1 June 2011

Ms. Jo Strang
Associate Administrator for
Railroad Safety / Chief Safety Officer
Federal Railroad Administration
1200 New Jersey Avenue, S.E.
Washington, DC 20003

RE: Positive Train Control Development Plan
Dockets: FRA- 2010-0061, FRA-2010-0060, and FRA-2010-0028

Dear Ms. Strang:

Enclosed please find the Interoperable Electronic Train Management System ("I-ETMS") PTC Development Plan ("PTCDP") version 2.0, prepared by Wabtec Railway Electronics ("WRE"), Union Pacific Railroad ("UP"), Norfolk Southern Railway ("NS"), and CSX Transportation, Inc. ("CSXT"). This submittal supersedes the previous version of the plan (*Vital Electronic Train Management System Positive Train Control Development Plan*, version 1.0, 24 March 2010). This PTCDP is being jointly submitted for FRA Type Approval as set forth under 49 CFR Part 236, Subpart I §236.1009(b) and includes documentation required by §236.1013.

The plan describes development of I-ETMS, an interoperable PTC system developed in compliance with requirements and standards defined through the Interoperable Train Control ("ITC") industry effort. This submittal includes material revisions to the previous version of the plan specifically to address comments provided by FRA to date, both in written form and during subsequent mutual discussions including those in connection with the settlement agreement between AAR and FRA regarding the PTC Final Rule.

Please note that the change in document title reflects a change in the trade name of the primary commercial product involved, I-ETMS®. I-ETMS was previously referred to as the Vital Electronic Train Management System (V-ETMS®). The product name change does not imply any departure from the nature of the system as a vital overlay, or any change to the underlying principles of functionality and safety utilized in design or development.

As noted in prior correspondence, receipt of Type Approval remains in the critical path of PTC implementation for all railroads planning to implement I-ETMS. UP, NS, and CSXT, on behalf of themselves and all roads planning to implement I-ETMS, request FRA to prioritize review and disposition of the revised PTCDP.

The primary contacts during review of this PTCDP submission are as follows:

UP:

Gregory M. Richardson
General Director – Train Control Systems
1400 Douglas Street, MS 0480
Omaha, NE 68179
Email: gmricha1@up.com Phone: 402-544-1968

NS:

Lisa Wilson
Manager ATC Regulatory Compliance and Training
1200 Peachtree St., N.E.- Box 123
Atlanta, GA 30309
Email: Lisa.Wilson@nscorp.com Phone: 404-962-5931

CSXT:

Denise Lyle
Director Advanced Engineering
500 Water Street, SC J340
Jacksonville, FL 32202
Email: Denise_Lyle@csx.com Phone: 904-359-4825

Please let the undersigned know if you have any questions or require additional information.

Respectfully submitted,

Union Pacific Railroad

By 

Jeff D. Young
AVP – Transportation Systems

Norfolk Southern Railway

By 

Lisa C. Wilson
Manager – ATC Regulatory Compliance and Training

CSX Transportation, Inc.

By 

Denise E. Lyle
Director – Advanced Engineering

Interoperable Electronic Train Management System (I-ETMS®) Positive Train Control Development Plan (PTCDP)

1 June 2011

Version 2.0

Submitted in fulfillment of 49 CFR 236, Subpart I, §236.1013

REVISION HISTORY

Date	Revision	Description	Author
03/24/2010	1.0	Initial FRA submission	WRE/UP/NS/ CSXT
06/01/2011	2.0	Re-submission addressing FRA comments	WRE/UP/NS/ CSXT

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Overview

This PTC Development Plan (PTCDP) is submitted in fulfillment of 49 CFR 236, Subpart I, §236.1013. The system described in this document is the Wabtec Railway Electronics (WRE) Interoperable Electronic Train Management System (I-ETMS®), a vital overlay system as defined in 49 CFR 236, Subpart I, §236.1015(e)(2). This system is based on the Electronic Train Management System (ETMS®) developed by WRE which has been approved by FRA under 49 CFR 236, Subpart H for use in revenue service on BNSF Railway (FRA-2006-23687-21), subject to certain conditions.

I-ETMS was previously referred to as Vital Electronic Train Management System (V-ETMS®). The modified name more accurately reflects the system that is being designed and developed with the support of CSX Transportation, Inc. (CSXT), Norfolk Southern Railway (NS), and Union Pacific Railroad (UPRR), as well as other Class 1 railroads through the Interoperable Train Control (ITC) industry effort.

The I-ETMS system is designed to support different railroads and their individual methods of operations and is intended to be implementable across a broad spectrum of railroads without modification. This design approach supports interoperability across railroads as I-ETMS equipped locomotives apply consistent warning and enforcement rules regardless of trackage ownership.

The I-ETMS system will be tested in a coordinated manner to ensure safe operation as well as interoperability, and provide the information necessary to submit a PTC Safety Plan (PTCSP) as defined in 49 CFR 236, Subpart I, §236.1015. Upon successful review of the PTCSP and issuance of the associated PTC System Certification, the I-ETMS system will be deployed as an interoperable PTC system, as discussed throughout this document, based on this PTCDP.

1.2 Document Overview

This PTCDP document is organized generally in accordance with Institute of Electrical and Electronics Engineers (IEEE) standard 1362-1998. The contents of the document are provided to specifically address required items in 49 CFR 236, Subpart I, §236.1013.

- Section 1 describes the scope of this document.
- Section 2 lists applicable documents that are referenced in this PTCDP.
- Sections 3-12 correspond to requirements from 49 CFR 236, Subpart I, §236.1013 and are cross-referenced between the applicable Subpart I section and the PTCDP section in Table 1 below.

Table 1 – §236 Subpart I Cross-Reference

§236 Subpart I Reference	§236 Subpart I Text	PTCDP Section/Chapter Reference
§236.1013 (a)(1)	a complete description of the PTC system, including a list of all PTC system components and their physical relationships in the subsystem or system;	3
§236.1013 (a)(2) §236.1007	a description of the railroad operation or categories of operations on which the PTC system is designed to be used, including train movement density (passenger, freight), operating speeds (including a thorough explanation of intended compliance with §236.1007), track characteristics, and railroad operating rules;	4
§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;	5
§236.1013 (a)(4)	a document describing the manner in which the PTC architecture satisfies safety requirements;	6
§236.1013 (a)(5)	a preliminary human factors analysis, including a complete description of all human-machine interfaces and the impact of interoperability requirements on same;	7
§236.1013 (a)(6)	an analysis of the applicability to the PTC system of the requirements of subparts A-G of this part that may no longer apply or are satisfied by the PTC system using an alternative method, and complete explanation of the manner in which those requirements are otherwise fulfilled;	8
§236.1013 (a)(7)	a prioritized service restoration and mitigation plan and a description of necessary security measures for the system;	9

§236 Subpart I Reference	§236 Subpart I Text	PTCDP Section/Chapter Reference
§236.1013 (a)(8)	a description of target safety levels (e.g., MTTHE for major subsystems as defined in subpart H), including requirements for system availability and a description of all backup methods of operation and any critical assumptions associated with the target levels;	10
§236.1013 (a)(9) §236.1013 (a)(11)	A complete description of how the PTC system will enforce authorities and signal indications. A complete description of how the PTC system will appropriately and timely enforce all integrated hazard detectors in accordance with § 236.1005(c)(3), if applicable.	11
§236.1013 (a)(10)	A description of the deviation which may be proposed under § 236.1029(c), if applicable.	12

1.3 Acronyms and Definitions

This section includes definitions of all terms, abbreviations, and acronyms required to properly interpret the Development Plan.

The following abbreviations and acronyms are used in this document.

Table 2 – Acronyms

Acronym	Definition
AAR	Association of American Railroads
ABS	Automatic Block Signal
ACS	Automatic Cab Signal
ATC	Automatic Train Control
BNSF	Burlington Northern Santa Fe
CDU	Computer Display Unit
CDU-I	Computer Display Unit – Interactive
CDU-NI	Computer Display Unit – Non-Interactive
CFR	Code of Federal Regulation
COBIT	Control Objectives for Information and related Technology
COT	Current of Traffic
CPU	Central Processing Unit

Acronym	Definition
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CSXT	CSX Transportation, Inc.
CTC	Centralized Traffic Control
DIO	Discrete Input Module
EBI	I-ETMS / ETMS Brake Interface
EIC	Employee In Charge
ETMS	Electronic Train Management System
FMEA	Failure Modes and Effects Analysis
FRA	Federal Railroad Administration
FTA	Fault Tree Analysis
GPS	Global Positioning System
HDLC	High-level Data Link Control
HMAC	Hash Message Authentication Code
I-ETMS	Interoperable Electronic Train Management System
ICD	Interface Control Document
ICE	Integrated Cab Electronics®
IEEE	Institute of Electrical and Electronics Engineers
IFC	Integrated Function Computer®
IOC	Input Output Concentrator
ITC	Interoperable Train Control
ITCM	Interoperable Train Control Messaging
LCD	Liquid Crystal Display
LRU	Line Replaceable Unit
LSI	Locomotive Systems Integration
LSL	Locomotive Speed Limiter
NS	Norfolk Southern Railway
NYAB	New York Air Brake
PHA	Preliminary Hazard Assessment
PTC	Positive Train Control
PTCDP	Positive Train Control Development Plan
PTCIP	Positive Train Control Implementation Plan
PTCSP	Positive Train Control Safety Plan
RF	Radio Frequency
RSM	Router / Switch Module
SMC	Spectrum Management Committee
TC	Traffic Control
TDMA	Time Division Multiple Access
TMC	Train Management Computer
TWC	Track Warrant Control
UPRR	Union Pacific Railroad
V-ETMS	Vital Electronic Train Management System

Acronym	Definition
WAAS	Wide Area Augmentation System
WIU	Wayside Interface Unit
WRE	Wabtec Railway Electronics

The following is a list of definitions of terms that are used in this document.

Table 3 – Definitions of Terms

Term	Definition
CAFTA®	Computer program for developing reliability models of large complex systems, using fault tree and event tree methodology.
Interoperability	The ability of a controlling locomotive to communicate with and respond to the PTC railroad's positive train control system, including uninterrupted movements over property boundaries.
PTC	Positive train control as further described in §236.1005.
PTCIP	PTC Implementation Plan as further described in §236.1011.
PTCDP	PTC Development Plan as further described in §236.1013.
PTCSP	PTC Safety Plan as further described in §236.1015
PTC System Certification	Certification as required under 49 U.S.C. §20157 and further described in §§236.1009 and 236.1015.
Segment of track	Any part of the railroad where a train operates.
Tenant railroad	A railroad, other than a host railroad, operating on track upon which a PTC system is required.
Track segment	Segment of track

2 Applicable Documents

This section contains a complete list of the documents and other sources referenced in this document.

Note: For dated references, only the edition cited applies. For undated references, the latest edition of the reference document applies, including amendments.

[1] 49 CFR 234.211, “Grade Crossing Signal System Safety”, Subpart D, “Maintenance, Inspection, and Testing Maintenance Standards”, “Security of Warning System Apparatus” – 5 December 2005

[2] 49 CFR 229.135, “Railroad Locomotive Safety Standards”, “Event Recorders” – 15 January 2010

[3] 49 CFR 236 Subpart I, “Positive Train Control Systems; Final Rule”, Docket No. FRA-2008-0132, 15 January 2010

[4] MIL-STD-882C, “System Safety Program Requirements” with Notice, 1 DoD, 13 March 1996

[5] IEEE STD 1362-1998, “IEEE Guide for Information Technology—System Definition—Concept of Operations (ConOps) Document -Description”, IEEE Computer Society/Software & Systems Engineering Standards Committee, 22 December 1998

[6] IEEE STD 1483-2000, “IEEE Standard for Verification of Vital Function in Processor Based Systems Used in Rail Transit Control”, IEEE Vehicular Technology Society, 30 March 2000

[7] FRA-2006-23687-0017, “BNSF Railway – Product Safety Plan” Version 2.1; 12 October 2006

[8] AREMA 2009 Communications and Signal Manual of Recommended Practices, Part 17

[9] PTC Back Office Segment - Energy Management Interface Control Document (ICD), version 1.0, 2 December 2010.

