both short-term and long-term timeframes.

- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered. The impact on the back-up in the event shall be assessed by the SE/Network Engineer.

- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.

- Mass Media Management: Who is in charge of giving information to the mass media?

- Guidelines on what data is appropriate to be provided.

- After creating the plan, their implementation shall be trained and tested as appropriate.

- During testing, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plans, at a minimum, shall be reviewed and updated on an annual basis.

Data Management

- Data shall be stored throughout its existence in an environment suited to its format and security classification, to ensure its preservation from physical harm (e.g. fire, flooding) or degradation and its security from loss or unauthorized access. Where appropriate, special storage equipment and environments should be used.

- Data, whether original or duplicate, shall not be kept outside ACESE II systems (e.g. on removable media) except as a temporary copy driven by a business need to work off-site or off-line, or for authorized transfer to other users or systems.

- Data storage protocol shall enable it to be readily identified and retrieved throughout its existence (e.g. CCTV recorded data by folder to include camera ID, location and timestamp).

- Data held in digital formats should be managed and stored in such a way as to ensure usability and accessibility through time. This may involve migration of information between environments and systems, conversion to current software versions, or conversion from obsolete to current formats.

- Physical access to data shall be restricted by locking it in rooms, cabinets, drawers, and other storage areas or units, and by ensuring that files and computer monitors are not left open to general or casual view.

- Data shall be retained for a period appropriate with business needs and legal requirements.

- Data shall not be destroyed if subject to open or pending investigation, audit or litigation.

- Data destruction methods shall be appropriate with the Security Classification of the asset/sub-system.

- Protection from unauthorized access may require mechanisms such as password protection or encryption of digital files and data, and sign-in sheets or request dockets for access to non-digital information.

- Where information is stored on a mobile device (e.g. USB drive, external hard drive), special care shall be taken to ensure that the device is physically protected from theft, loss, or damage, particularly if it is transferred or used away from sites.

- Provide data recovery following security breach, catastrophic failure or data corruption.

- Provide roll-back data following unsuccessful upgrade.

- Provide baseline data in the event a Vendor ceasing to trade.

- All data required to rebuild each sub-system in the event of a disaster or catastrophic failure shall be identified, including Vendor support where applicable.

- Full recovery data back-ups shall be kept in a secure off-site location.

- Incremental data back-ups shall be kept in a secure facility (e.g. fire-proof cabinet), preferably in an adjacent building or bank locker.

- Vendor specific Data e.g. Configuration Profiles submitted into Unifier shall be catalogued using the Configuration Management Process and back-up.

- Details of full and incremental back-up shall be developed for each sub-system, including the storage media to be used, storage location and transportation mode where applicable.
- System Administrators responsible for conducting data back-up shall perform this according to the back-up schedule provided in sub-system specific plans.
- Records of all back-up activities shall be kept in accordance with the sub-system plans.
- Each sub-system asset owner shall define the back-up criteria for that sub-system, including, but not limited to, the type of back-up (manual or automatic), frequency schedule and storage and retrieval information.

Network Segmentation

- The Security Engineer (SE) will maintain a list of the firewalls deployed across the Metrolinx network, the approved paths and the rules applied, and distributed to applicable System Administrators.
- SE will keep and approval log which will be kept up to date.
- All changes to firewall configuration shall be recorded by the SE.
- Connections between machines on separate ACSES II networks will not be permitted unless approved by the SE and passed through a firewall.
- Connections from external machines or networks will not be permitted unless a business need is established and approved by the SE and passed through a firewall.
- Regular testing of firewalls shall be conducted to ensure compliance with policy, firewall-specific rules and are still effective.
- Testing shall be conducted by competent persons, which may be third-party specialists where appropriate, and include vulnerability and penetration testing.
- Suspicious activity or known security breaches shall be logged and reported to the SE.
- Suspicious activity or known security breach logs shall be kept in accordance with the LIRR/MNR Data Management Policy.
- Firewalls deployed shall contain intrusion detection facilities that will detect, as a minimum, modification to firewall system files and Distributed Denial of Service (DDoS) attacks.
- Intrusion detection systems will provide immediate notification to the System Administrator (or specified technical persons) so corrective actions can be instigated.
- Remote access and privilege rights will be provided such that specified technical staff can provide immediate response to live incidents.
- Firewall systems shall only be accessed by authorized personnel.
- Logon screens shall provide a warning indicting that the system shall only be accessed by authorized personnel and that unauthorized access may be subject to disciplinary action.
- Firewall access shall be logged and timestamped.
- Firewall access shall be subject to unique identification username and password.
- The same username and password shall not be used on more than one firewall.
- At least two personnel shall be trained and provided access privileges for every firewall deployed.
- Firewalls will be configured so that they are visible to the Network Management System (NMS).
- Firewalls will run on standalone machines not running any other services.

- Firewalls shall not store sensitive or business-critical information on them.
- Firewall software shall be kept up-to-date.
- Firewalls are to be located in secure rooms, accessible only by authorized personnel.

Anti-Virus and Anti-Malware

- All sub-systems in use on the ACSES II network shall run effective anti-virus and anti-malware software
- Anti-virus and anti-malware software shall:
    - Detect and remove known viruses and malware.
    - Approved for use by the Security Engineer (SE) prior to installation and use on the ACSES II network.
    - Run only one of the approved products at any time on each machine.
    - Maintained to keep both software and virus definition files up-to-date, and where practicable deployed automatically across the network.
    - Configured for real-time scanning and regular scheduled scans.
    - Prevent end-users or malware altering the anti-virus and anti-malware configuration or disabling the protection through tamper protection.
- All IT equipment shall be scanned for viruses and malware before being introduced onto the ACSES II network, system or devices.
- Removable media shall be scanned on an isolated and safe test environment (e.g. dedicated standalone machine for viruses and malware) before being introduced onto the ACSES II network, system or devices.
- Infections that the anti-virus or anti-malware software has not been able to deal with shall be quarantined from the ACSES II network until virus free.
- Any instance of virus or malware infection or detection shall be reported and documented as a security incident as detailed in section 8.2 above.

Remote Access

- Remote access and source IP addresses shall only be granted where there is a clear business need and agreed by the Security Engineer (SE).
- Use of external resources to conduct ACSES II business shall be approved in advance by the SE i.e. permit process.
- Secure remote access shall be strictly controlled with encryption and strong passwords.
- While using LIRR/MNR-owned computer to remotely connect to the ACSES II network, authorized users shall ensure the remote host/client is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an authorized user or third party.
- All hosts/clients that are connected to the ACSES II network via remote access technologies shall use the most up-to-date anti-virus software, this includes personal computers.
- Personal equipment used to connect to the ACSES II network shall meet the requirements of the remote access as defined by the CSE.
- All remote access tools or systems that allow communication to the ACSES II network resources from the Internet or external partner systems shall require multi-factor authentication such as authentication tokens and smart cards that require an additional PIN or password.
- The authentication database source shall be Active Directory or LDAP, and the authentication protocol shall involve a challenge-response protocol that is not susceptible to replay attacks.
- The remote access tool shall mutually authenticate both ends of the session.
- Remote access tools shall not support direct connections through the perimeter firewall(s) (e.g. a separate network zone may be provided within the demilitarized zone to specifically support remote access).
- Digital Signatures shall be used (not pre-shared keys).

Removable Media

- An anti-virus/malware software, approved for use by the LIRR/MNR Security Engineer, shall be installed on all machines within the ACSES II network that will scan any device that connects to a machine via a peripheral port (such as USB, external hard drive). A system to ensure all the software is the most up-to-date shall be introduced. See the Anti-virus and Anti-malware Policy.
- Virus/malware scanning of Removable Media shall be conducted using a non-networked, dedicated standalone machine using anti-virus/malware software that has been approved for use by the ACSES II Security Engineer before being connected to the ACSES II network.
- Connecting an unidentified USB Flash Drive or media device to a machine is prohibited.
- Any unknown storage device shall be handed to security or IT personnel.
- Autorun and Autoplay features for all Removable Media devices shall be disabled.
- Storage of personal data on Removable Media is prohibited.
- Plugging in personal audio players into a ACSES II network machine is prohibited.
- Sensitive data shall also be stored on a backup copy located in a secure location.
- Sensitive data shall be deleted from a USB drive following transfer using a secure delete utility.
- Where possible, USB Flash Drives shall have onboard anti-virus capability.
- Any requirement to utilize Removal Media shall be identified in advance and approved by the Configuration Manager.

Portable Devices

- Hands-free enabling devices, such as the Bluetooth, may be issued to authorized LIRR/MNR personnel where authorized by higher-level management personnel. Personnel should make sure that to avoid being recorded when peering Bluetooth adapters.

- Files containing confidential or sensitive data may not be stored on ACSES II Portable Devices unless protected by approved encryption. Confidential or sensitive ACSES II data shall never be stored on a personal portable device.

- Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the employee, as determined on a case-by-case basis.

- The cost of any item beyond the standard authorized equipment is also the responsibility of the employee.

- Lost or stolen equipment shall be reported immediately.

- Portable devices shall not be plugged into the ACSES II network, accept where compliant with the Removable Media Policy.

System Updates and Configuration

- Specific instructions should be provided for System Administrators on how to perform each update.
- System updates shall be approved in advance by the Configuration Manager prior to update.
- System updates shall only be approved by competent personnel.
- Risk assessments and testing shall be undertaken to check for conflict and compatibility, and the impact on the system, interfaces and personnel prior to approval.
- The Configuration Manager shall obtain and track the software licenses.
- A Reversion Plan shall be approved in advance by the Configuration Manager for all business-critical systems or assets.
- All new software shall be selected from an approved software list, maintained by the Security Engineer.
- Required software shall be adequately assessed before being accepted onto the approved software list.
- The Configuration Manager shall maintain and document, applying appropriate change control, a baseline configuration of the ACSES II system.
- The baseline configuration shall include installed applications, operating systems, version and patch-level identifications, standard software load for workstations, servers, network components, and portable devices.
- The Configuration Manager shall be informed following successful system updates or changes.

User Management

- Unique User Accounts shall not be shared
- The Security Engineer should maintain a record of all User Accounts to be updated on a weekly basis.
- LIRR/MNR Human Resource Management should inform the SE of all staff, contractors or third party leavers within one week of the leave date. For the purposes of this Policy, 'leavers' includes those transferring to another project or role.
- All requests for new or enhanced privileges should be accompanied by justification and will include, as a minimum: details of person requiring access, system(s) to be accessed, access rights/privileges and business need. The SE shall review requests and approve or reject as appropriate.
- The SE should inform System Administrators of required changes to User Accounts on a weekly basis.
- System Administrators should update User Account configuration on a weekly basis (e.g. disable/add accounts) and inform the SE that the changes have been enacted.
- Systems shall be equipped with event logging and log extraction facilities that will be, as a minimum, in a common readable format with logged events that contain a user-identifier and event time stamp.
- Applications should support authentication of individual users, not groups.
- Applications should not store passwords in clear text or in any easily reversible form.
- Applications should not transmit passwords in clear text over the network.
- Applications should provide role management functionality; such that one user can take over the functions of another without having to know the other's password.
- Passwords should not be inserted into email messages, or other forms of electronic communication.
- Passwords should not be revealed over the phone to anyone
- Passwords should not be revealed on questionnaires or security forms
- The format of passwords should be hinted at (for example, "my family name")
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption
- Do not use the "Remember Password" feature of applications (for example, web browsers)
- Any user suspecting that his/her password may have been compromised should report the incident and change all passwords
- All personnel, contractors and third parties assigned with a User Account should not disclose unique identifiers (e.g. username and password) with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members
- Systems should be configured so that all passwords should meet or exceed the following:
    - Contain at least alphanumeric characters
    - Contain both upper and lower case letters
    - Contain at least one number (for example, 0-9)
    - Contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:";'<>?,/)

- Where possible, users should not use the same password for various access needs.
- All user accounts should be configured for individual access only (i.e. group or shared accounts should not be permitted)
- All user-level passwords should be changed at least every six months. The recommended change interval is every four months

- Access rights and privileges should be granted depending on the business need, type sub-system/asset/application to be accessed, and the Security Classification of the sub-system/asset.

- Notwithstanding weekly updates to User Account records, Access rights and privileges should be reviewed on a quarterly basis by the SE and amended as necessary.