[10] AAR S-9202, “ITC Wayside Interface Unit Requirements”

[11] AAR S-9355, “Class C Messaging Specification”

[12] AAR S-9356, “Class D Messaging Specification”

[13] AAR S-9354, “Edge Messaging Protocol Specification”

[14] AAR S-9352A, “ITC Locomotive-Office ICD”

[15] AAR S-9352B, “ITC Wayside-Locomotive ICD”

[16] AAR S-9501, “PTC Data Management Architecture”

[17] AAR S-9350, “ITC Message (ITCM) System Specification”

[18] AAR S-61213, “Railroad Use of 802.11”

[19] AAR S-9054, “I-ETMS Human Machine Interface (HMI) Standards Guide”

Note: The AAR referenced standards, documents 10-17, are publicly available through the AAR website. It is recommended that any organization that requires access to these standards subscribe to the AAR circular letters. This does not require either an AAR membership or an AAR associate membership, but a discount is provided with membership. The URL for the circular letters is http://aarcirculars.aar.org.

3 I-ETMS System Description - §236.1013 (a)(1)

This section provides a complete description of the I-ETMS system, including a list of all PTC system components and their physical relationships in the subsystem or system as required by 49 CFR 236 Subpart I §236.1013 (a)(1).

3.1 I-ETMS System Overview

I-ETMS consists of four primary subsystem segments: the Office Segment, the Wayside Segment, the Locomotive Segment, and a Communications Segment that connects the other three segments as depicted in Figure 1. Each segment is discussed in detail in Sections 3.2 – 3.5 respectively.

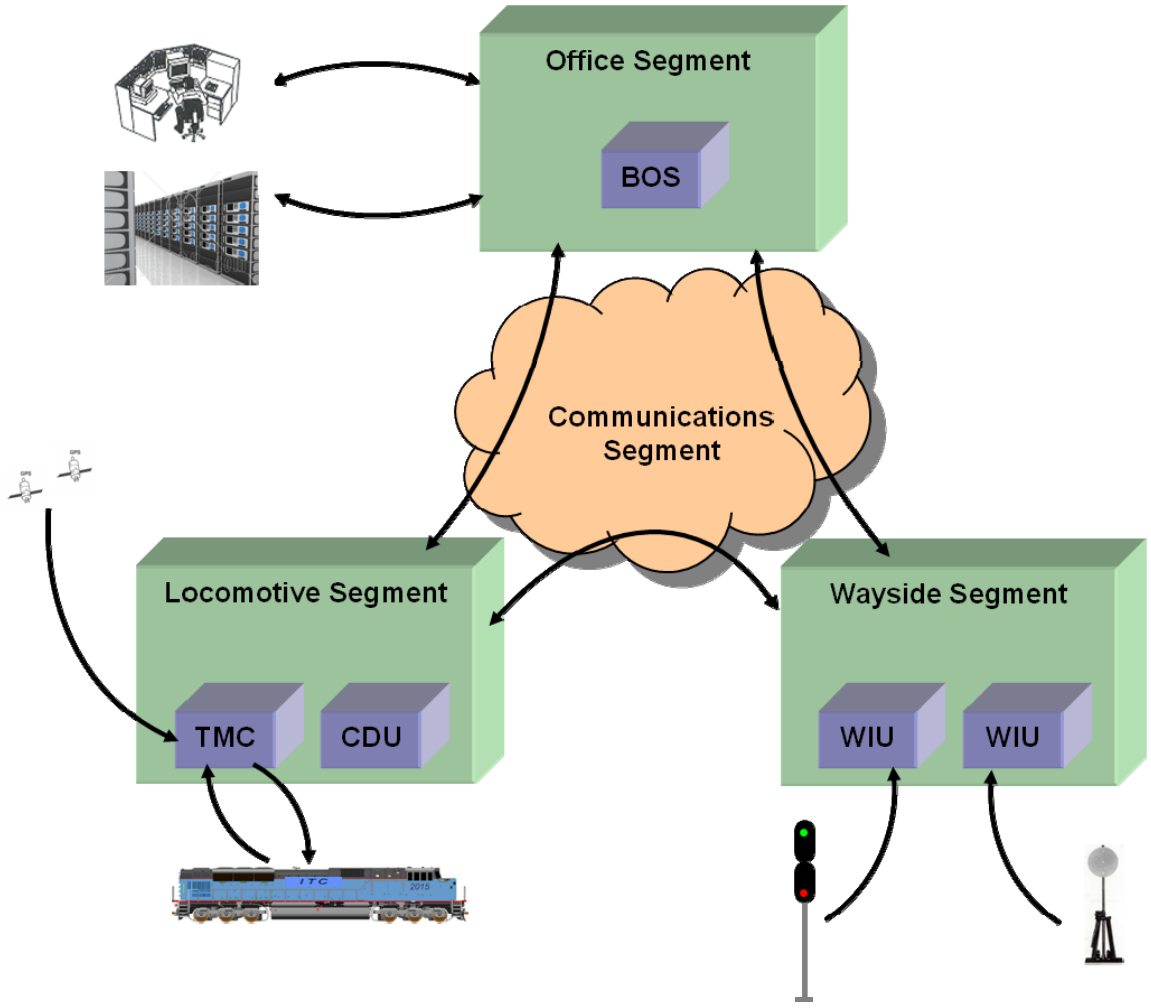

Figure 1 – I-ETMS System Segments

The locomotive-centric system operates primarily through the assimilation and processing of data by the Locomotive Segment. The Locomotive Segment continuously accepts, validates, and processes operating data obtained from onboard peripheral devices, from the Office Segment of one or more railroads, and from local Wayside Segments. All communication is facilitated by the Communications Segment using Class D [12] and EMP protocols [13], which are defined in AAR specifications, and are in accordance with the ITC Wayside-Locomotive ICD [15]. Other data, such as locomotive control settings and GPS positioning data, are obtained from onboard peripheral devices connected to the TMC. This locomotive-centric approach provides the Locomotive Segment with the independent capability to detect data errors, data conflicts, and data latency, facilitating its safe operation.

The I-ETMS track database is a component of the system configuration. This database contains data elements (identified in Section 5.5.5), some of which are safety-critical, that provide information required to support the I-ETMS navigation function and enforce authorized train movement. The database originates from railroad track data obtained from multiple sources external to I-ETMS. The railroad track data must be formatted to interface with and be utilized by the Locomotive Segment TMC. An ITC track data standard has been developed for that purpose, [16] AAR S-9501, "PTC Data Management Architecture." The Office Segment is responsible for distributing the track database to the Locomotive Segment. Distribution of the track data typically occurs prior to I-ETMS initialization, i.e. the track data should be staged onboard as early as possible. During initialization a check occurs to ensure the correct version is onboard. The Locomotive Segment utilizes the track database in enforcement of the PTC safety requirements for authority limits, speed limits, switch positions, and signal aspects. The data elements critical to operation are validated with the TMC and Wayside Segment through lab and field testing and a formal track validation plan. Further discussion of the track database is provided in the Concept of Operations in Section 5.

3.2 I-ETMS Office Segment

The Office Segment is comprised of one or more Back Office Server(s) (BOS). It interfaces with other railroad back office systems or applications, the railroad dispatch system and the Locomotive and Communications segments. The Office Segment serves as a conduit for information conveyed to the Locomotive Segment where the system's vitality resides.

3.2.1 Office Segment Functionality

The Office Segment accepts mandatory directives and other information generated by the railroad's dispatching system and other railroad information systems, and provides it to the Locomotive Segment. The interface between the Office Segment and railroad dispatching and railroad information systems may be proprietary to a particular railroad. However, the Office Segment normalizes the operating data provided by a particular railroad's dispatching and information systems for exchange over an interoperable interface with the Locomotive Segment.

The Office Segment may also provide operating data received from the Locomotive Segment, such as position reports, system state changes, and fault/failure reports back to the railroad dispatching and information systems. This information may be forwarded to non-I-ETMS, external railroad applications through the railroad network interface using protocols and message formats specified by each operating railroad. However, the Office Segment performs no tracking of trains or wayside status. "Tracking of trains" typically infers that the tracking entity is performing some sort of spatial or proximal functions. The Office Segment simply accepts position reports as a pass through of data from equipped locomotives and forwards them to other railroad back office systems for the railroad's use as it sees fit; the use of train location data is not a "train control" function. The Office Segment does not perform any tracking functions or calculations on the data in those reports nor does it utilize the position reports in any manner to perform any function. GPS information is used in the Locomotive Segment to calculate the train's position and compute proximity to authority and speed limits.

The typical Office Segment configuration is depicted in Figure 2.

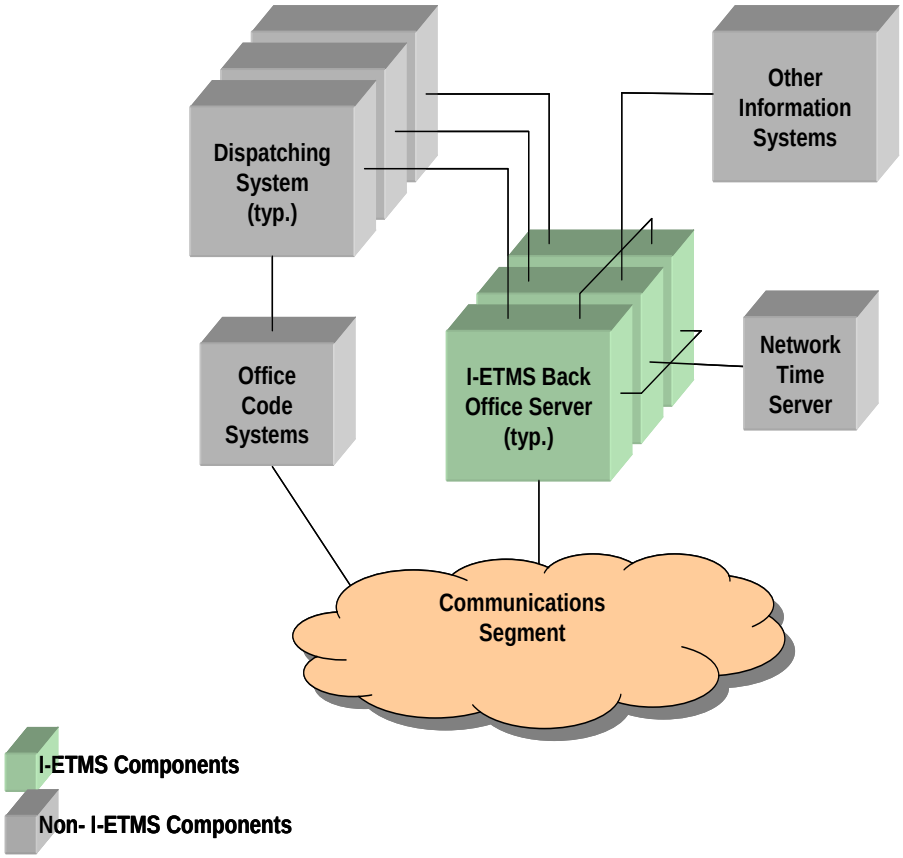

Figure 2 – I-ETMS Office Segment Configuration

The Office Segment will provide secure configuration management for I-ETMS equipped locomotives. Configurable items controlled by the Office Segment will include, but are not limited to, onboard software versions, onboard configuration and startup files, security certificates, and track database versions. The management of the configurable items may be performed globally (e.g. default configuration for all locomotives), by specific locomotive groups, or at the individual locomotive level. The Office Segment also retrieves detailed logs from the Locomotive Segment. The retrieval rate of detailed logs from the Locomotive Segment is a configurable value. When the configurable time has passed and acceptable quality and availability of communications is present, Office Segment retrieval of Locomotive Segment logs occurs. A subset of data from the Locomotive Segment logging is transmitted to the PTC event recorder.

In the current I-ETMS design, no safety-critical functions have been allocated solely to the BOS. The Office Segment data delivery function is non-vital in the overall architecture as the vital Locomotive Segment protects itself from potential hazards caused by data delivery failures. The Office Segment provides a non-vital check of the reasonableness and integrity of data received from external sources and provides delivery of data to the Locomotive Segment; however, the Locomotive Segment provides a vital range check.

The Office Segment holds all movement authorities for trains operating on a subdivision. When a new movement authority is received, the Office Segment performs a check to ensure that no unsafe overlap of limits exist after the transformation of those limits from dispatching system format into I-ETMS format. This transformation check is illustrated below in Figure 3.

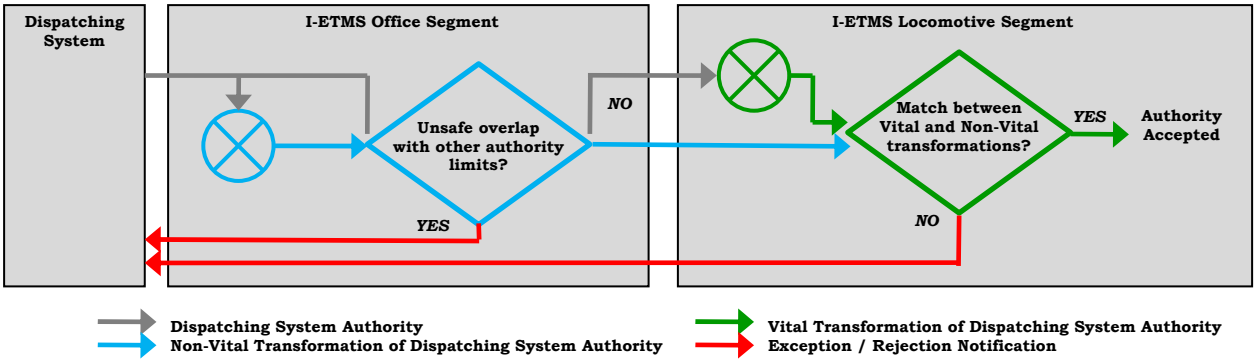

Figure 3 – I-ETMS Transformation Check

If the transformation is successful, the Office Segment will calculate a track limit Cyclic Redundancy Check (CRC) over the transformed movement authority limits, which will be sent to the corresponding Locomotive Segment, along with the movement authority limits. The vital Locomotive Segment also transforms the received movement authority limits into I-ETMS format and calculates a CRC. Subsequently, the Locomotive Segment compares the CRC received from the Office Segment to the one calculated onboard. If the CRC's match, no unsafe overlaps in the movement authority has occurred due to the PTC system. If the CRC's do not match, the Locomotive Segment will reject the movement authority and a negative acknowledgement is sent back to the Office Segment indicating the rejection.

3.2.2 Office Segment Platform

The Office Segment is designed to operate in a distributed environment with scalability through hardware and software to support growth throughout the product life cycle. The Office Segment architecture is scalable and may be deployed by a railroad across multiple Office Segment servers to distribute control of its own I-ETMS tracks to increase performance, availability, and reliability. Additional performance requirements for processing and storage capacity have been established as well.

The Office Segment utilizes commercial off-the-shelf operating systems and relational database management systems. In order to achieve high-availability, multiple hardware platforms are used to distribute load and provide fail-over.

Hardware selection of the Office Segment is dependent upon system performance requirements and individual railroad datacenter design factors. "Proof of concept" tests conducted to date have established that enterprise-class mid-tier servers may be capable of meeting Office Segment performance requirements. Performance tests are to be executed in various phases of testing.

3.2.3 Office Segment Interfaces to Other Back Office Systems

I-ETMS is designed and developed to interface with dispatching systems with capabilities prevalent on North American heavy-rail freight and passenger railroads. The Back Office Server (BOS) acts as the interface between the implementing railroad's proprietary dispatching system and the interoperable Locomotive Segment. The interface between the BOS and the implementing railroad's dispatching and other MIS systems is itself proprietary, and it is incumbent upon the implementing railroad to design and specify an interface which supports I-ETMS operation. The interface must include the ability to convey mandatory directives and train sheet data from the dispatching system to the BOS utilizing protocols that support fail-safe operation.

The Office Segment interfaces to several other railroad back office systems for a variety of operational data. These interfaces are railroad-specific and do not affect interoperability. The Office Segment is supplied with operational data such as train IDs, summary consist, rail car consist updates, authorities, temporary speed restrictions, work zones, advisory or cautionary notices, weather and other critical alert information in accordance with protocols and message formats defined by each implementing railroad. These pieces of data may be received by the Office Server directly or indirectly from dispatching systems and one or more railroad back office systems depending on the individual implementing railroad's capabilities and architecture.

3.3 Wayside Segment

The Wayside Segment monitors and reports switch position, signal indications, or status of other monitored wayside devices directly to the Locomotive Segment and Office Segment using one or more radio networks. Section 3.5 provides Communication Segment information. The Wayside Segment consists of traditional signaling equipment to which Wayside Interface Unit (WIU) function has been added. This signaling equipment is designed to be compliant with 49 CFR 236 Subparts A through G and have been implemented such that they incorporate closed loop principles consistent with Subpart A 236.5. As a Vital Overlay system, I-ETMS is intended to function as designed by utilizing the existing signal system infrastructure with the WIU acting as a data gathering device. The various WIU products are expected to be approved for use prior to any deployment with I-ETMS by means of Interface and Standards adherence verification as well as WIU vendor provided safety documentation which supports the overall I-ETMS safety analysis. The WIU vendor provided safety documentation could be created in compliance with 49 CFR 236 Subpart H or as an existing 49 CFR 236 A through G compliant device. It is required that whatever process the WIU vendor utilizes to document the product safety analysis, the resulting WIU will interface in a safe manner with I-ETMS.

The WIU function is responsible for interfacing the signal equipment to the Communications Segment and may be implemented as additional equipment or a software upgrade to existing equipment. Where Cab Signals are integrated with I-ETMS, the state of the current block will be provided directly to the Locomotive Segment. The Wayside Segment configuration is depicted in Figure 4.

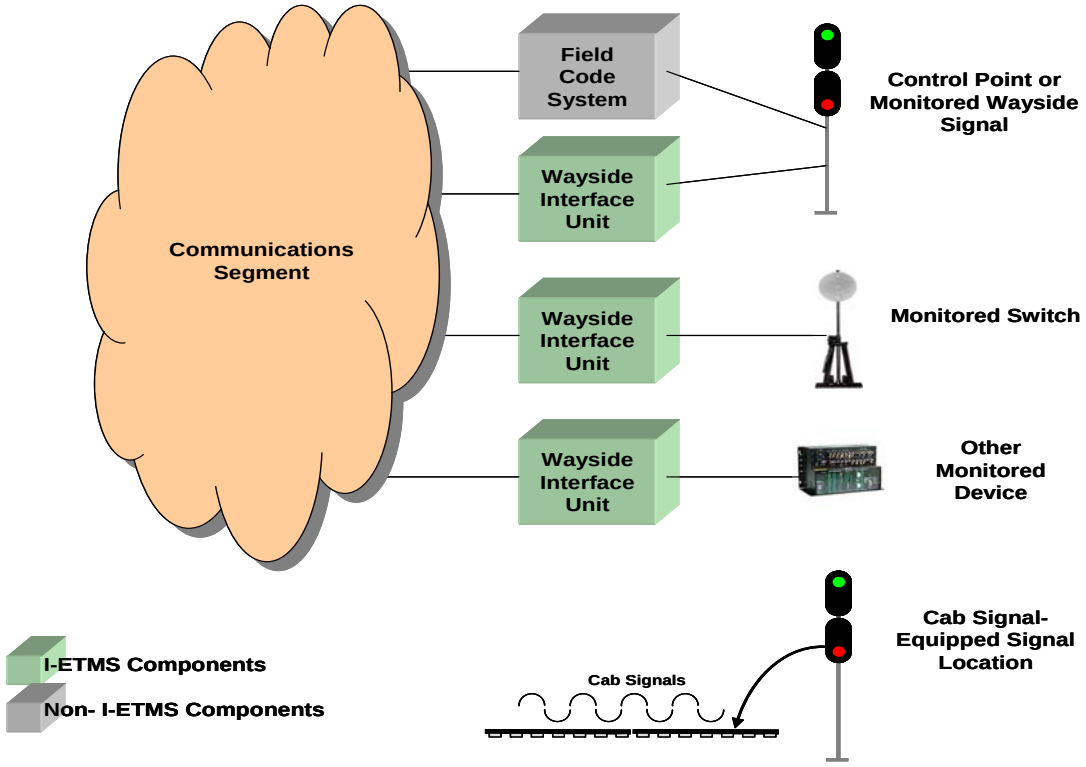

Figure 4 – I-ETMS Wayside Segment Configuration

The Wayside Segment consists of those signaling appliances located in the field whose status impacts I-ETMS operations, along with any WIUs used to monitor and report their status. Such appliances include interlocking controllers, signal controllers, switch circuit controllers, track circuits, track/route hazard detectors, or other field devices. Wayside Segment components may exist in either signaled or non-signaled territory. The Locomotive Segment utilizes the status of wayside devices in the route of a train during calculation of its safe operating profile. Wayside device status may be provided through three different configurations:

- **WIU-connected** – In this configuration, a WIU is directly connected to a wayside device that publishes its status to the Locomotive and/or Office Segments via the Communications Segment. The WIU publishes device status at periodic intervals in order to satisfy the data timing and latency tolerances of the Locomotive Segment train control application. WIUs may also be configured to continuously publish status, or in order to conserve battery power at the WIU location and/or communications bandwidth, only publish status upon receipt of a "wake-up" from the Locomotive Segment. Typical implementation of WIUs in the Wayside Segment include monitoring of signals and power switches in signaled territory and monitoring of hand-operated switches in non-signaled territory.

- **Office-connected** – In this configuration, the status of a wayside device is published to the railroad office via an existing method and communications path. The wayside device status is in turn forwarded to the Office Segment, which relays it to the Locomotive Segment. However, where such methods of publishing status are non-vital, the Locomotive Segment provides cross-checks with other vital data provided by a Cab Signal system or WIU in order to ensure safety. Additionally, data must move in a fashion sufficient to meet the timing tolerances of the Locomotive Segment train control application. Typical implementation of office-provided wayside status may be in Traffic Control territory where code systems exist and where cab signals are operative.
- **Cab Signals** – In this configuration, the Locomotive Segment obtains wayside device status through monitoring of the onboard cab signal system. Cab signals are monitored through the lamp circuits of the in-cab aspect display unit. Cab signal aspects provide information about the conditions of the current block as well as the track ahead. The cab signal system and aspect display unit remain independent of the PTC system and fully-operational, regardless of whether cab signals are integrated with I-ETMS. The Locomotive Segment also requires the status of wayside devices not indicated through cab signal aspects, such as power switch position, to be provided by WIU- or office-connected wayside devices.