- User Accounts should be created using standardized permissions that are mapped to job role. This will depend on the type of sub-system and need; however, a generic example is included below:

- A 'Standard User' type account would be expected for most users where regular system access is required. Permissions for a Standard User will vary according to the system/control system being accessed, operating system, application, security rating, safety integrity level and tasks to be performed. Standard User Accounts may be differentiated further by specific worker need (e.g. Standard User Level 1 – supervisor, Standard User Level 2 – subordinate). However, a typical Standard User account might be expected to include similar functionality from the below examples:

    - Access standard applications installed
    - Access hardware, such as a connected printer, as required to perform standard tasks
    - Change personal details associated with an account (depending on application)
    - Change basic settings (e.g. zoom level)
    - Access removable media (if required to perform standard tasks)

- A 'System Administrator' type account would be expected for a minimum number of users. Again, actual functionality will depend on a variety of functions, however a typical System Administrator account may be expected to include similar functionality from the below examples:
    - Installation of new software and manual updates/patches
    - Management of User Accounts such as;
        - Adding new User Accounts
        - Deleting dormant or expired User Accounts
        - Changing User Account permissions
    - Accessing system folders
    - Configuring or adding hardware (e.g. installing new printer)
    - Security functions such as;
        - Virus scanning
        - System back-up

        - Firewall configuration
        - Port forwarding
    - Network monitoring and maintenance

- A ‘Local System Administrator’ type account would be expected for a minimum number of users. This type of account will have similar functionality to that of the System Administrator, but access will be limited to a local machine (e.g. non-networked). Additionally, a variant of this type of account may be associated to administer a particular sub-system (networked or otherwise).

9 Attachment A – System Vulnerability Assessment Matrix

3035840_Attachment_A_Rev_F

Metropolitan Transportation Authority
Long Island Rail Road / Metro-North Railroad
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712/29544

Site Security Control Plan (SSCP)

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT-SRA	Eng	Plan	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Kenneth Sundberg Area System Safety Manager		2014-04-17
Verified:	Kenneth Fair Project Manager		2014-04-17
Approved:	Carolyn Hayward-Williams Project Director		2014-04-24
SI Quality Process Review:	Michael Giometti BT Quality Assurance Group	Michael Giometti	2014-04-24
BT/SRA Review:	NA Title		
BT/SRA Review:	NA Title		

J. Barkley 4.30.14 7:50

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages.

© 2014, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc.. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc.

Copyright © 2014 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: **3035470**

Effective Date:	Revision:	Language:
2014-04-17	_A	EN

Released
Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2013-12-09	First Issue
_A	2014-04-17	Updated with MTA Comments incorporated

Table of Contents

Section	Subject	Page
1	Executive Summary	4
2	Introduction	4
2.1	Compliance Matrix	4
2.2	Reference Documents	5
2.3	Glossary	5
3	Site Information	5
3.1	Bombardier Field / Project Office	5
3.2	MTA Property Sites	6
3.3	Vehicles and Storage On-Site	7
4	Background Verification	7
4.1	Purpose	7
4.1.1	Criminal History / Record Checks / Gross Negligence Incidents	8
4.1.2	Professional License Verification and Check for Sanctions	8
4.1.3	Verification of American Citizenship or Visa for Foreign National Status	8
4.2	Verification by MTA	8
5	Credentials – Identification	8
5.1	Bombardier and Approved Sub-Contractors	8
5.2	Visitors and Non-Working Guests	9
5.2.1	Project Offices	9
5.2.2	MTA Property	10
Attachment A - Workplace Security Inspection Report		11

List of Tables

Table 1: Compliance Matrix 4

Table 2: Reference Documents 5

Table 3: Acronyms Specific to this Document 5

1 Executive Summary

Worldwide attacks on transportation systems have created a climate of heightened risk and security awareness. The inherently open and easily accessible nature of transportation systems, coupled with the heightened focus, has greatly increased the importance of security throughout the transportation industry. The Federal Transit Administration (FTA), Federal Railroad Administration (FRA) and Transportation Security Administration (TSA) have recognized and responded to this increased risk by placing their own emphasis on transportation security. Bombardier Transportation, in support of its mission to enhance safe and secure transportation services, has developed this Site Security Control Plan (SSCP) as a means of integrating security into our site activities at the MTA Long Island Rail Road and Metro North Railroad.

2 Introduction

The SSCP describes the expectations, procedures, and responsibilities to be fulfilled by our team and visitors working at the sites. All Bombardier personnel and subcontractors are required to adhere to the policies, procedures, and requirements stated herein, and to properly and diligently perform the security-related functions of their jobs as a condition of employment. Further, Bombardier's management team will be continually and directly involved in formulating, reviewing and revising security policies as required as the project evolves.

It is a Bombardier's goal, through the effective implementation and administration of this SSCP, to take proactive measures to improve the overall security of our sites and the transportation clients we serve. To achieve this goal, all employees will report potential threats, vulnerabilities, and/or hazards to the project management team, who will communicate them to the client where appropriate. They are also encouraged to provide assistance as necessary to ensure that potential threats, vulnerabilities and/or hazards are eliminated, mitigated or controlled.

This SSCP is applicable to all Bombardier project team members including subcontractor personnel, consultants, vendors, or suppliers. (See attached Organization Chart)

Unless or until another person is designated and approved by the MTA, Bombardier's on-site Superintendent shall be responsible for work site security and administration of this plan. The Superintendent shall assist the railroads in auditing the SSCP as requested, regardless of prior notice.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
1	Terms & Condition	Article 503	Work Site Security Requirements	3-5

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Workplace Security Inspection Report	SC-A-14-001
[2]	System Product Safety Plan (LIRR)	3035815
[3]	System Product Safety Plan (MNR)	3036437

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms, document number 3035624. Acronyms only related to this document are listed below in Table 3.

Table 3: Acronyms Specific to this Document

Acronym	Definition
ANSI	American National Standards Institute
FRA	Federal Railroad Administration
FTA	Federal Transportation Administration
ID	Identification
RWP	Roadway Worker Protection
SSCP	Site Security Control Plan
TSA	Transportation Security Administration

3 Site Information

3.1 Bombardier Field / Project Office

Bombardier and its subcontractors shall maintain security of its field offices regardless of its location on, near, or remote from MTA property. At a minimum, all field offices shall:

- Maintain a daily Employee Sign-In / Out Log at each reporting location. Copies of the log shall be retained on site for review and / or submission to the MTA Project Management as requested.
- Provide a schedule of work activities, site hours, any pick up or deliveries, inclusive of the specific work location, to Project Management, as required in the contract specifications and in the interest of security review.
- Require all employees review and sign a Statement of Acknowledgement and Compliance with the Work Site Security Requirements when joining the site team.
- Ensure all field offices are locked at the end of each day.
- Ensure that security window guards are installed on all windows of trailers or similar facilities.
- Ensure that all work site gates, perimeter fences, or other entry points are locked at the end of each day.
- Ensure that a key control plan is in place, and that keys are only distributed to Contractor management staff and where necessary, the Railroads Project Staff as directed by the Railroad.
- Establish and apply disciplinary procedures for violations of site security control protocols.
- Perform weekly audits of site security and document the findings. (See attached form template)
- Install and maintain proper storage for files, drawings, photos, and plans associated with the project, ensuring proper security and control of these documents.
- Ensure all computers or other electronic media storage is properly secured via encryption, password protection, or other appropriate methods.
- Report any work related injury consistent with safety plan.

3.2 MTA Property Sites

Where applicable to secure a work site, Bombardier and its subcontractors shall:

- Provide and maintain substantial, durable, and effective security devices as required to ensure security during the performance of work.
- Security Devices shall be of designed, applied, and maintained to withstand anticipated external forces of the work area inclusive of wind, and other natural or manmade conditions
- Security Devices shall be void of conditions such as sharp edges so as to not cause nicks, splinters, or cuts
- Bombardier or its subcontractors shall ensure security devices are removed when they are no longer required

- Barricades and fences are not anticipated. If required, they shall be provided in an unbroken line along work areas where security is required. Barricades and fences shall be a minimum of 8 feet in height, rigid, and capable of preventing unauthorized entry into the work area.
- Utilize and maintain security and proper operation of any devices installed by others including gates, doors, fences, or similar associated with the site.
- All Bombardier employees, as well as its subcontractors, agree to random search of their persons, vehicles, equipment, materials, and containers by MTA Police or others law enforcement within jurisdiction, while on MTA Property.

3.3 Vehicles and Storage On-Site

- Prior to the commencement of work, and as the project matures, Bombardier shall provide a vehicle list identifying those vehicles that will be used in performing or supporting this project.
- All vehicles shall be marked with the Bombardier or approved sub-contractor logo.
- Except for deliveries, pickups, and other approved and essential functions related to the work, vehicles shall be prohibited from entering the work site.
- Where required within the job site, a vehicle log shall be kept current throughout the work day and shall identify those vehicles used in performing the work. The Log shall be available to the Railroads for review or submission.
- Vehicles shall be parked in authorized areas as designated by the Railroads.
- All storage containers, job boxes, or similar shall be placed in areas designated and approved by the railroads. All such containers shall be clearly labeled inclusive of a listing of contents.
- Deliveries and Pickups shall be limited to controlled areas as determined and approved by the railroads.

4 Background Verification

4.1 Purpose

The Bombardier SSCP requires a background check of all workers expected to enter active transportation sites, support facilities, or have access to security critical information as a course of their project involvement. The purpose of the review is to reduce the risk of security threats by preventing unlawful interference with the transportation system by screening employees who will perform certain duties or who have access to certain restricted areas and system design attributes. The verification process will confirm residency and qualification to perform work on the transportation systems, benefiting the public, passengers, other employees, and operators of transit system. All background checks shall have been performed post the bid proposal submission date. Background checks will be consistent with applicable federal and state parameters.

4.1.1 Criminal History / Record Checks / Gross Negligence Incidents

No employee will be allowed on site nor allowed access to safety critical information, if the results of a background investigation reveal that the individual has been culpable in an incident of gross negligence or otherwise convicted or found guilty by reason of insanity, in any jurisdiction. All background checks will be consistent with applicable federal and state parameters.

4.1.2 Professional License Verification and Check for Sanctions

Professional licensure protects the integrity of the project as well as the public by enforcing standards that restrict practice to qualified individuals who have met specific qualifications in education, work experience, and exams. As specified and appropriate for this project, any employee that must possess a license or similar certification will be required to submit proof of their current status. Bombardier will verify the qualification is valid and ensure the current licensure is void of sanctions.

4.1.3 Verification of American Citizenship or Visa for Foreign National Status

All employees on site or otherwise dedicated to this MTA Project shall submit verification of US Citizenship or an appropriate Visa as a precursor to employment / assignment to the team.

4.2 Verification by MTA

Security Documents shall be submitted to the MTA a minimum of 15 days prior to attending the Roadway Worker / Contractor Safety Orientation or entering the work site. Security Documents shall include:

- Verified identification and certified background check documentation
- Copy of the Bombardier issued ID Card
- As required – Foreign National Registration Documents for each foreign national employee assigned to the Contract.
- Completed MTA Access Control Forms (Attachment A)

5 Credentials – Identification

5.1 Bombardier and Approved Sub-Contractors

Neither Bombardier nor its Sub-Contractors shall be permitted to wear or display any item on their person that would identify them as RAILROAD personnel.

Bombardier and approved Sub-Contractors shall be issued identification cards containing:

- Employees full name
- Company Name and Logo

- Expiration Date of the Identification Card
- Employee Photo
- Employee Number

Bombardier and approved Sub-Contractors shall display their company issued ID at all times while on MTA property and within the project field offices.

Bombardier and approved Sub-Contractors shall attend the Railroads Contractor Safety Awareness and Roadway Worker Protection classes. Prior to entering any MTA Work Site, regardless of proximity to right of way, all Bombardier employees and approved subcontractors shall display their issued RWP and Contractor ID cards. The IDs shall be clearly evident by:

- Wearing the IDs on the exterior of the outermost garment
- Displayed within an appropriate arm band or
- Displayed within a clear pocket on the front of the LIRR Approved High Visibility Safety vest or
- Displayed within a clear pocket on a breakaway lanyard around the neck

Bombardier and approved Sub-Contractors shall wear all required safety gear inclusive of footwear, hardhats, safety glasses and LIRR Approved High Visibility safety vests consistent with the expectations outlined in the site safety plan. Task specific PPE shall also be worn consistent with industry standards. Safety vests shall minimally be ANSI Class II Type II vests with tear away construction of Orange or Yellow as specified by the railroads. Safety vests shall be discernible from MTA employee vests by conveying Contractor Employee or otherwise as specified by the railroads. Non- LIRR / MNRR employees shall not be permitted to wear or display any garment that may identify them as an MTA Employee. This includes hard hats, vests, uniforms, jackets or similar.

No Bombardier or approved Sub Contractor shall enter the Right of Way or secure MTA area without proper approval, training, established protection, and participating in a briefing as required and consistent with the System Product Safety Plans [2], [3].

5.2 Visitors and Non-Working Guests

Though not anticipated, there may be occasion in which Bombardier Leadership or other authorized personnel would request to visit the Project Office, or MTA Property. All visitors or non-working guests to the site would require advance notice to Project Staff from both Bombardier and the MTA.

5.2.1 Project Offices

- Visitors or guests to the Project Office must pre-arrange for visit.
- All visitors or guests must sign the daily log located in the Project Office.

5.2.2 MTA Property

- Visitor or guests in associated with this project must pre-arrange for a visit.
- Upon approval, any site review shall be limited to areas generally accessible to the public, and in coordination with a proper escort.
- Entry to the right of way, ancillary rooms, or other secure areas is prohibited without prior screening, training, and other approvals as required by the Railroads.