Where other signaling appliances or track hazard detectors are integrated with a signal system, their status is implicitly reflected in the status of signals provided to I-ETMS.

Hazard detectors may or may not be integrated with a signal system. When integrated with a signal system, a hazard detector will cause the attached track or signal control circuit to assume its most restrictive state upon detection of a potential hazard. This state is published by the WIU to the Locomotive Segment via the Communications Segment, effectively causing the Locomotive Segment to act upon the hazard detector state. The status of a hazard detector not integrated with a signal system may be published to the Locomotive Segment by a WIU directly-attached to the detector. If a railroad elects to directly attach a WIU to a detector not otherwise integrated with the signal system, its status will be published to the Locomotive Segment via that WIU.

The industry ITC consortium has developed an open-standard for WIU interfaces and functions. The WIU requirements can be found in AAR standard reference [10]. Several suppliers to date are developing products meeting this standard.

3.3.1 WIU Architecture

Possibilities for the Wayside Segment architecture are illustrated in Figure 5 below. Its architectural components are the monitored wayside devices, switch and signal logic controllers, the WIU, the wayside messaging system and the communications network link. The WIU can share hardware with either the logic controller or the wayside messaging system or each component can be implemented on separate hardware

platforms. The WIU will interface with the logic controller to retrieve the signal aspect and/or switch position and transmit this information via the Communications Segment.

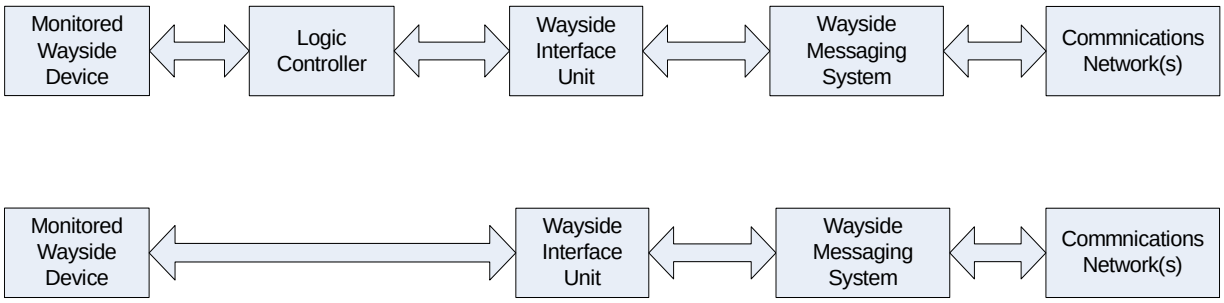

Figure 5 – I-ETMS Wayside Segment Architecture Diagram

3.3.2 WIU Configurations

AAR specifications establish the behavioral and interface requirements for WIUs. The protocol utilized by the WIU attaches information to be validated for authentication, integrity, and latency. WIU technology deployed as part of I-ETMS consists of vital signal-grade components and may be deployed in either of two configurations. In the first configuration, the WIU function is added to the chassis of an existing signaling processor. Hardware and/or software upgrades are deployed, often without requiring disarrangement of the signaling processor, its connected equipment, or pre-existing application software. In the second configuration, a complete WIU hardware and software component is collocated with an existing signaling processor and separately interfaced to the appliances it monitors or controls, such as lamp circuits, switch circuit controllers, or other outputs. In either configuration, the WIU also provides an interface to the Communications Segment, through which it indicates the status of any monitored devices.

3.3.3 Wayside Messaging System

The WIU connects to the communications network via the Wayside Messaging System. Its task is to receive the status message from the WIU and convey it via the interoperable messaging system to the locomotive or other systems that may be interested in the status of the monitored wayside devices. The Wayside Segment implements the interoperable messaging system at the wayside.

The Wayside Messaging System hosts a Class D link with the WIU to receive and transmit messages using the EMP protocol. When the WIU is beaconing, the wayside messaging system receives a status message from the WIU every second. Those status messages are placed into the interoperable messaging system and transmitted by the communications network at configured beacon rate which may be less frequent than the rate at which they are received from the WIU. Messages that are intended for the WIU are received and transmitted using EMP over the Class D link with the WIU.

Communications devices that can be attached to the wayside messaging system include 220MHz radios, cellular modems, satellite receivers and IP routers. The wayside messaging system is responsible for formatting the messages for transport across these networks.

The wayside messaging system may also implement Class C data streams to share data with the WIU. This data stream may be used to convey time synchronization information from the messaging system to the WIU. The WIU will not start transmitting its status after a reset unless its time is synchronized with the messaging system.

3.4 Locomotive Segment

The Locomotive Segment refers to a set of independent onboard hardware, software, and devices that interface with locomotive control equipment (e.g. air brakes, train line) and includes a Train Management Computer (TMC), a Computer Display Unit (CDU), a Locomotive ID module, a GPS receiver, and a brake Cut-Out switch as shown in Figure 6. The Locomotive Segment does not include the Communication Segment components.

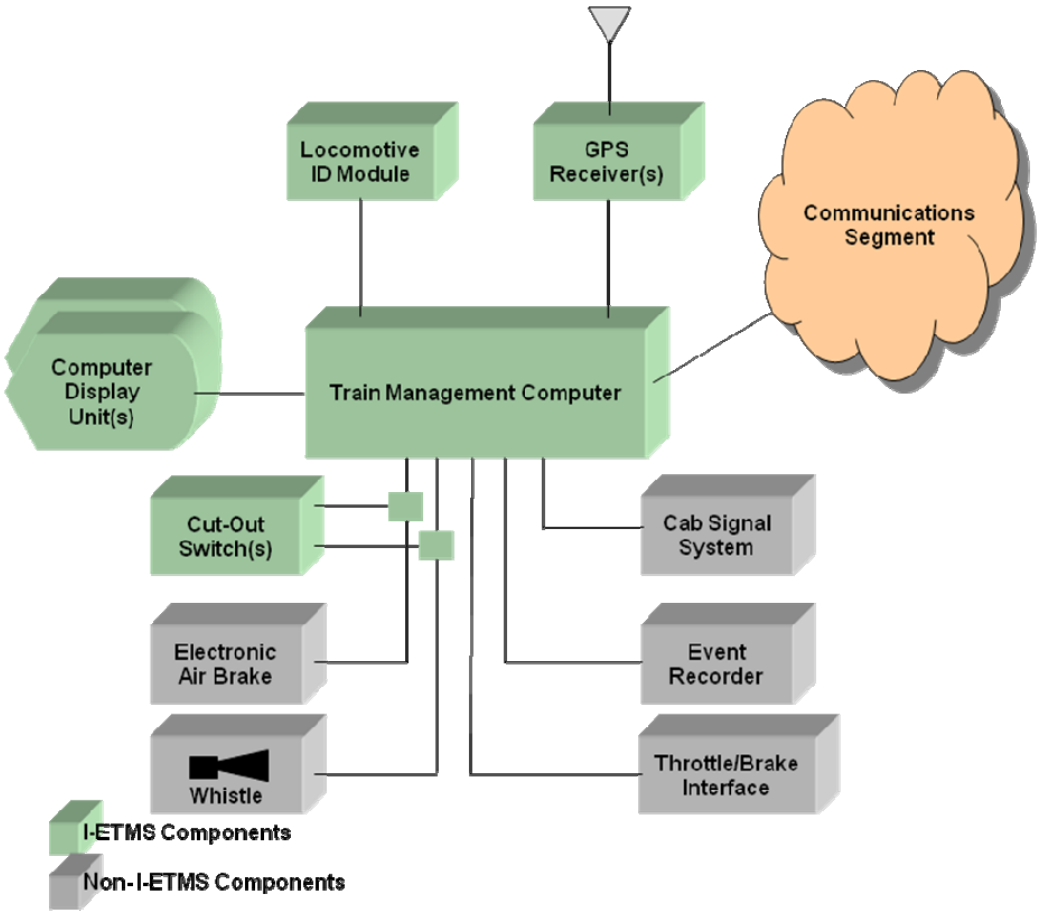

Figure 6 – I-ETMS Locomotive Segment Configuration

A single instance of the Locomotive Segment is installed on each equipped locomotive (or cab car). The Locomotive Segment accepts movement authorities, temporary speed restrictions, other mandatory directives, train consist data, and other information from the Office Segment. Switch position and signal indications may be directly received by the Locomotive Segment via Peer-To-Peer communication with the Wayside Segment. The Locomotive Segment interfaces with other locomotive devices including an event recorder, train line data sensors, the horn circuit, brake systems, cab signal system (if equipped), and the Communication Segment.

To determine the locomotive's on-track location and for navigation, the Locomotive Segment uses a complement of GPS technology and wheel tachometer information, along with an onboard geo-referenced track database. Movement authority information and applicable speed restrictions are accepted from the Office Segment and/or the Wayside Segment which are continuously compared against the train's location to provide real-time compliance with authority and speed limits. The state of the current block will be directly received by the Locomotive Segment where cab signals are in use and integrated with I-ETMS.

Multiple train control processing modules, executing identical application software, are used to perform all train control functions such as determination of current position, calculation of warning and braking distances, management of limits or restrictions conveyed by verbal or electronic mandatory directive or signal indication, management of off-board communications, and communication with the CDU. Graphical displays on the CDU reinforce situational awareness to promote compliance with movement authorities and speed restrictions in a safe manner. Failure to comply with warnings related to authority limits, speed restrictions, or improperly lined switches will result in a penalty brake application to stop the train.

The Locomotive Segment includes diagnostic capabilities to identify and report module-level failures. Failure reports are transmitted to the back office when possible and may be forwarded to the railroad's existing maintenance or monitoring systems to facilitate the issuance of repair or trouble tickets for critical faults and to prevent non-critical faults from degrading further. In the event of a critical failure the Locomotive Segment would have to be manually cut-out to allow locomotive movement until the failure can be repaired.

The Locomotive Segment provides status information and position reports to the Office Segment and acknowledges messages received from the Office Segment.

3.4.1 I-ETMS Train Management Computer

The I-ETMS Train Management Computer (TMC) is a modular hardware unit that includes redundant train control processors, optional business application processors, serial interfaces, discrete interfaces, and the penalty brake interface. Software running on the processor modules is used to perform all train control functions such as determining current position, calculating braking distance, managing restrictions, managing off-board communications, and communicating with the CDU.

The minimum train control configuration requires at least 2 CPU modules, 1 I-ETMS Brake Interface (EBI), 1 Input Output Concentrator (IOC), 1 Discrete Input Module (DIO), and 1 Router / Switch Module (RSM). There is no difference in operation between 2 and 3 train control processor configurations; the 2 processor configuration has less availability than the 3 processor configuration. The Locomotive Segment architecture is show in Figure 7. The specific modules within the I-ETMS system will vary depending upon the specific locomotives deployed. I-ETMS hardware is configurable to accommodate various locomotive types. Each locomotive type will be specified and disclosed in individual PTC Safety Plans (PTCSP). Each locomotive type will be equipped with the appropriate wiring harness and will obtain specific information from a Loco ID embedded in the wiring harness. Details on each hardware module within the TMC are included in the following sections.

3.4.1.1 Chassis

The I-ETMS chassis has been designed to fit either in a Locomotive Systems Integration (LSI) rack, or onto a mounting bracket that may be mounted directly to an available interior bulkhead in the locomotive thus providing maximum flexibility for installing in space-constrained locations.

The chassis integrates each of the I-ETMS modules into a cohesive unit by allowing the internal modules to be configurable to account for a wide variety of locomotives chassis. It is designed to accommodate up to ten (10) modules, which includes the following:

- CPU – Standard Processor Module (up to 3 may be used for train control)
- IOC – Input Output Concentrator
- EBI – I-ETMS Brake Interface
- DIO – Discrete Input Module
- RSM – Router / Switch Module

The base includes card guides and a backplane for interfacing with any of the up to ten (10) supported modules. The matching I/O connector for each module is part of the cable assembly and is installed as needed. For example, if only a CPU, IOC, and Enforcement module are required, there would only be cables to those slots. This allows for flexible growth as new functions and interfaces are added. If more inputs are required than are on a single card, a second card may be installed. External wiring harnesses, designated for the specific locomotive, will be required to interface to the second card.

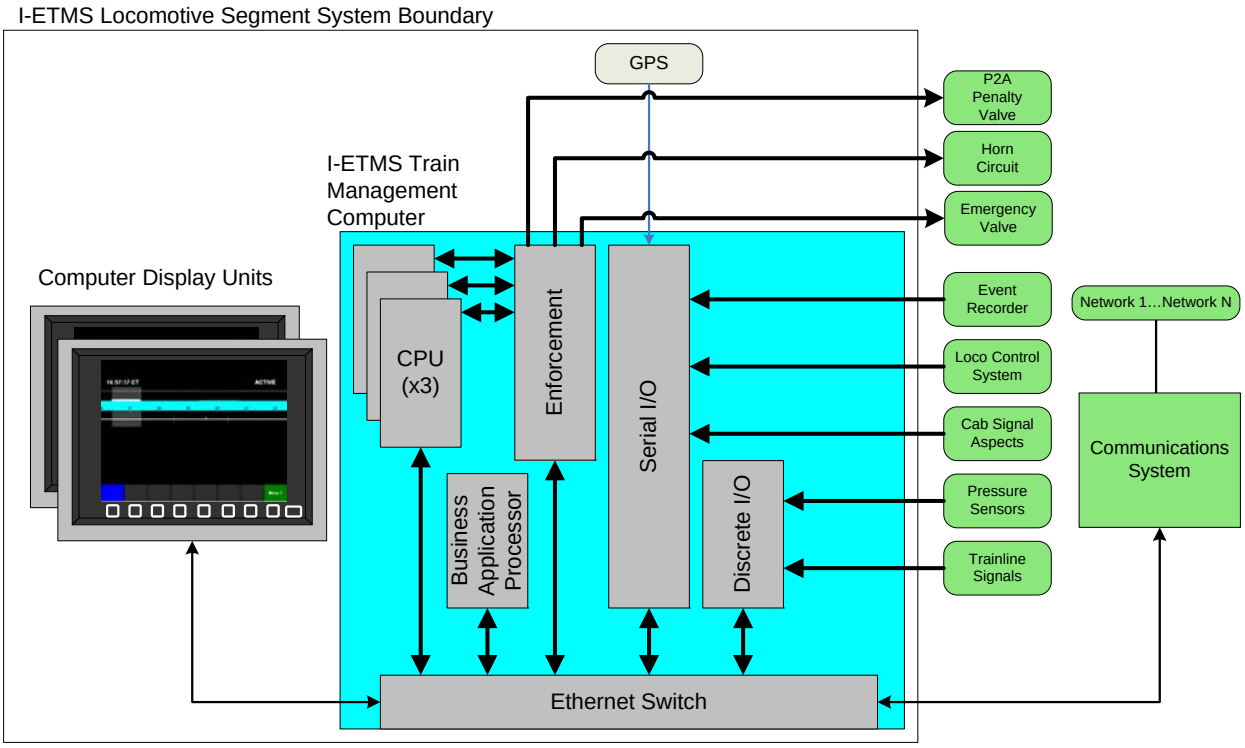

Figure 7 – I-ETMS Locomotive Segment Architecture

The common backplane includes two independent paths available to provide redundant power distribution and safety critical inter-slot communication paths. Each slot has a unique ID configuration that allows a board to determine which slot it is installed in. The system will detect a configuration failure if the board is in the wrong slot.

Slots 1 through 4 are shielded to better support CPU modules: CPU slots 1, 2, and 3 can host train control CPU modules, while slot 4 is reserved for an optional business application. Slot 5 is reserved for the RSM, which includes an Ethernet switch that allows all slots in the chassis to communicate with one another and with up to four external devices. Slots 6, 7, and 8 house the EBI, IOC, and DIO, respectively. Slot 10 hosts a 5th CPU module running ITCM application gateway software. The remaining slot, slot 9 is open and can host any of the I-ETMS modules.

The chassis supports up to three train control processors in slots 1, 2, and 3. For vital calculations, a minimum of two processors are required and a third may be included for added redundancy to increase overall system availability. The overall system availability constraints of the customer determine whether a third CPU is installed in the system. Each of slots 1, 2, and 3 provides a direct connection from the CPU to the enforcement module through the chassis backplane.

The I-ETMS TMC supports applications running on independent processors in other slots such as may be required for a third-party Energy Management (EM) product.

3.4.1.2 CPU Module

The I-ETMS Central Processing Unit (CPU) is a standard module that is used for both train control and business applications. Train control application software operates on CPU modules that are separate from a CPU module designated for a business application. The majority of system-level I/O are handled by other modules within the chassis (refer to IOC and DIO) and the data from those modules is conveyed to the processors via Ethernet. In addition to Ethernet, the processors also have serial ports and USB connectivity for interfacing to other devices. Each train control CPU uses a dedicated serial port for independent communication of braking commands to the EBI through the TMC internal backplane.

3.4.1.3 Input/Output Concentrator

The Input/Output Concentrator (IOC) is a module for use within the I-ETMS chassis and provides for consolidation of a number of functions as listed here.

Where I-ETMS is integrated with a cab signal system, a portion of circuitry on the IOC monitors cab signal lamp indications in a parallel, dissimilar manner and makes the redundant data available to the processors for validation. Failures such as burnt-out lamps, improperly-displayed aspects, or broken wires are detected and reported to the TMC. The IOC provides a hardware interface suitable to a variety of cab signal systems; however, I-ETMS is designed to fully integrate with and enforce only four-aspect systems with or without speed control at this time. All the railroad signatories to this PTCDP, who plan to integrate I-ETMS with a cab signal system, will do so strictly where four-aspect systems are in operation. (The four-aspect mode of the NEC cab signal system will be used for tenant freight operations, as it is today for LSL.) However, the I-ETMS architecture can support integration of additional cab signal indications and it could be modified to support the processing of same into corresponding enforcement targets. Any railroad that will deploy I-ETMS in a non-four-aspect configuration would need to identify a deviation from this PTCDP in their PTCSP per §236.1015 (c).

The IOC microcontroller also consolidates communications to two HDLC ports and 3 asynchronous serial ports. The interface allows bridging between the system Ethernet and system-level serial interfaces. The serial interfaces of the IOC are connected to a GPS receiver, the locomotive event recorder, and to the locomotive control computer (e.g. ICE or IFC). These serial interfaces provide data required for the train control computer calculations such as GPS position, speed, brake system pressures, and throttle control settings (may vary by locomotive). Finally, the IOC provides the system level interface to the locomotive ID configuration data module within the chassis.

3.4.1.4 I-ETMS Brake Interface Module

The I-ETMS Brake Interface (EBI) Module, for use within the chassis, provides a vital interface to the locomotive brake system for penalty and emergency brake applications, and provides an interface to the locomotive horn system to allow the system to render horn activation. The EBI Module interfaces to the triple-redundant processor architecture through dedicated communication buses. The enforcement module provides additional inputs to allow other systems, such as cab signals, to have vital access to the brake system. Aspects of the fail-safe design are described below.

Penalty Brake Interface: The penalty brake interface for the EBI Module is Class II Vital Hardware as defined by AREMA17.3.3.E. Some characteristics of this interface are as follows:

- No single point of failure in the enforcement circuit will prevent the ability to command a penalty brake application.
- The penalty brake module is continuously tested to verify I-ETMS's enforcement capability without causing a brake application.
- If the Locomotive Segment loses power, a penalty brake application will occur in a fail-safe manner.

The Locomotive Segment provides penalty brake enforcement by supplying an isolated, two wire, 32V differential signal to the locomotive's air brake system. This interface may be through an input to the locomotive's air brake computer or through an interface to the magnet valve P2A circuit on locomotives without an air brake computer.

An explicit penalty brake application occurs when two of the three operational train control processors agree to apply the brakes (or actively fail to hold off penalty application). If one processor is in a failed state, only one of the two remaining functional processors needs to request a brake application for it to occur. If more than one processor is faulty, the penalty brake is automatically applied in a fail-safe manner.

In the event of a fault in the Locomotive Segment where the penalty brake is applied and cannot be released, the manual “Cut-Out” switch provided with the I-ETMS system may be used to isolate I-ETMS from the locomotive's air brake system, allowing recovery of the air. This switch should be used only under equipment failure conditions and its state is monitored through a connection to the EBI. If the position of the switch changes from “Cut-In” to the “Cut-Out” state or from “Cut-Out” to the “Cut-In” state, the change is reported to the rest of the Locomotive Segment and is logged onboard and in the Office Segment. Transition from “Cut-Out” to the “Cut-In” state requires an I-ETMS departure test to initialize the system.

Emergency Brake Interface: Another aspect of the EBI Module is the ability to command an emergency brake application. This is accomplished through a magnet valve connection to the brake pipe. An emergency brake application will only be invoked when the Locomotive Segment determines that a previously invoked full-service penalty brake application was not sufficient to prevent a violation of authority limits. Invoking of the emergency brake application is limited to conditions which require predictive enforcement. For example, in the event of a revoked authority, if the revoked authority is one in which the train is currently located, revocation would cause a full-service reactive enforcement, without any transition to emergency. If the revoked authority is one in which the train is NOT currently located, its revocation may or may not result in a predictive enforcement (including potential emergency enforcement), depending upon the proximity of the train to the authority limit and its predicted braking distance. Emergency enforcement brake applications will be rare and only occur upon gross mismatch between predicted and actual train braking performance. A “gross mismatch” is defined as any distance beyond the speed target. Some characteristics of this the emergency brake interface are as follows:

- If the system loses power, an emergency brake application will NOT occur.
- An explicit emergency brake application occurs when a penalty brake application has first been invoked, the reduction in brake pipe pressure has been detected at the rear of the train or sufficient time has elapsed to permit the brake pipe reduction to reach the rear of the train and two of the three operational train control processors agree to apply the emergency brake.
- If one processor is in a failed state, the two remaining functional processors both need to request a brake application for it to occur. If more than one processor is faulty, the emergency brake cannot be commanded from the I-ETMS system.

Horn Interface: The Locomotive Segment provides automatic horn activation in the event that the locomotive engineer fails to sound the horn while in approach to a rail-highway crossing at grade when required. The automatic horn activation is resident in all installations of I-ETMS described in this Plan, but is configurable by the individual railroads. A railroad may configure the horn function in one of three manners: off, continuous, or sequenced. Sequenced horn activation is a patented function that requires an external agreement. In addition, to accommodate quiet zones, each crossing may be designated as a quiet zone within the track database in accordance with the conditions of approved quiet zones. When the locomotive engineer actuates the horn, the Locomotive Segment ceases its actuation. As such, the horn interface is a non-vital function as it is acting as a backup under conditions whereby the train is within a threshold time/distance from a highway crossing and the locomotive horn has not otherwise been manually sequenced. Some characteristics of the horn interface are as follows:

- No single point of failure in the horn interface circuitry will prevent the ability for a locomotive engineer to sound the locomotive horn.
- If the system loses power the horn will NOT be sounded by the system.
- The system may command the locomotive horn to be sounded as a continuous blast or a sequence of long and/or short blasts.
- The horn is sounded when commanded by the locomotive engineer, or when any one of the three operational train control processors determines the need to sound the horn. Discrete logic that accounts for the fault status of each processor determines which of the three processors controls the sounding of the horn to prevent a superset of multiple processors sounding the horn.