Attachment A - Workplace Security Inspection Report

BOMBARDIER
the evolution of mobility

For use with: MTA – PTC SYSTEM INTEGRATION

WORKPLACE WEEKLY SECURITY INSPECTION REPORT

Area Inspected:	Date:
Supervisor or Manager:	Time:
Worker Representative(s):	

DESCRIPTION	*YES*	*NO*	*N/A*	*COMMENTS*
SITE SECURITY RELATED DOCUMENTATION				
Daily Employee Sign In / Out Log – current and available?				
All site personnel have signed Security Acknowledgement?				
Project schedule, work hours, expected deliveries posted?				
Key Control Plan in place – up to date?				
FIELD OFFICE / PROJECT OFFICE				
Office / trailer doors have provisions for daily securement?				
Windows guards / locks available and used for daily securement?				
Perimeter fencing, gates, and skirting in place, secured each day?				
Provisions and use of securement areas for all documents, drawings, maps and similar? File cabinets or rooms.				
All computers or other media storage secured via encryption, password, or other security measures?				
MTA PROPERTY – ASSOCIATED SITES				
All access points secured per original design or enhancement for project?				
All security, fencing, gates or similar void or sharp edges and pinch points?				
Are materials stored in areas that do not interfere with workers or accessible to the public?				
Are all storage areas clearly marked and within security perimeter?				
VEHICLES				
All project vehicles identified and included on site log?				
All project vehicles marked with Bombardier or Sub Contractor Logo?				
All vehicles properly secured and parked in pre-approved locations?				
Are body belt and safety straps being properly stored when not in use?				

BOMBARDIER
the evolution of mobility

For use with: MTA – PTC SYSTEM INTEGRATION

WORKPLACE WEEKLY SECURITY INSPECTION REPORT

	YES	*NO*	*N/A*	*COMMENTS*
DESCRIPTION	***YES***	***NO***	***N/A***	***COMMENTS***
WORKER- BOMBARDIER AND CONTRACTOR				
Employees display proper ID – outside of garments?				
Employees in field wearing LIRR Approved High Visibility Safety Vest?				
All required and appropriate PPE in place – shoe, hard hat, gloves, glasses or task required?				
All equipment void of any MTA related identification?				
OTHER OBSERVATIONS				

Additional Comments:

Supervisor Signature: _____ Date _____

Manager Signature: _____ Date _____

Positive Train Control

Security Management Plan

April 1, 2019

This is a controlled document; please do not duplicate. If additional copies are required, request them from the LIRR Document Control Department. This procedure will assure that all recipients of the document will receive revisions and additions as they are approved. Any unauthorized duplications will be considered uncontrolled copies.

Revision History

Revision	Date	Description	Author
-	04/01/19	Initial release	

Table of Contents

Reference 4
Building a Security Management Plan 5
Asset Management 6
Identity Management, Authentication and Access Control 8
Configuration Management 10
Awareness and Training 11
Governance 12
Communications Protection 14
Data Security 16
Incident Response 17
Physical and Environmental Protection 18
Remote Access 19
Risk Assessment 20
Security Continuous Monitoring 22
System Updates 22
Security Monitoring 22
APPENDIX A: Office Subsystem Network and Infrastructure 24
APPENDIX B: Management of security certificates and Operational Private Keys 26
APPENDIX C: Communications Subsystem 33
Appendix D: Roadway Workers Protection Subsystem (RWPS) 34
Appendix E: Vehicle Subsystem 36
APPENDIX F: Management of Wayside Interface Unit (WIU) security keys 38
Appendix G: Physical Security of Positive Train Control (PTC) Workstations and Operating Facilities 39

Reference

REF	DOCUMENT NAME	DOCUMENT NO.
A	RWPS SUBSYSTEM DESIGN DOCUMENT	2-201
B	COMMUNICATIONS SECURITY ADDENDUM, COMMUNICATIONS SYSDD	7-001
C	SYSTEM VULNERABILITY ASSESSMENT	2-137
D	LIRR/MNR SECURITY ASSESSMENT	3151743
E	CELLULAR DESIGN WHITE PAPER	3151137
F	LIRR SECURITY KEY MANAGEMENT PLAN	N/A
G	SYSTEM DESCRIPTION DOCUMENT	2-027
H	OFFICE SUBSYSTEM DESIGN DESCRIPTION	6-001
I	COMMUNICATIONS SUBSYSTEM DESIGN DESCRIPTION AND SECURITY ADDENDUM	7-001
J	MTAHQ, BEST PRACTICES POLICY INSTRUCTIONS	MTA-SEC

Building a Security Management Plan

FRA rules require each railroad to implement an appropriate Information Security program to protect the implementation and operation of the LIRR PTC ACSES II system. While railroads likely have existing Information Security policies and practices, Positive Train Control (PTC) expands the need for Information Security outside the traditional areas of responsibility covered by Information Technology departments. A comprehensive review of each railroads Information Security program must be conducted to ensure PTC assets are properly protected.

This documented Security Management Plan which intended to define the security measures that are implemented to protect information assets leverages the NIST Cybersecurity Framework as the foundation for defining the implementation of security best practices to manage cybersecurity related risk by promoting the protection and resilience of the railroad. The key components of the NIST Cybersecurity Framework are to define the implementation statements of the information system controls which; Identify, Protect, Detect, Respond, and Recover the LIRR PTC ACSESS II.

This plan highlights LIRR's commitment to ensuring the integrity, privacy, security, and confidentiality of LIRR's PTC ACSES II information, especially highly sensitive information, and defining the responsibilities of departments and individuals for such information.

The following areas of the LIRR PTC ACSES II system should be included in the security management plan:

- Policies and practices that manage access and use of PTC secure information and assets;
- Office Subsystem Network and Infrastructure;
- Management of WIU security keys and the systems that use them, including the Subdiv file;
- Management of security certificates and Operational Private Keys used by many PTC systems;
- Protection of computer systems and communications on Locomotives
- Protection of wayside signal systems and supporting networks.

The goal of the security management program is to manage the identified risks, understand their likelihood and impact on the business, and then put in place security controls that mitigate the risks to a level acceptable to the organization. In addition to assessment and mitigation, the plan includes ongoing evaluation and assessment of cyber security risks and controls throughout the life cycle of the LIRR PTC ACSES II information system.

The Governance section provides the security requirements as § 236.1033 Communications and Security Requirements

The referenced (G) System Design Description and (H) Office Subsystem Design Description documents provides a detailed system overview. Including the overall system and security overview, interoperability with Amtrak, the security design of the ground based network and the use of redundant Active Directory Controller (ADDC) servers to provide Single Sign-On (SSO) administration and management to the ACSES II system.

ASSET MANAGEMENT

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

LIRR PTC ACSES II has a defined Configuration Management Plan that describes the specific methods and procedures that is being used for Configuration Management (CM) by the System Integrator and LIRR on the ACSES II project. The plan is designed and developed to meet specific industry requirements including the following:

a) Addresses roles, responsibilities, and configuration management processes and procedures;
b) Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c) Defines the configuration items for the information system and places the configuration items under configuration management; and
d) Protects the configuration management plan from unauthorized disclosure and modification.

Each of the critical assets identified on the LIRR PTC ACSES II platform have a defined Software Configuration Items List associated. These lists are maintained in the System Integrator provided SharePoint site.

Each of the Software Configuration Items Lists (CIL) necessary for tracking and reporting; and

a) Includes the following:

- Software Item Reference Number – configuration item list index number
- Software Type – description of the configuration item
- Software Name – name of the configuration item
- Vendor/Developer/Manufacturer – manufacturer or vendor of the configuration item
- Software Version – version of the configuration item (revision number, etc.)
- SI Level SW/DB
- Proprietary / Non - Proprietary
- COTS, Standard, New, Modified COTS or Modified Standard
- COTS Sub Components
- Quantity of Software Licenses for Railroad Use – number of software licenses or software rights available for the railroad to use
- License details, duration, #of Users, etc.
- Warranty details of the Licenses
- CI Modifiable by Railroad – indicates whether the item is modifiable by the railroad (Yes or No)
- Software Item Functional Description – functional description and purpose of the configuration item as it applies to the system. Should match the SDD/SysDD Functional Description.

LIRR PTC ACSES II enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on regulating information transfers between interconnected systems, employing hardware mechanisms to enforce controlled bi-directional

information flows; and implementing trustworthy mechanisms to reassign security attributes and security labels.

LIRR requires that any external information systems that are external to the boundary of the LIRR ACSES II Information systems establish a Network Interconnection Agreement. The agreement establishes that terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a) Access the information system from external information systems; and
b) Process, store, or transmit organization-controlled information using external information systems.
c) Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
d) Monitors security control compliance by external service providers on an ongoing basis.

LIRR PTC ACSES II Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Five System Architecture levels have been defined with L0 as the highest level possible and L4 as the most detailed level. Four subsystems have been defined in the L0 and L1 System Architecture.

- Office Subsystem – Comprising the Office Servers, the Office LAN and the SDMF on both the Primary and the Backup control centers.
- Wayside Subsystem – Comprising the WIU, Wayside Network, RF equipment and Transponders.
- Vehicle Subsystem – Including the OBC, Communications equipment and interface with the Train.
- Roadway Worker Protection Subsystem (RWPS) – Formed by the Office RWPS, Office RWPS LAN, Wayside communications equipment and EIC terminals.

LIRR establishes personnel security requirements including security roles and responsibilities for the entire workforce and third-party stakeholders. Within the LIRR PTC ACSES II cybersecurity roles and responsibilities are primarily functions within the Office and RWPS Subsystems. The LIRR PTC ACSES II documentation provides a definition of the roles which are primarily divided between the PTC Office Subsystem and the Roadway Worker Protection Subsystem:

Primary Functions include:

- Temporary Speed Restrictions (TSR) Management
- Log/Store Events
- Monitor System State
- Manage System Maintenance

Key Roles include:

- System Administrator
- Database Administrator,
- System Maintainer/Network Maintainer
- Configuration Manager

IDENTITY MANAGEMENT, AUTHENTICATION AND ACCESS CONTROL

Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

The Active Directory Domain Controller (ADDC) Server is used to provide Single Sign-On (SSO) administration and management for all the Office and RWPS Subsystems in the ACSES II system. ADDC provides ability for the System Administrator to configure access rights to the office applications. Individual office application with the support from ADDC provide access rights to functions and features of the application as defined by the different user classifications assigned to individual user groups. All the devices/workstations within the Office Subsystem (except for STS Server) are authenticated with the ADDC server. ADDC also provides the security policing for all the servers/workstations of the ACSES II Office. ADDC stores the user account information, authenticates a user upon request and enforces the security policy for the office domain. Different domains are set up throughout the system to ensure system security and meet all the user authentication requirements upon logging into a workstation or server within the domain. Lightweight Directory Access Protocol (LDAP) is used by the office applications to interface with ADDC server to authenticate the user credentials. The LDAP is used by applications in place of Windows' normal authentication. The administrator and maintainer workstation is provided with single sign-on dashboard.

The primary functions of an ADDC throughout the system are:

1. Active Directory User and Computer accounts
2. User authentication and authorization
3. Single Sign-On (SSO)
4. Time Synchronization
5. Security policing
6. Backup, Restore and Disaster Recovery
7. Domain Name Server (DNS)
8. Primary Domain Controller (PDC) Emulator
9. Replication and failover
10. Prevents multiple simultaneous log-ins by a single user.

LIRR PTC ACSES II employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. These functions include the ability to logon locally or backup and restore files and directories.

LIRR PTC ACSES II monitors and controls communications at the external boundary of the system and at key internal boundaries within the system leveraging firewalls. The firewalls are configured with Access Control Lists (ACLs) that are designed to create physical and logical subnetworks separating both internal and external organizational networks. Connections to external networks or information systems are allowed only through managed interfaces consisting of boundary protection. The devices are arranged in accordance with an organizational security architecture which is a bridging of the two adjacent networks

occurs at the line boundary. The network bridge is protected through a firewall connection between railroads as defined in the Interconnection Agreement.

CONFIGURATION MANAGEMENT

Successful configuration management within the LIRR PTC ACSES II system relies on the following:

- Identifying the configuration items, components, and related work products that are placed under configuration management
- Establish and maintain a configuration management and change management system for controlling configuration items
- Create or release baselines for internal use and for delivery to the customer
- Track change request for the configuration items
- Control Changes in the content of configuration items
- Establish and maintain records describing configuration items
- Perform configuration audits to maintain the integrity of the configuration baselines

LIRR PTC ACSES II baseline configuration standards for each of the subsystems are managed through the System Data Management Facility (SDMF). The SDMF provides tools to allow for secure retention of system data and configuration files as well as the life cycle management of those assets through released baselines. Baselines are contained in the BaseDB. The BaseDB configuration files are used by the ACSES II PTC components to configure the devices and applications parameters that are set for the PTC project.

Each subsystem maintains a current inventory of systems, hardware, and software assets, and information (data) under its control throughout the respective Software Configuration Items Lists (CIL), and establish and enforce security configuration settings for information technology products employed in the LIRR PTC ACSES II system.