3.4.1.5 Discrete Input/Output Module

The Discrete Input/Output (DIO) Module used within the I-ETMS chassis provides a consolidation of digital and analog inputs from both high voltage signals and low voltage transducers.

The module accepts discrete inputs from multiple high voltage sensors, broken into discrete groups for situations where isolated returns are required. The module also accepts analog inputs from a high-voltage traction motor current sensor and low-voltage sensors for signals such as brake pipe pressure, brake cylinder pressure, and equalizing reservoir pressure. Speed from the locomotive axle alternator is also measured through the DIO module.

At a system level, the DIO module provides locomotive operational data for non-electronic models (e.g. SD40, GP38, etc.) and also provides a redundant data source for locomotives with an electronic control system.

Signals read from external interfaces are considered “raw” signals. The I--ETMS application software processes raw signal (or sets of raw signals) by “validating” and “conditioning” them to produce a PTC signal to be used by the system. PTC signals can be used to generate other PTC signals.

The PTC signal generation process is as follows:

- Signal Validation – performed on each raw signal by interface handling function
- Read raw signal from sensor
- Validate signal (signal presence, signal in proper format, signal within proper range, etc.)
- Submit raw signal and associated validity
- Capture required raw signal and validity (1 to n raw signals required to generate particular PTC signal)
- Capture required PTC signal and validity (1 to n PTC signals required to generate particular PTC signal)
- Perform signal conditioning process to generate a PTC signal

The locomotive configuration determines which raw and PTC signals the PTC signal conditioning process uses. Raw sensor signals no longer have a priority associated with them, instead, each raw sensor signal will have a source identifier (Loco Data, LIG, Discrete Sensor, etc.) associated with it. The conditioning process for each PTC signal can determine, based on the configuration, which of these raw sensor signals to use when formulating the PTC signal.

3.4.1.6 Router / Switch Module

The Router/Switch Module (RSM) provides the communication backbone for all modules within the chassis and for a number of components outside of it. The RSM is an Ethernet switch providing a dedicated, internal switchport for each of the other 9 slots within the chassis (the 10th slot holds this module). The RSM Ethernet switch also provides five external switchports for networking other systems with the TMC. Train control processing takes priority over any business application. Throughput analyses will be included as part of the PTCSP. The external switchports terminate at connectors on the front of the RSM to support connection to devices such as the Computer Display Unit (CDU), PTC Crash Hardened Memory Module (CHMM), maintenance laptop, or communication systems.

3.4.2 Computer Display Unit

The crew interface to the Locomotive Segment is provided by one or more Computer Display Units (CDU). The display that is interactive will be designated as CDU-I. The non-interactive display will be designated as CDU-NI. The CDU-I contains a 640x480 LCD monitor with a series of eight function keys located along the bottom for use as soft-keys. The CDU-I is based upon a PC-class processor and interfaces to the processor modules through an Ethernet link. Audible alerts are generated through a single, external Sonalert® device. Illumination of the CDU is provided by an internal fluorescent backlight with dimming control. Crews will be trained on the procedures in the event a lamp failure occurs. Where multiple displays are utilized, the TMC will monitor the presence of all CDU's installed.

The Wabtec CDU is shown in Figure 8. I-ETMS is being designed to accommodate two CDUs, the second of which will be non-interactive (CDU-NI) has the same dimensions and physical appearance as the CDU-I. The location of each type of CDU will vary by railroad and class of locomotive.

Figure 8 – I-ETMS Computer Display Unit

3.4.3 Locomotive ID Module

The Locomotive ID module is a single-wire, serial EEPROM device embedded within the locomotive wiring. This device, which interfaces directly to the TMC, is used to store installation / configuration information on the locomotive.

3.4.4 GPS Receiver

The Locomotive Segment utilizes one or more external GPS receivers to determine location and to drive the train control navigation algorithms. The standard receiver used in this system provides 10m (95%) accuracy under normal operation with 3m (95%) accuracy when WAAS correction information is available through the satellite system. This accuracy level, along with navigational aids such as switch position, provides the accuracy required for I-ETMS to determine on-track position.

GPS data is provided by a receiver connected through TMC IOC serial ports. If two receivers are utilized, additional checks on data are performed which allow the system to operate in the absence of one receiver for greater fault tolerance.

Position and speed information from each receiver will first be validated against previous position and speed information to discard erratic reports. The basis for evaluating speed reports will be to use a maximum acceleration or deceleration rate for the train (based upon worst case train weight, number of locomotives, and braking force) and to compare currently reported speed against prior reports. If the reports differ by more than the allowable acceleration limits, speed will be considered invalid within that report. The same principle will be used for position where a maximum positional change will be considered valid based upon the same acceleration or deceleration limits.

After the first validation check has been completed, valid results from each receiver are independently evaluated based upon GPS NMEA Quality and Dilution of Precision (DOP) values from each receiver. The solution with the best DOP will be selected to yield the PTC GPS Speed, Latitude, Longitude, Altitude, and Heading signals. Number of satellites, HDOP, and Quality values will be reported from the GPS receiver selected.

Altitude and direction information is not used by the Locomotive Segment, but that data is provided to Energy Management. Those signals from each receiver will be averaged over an interval of 5 seconds and if the standard deviation of those samples exceeds 10ft for altitude or 5 degrees for heading, the signal for that receiver is considered invalid.

3.4.5 Locomotive Event Recorder

The Locomotive Segment obtains status information by monitoring data sent to an existing I-ETMS compatible locomotive event recorder including indications from the locomotive train line discrete and pneumatic pressures.

Standards defined in §229.135 and §236.1005(d)(2) provide the requirements for event recorders, including requirements for crashworthy event recorder memory modules for locomotives originally ordered on or after October 1, 2006, and placed in service after October 1, 2009. A new recorder will be required due to the volume of data that will need to be captured. I-ETMS is capable of supporting an open standard recorder. The

crash hardened memory module is connected to the Ethernet Switch physically located in the TMC.

3.4.6 Train Control Application

The Locomotive Segment continuously computes both safe braking and warning distance curves to provide both predictive and reactive warnings and enforcement. Braking and warning curves are calculated based upon train and track characteristics and locomotive control settings. Curves are compared to authorized speed profiles generated from authority and speed limit data. The train's current authority limits are derived from applicable signal indications and/or movement authority provided by the railroad dispatching systems. Permanent speed restrictions are established from the I-ETMS track database. Temporary Speed Restrictions (TSR's), provided by the railroad dispatching systems, may impose additional enforceable restrictions on the train.

Predictive warnings provide the opportunity to respond to signal indications requiring a stop or reduction in speed, overspeed conditions, improperly lined switches, or work zones in advance of the train. If sufficient action is taken to properly control movement of the train, the warning is cleared. Failure to take sufficient action to control train movement in response to a warning, will result in a full-service penalty brake application when the train reaches the safe braking distance to the restriction. Once a penalty brake application is initiated, a freight train must come to a complete stop before the brakes may be released. When a penalty brake application is initiated on a passenger train for an overspeed condition, the Locomotive Segment may provide the capability for the locomotive engineer to invoke a running release of the brakes prior to stopping, after the over-speed condition is corrected, subject to the train-handling rules.

Reactive warnings may provide the opportunity to respond to the warning and properly control train movement. Under certain conditions, such as revoked authority, reactive enforcement braking may be initiated without prior warning.

The CDU provides a series of graphical and textual displays as shown in Figure 9 and Figure 10. Note these two figures do not represent actual displays; displayed elements have been enabled to show placement. A description of the HMI standards implemented for I-ETMS can be found in AAR specification [19].

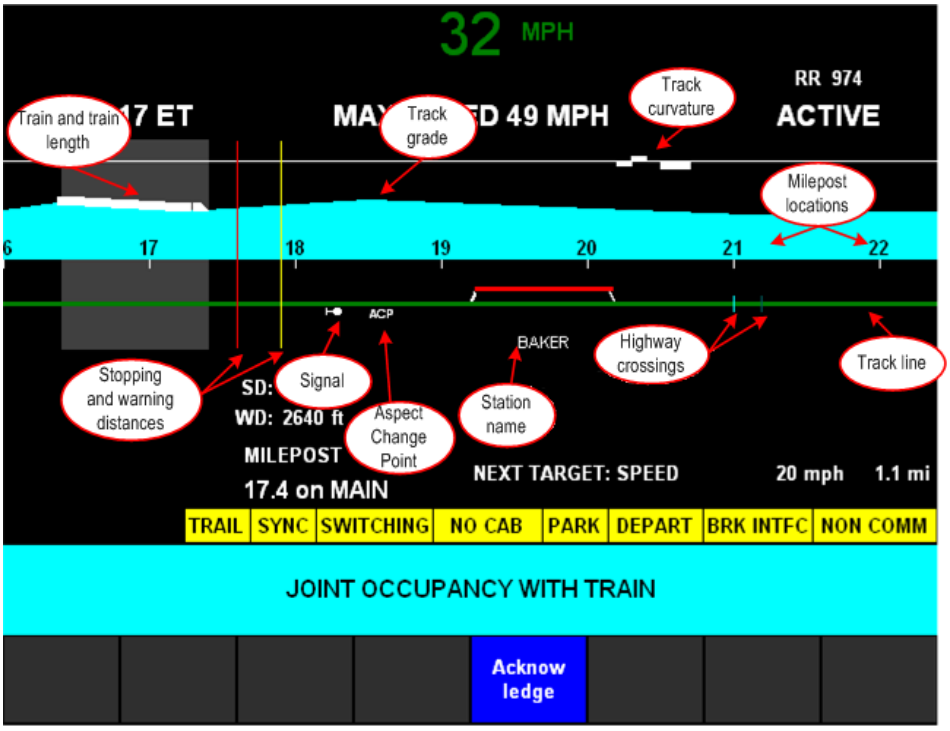

Figure 9 – Primary I-ETMS Display Screen - Graphical Elements

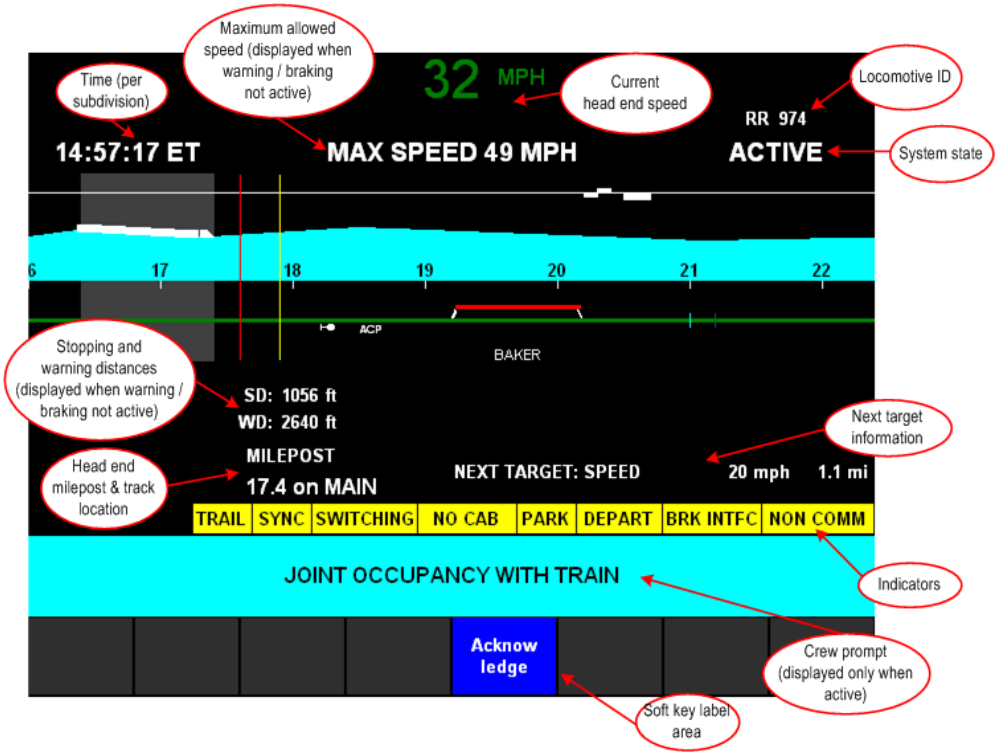

Figure 10 – Primary I-ETMS Display Screen - Textual Elements

Current speed, locomotive ID, and system state are always visible along the top edge of the display, even when warning or enforcement messages are displayed. In the event of an I-ETMS warning or enforcement, any non-safety critical data becomes subordinate and full display attention is given to data pertinent to the safety critical event and I-ETMS functions.