Designated Project Managers are responsible for configuration management in accordance with industry best practices, to include the establishment of single baselines, and ensuring a current and full inventory of all hardware and software configuration items.

The Configuration Management Plan adheres to the guidance established in Software Configuration Management Directive, GRP-20-20-30-000280.

The Change Control Board (CCB) is responsible for reviewing and approving all changes mate to configuration items (CI) after the CI has been baselined in each LIRR PTC ACSES II subsystems.

AWARENESS AND TRAINING

The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

All personnel supporting the LIRR PTC ACSES II system must receive training including Cybersecurity awareness both prior to accessing the LIRR PTC ACSES II information systems and on an annual basis. Certain personnel with specific functional roles (System Administrators, Database Administrators, System Maintainers/Network Maintainers) are also identified and required to be further trained to carry out specialized asset, data, and information security-related duties and responsibilities.

In addition, a comprehensive railroad-specific training program that prepares railroad personnel to fully use and maintain each ACSES II subsystem (Office, Wayside, Communications, OBC, RWPS, and SDMF). Specific training is provided for equipment installation, operations, preventive and corrective maintenance, administration, reconfiguration necessary to adapt the railway for changes due to the implementation of the ACSES II System, and how to build software releases for each subsystem.

Noncompliance with training requirements can result in disciplinary action, which may include but is not limited to suspension of LIRR PTC ACSES II accounts.

GOVERNANCE

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

The Rail Safety Improvement Act (RISA) of 2008 established parameters for developing security measures to improve railroad safety. The primary function of the act was to mandate the implementation of the Positive Train Control (PTC) system. This initiative was led by the Association of American Railroads (AAR) in coordination with the Federal Railroad Administration (FRA). To provide oversight and best practices on the deployment and management of the PTC with consideration for communication, security awareness, analysis, and continuous monitoring; AAR established in advance of the RISA a Rail Information Security Committee (RISC). RISC provides the guidance for the development of the Security Management Plan.

LIRR PTC ACSES II system shall be compliant with all applicable FRA regulations including 49 CFR 236 subparts (inclusive of subpart I), standard practices, and equipment of LIRR; incorporate the latest technologies; and provide for full ACSES II interoperability with supporting PTC and ACSES II implementations.

Section 236.1033 (Communications and security requirements) provides the baseline encryption standards required for the confidentiality and integrity of communication channels in accordance with best practices established by the National Institute of Standards (NIST) or a similarly recognized and FRA approve standards body.

LIRR PTC ACSES II system establishes personnel security requirements including security roles and responsibilities for the entire workforce and third-party stakeholders. Within the LIRR PTC ACSES II cybersecurity roles and responsibilities are primarily functions within the Office and RWPS Subsystems. Additionally, LIRR is an active member of the Northeast Corridor Safety Commission (NECSC). The NECSC is made up of stakeholders operating on the Northeast Corridor, and the purpose of the NECSC is to provide annual recommendations to the Secretary of Transportation.

FRA Regulations: § 236.1033 Communications and Security Requirements.

(a) All wireless communications between the office, wayside, and onboard components in a PTC system shall provide cryptographic message integrity and authentication.

(b) Cryptographic keys required under paragraph

(a) of this section shall:

(1) Use an algorithm approved by the National Institute of Standards (NIST) or a similarly recognized and FRA approved standards body;

(2) Be distributed using manual or automated methods, or a combination of both; and

(3) Be revoked:

(i) If compromised by unauthorized disclosure of the cleartext key; or

(ii) When the key algorithm reaches its lifespan as defined by the standards body responsible for approval of the algorithm.

(c) The cleartext form of the cryptographic keys shall be protected from unauthorized disclosure, modification, or substitution, except during key entry when the cleartext keys and key components may be temporarily displayed to allow visual verification. When encrypted keys or key components are entered, the cryptographically protected cleartext key or key components shall not be displayed.

(d) Access to cleartext keys shall be protected by a tamper resistant mechanism.

(e) Each railroad electing to also provide cryptographic message confidentiality shall:

(1) Comply with the same requirements for message integrity and authentication under this section; and

(2) Only use keys meeting or exceeding the security strength required to protect the data as defined in the railroad's PTCSP and required under §236.1013(a)(7).

(f) Each railroad, or its vendor or supplier, shall have a prioritized service restoration and mitigation plan for scheduled and unscheduled interruptions of service. This plan shall be included in the PTCDP or PTCSP as required by §§236.1013 or 236.1015, as applicable, and made available to FRA upon request, without undue delay, for restoration of communication services that support PTC system services.

(g) Each railroad may elect to impose more restrictive requirements than those in this section, consistent with interoperability requirements specified in the PTCSP for the system.

[redacted]

COMMUNICATIONS PROTECTION

LIRR PTC ACSES II networks have ensured that communications channels are adequately protected. Protections ensure the continued confidentiality, integrity, availability and non-repudiation of all sensitive communications.

LIRR PTC ACSES II is required to use trust relationships to facilitate communications that cross network boundaries. Tools and equipment used for communications must be authorized by the System Integrator.

LIRR PTC ACSES II has implemented Hash Message Authentication Code (HMAC) cryptographic algorithm to provide the necessary authentication, and to elect NOT to apply message confidentiality. This approach satisfies all of the mandatory requirements levied by the Federal Railroad Administration (FRA) and the railroads for cryptographic security in accordance with FRA 236.1033 specification for communication and security requirements which is split into two parts. Subparts (a) through (d) describe the requirements for cryptographic message integrity for all wireless communications for PTC systems. Subparts (e) through (g) describe the requirements for cryptographic message confidentiality.

In order to provide integrity and authentication of messages that are sent (either over the air or via a wired connection) an HMAC cryptographic algorithm has been deployed. An HMAC cryptographic algorithm works by taking a message and applying a hash function (SHA2) to it (SHA2 is approved by NIST as strong hashing functions). Hash values are calculated with SHA2 by MTA devices. The hash function is calculated over the message content using a secret key, which outputs a unique hash value of the message. Since the message content is an input into the hashing function, cryptographic message integrity is achieved. In addition, the use of a secret key in the hashing function provides cryptographic message authentication. The key only given to authorized devices (users).

Those messages that are secured using HMAC over 220 MHz radio is as follows.

Appendix B shows watermarking scheme between the Vehicles and the Signal System and Back Office System.

- Message Type 21



[redacted]

Cellular communication of the above messages are encrypted using the standard encryption methods used by cellular technologies such as CDMA, GSM or LTE. Selection of these methods are standard features of the service providers.

[redacted]

DATA SECURITY

Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

The LIRR PTC ACSES II system protects the confidentiality and integrity of information stored on each of the components within the subsystems. Data Security is achieved via the System Data Management Facility (SDMF) through the implementation of principles of least privilege, separation of functions/duties, and device security. The System Data Management Facility (SDMF), described in CDRL 2-030 SDMF Design Document (PDM 3035727) provides tools to allow for secure retention of system data and configuration files as well as the life cycle management of those assets through released baselines. Features of the SDMF include tools for Life Cycle Management, Asset Management, Data Maintenance, and Failure Tracking systems.

Information in transit is protected through the implementation of HMAC which is a NIST-approved strong hashing function (See Appendix B). To further ensure the transmission of information throughout the LIRR PTC ACSES II system is closing all unused physical ports in the switch, allowing traffic only for the known IP addresses, filtering unauthorized message protocols, including CRC for all vital ACSES messages, verifying messages upon arrival for the correctness of source, destination before processing it, and generating alert and alarms to notify users about invalid or erroneous messages. Errors or malicious activity through the transmission of information is handled by the System Administrator.

Device Security Device security is implemented by configuring IP Access Control Lists (ACLs) in Office/RWPS/Remote network equipment for SNMP and to access the device remotely using SSH. IP based ACLs has been implemented for all the servers/workstations are connected in respective VLANs in each Cisco switch that are installed in above said locations to filter network traffic by controlling whether routed packets are forwarded or blocked at the device's physical interfaces. Each Cisco device in above said locations examines each packet to determine whether to forward or drop the packet, on the basis of their criteria that we configure within the access lists. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

INCIDENT RESPONSE

Security Incidents

Every person who uses, handles, or otherwise accesses sensitive material must report security incidents immediately to authorized personnel (e.g., Supervisor, Security Officer).

Incidents could include—

- Unauthorized use of systems for other than its intended purpose
- Unauthorized hardware and software access
- Premature use of key
- Maintenance by unqualified personnel
- Tampering with key material or critical systems
- Unauthorized disclosure of information
- Sensitive material left unsecured and unattended where unauthorized persons could have had access

Incident Report

The report should include the following information:

- Material involved
- Personnel involved
- Location of incident
- Circumstances of incident
- Additional reporting requirements including specific incidents or items
- Possibility of compromise
- Point of contact.

Inter-agency response to incidents are defined through multiple inter-rail communication sessions which happen between Amtrak and LIRR. It also provides information about various hardware, physical and logical requirements.

PHYSICAL AND ENVIRONMENTAL PROTECTION

Long Island Railroad to provide physical and environmental security for all of the PTC ACSES II information systems, IT infrastructure, and assets, information, and data. Controls are common across the sub-systems and must adhere to the physical security guidance established in each sub-system description documents. In addition to logical controls managing user facility access, the physical facilities supporting the LIRR PTC ACSES II system components are locked in cabinets or enclosures, are subject to periodic security inspections, and are monitored via security cameras.

The primary areas of concern within the LIRR PTC ACSES II sub-system components (e.g., server rooms, media storage areas, data centers, etc.) must have appropriate physical access controls. LIRR PTC ACSES II system employs a process in which only authorized users are granted access to the sub-systems that house and maintain the physical components of the information system. User facility access is managed through the use of access cards which are primarily based on security privileges. System Administrators who administers such facilities is required to be granted full and continuing access to all assessments, visitor logs, and all other documents necessary to verify and monitor the efficacy of these controls.

Users of the LIRR PTC ACSES II IT resources must use only software that is properly licensed and registered for use. Users may access, use, and share LIRR PTC ACSES II maintained sensitive assets, data, and information only to the extent that it is authorized and necessary to fulfill their assigned job duties.

Additional Physical Protection of Positive Train Control (PTC) assets include Physical Access Security across Buildings, Floors, Rooms, and Cabinets. The measures in place to minimize risks associated with threats to these physical areas include Security Guards, and RFID Key Locks.

Appendix E provides a detail listing of the facilities, number of workstations, physical security measures and authorized users.

REMOTE ACCESS

Remote access within the LIRR PTC ACSES II is prohibited except for authenticated, encrypted users. Users granted remote access are expected to employ reasonable security measures and comply with the LIRR enforced access agreements to protect the LIRR PTC ACSES II information and assets, and data, when accessing any of them remotely.

DMZ proxies' communication from unsecured areas to secure zones to manage remote access to LIRR PTC ACSES II systems components by users (or processes acting on behalf of users). Remote offices, which redundantly connect to the GBN, are protected by their own firewalls and Layer-3 switches. The same security principles apply to the Remote Offices as the Office Network.

LIRR PTC ACSES II uses network interconnection agreements to authorize remote access connections.

The Office Network also connects to the Amtrak network. The Amtrak network has a redundant pair of firewalls facing a redundant pair of routers in front of the Office Network. These routers use Access Control Lists to control and monitor traffic to and from Amtrak.

RISK ASSESSMENT

Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

LIRR PTC ACSES II system has invested a considerable number of resources to conduct comprehensive security assessments leveraging threat scenarios built on intelligence analysis and past experiences. These threats and vulnerabilities risk responses are highlighted in the ACSES System Security Mindmap and the process is documented in the Security Vulnerability Assessment CDRL 2-137 | Identity Number: 3035840.

LIRR PTC ACSES II system conducted an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the LIRR PTC ACSES II system and the information it processes, stores, or transmits. The Security Vulnerability Assessment Security Vulnerability Analysis (SVA) SVA is a comprehensive study of the LIRR Systems to identify threats and vulnerabilities of the LIRR ACSES II System assets and to make recommendations for their elimination or control during all life cycle phases. The assessment was executed following a 5-step Risk Assessment Process Model. The five steps are: Target or Threat Identification, Critical Asset Value Assessment, Vulnerability Assessment, Conduct a system threat and vulnerability assessment, and Emphasize counter measures and mitigation recommendations.

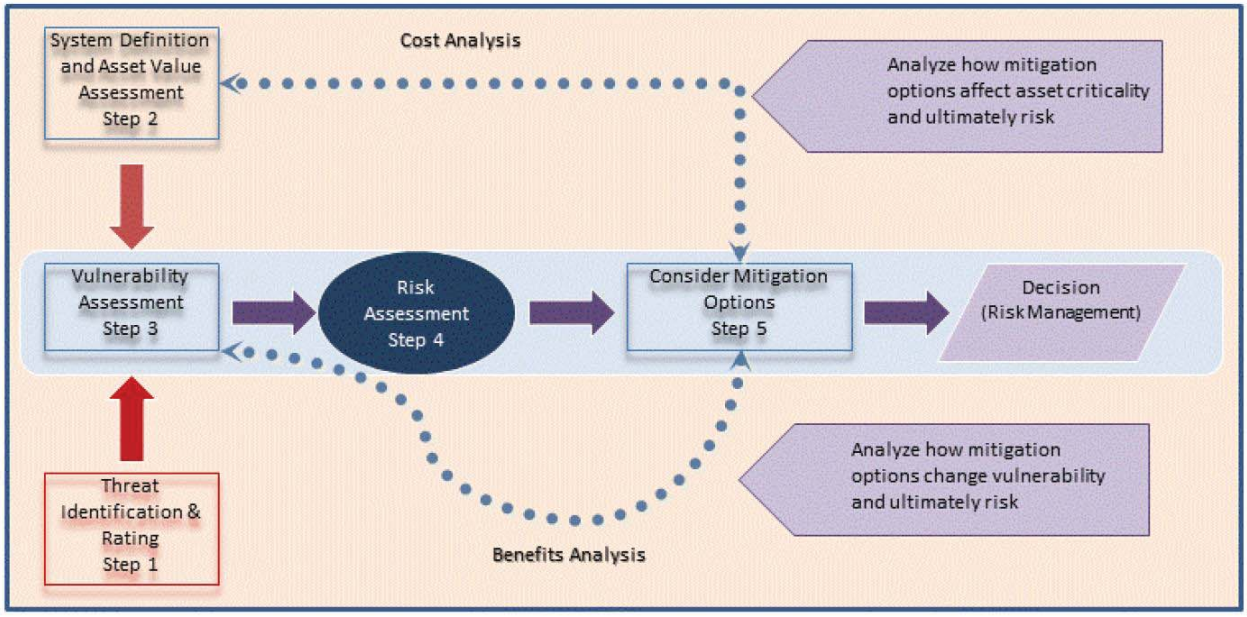


Figure 4-1: Risk Assessment Process Model

Threats and vulnerabilities are not limited to the internal functions of the LIRR PTC ACSES II system. There are also interconnections with adjacent systems defined in Interconnection Agreements which define the inter-rail communication sessions. The outcome of the interconnection agreements is to provide clear understanding of the relationship while maintaining currency with recommended security practices, techniques, and technologies.

The LIRR PTC ACSES II System Security and Vulnerability Analysis is recorded in a matrix form in excel spreadsheets. It is generally expected that security assessment are executed annually and results updated accordingly.

SECURITY CONTINUOUS MONITORING

Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

The LIRR PTC ACSES II Office subsystems are authorized for operation in accordance with the FRA PTC implementation program. System Maintainers are responsible for the continuous monitoring of the effectiveness of security controls employed within or inherited by the system, and monitoring the impact of any proposed or actual changes to the system and its operational environment.

Events within the Data and Maintenance System (DMS) from the continuous monitoring of security controls are correlated and provided to the LIRR System Administrator, who uses the content when assessing system risk and making system authorization decisions.

The primary function of the DMS subsystem is to provide data storage to other subsystems that produce data. This data includes operational data created by operators through user interface forms, events generated by various subsystems, and all the ACSES messages.

LIRR PTC has a database centric specification where all ACSES message information is stored in a Highly Available Relational Database Management System (RDBMS) for subsequent Event Review and Reporting.

System Updates

System Administrators are responsible for enforcing system updates of the operating systems and supporting LIRR PTC ACSES II subsystems including workstations and network equipment. LIRR PTC ACSES II system has a configuration management plan that addresses the prompt installation of system updates. When applicable, updates are installed and tested on a non-production system prior to implementation on a production system. Patches are pushed to the production environment via the Security Server.

All updates including patches must be approved through the change management process prior to installation on systems.

Security Monitoring

Security Functions, best practices for office equipment is also followed, including:

• There is only one SEC server per control center. The User interface to the above mentioned tools are available through web links on the windows. These web links are controlled through appropriate Function Assignments to limit access to System Maintainer and System Administrator only.

• McAfee ePO is configured on a cluster environment between SEC servers across the control centers. The McAfee ePO hosts its database on the ACSES II Office SQL Server, which is clustered, and replicated across the control centers.

• Manage Engine Event Log Analyzer instances are deployed on PCC SEC and BCC SEC on a Windows cluster. Each of these captures the logs of the entire ACSES II Office system including PCC and BCC. The Event Log Analyzer provides a unified log management console to the System Maintainer by collecting logs from all Office servers, workstations, and network devices. It also monitors file integrity, conducts log forensics analysis, monitors privileged users and complies with different compliance regulatory bodies by

intelligently analyzing logs and instantly generating a variety of reports like user activity reports, historical trend reports, and more

• Tenable Nessus instances are deployed on PCC SEC and on BCC SEC as two independent instances. Each of these instances can perform a vulnerability scan and penetration test of the entire ACSES II Office system including PCC and BCC which is executed by the System Administrator. Penetration tests are performed manually or scheduled by System Administrator who is also responsible for providing a report after finishing the test.

• The Intrusion Detection and Prevention system (IDS/IPS), is located on the firewalls (Cisco 5545-X), which perform state-full packet inspection and respond to various attack signatures. An attack signature is a pattern that identifies attacks or classes of attacks on an application and its components. Signatures for various attacks including Denial of Service (DoS), Man-in-the-middle (MitM) and various other attacks are supplied by Cisco (similar to virus signatures from McAfee).

• Advanced Malware Protection (AMP) is also enabled on firewalls for continuous monitoring of malicious behavior, malware detection & removal.

• SEC COTS (McAfee ePo, ADAudit+ & ELA) databases shall hosted on ACSES II Office SQL servers, which is clustered and replicated across the control centers

• SEC COTS (ELA and ADAudit Plus) shall not support SNMP to send the message traps to NMS, whereas SNMP support for hardware monitoring on SEC servers.

APPENDIX A: OFFICE SUBSYSTEM NETWORK AND INFRASTRUCTURE

The ACSES II Office Subsystem is comprised of Primary and Backup Control Centers which have identical hardware and are capable of operation of the Positive Train Control (PTC) systems independently. The control centers share data between each other using the Office LAN and Railroad fiber optic 10 Gigabit per second Layer 3 routed network which all have redundancy and resiliency designed into the network architecture. A redundant pair of firewalls (one active, one standby) sit before both of the PCC and BCC office networks to control traffic to and from the Ground-based Network (GBN). These pairs of firewalls also control Wayside-to-Office and Office-to-Wayside traffic. These same firewalls redundantly connect to a pair of layer-3 switches on the RWPS network. The office network (PCC & BCC) has device redundancy for every zone. In LIRR LSW, Amtrak, OSW and RWPS zones have dual switches and firewalls. If one device fails, the redundant device takes over to ensure minimal downtime and continuity of network services.

The firewalls are configured to only allow traffic inbound and outbound from a defined list of devices. In addition, only specific protocols or applications are allowed through the firewalls. This helps to limit exposure to network probes and attacks by only allowing traffic that is applicable to the train system. The firewalls are also configured for stateful inspection, Intrusion Detection (IDS) and Intrusion Protection (IPS). Intrusion Detection compares the traffic flows against a list of known exploits and generates alerts when a match is found. Intrusion Protection enhances IDS by apply an action (e.g. blocking traffic) when a security alert is detected.

Any violations of the firewall policies or detected threats are reported to the network Monitoring System (NMS). The DMS and NMS are the two main components where alarms are generated.

Based on Administrator configured alarm rule, any system event can be send to specific component (UIS, NMS), DMS users, device (printer, FAX) or all of them. The DMS is the dedicated maintenance system in the ACSES II office to maintain and manage events history.

The NMS receives data from all devices (primarily via SNMP) and is preconfigured with a series of thresholds for various performance parameters. These threshold rule violations result in alarms on the NMS. Alarms can have varying priority levels indicating the severity (trouble, warning, critical etc.) of the issue. SNMP traps (such as those sent by the DMS) can be presented as prioritized events on NMS. Once the alarm is sent to the presentation component, UIS or NMS, the lifecycle of that Alarm is managed from within the component. Every state change of an alarm is logged back into DMS (Database Management System).

DMS is made up of data collector, data display, and SQL server components. The DMS stores all communication messages, Alarms, Events, Notifications, between all the sub-systems which are configured by the System Administrator. By default, one node (server) is specified as the Active node, and the other node is specified as Dormant. The Dormant node assumes Active status only if it doesn't receive a heartbeat from the Active Node for a configurable period of time. Both DMS Collectors establish a TCP/IP connection with the STS and other components within the control center based on the Server/Client contract between it and its peer. Once one of the DMS collectors becomes Active, it starts sending heartbeats to other component servers within the same control center. STS also sends heartbeats to both

Active and Dormant DMS components. The DMS (Database Management System) provides for Data archiving, retrieval, and review, generates SNMP messages to be sent to NMS for the PTC devices that do not support SNMP, and generates acknowledgment for the OBC ACSES II maintenance message. All events, and any state changes of those, are always logged into DMS for historical analysis. To make sure that events originated in multiple components are chronologically ordered when stored into DMS, components capture and forward the event generation time along with other event data to DMS. DMS uses this timestamp as the event generation time while storing the event into the SQL database. Since all the servers have their clocks synchronized to the ADDC server, two event timestamps from two components can be assured to represent correct chronological order.

Events are further classified as Alarms, Alerts, or they stay as simple Events which are configured by the System Administrator. This classification is based on the severity and the response that is warranted from an authorized user in response to the occurrence of the event. Run time diagnostic events are displayed on one of the user Interface components, UIS, NMS, or SEC. Most of the events have their destinations statically specified as the intended recipient is already defined. However, rule based event generation facility within the DMS component that scan the SQL database for patterns provides an interface to route alarms to be displayed at appropriate workstations.

Alarm System includes DMS, NMS, UIS, and SEC. The rules and logic to generate alarms/alerts and/or present them to the authorized users are included in the alarm system design. The DMS is the dedicated maintenance system in the ACSES II office to maintain and manage events history.

The system provides capabilities for the System Administrator to modify existing or/and create new rules in the DMS based on the available event types. At a minimum, the rules can consist of event types, alarm or alert selection with priority/type, description, corresponding user groups and component to display.

General event types that are addressed by the alarm system:

- Hardware/equipment state
- Software health and behavior
- ACSES Messages, error and maintenance
- COTS Products error logs
- SNMP and Non-ACSES Messages
- Failover state and progress
- Database connectivity

APPENDIX B: MANAGEMENT OF SECURITY CERTIFICATES AND OPERATIONAL PRIVATE KEYS

Long Island Railroad (LIRR) acknowledges the need for encryption; thus establishing key management processes. The secure generation, distribution, storing, and revocation of keys are essential to make encryption implementation effective. Generating encryption keys and distributing keys to all units is a complex process and there are inherent risks, so proper key management processes are implemented during the key life cycle. Compromise of encryption keys could affect the integrity, confidentiality, and availability.

The LIRR Engineering Signal group acts as the central authority for the key management infrastructure. As the central authority the LIRR Engineering group establishes the policies and procedures for the management of the encryption keys, serve as the source for system level information, and maintain continuity of operations for the life cycle of the key management infrastructure. This is described in the Security key Management Plan [Ref F].

Roles and Responsibilities

LIRR Engineering Signal Group

- Provide security guidance on the implementation of key management
- Authority over written guidelines in the form of a key management plan for the handling and safeguarding of keying material
- Ensure that all individuals who handle keying material are fully cognizant of the key management requirements
- Establish and close custodians'/operators' accounts
- Maintain accounting reports
- Verify regularly the inventory of controlled key account
- Establish an audit and inspection program for the verification of the inventory of key management accounts
- Be responsible for receiving and investigating any security-related incidents
- Provide formal training courses for new custodians/operators and regular training thereafter.

Key Management Manager (System Maintainer / Network Maintainer)

- Perform key management functions on a day-to-day basis
- Protect keying materials and limit access to individuals with a valid need-to-know and clearance, if applicable
- Configure security features of key management system components in accordance with agency policies
- Maintain all required key accounting and related records
- Conduct inventories of all accountable keying material periodically (ex. annually), upon appointment or termination of a custodian or as required by the organization
- Perform routine destruction of key material
- Maintain up-to-date records and submit all required accounting reports

- Ensure that all material received is inspected for evidence of tampering
- Report immediately any known or suspected incident involving keying material and submit incident reports.

Key Management

Key Generation

The generation of keys is the most sensitive of all key management functions. LIRR employs a combination approach to Key Generation. LIRR keys are generated using a Random Number Generation (HMAC section describes the approach for HMAC Keys and Appendix X defines the process for cellular keys).

Key generation is initiated primarily in the Key Management Server. Within the LIRR infrastructure the key management server is the Wayside Communications Controller (WCC) Server. The WCC Server within the Wayside Interface Unit (WIU) handles key management through a key server located in the WCC server. The key server is installed on all instances of the WCC and provides full redundancy both within a control center and across control centers.

Key Distribution

After a key is generated different techniques are used to distribute encryption keys, depending on message flow.