I-ETMS stores log information to an external recorder in accordance with §229.135 as required.

3.4.7 Business Applications

I-ETMS provides three mechanisms for the support of external business applications.

- Business Processor – The TMC supports addition of a business processor module to its chassis, which provides a platform for hosting business applications and isolation from the train control processors and applications.

- Data Interface – The I-ETMS train control application includes an interface by which data may be exchanged between the train control application and external business applications. The interface may be utilized between the train control application and business applications running on a business processor added to the TMC chassis or on processors external to the TMC.

- Display – The I-ETMS train control application reserves space on the CDU for display of information provided by external business applications. A business application may send information to the train control application via the data interface to be displayed on the reserved CDU space. However, the train control processors retain control of the display and display of safety critical train control information always preempts display of business information.

An Energy Management (EM) application is currently the only business application specified that utilizes any of the business application integration features of I-ETMS. Section 5.6.16 further describes this EM application and the nature its use of the data interface, which is specified in the Train Control and Energy Management Integration Onboard Interface Control Document.

Examples of graphical and textual information provided by EM to the train control application are shown in Figure 11 to support EM. Note this figure does not represent an actual display; displayed elements have been enabled to show placement.

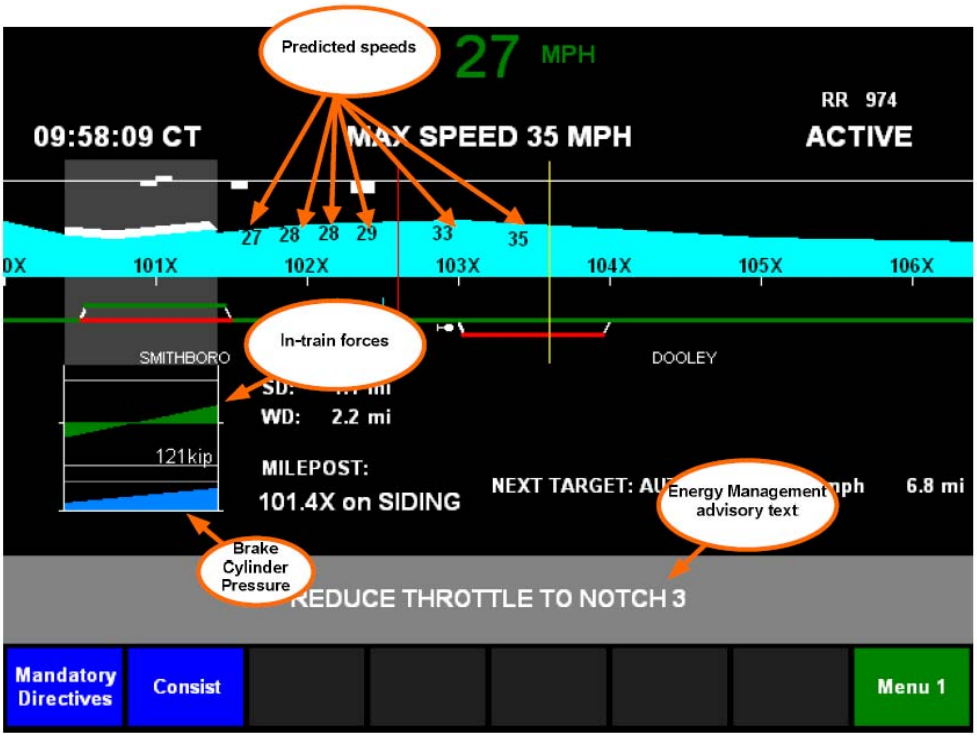

Figure 11 – Primary I-ETMS Display Screen - Energy Management

3.5 Communications Segment

The Communications Segment consists of a messaging system and multiple wired and wireless networks as depicted in Figure 12 and Figure 13 below, through which messages are exchanged between the Locomotive, Wayside, and Office Segments. The deployment of multiple wireless network technologies, as part of the Communications Segment, is used to maximize its capacity, throughput, and to mitigate against coverage issues.

The wireless networks may consist of one or more private and commercial communications paths that manage PTC system data traffic allowing for seamless routing across the prescribed path.

I-ETMS application functions connect to the Communications Segment via a standard interface and communicate with each other using protocols that are independent of any particular communications network. The I-ETMS application fully protects itself from hazards introduced by the characteristics or performance of the communications networks underlying the Communications Segment. This allows I-ETMS to utilize a wide variety of communications networks as coverage conditions and/or technologies change, without the need for system reconfiguration or disarrangement.

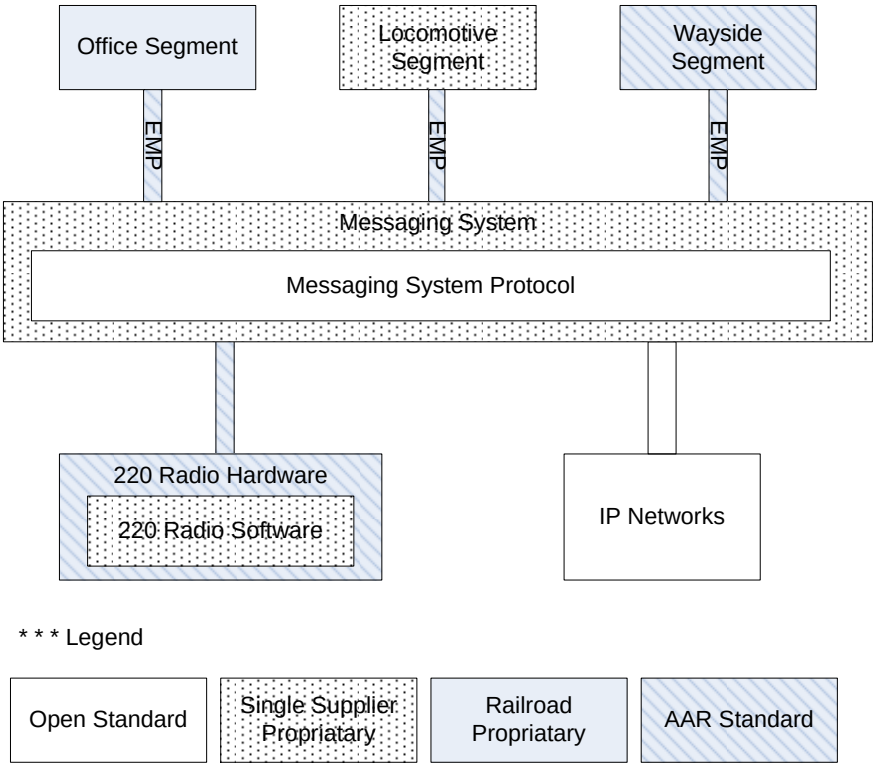

Figure 12 – I-ETMS Communications Network Architecture

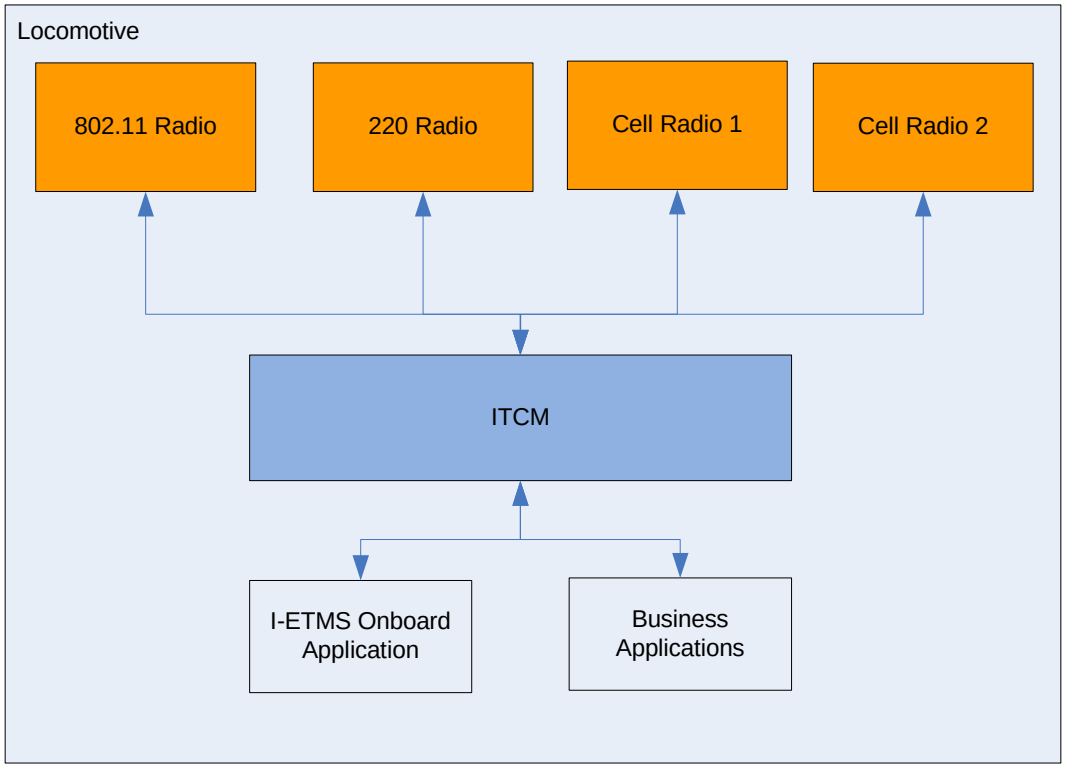

Figure 13 – I-ETMS Locomotive Communications Architecture

3.5.1 Wireless Networks

The Communications Segment will be deployed with multiple wireless networks. Wireless networks that are planned as part of the initial deployment with I-ETMS include the following:

- 220MHz Private narrowband radio network (Interoperable standard)
- Broadband – Wi-Fi network infrastructure deployed by railroads
- Cellular and satellite – Public wireless data networks

3.5.1.1 220 MHz Radio Network

The 220 MHz narrowband radio will be an industry-standard radio implementation specified and designed by the ITC consortium. The frequency band of the radio will be: Upper – 222 MHz; Lower – 217.6 MHz. The 220 MHz band-plan divides the spectrum in 5 kHz slices and the ITC-designed radio will aggregate those 5-5 kHz channels together to achieve a 25 kHz channel needed to support data requirements for train control messages. This channel aggregation scheme (as allowed under 47 CFR 90.733(d)) is used to achieve spectral efficiency, the primary goal of narrow banding.