Keys are distributed manually (with a planned process for automatic distribution). This is a limited risk as the LIRR Key Management Infrastructure only maintains one tenant. Keys distributed manually are protected throughout the distribution process. During manual distribution, secret or private keys are either wrapped (i.e., encrypted - HMAC) or distributed using appropriate physical security procedures. The manual distribution process shall assure that:

1. The distribution of the keys is from an authorized source. Keys are pushed in advance of production implementation from Railroad to Railroad via Key Files.

2. Any entity distributing plaintext keys is trusted by both the entity that generates the keys and the entity(ies) that receives the keys,

3. The keys are protected

4. The keys are received by the authorized recipient.

5. Keys generated within the Key Management Server are activated and pushed via the interface

Key Storage

Once keys are generated, they are stored properly to prevent unauthorized persons from accessing, using, or compromising them. The session keys and the key encrypting keys are kept in protected storage. If keys or key components are generally stored on a physical medium (laptop) this token may need to be stored in a special manner to prevent unauthorized individuals from accessing the key or key components.

Additionally, keys are stored in encrypted format on electronic media. The original keys are also stored in key files the computer until they are deleted manually.

Key Destruction

LIRR employs a variety of mechanisms for the destruction of keys, including erasing electronically stored data, cryptographic keys, and critical stored parameters by altering or deleting the contents of the data storage to prevent recovery of the data.

Key Components for Recovery

When keys are compromised or damaged, the following procedures should be considered:

If the key stored in the Key Management Server is destroyed,

- Retrieve backup media containing active keys
- Examine whether the key stored in the media is the latest version
- Upload the key into the Key Management Server (WCC)

If keys are compromised,

- Destroy the compromised key in a proper manner
- Generate a new key
- Follow the normal procedures for generating, distributing, and storing keys

Critical components of the LIRR Key Infrastructure

Components	Functions
Key Management Server (KMS) (WCC Server)	Acts as the main server for the key management functions on the network
Wayside Interface Unit (WIU)	Monitor the status of wayside devices to vitally transmit a response to an interlocking status request to the OBC.
Wayside Data Radio Network	Provides the message transfer between the base communications package (BCP) and the mobile communications package (MCP).
Radio Configuration Files (RCF)	Contains information to establish proper radio communication. Stores encryption key files.
Mobile Communications Manager (MCM)	Maintains the proper communication path for ACSES II messages to and from the Onboard Computer.
Base Communications Manager (BCM)	Manages communication with the WCC and WIUs. Controls time slot management for the PTC Data Radio.
☐ Other (specify):	

Hash Message Authentication Code (HMAC)

The ACSES II has implemented Keyed-hash Message Authentication Code (HMAC) cryptographic algorithm to provide the necessary authentication, and to elect NOT to apply message confidentiality. This approach satisfies all of the mandatory requirements levied by the Federal Railroad Administration (FRA) and the railroads for cryptographic security in accordance with FRA 236.1033 specification for communication and

security requirements. The use of HMAC is to provide encryption assuring the integrity and authentication of messages that are sent over the air or via a wired connection.

Radio security includes applying an HMAC value to each message that ensures message integrity and authentication.

The general concept of the Communications Security Design depends on applying an HMAC value to each message that is transmitted over-the-air. The HMAC value is calculated using SHA2. The inputs to the HMAC calculation are the message itself and an HMAC key that uniquely identifies all ACSES II devices. The communication manager that directly interfaces with the message sender calculates the HMAC value and exclusively or (XOR) the value into the ACSES II 72bit CRC. The communication manager that directly interfaces with the destination ACSES II device attempts to calculate the same HMAC value as the sender. If the message originated from a valid sender and was not tampered with in transit, the two calculated values are the same. The receiving communication managers XOR the HMAC value into the 72bit CRC. If the two values are equivalent, then the CRC restores to the same value that was calculated but the ACSES II sender. The communication managers provide HMAC protection regardless of the wireless bearer method.

HMAC provides cryptographic authentication and integrity of messages being transmitted by ACSES devices. By encoding and decoding the HMAC values in the communication manager closest to the source or destination ACSES device protection is provided nearly end to end. Encoding and Decoding is provided for all over-the-air ACSES messaging within the following subsystems:

- MCM: Provide HMAC for ACSES RF messages to and from the OBC
- BCM: Provide HMAC for ACSES RF messages to and from the WIU
- WCC: Provide HMAC for ACSES RF messages to and from the Office in addition to HMAC, AES 128 encryption can be turned on in the GE MDS TD220MAX radio in order to provide cryptographic confidentiality of the ACSES messages. This function is a native function of the GE 220 radio. AES 128 does not inherently provide cryptographic message integrity and authentication. Therefore, it is suggested as an added level of security, not a replacement for HMAC. AES 128 encryption can be turned on using the following steps:

    1. In the Radio's Configuration Menu select the Security Configuration option.
    2. Under the Security Configuration menu select the Wireless Security option
    3. Under the Wireless Security menu select the AES Phrase to enter the AES Secret Key
    4. Under the Wireless Security menu select the AES Encryption option to toggle AES encryption on or off.

The radio's configuration menu is accessible remotely via the same means as the MCM remote diagnostic cellular connection. Thus, the AES encryption can be activated and deactivated from a remote workstation.

The key list is not persistent within the BCM after a recycle of power. The BCM requests a new list from the Key Manager after each reboot.

The MCM does not remove the ACSES Keys when powered off therefore if an MCM is removed the approved key removal process must be followed. Subsequently the replacement MCM requires having a new key installed. For both removal and installation the approved process as detailed in the reference (a) maintenance document must be followed.

Operational Considerations: Radios not using AES 128 or using an incorrect key are not able to decode communicated messages. Additionally, trains using an out dated HMAC key file are not able to decode messages correctly. Both AES and HMAC require strict change control management in order to ensure all necessary devices have the correct security keys.

Flow of HMAC Protected Data

ISR (Interlocking Status Request)

For the Interlocking Status Request (ISR) message, a modified approach is used since the message does not have a CRC. ISR messages are protected in order to prevent an attacker probing the system with fake ISRs. For this message only, the HMAC value is XOR'd into static byte fields in the ACSES ISR payload since this message type does not include a CRC.

ISRs flow from the OBC to the MCM to the BCM to the WIU. The MCM calculates an HMAC value for the ISR using the appropriate HMAC Key from the key file for the WIU corresponding to the ATCS destination address in the ISR. The HMAC Value is truncated to 4 bytes and those 4 bytes are XOR'd into bytes 1, 4, 5 and 6 of the ISR. This can be done without loss of information because those bytes can be completely reconstructed. This process is how the MCM performs HMAC encoding of ISRs.

The BCM extracts the 4-byte HMAC value that was placed in bytes 1,4,5, and 6, and restores the original 4 bytes to the ISR. The BCM calculates an HMAC value on the message using the HMAC key corresponding to the WIU being addressed. This value is truncated to 4 bytes and compared with the extracted 4-byte HMAC value. This process is how the BCM performs ISR HMAC decoding and validation. The ISR is being forwarded to the appropriate WIU if the MCM used the correct HMAC key. If an intruder sent a spoofed message or an incorrect key was used to calculate the HMAC value, the message fails validation and is being dropped by the BCM.

IS (Interlocking Status)

The BCM calculates an HMAC value for the IS (Interlocking Status) from the WIU using the appropriate HMAC Key for the WIU corresponding to the ATCS destination address in the IS. The HMAC Value is truncated to 9 bytes and XOR'ed into the 9 bytes of the ACSES CRC. This process is known as HMAC encoding.

The IS message is sent to the MCM, which performs HMAC decoding, restoring the original CRC of the ACSES message. The OBC validates the message using the CRC. If the message is successfully validated, then the message originated from an authenticated source and was not interfered with by an outside entity.

TSRR (TSR Request)

TSRR (TSR Requests) from the OBC are HMAC encoded by the MCM using the STS HMAC key, and decoded by the WCC. The flow is OBC to MCM to BCM to WCC to STS. The STS validates the authenticity of the TSRR when it checks the vital CRC.

TSR

TSR (Temporary Speed Restrictions) are HMAC encoded by the WCC using the STS HMAC Key, decoded by the MCM, and validated by the OBC. The flow is STS to WCC to BCM to MCM to OBC.

MTA

MTA messages from the OBC are HMAC encoded by the MCM using the DMS HMAC Key. The message is decoded by the WCC using the same key. The MTA message is then delivered to the DMS.

MTAA

MTA Acknowledgement messages are encoded by the WCC using the DMS HMAC Key. The message is decoded by the MCM and delivered to the OBC to acknowledge the delivery of an MTA message.

Cellular communication of the above messages are encrypted using the standard encryption methods used by cellular technologies such as CDMA, GSM or LTE. Selection of these methods are standard features of the service providers.

APPENDIX C: COMMUNICATIONS SUBSYSTEM

The ACSES II Communications subsystem consists of a Ground Based Network (GBN) and a Data Radio Network.

The GBN includes network switching equipment that allows IP-based communication between the Office and the wayside network equipment. The Data Radio Network provides the message transfer between the base communications package (BCP) and the mobile communications package (MCP). This includes the 220 MHz PTC Data Radio (PDR) and all the RF signal distribution system to support the non-IP based wireless link.

The communications system is designed to expand to use other radio access bearer methods depending on Railroad requirements. The additional radio access bearer methods designed for this system includes Cellular, and Wi-Fi.

APPENDIX E: VEHICLE SUBSYSTEM

The ACSES II vehicle subsystem is based on the Amtrak ACSES II type approved system. The ACSES II vehicle system consists of the following high level components:

- Onboard computer (OBC) for vital ACSES II functionality and I/O processing
- An ADU (or ADUs) for train engineer display of ACSES II and ATC information
- CTV and transponder scanner for reception of transponder messages
- A speed sensor for determining vehicle speed
- A Decelerometer for suppression compensation of wheel spin, wheel slide, and speed sensor crosschecks. The Brake Assurance function (LIRR only) also utilizes the decelerometer for measure braking effort.
- Vital interface to the ATC (via AIU where applicable) to determine when ATC is operational and to allow ATC to enforce stop aspect
- Interface to the mobile communications manager (MCM)
- External Memory Module (where applicable)
- An ACSES II Alarm for providing audible indications to the train engineer
- Absolute Stop Bypass (ASB) Pushbutton for granting movement past a PTS stop
- A Cut-out switch for bypassing the ACSES II OBC (Sealed and located away from crew position)
- The Acknowledge pushbutton for train engineer acknowledgment.
- MCM for providing all mobile communication management on the train and interface to the OBC
- Interface to the OBC
- 160 MHz Filter to provide band pass filters for the train's existing communications system
- 220 MHz Filters for providing band-pass filters on the train
- 220 MHz PDR for communicating with the BCP at 220 MHz
- 220 MHz Antenna
- Digi Router including:
  - Cellular PDR for communicating with the Office over Cellular
  - Wi-Fi PDR for communicating with the BCP over Wi-Fi
  - GPS
- Wi-Fi Antenna
- Cellular Antenna
- GPS Antenna

Interfaces from the OBC to other ACSES II subsystems as well as external to ACSES II.

- **OBC to Comms** – Primarily, the OBC interfaces to the MCM for the purpose of communicating to the wayside. Logically, the OBC utilizes the link to the MCM in order to receive status from wayside signals (through the WIU) and to receive TSRs from the STS. The OBC to MCM is a type approved interface; however, there are additional messages added to support new ACSES II functions.
- **OBC to Transponders** – The OBC utilizes its transponder scanner to energize passive transponders in the track bed to receive static information for train location and ATCS addresses for wayside

devices. The transponder also contains any approaching civil speed restrictions for the direction of travel, including route dependent speeds through an interlocking. The OBC to transponder is a type approved interface; however, there are additional transponder packages added to support new ACSES II functions.

- **OBC to Car Systems –** The OBC interfaces to the following car systems: Inputs: - Car battery for power - Acknowledge switch (also utilized by the ATC) - Absolute Stop Bypass (ASB) Pushbutton - Reverser or Master Controller for Forward and Reverse indication - Cab Make-up to determine cab activation - Departure Test Switch

APPENDIX F: MANAGEMENT OF WAYSIDE INTERFACE UNIT (WIU) SECURITY KEYS

The Wayside subsystem is the interface between the ground network and the vehicle. The Wayside subsystem consists of the Wayside Interface Unit (WIU), Base Communications Manager (BCM), the base radio, and the interfaces to the Signaling system and Ground Based Network (GBN). The Wayside subsystem has redundant connections into the GBN.

WIU (Wayside Interface Unit) – The WIU is provided to vitally monitor the status of wayside devices (Switches and Signals) in order to vitally transmit a response to an interlocking status request to the OBC. The interlocking status includes the signal status (including interlocking speed), tracks to be crossed (including distance to change track), exit track (including distance to exit track), and any additional Loma information to the next interlocking when nested.

The Wayside Data Radio Network provides the message transfer between the base communications package (BCP) and the mobile communications package (MCP). This includes the 220 MHz PTC Data Radio (PDR) and all the RF signal distribution system to support the non-IP based wireless link. The Wayside subsystem is designed to expand to use other radio access bearer methods depending on Railroad requirements. The additional radio access bearer methods designed for this system includes Cellular, and Wi-Fi.

Metropolitan Transportation Authority
Long Island Rail Road / Metro-North Railroad
PTC – SYSTEM INTEGRATION
Bombardier Siemens PTC Project Consortium
Contract Numbers: 1712/29544

Communications Security Addendum Communications Subsystem Description Document

CDRL 7-001

Responsible Division:	Responsible Unit:	Document Type:	Distribution Status:	Document State:
BT	ENG	CDRL	Project	Released

	Name / Title, Group	Signature	Date
Prepared:	Jonathan Worsley Communications System Engineer	Jonathan Worsley	2018-10-31
Verified:	Chuck Wisniewski Wabtec General Manager	Charles A Wisniewski	2018-10-31
Approved:	David Depardieu SI Comms Manager	David Depardieu 2019.08.09 07:48:23 -04'00'	
SI Quality Process Review:	Phil Magloire BT Quality Assurance Group	Phil Magloire 2019.08.09 07:42:37 -04'00'	
BT/SRA Review:	N/A Title		
BT/SRA Review:	N/A Title		

Nothing herein shall limit the rights of the Railroads under Article 404 of Contract Nos. 1712/29544.

This document and its contents are the property of Bombardier Inc. or its subsidiaries. This document contains confidential proprietary information. The reproduction, distribution, utilization or the communication of this document or any part thereof, without express authorisation is strictly prohibited. Offenders will be held liable for the payment of damages. © 2018, Bombardier Inc. or its subsidiaries. All rights reserved.

This document contains proprietary information. The ownership of this document and its contents is retained by Siemens Industry, Inc. By supplying this document, Siemens Industry Inc. neither grants nor waives any right or license to this document or its contents. The contents of this document as a whole, or any portion thereof, may not be disclosed to other parties or reproduced by any means electronic or mechanical without prior written permission from Siemens Industry Inc. Copyright © 2018 Siemens Industry, Inc. All rights reserved.

Reference Document #:

Identity Number: 3041191

Effective Date:	Revision:	Language:
2018-10-31	_B	EN

Released
RCS Pittsburgh

Revision Log

Revision	Date (yyyy-mm-dd)	Description of Changes
__	2015-04-16	First issue
_A	2016-02-08	Updated with corrections from RR comments
_B	2018-10-31	Updated to describe ACSES Security design for ISRs.

Table of Contents

Section	Subject	Page
1	**Executive Summary**	4
2	**Introduction**	4
2.1	**Compliance Matrix**	4
2.2	**Reference Documents**	4
2.3	**Glossary**	4
3	**Security Design**	5
3.1	**FRA Requirements for Wireless Security**	5
3.2	**MTA Security Solution**	5
3.2.1	Introduction to HMAC	5
3.2.2	Architecture for HMAC on the MTA project	6
3.2.3	Flow of HMAC protected data	7
3.2.3.1	ISR	7
3.2.3.2	IS	7
3.2.3.3	TSRR	7
3.2.3.4	TSR	7
3.2.3.5	MTA	7
3.2.3.6	MTAA	8
3.2.4	HMAC Time Variance	8
3.2.5	Wi-Fi and Cellular Protection	8
3.2.6	Degraded Operation	8
3.2.7	Interoperability Impacts	9

List of Tables

Table 1: Compliance Matrix 4

Table 2: Reference Documents 4

Table 3: Terms Specific to this Document 4

Table 4: Acronyms Specific to this Document 5

1 Executive Summary

The content of this document outlines the design plan for cryptographic message integrity and authentication. The use of HMAC for integrity validation and source authentication is to satisfy FRA CFR 236.1033.

2 Introduction

This is an addendum to the Communications Subsystem Description Document Ref [2]. This addendum supersedes the information provided in the main document.

2.1 Compliance Matrix

Table 1: Compliance Matrix

Specification Volume	Specification Section	Requirement Title	Requirement Summary	Document Section Reference
NA				

2.2 Reference Documents

Table 2: Reference Documents

Reference Number	Document Name	Identification Number
[1]	Dictionary of Terms and Acronyms	3035624
[2]	Communications Subsystem Description	CDRL 7-001: 3035965
[3]	Office Subsystem Description	CDRL 6-001: 3035943

2.3 Glossary

Please refer to the Dictionary of Terms and Acronyms [1]. Terms and acronyms only related to this document are listed below in Table 3 and Table 4 respectively.

Table 3: Terms Specific to this Document

Term	Definition
AES-256	Advanced Encryption Standard 256
HMAC-SHA-256	Hash Message Authentication Code, Secure Hash Algorithm 256

Table 4: Acronyms Specific to this Document

Acronym	Definition
NA	

3 Security Design

3.1 FRA Requirements for Wireless Security

The FRA 236.1033 specification for communication and security requirements can be split into two parts. Subparts (a) through (d) describe the requirements for cryptographic message integrity for all wireless communications for PTC systems. Subparts (e) through (g) describe the requirements for cryptographic message confidentiality.

3.2 MTA Security Solution

The adopted solution is to use the HMAC cryptographic algorithm to provide the necessary authentication, and to elect NOT to apply message confidentiality. This approach satisfies all the mandatory requirements levied by the FRA and the railroads for cryptographic security.

An important goal of the approach is to eventually perform the HMAC calculations at the application level, and not within the communications layer. The design facilitates the OBC / STS / WIU vendors releasing future products with such capability in a backwards compatible fashion without requiring an upgrade of existing equipment.

The below sections provide an introduction into HMAC and a description of the design to be deployed on the MTA system.

3.2.1 Introduction to HMAC

In order to provide integrity and authentication of messages that are sent (either over the air or via a wired connection) an HMAC cryptographic algorithm will be deployed. An HMAC cryptographic algorithm works by taking a message and applying a cryptographic hash function to it. Hash values will be calculated with SHA256 by MTA devices. The hash function is calculated over the message content using a secret key, which outputs a unique hash value of the message. Since the message content is an input into the hashing function, cryptographic message integrity is achieved. In addition, the use of a secret key in the hashing function provides cryptographic message authentication. The key is provided only to authorized devices (users).

Despite other systems where the hash value is then appended to the message and sent to the remote receiver, for MTA an alternate approach is used. Instead of appending the hash value to the message, thereby increasing its size, the hash value is instead applied to the existing 9-byte vital CRC portion of the application message, using an XOR function to flip some of the bits to their opposite state. The receiver then performs the reverse function, flipping the same bits back to their original value. The benefit of this approach is that the (non-safety critical) communication system itself does not perform the hash comparison – instead the validity of the hash value is established when the vital CRC is validated by the OBC, WIU, or STS. With this method the following benefits are achieved:

- A safety critical validation of the hash value by the receiver
- A much stronger hash value, since 9 bytes of hash value is transmitted to the remote receiver, instead of just 4 or 5 bytes used in other systems.

Note that this approach does not hide the hash value since the proper CRC can be calculated, and the hash value recovered through subtraction.

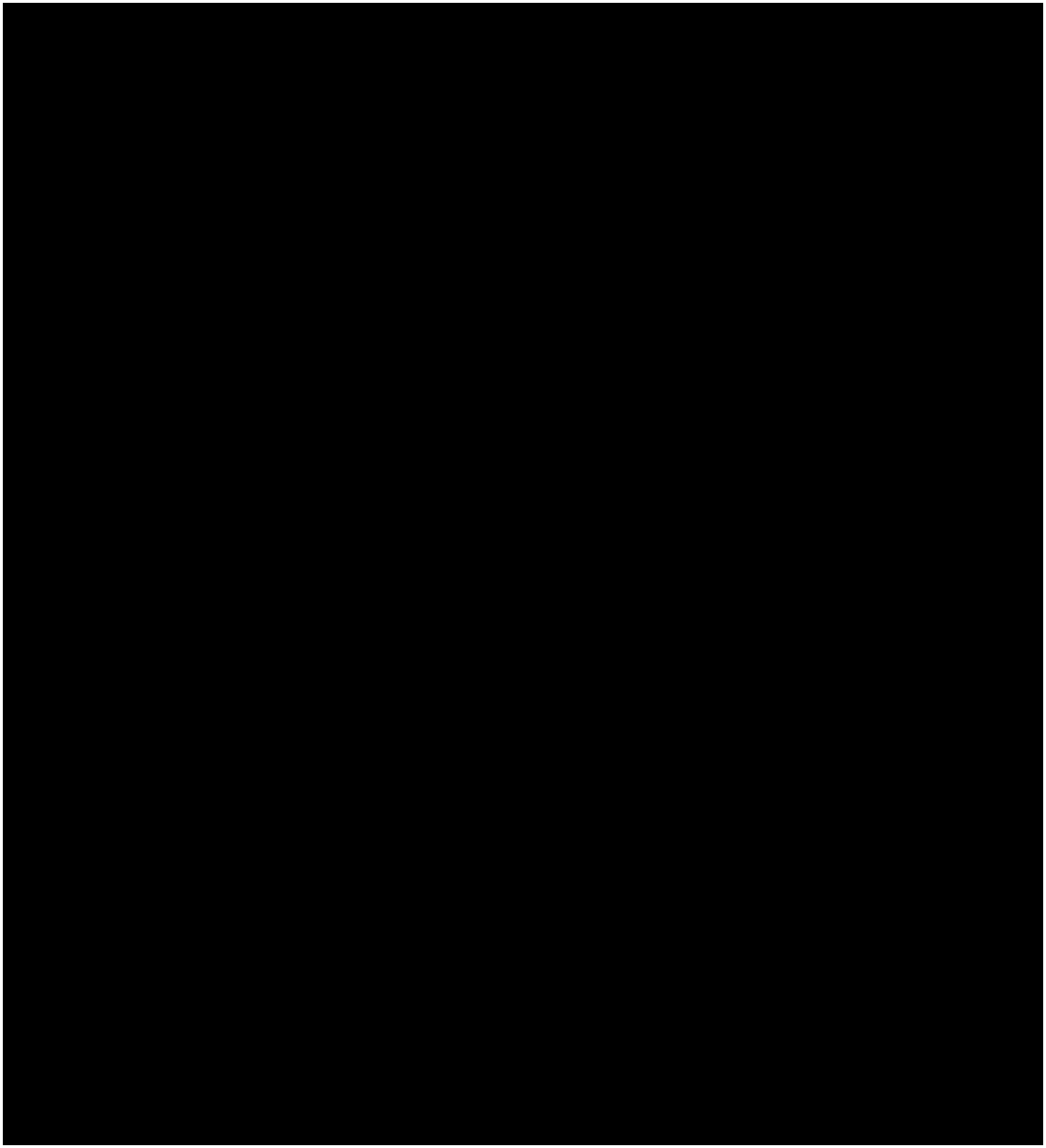
For the Interlocking Status Request (ISR) message, a modified approach is used due the fact that the message does not have a CRC. Instead, the HMAC value is XOR'd into the static byte fields 1, 4, 5, and 6 in the ACSES ISR payload. The MCM will perform the replacement prior to transmission of the ISR. The receiving BCM will remove the applied HMAC and verify ISRs before forwarding them to an attached WIU. If verification fails, the BCM will not forward the message to the WIU. An error statement is logged in the BCM log file and an SNMP trap is sent to the NMS indicating an HMAC failure.

3.2.2 Architecture for HMAC on the MTA project



3.2.3 Flow of HMAC protected data

Within the context established above, HMAC protection is applied as follows:





3.2.6 Degraded Operation

One degraded operational state is defined when the BCM is unable to communicate with the back office, and TSRR/TSR delivery is no longer possible. The architecture allows ISR/IS traffic to flow directly between the BCM and WIU with proper HMAC validation.

Another degraded state exists when either a MCM or BCM contains an outdated HMAC Key File. In this state HMAC values calculated by the MCM and BCMs will not match. This will cause the messages to be rejected by the end devices because the CRC check will fail during the validation process. When this occurs the BCM reports the mismatch, along with the ATCS of the train involved, to the NMS via an SMNP trap.





PTC Restoration Plan

Prepared by:



February 2019

Rev 0.1

Revision History

Revision	Date	Description
draft	Feb 2019	Initial document and onboard section
0.1	Feb 2019	Updates based on LIRR (DC) comments

Table of Contents

1 Introduction 1
1.1 Purpose 1
1.2 Scope 1
1.3 Document Overview 2
1.4 Reference Documents 2
2 PTC System Overview 3
2.1 Overall System Architecture 3
2.2 Design Mitigation Principles 4
2.2.1 Office Systems 4
2.2.2 Communications 4
2.2.3 Transponders 5
2.2.4 Onboard Systems 5
3 Service Recovery Concepts 6
3.1 Detecting Service disruptions 6
3.1.1 General Steps and Tools 6
3.1.2 FRACAS 7
3.2 LIRR Service Recovery and Prioritization 8
3.2.1 Incident Severity Assessment 8
3.3 Failures Modes and Responses 8
3.3.1 Office Failures and Response 8
3.3.2 ACSES Onboard Failures and Response 11
3.3.3 Communications Failures and Response 14
3.3.4 Transponder failure, Damaged or Missing : 14

3.3.5 ACSES WIU Failures and Response 14
3.3.6 Regression testing after Restoration from Failure 15
3.4 System Wide Outage Responses 16
3.5 Preventive Maintenance 16
3.5.1 Fleet Management 16
3.5.2 Wayside Equipment 17
3.5.3 Office Equipment 17
4 Testing, Validating and Communicating the Restoration Plan 17
4.1 Testing and Validating the Restoration Plan 17
4.1.1 Testing 17
4.1.2 Training 18
4.2 Communicating the Restoration plan 18
5 Roles and Responsibilities 18
5.1 ACSES Component Allocation to Departments 19
5.2 PTC Maintenance Roles and Responsibilities 19
6 Appendix A. Acronyms and Definitions 21

List of Tables

Table 1 : Document Overview 2
Table 2 : Reference Documents 2
Table 3 : Office Failure and Answers 11
Table 4 : PTC Maintenance Roles and Responsibilities 21

List of Figures

Figure 1: PTC ACSES II System Architecture 3
Figure 2: En Route Failure Response Sequence Diagram 13
Figure 3: ACSES Component Allocation to Departments 19

1 Introduction

1.1 Purpose

The purpose of PTC Restoration Plan document is to provide a summary overview of the PTC restoration strategies in order for Long Island Rail Road (LIRR) to establish how its maintenance staff will restore service in the event of the loss or disruption of the operation and to make this plan available to FRA.

Overall goals for LIRR PTC Restoration plan include:

- Defining the maintenance elements of the ACSES system.
- Allocating maintenance responsibilities to affected LIRR departments.
- Compliance with FRA regulations and LIRR Engineering and MoE Departmental Standards.
- Integration of the ACSES maintenance elements into the existing practices and intervals to the extent practical.

1.2 Scope

This Prioritized Service Restoration and Mitigation Plan has been developed in accordance with 49 CFR §§236.1015(d)(20) and 236.1033(f).

- §236.1015(d)(20) –The documents and information required under §§236.1007 and 236.1033.
- §236.1033(f) – Each railroad, or its vendor or supplier, shall have a prioritized service restoration and mitigation plan for scheduled and unscheduled interruptions of service. This plan shall be included in the PTCDP or PTCSP as required by §§236.1013 or 236.1015, as applicable, and made available to FRA upon request, without undue delay, for restoration of communication services that support PTC system services.

In paragraph (f), FRA requires that each railroad implement a service restoration and mitigation plan to address restoral of communications services in the event of their loss or disruption and to make this plan available to FRA. Loss of communications services reduces or eliminates the effectiveness of a PTC system and FRA requires that these critical safety systems, once implemented, are restored to operation as soon as practical.

This document provides an overview of the elements for service restoration of the four main ACSES subsystems and their interfaces to each other and to existing LIRR signaling, communications, and onboard systems:

1. Onboard
2. Wayside including transponders
3. Communications
4. Office (including RWPS)

The scope of this document does not address “planned” maintenance related to post-installation periodic maintenance, troubleshooting, and system modification to reflect changes in the LIRR infrastructure of the ACSES system components. This is addressed in the LIRR Operating & Maintenance Manual [ref # 15].

1.3 Document Overview

The following table provides the structure of this document:

Section	Description
1	Introduction
2	PTC System Overview
3	Service Recovery Concepts
4	Testing, Validating and Communicating
Appendix A	Acronyms and Definitions

Table 1 : Document Overview

1.4 Reference Documents

Reference Number	Document Name	Identification Number
1.	Configuration Management Plan	CDRL 2-13, 2-15, 2-17
2.	Maintenance Plan	CDRL 2-110
3.	Maintenance Manuals	CDRL 2-36
4.	Maintainability Demonstration Test Plan (MDTP)	CDRL 2-143
5.	SDMF Design Document	CDRL 2-30
6.	Maintenance Database	CDRL 2-112
7.	Office Subsystem Description Document	CDRL 6-001 / 3035843
8.	Communications Subsystem Description Document	CDRL 7-001 / 3035865
9.	Onboard Subsystem Description Document	CDRL 5-001 / 3035902
10.	RWPS Subsystem Description Document	CDRL 2-201 / 3035851
11.	Railroad Operating Procedures	
12.	ACSES II Maintenance Plan	CDRL 2-110
13.	ACSES II Training Plan	
14.	FRACAS Process Plan	PDM # 3049002
15.	LIRR Operating & Maintenance Manual	
16.	LIRR Recovery Plan	
17.	LIRR Master Test Plan	CDRL 2-047
18.	Maintainability Demonstration Test Plan	CDRL 2-143

Table 2 : Reference Documents

2 PTC System Overview

2.1 Overall System Architecture

A high level schematic block diagram of the ACSES System is depicted in Figure 1 below.

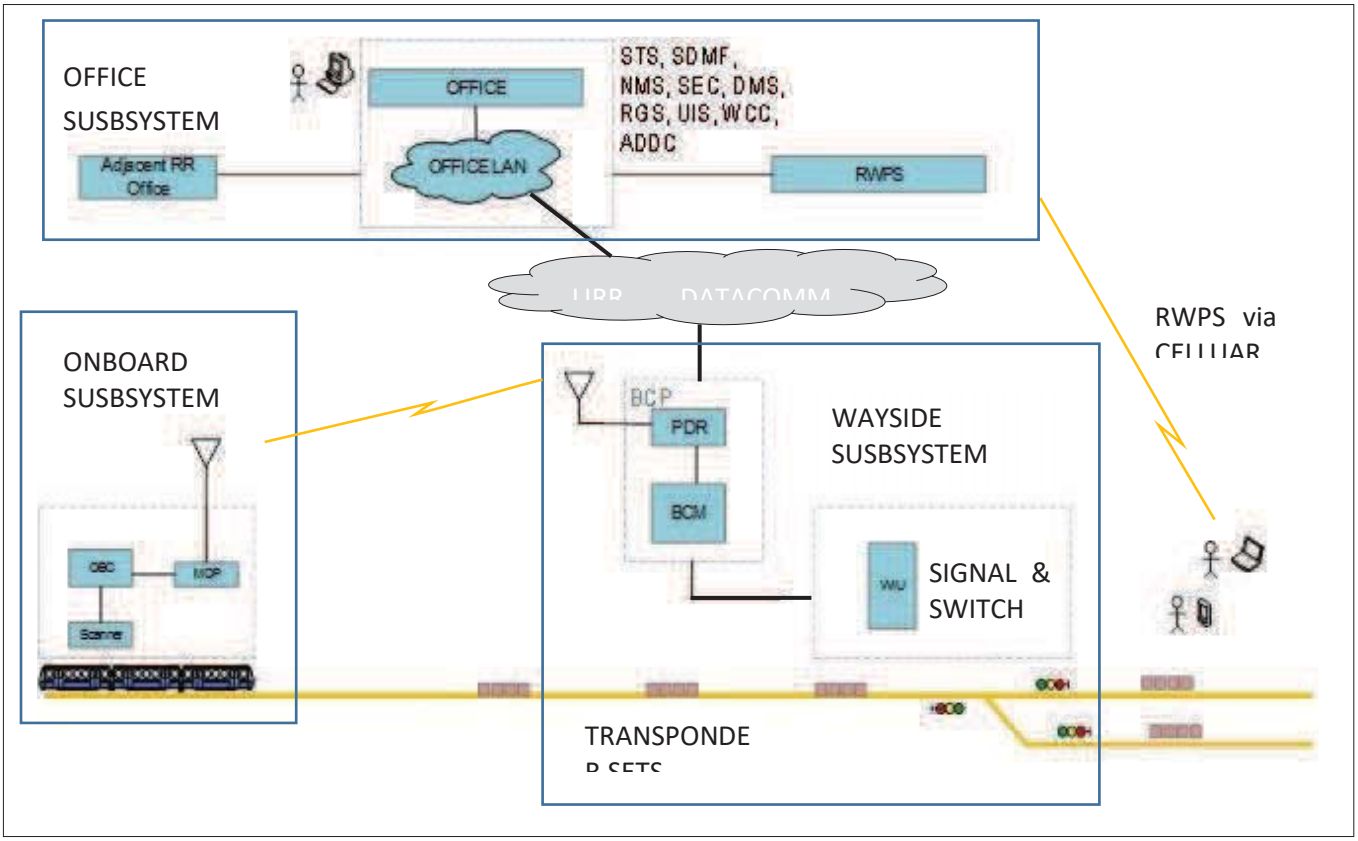


Figure 1: PTC ACSES II System Architecture

The LIRR ACSES II System is made up of the following subsystems and main components.

Onboard Subsystem: Includes ACSES II Onboard Computer, Aspect Display Unit (ADU), CTV and Transponder Scanner, ATC Interfaces (AIU), Mobile Communications Manager (MCM).

Wayside/Signals Subsystem: Includes Wayside Interface Units (WIUs) and WIU connectivity to ACSES networks, and Transponders.

Communications Subsystem: Includes networks and network connectivity, Base Communications Packages, PTC Data Radios

Office Subsystem: Includes Redundant Network, Safety TSR Server (STS), Software and Data Maintenance Facility (SDMF), Network Monitoring System (NMS), Active Directory Domain Controller (ADDC), Security Server, Data and Maintenance System (DMS), Railroad Gateway Server (RGS), User Interface System (UIS), and Wayside Communication Controller (WCC).

RWPS Subsystem: Includes RWPS Server, RWPS Workstations, Truck Mounted EIC Terminals, Handheld EIC Devices, Redundant Network, Network Monitoring System, Active Directory Domain Controller, Security Server, Data and Maintenance System.

2.2 Design Mitigation Principles

2.2.1 *Office Systems*

a. Redundant Architecture

- There is a backup location (BCC) for the complete Office System replicating all PTC functionalities.
- All equipment (except SEC server) including STS servers, RWPS Servers, DMS servers, and NMS Servers are redundant within each control center/backup Control Center and perform switchover from standby to active automatically when failure detected on the active components. This configuration provides state replication and fast recovery in case of a single failure of one node of the redundant pair.
- For the STS/UIS/DMS/NMS equipment, the two redundant servers within a control center are in a hot-standby configuration with one in Active and another in Standby mode.

b. A complete PTC Office system recovery at the backup location is available within 2 Hours.

2.2.2 *Communications*

From a general point of view, all single points of failure of the ACSES networks are eliminated through hardware redundancy achieved at every level possible from :

- Power Redundancy
- Media/Link Redundancy (HSRP)
- 3. Device/hardware Redundancy
- Network Redundancy Protocols (STP/OSPF)
- Application/Server Redundancy

a. Communication within/between Control Centers is based on :

- Redundant networks set up between Control Center/Backup Center, and between LIRR and Amtrak Control Centers
- Routing functions in the Office environment is serviced by dual redundant switches.

b. Communication between the Office locations and the Wayside locations :

Communication between the Office and wayside equipment is achieved via the Ground Based Network (GBN). The GBN consists of two parts :

- Railroad Fiber Backbone that provides the physical medium for the communication between the Office and Wayside locations. The SONET/ATM fiber network consists of multiple redundant rings of fiber optic cable and provides redundant, fault tolerant connections between two physical places. Therefore for connections between the Office and the Wayside, multiple point to point links are available.
- Redundant physical connections from each wayside location to the wayside network, from which four logical point to point links are established between the Control Centers and each wayside location, two from each control center. This provides redundancy for the physical

connections. If a physical connection fails a logical connection still exists to both control centers via the other remaining physical connection.

2.2.3 *Transponders*

a. Transponders are passive devices. They require no local energy source, functioning on energy transmitted from the passing trains. They are, therefore, not susceptible to local wayside power failures.
b. The ACSES II PTC system functions in a fail-safe manner such that missed transponder data will not result in an unsafe condition, enforcing the lowest speed restriction until a "good" transponder set can be read. Normal system operation resumes once the next "good" transponder set is read.

2.2.4 *Onboard Systems*

a. If the ACSES II apparatus fails en route, Train Engineers are authorized to cut-out the onboard ACSES II apparatus. Train Engineers are required to notify the Train Dispatcher of the PTC failure as soon as possible without delay to the train. In such circumstances, a train will proceed as follows:
    a. Non-Cab-Signal Territory with Intermediate ABS Block Signals – Proceed not exceeding Medium Speed (30 MPH) in accordance with signal-system indications until report is made to the Train Dispatcher. Then proceed not exceeding Medium Speed (30 MPH) in accordance with signal-system indications until an absolute block is established in advance of the train. After an absolute block is established, the train will be authorized by the Train Dispatcher to proceed in accordance with signal-system indications at not exceeding 59MPH passenger and 45 MPH freight.
    b. Non-Cab-Signal Territory with CMB Signaling – Not exceeding Medium Speed (30 MPH) in accordance with signal-system indications until report is made to the Train Dispatcher. Then, since the CMB signaling inherently provides an absolute block in advance of the train, train may proceed in accordance with signal-system indications not exceeding 59 MPH passenger and 45 MPH freight.
b. Tenant trains will follow similar operating rules in identical situations