While the 220 MHz path could be used for large file transfers, railroads may additionally use IEEE 802.11x or 3G cellular services for high-bandwidth requirements. The 220MHz network will support communications between all I-ETMS segments. Meteorcomm, LLC, will develop functional specifications for standard radio and protocol implementations intended to support I-ETMS and other business applications. Railroads will utilize 220MHz spectrum owned and managed by PTC220, LLC, or purchase their own.

Additional wireless networks may be added at any time but railroads must deploy the 220 MHz PTC data radio system to achieve interoperability in the Communications Segment.

While not a condition of interoperability, many railroads will also support the use of interoperable 802.11 capabilities in accordance with AAR Specification S-61213 “Railroad Use of 802.11” reference [18]. Additionally, railroads may choose to leverage non-interoperable, private wireless network technologies they already own such as 900 MHz ATCS radio networks or 44 MHz data radio networks in their Communications Segment. Railroads may also choose to subscribe to commercial cell in their Communications Segment. These non-interoperable wireless networks augment the 220 MHz PTC data radio system and as such do not need to support stringent network performance characteristics. Where they are used, these auxiliary communications simply add capacity, throughput, and limited local backup capabilities to the local 220 MHz PTC data radio system.

The 220 MHz radio is being designed with a combination of TDMA and CSMA channel access methods intended to maximize efficiency and throughput. The Wayside to Locomotive link is especially time sensitive, requiring frequent status updates. The current design of the Wayside RF link will use a fixed TDMA scheme where each Wayside will be assigned a unique "time slot" facilitating an efficient use of the channel.

The RF link between the Office and Locomotive uses a dynamically assigned TDMA time slot provisioned by the base station upon request from the locomotive radio. Once an I-ETMS train is fully initialized and on line-of-road, at a minimum, the Locomotive must receive a periodic "heartbeat" message from the Office Segment within a threshold tolerance in order to remain in the Active state. This heartbeat message is used by the Locomotive Segment to ensure that locomotive data is synchronized with the Office.

In order minimize system latency, the 220 MHz spectrum used by the radio links must be properly managed to maximize efficiency and throughput. To meet these goals, the ITC member roads formed PTC-220, LLC, a holding company for the 220MHz spectrum charged with the efficient deployment of 220 MHz spectrum nationwide. In support of PTC-220, LLC an internal technical team was created, the Spectrum Management Committee (SMC), which is directly responsible for managing frequency coordination, frequency reuse, interference mitigation, and build out plans.

To provide the strategic support for the nationwide deployment of the 220 MHz spectrum, the SMC is developing management tools that will be used in specific geographic locations to assess channel loading issues. To that end, the SMC has agreed to set a channel utilization metric threshold of 80%. This metric will be used to provide guidance to the SMC as to when congestion limits may begin to adversely impact RF network performance.

The actual bandwidth requirements are evolving as the I-ETMS application and radio are still under development, however, the Interoperable consortium has undertaken an effort to model one of the most dense US freight corridors consisting of one base covering 30 miles of triple-track territory with 21 trains and 25 waysides.

The modeling indicated channel loading to be approximately 6.8 kbps. The most current bandwidth capacity estimates for the 220 MHz radio is a 14 kbps offered load. In the current load models, assuming there are no limitations due to radio development and refinement of the I-ETMS application, the estimated worst-case scenario indicates that PTC traffic will fit within the channel.

In areas where there are overlapping 220MHz radio base stations belonging to different railroads, the PTC data radio system has been architected to provide the opportunity for users to share base stations. Incoming radio traffic received on a base station operated by a "foreign" railroad would simply be forwarded through an interconnected back office, to the appropriate back office servers for processing. This functionality will help in managing deployment costs where sharing takes place and can also support redundant base station coverage yielding improved reliability.

3.5.1.2 802.11

While not a condition of interoperability, many railroads will also use 802.11 capabilities in accordance with AAR Specification S61213 “Railroad Use of 802.11”. The usage of 802.11 communications is primarily targeted for use while in railroad yard facilities to support the file transfer requirements of the I-ETMS application during system initialization.

3.5.1.3 Cellular and Satellite

Railroads may also choose to subscribe to commercial cellular or satellite services in their Communications Segment. These non-interoperable wireless networks augment the 220 MHz PTC data radio system and as such do not need to support stringent network performance characteristics. Where they are used, these auxiliary communications simply add capacity, throughput, and limited local backup capabilities to the local 220 MHz PTC data radio system.

3.5.2 The Messaging System

The messaging system is designed to allow applications in the back offices, locomotives, and waysides to communicate with each other in an interoperable fashion across railroad boundaries. The messaging system, known as Interoperable Train Control Messaging or ITCM, is a messaging solution based upon open source software that has been customized to meet the requirements of I-ETMS. The architecture consists of redundant, scalable back office servers with messaging clients on remote assets, such as locomotives and wayside equipment. The ITCM is a loosely coupled, asynchronous message delivery system. Wayside, Locomotive, & Office applications communicate by simply addressing messages to one another and handing them off to the ITCM for delivery; without being concerned about how messages are routed through the system.

The messaging system insulates the I-ETMS application from the underlying communications networks of the Communications Segment. It manages access to the available wireless networks to ensure that available bandwidth is used efficiently and that I-ETMS message traffic has first priority. The messaging system also supports transfer of messages between railroad offices and allows deployment of shared wireless infrastructure. Messaging functions provided by the Communications Segment include the following:

- Asynchronous, connectionless message transfer;
- Quality of Service based network selection and bandwidth management;
- Message Queuing;
- Message Routing;
- Translation of application protocols to Communications Segment transport protocols;
- Mobility;
- Multiple RF paths and supporting protocol adapters.

Messaging system requirements are identified in ITC Messaging (ITCM) specification [17] and an implementation that meets those requirements will be developed. The messaging system allows both mandatory and optional attributes. Mandatory and optional attributes are applicable both at the message level and the system configuration level. These requirements include a standard interface for access to the messaging system by I-ETMS or any other compliant application.

Figure 14 depicts the ITC Messaging System architecture, including the component functions of the messaging system. Items in blue are components of the messaging system; items in orange are specifically related to communications networks.

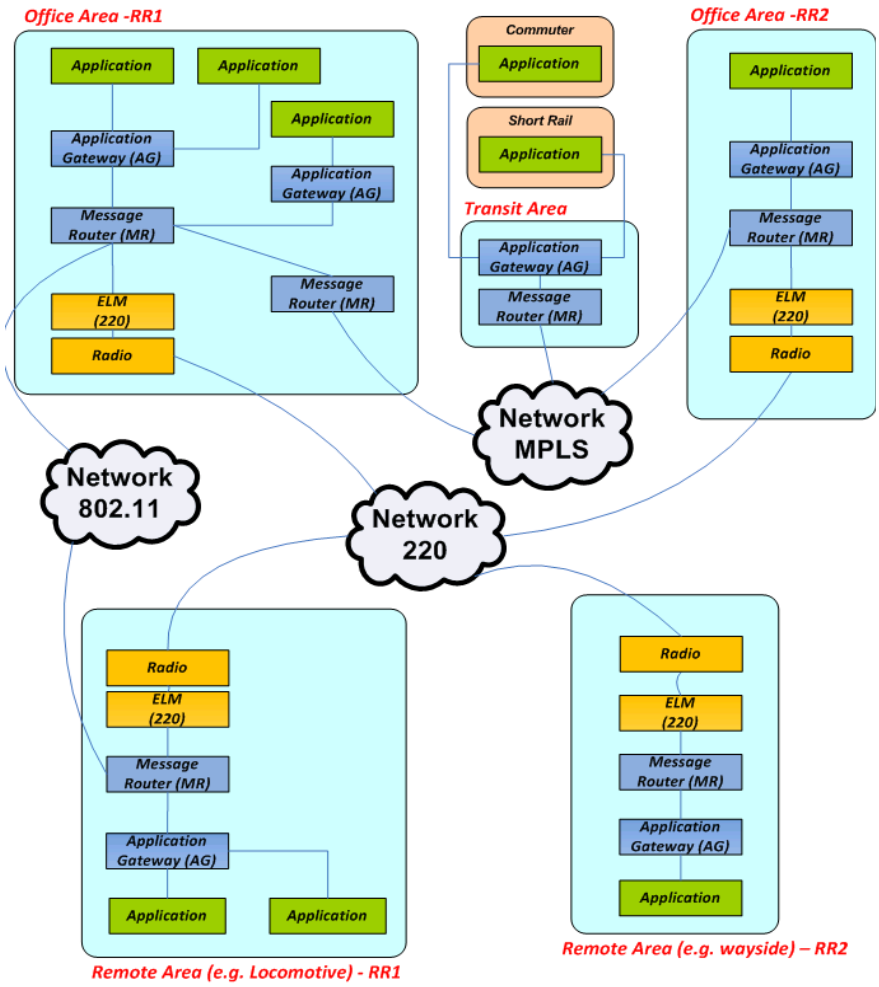

Figure 14 – ITC Messaging System Architecture

3.6 I-ETMS Interoperability

Interoperability means the ability of diverse systems and organizations to work together (inter-operate), taking into account the technical, operational, and organizational factors that may impact system-to-system performance. I-ETMS is designed to achieve interoperability through technical and semantic means.

There are several options for attaining technical interoperability:

- An I-ETMS railroad and its interoperability tenant partner will both install and operate the system on their respective locomotives, office, and wayside. By design, I-ETMS provides for full functionality for any equipped locomotives, regardless of ownership, with any office or wayside correspondingly equipped. Interoperability is achieved through native operation of I-ETMS without the need for data, function, or human-machine interface (HMI) translation. Interoperable communications are achieved through adoption of the common ITC specifications for communications and message protocols, and application behavior specifications described in ITC interoperability requirements. The I-ETMS design encompasses the methods of operation and rules of both railroads and accommodates any differences in the data provided by back office systems. The three roads signatory to this PTCDP are only deploying the I-ETMS system.

- In certain locations, a railroad may operate I-ETMS while its interoperability partner operates a different resident PTC system. For track where both party's trains operate, the necessary wayside infrastructure will be installed to support trains equipped with either PTC system. Locomotives will only be equipped with one of the PTC systems. Interoperability is achieved by allowing the equipped locomotive to operate with its compatible PTC office and the wayside infrastructure deployed along the track segment. This interoperability scenario is commonly referred to as "dual-equipping of the wayside."

- Some carriers may elect to install a different PTC system and I-ETMS on their locomotives to enable them to operate on I-ETMS territory and smoothly transition their locomotives back to their "home" territory where another system is the resident system. This interoperability scenario is commonly referred to as "dual-equipping of the locomotive."

I-ETMS is designed and developed to provide PTC functionality under the types of operations prevalent on North American heavy-rail freight and passenger railroads. It includes no explicit interfaces that provide interoperability with other complete PTC systems. However, its current architecture allows interoperation with WIU implementation, which complies with WIU interface and behavioral requirements. Interoperability will be achieved by "dual-equipping of the wayside" or "dual-equipping of the locomotive."

In all cases, interoperability is achieved through compliance with interoperable interfaces to I-ETMS and any other PTC system. The use by a railroad of any particular function of I-ETMS is driven by entries in the I-ETMS track database, messaging generated by the railroad's non-PTC back office systems, and/or railroad-specific configuration items. The operating railroad must properly construct its track database and configuration files and provide the external messaging consistent with its operating rules.

Semantic interoperability is achieved through the common use of documented system behavioral specifications. In October of 2008, an Interoperable Train Control (ITC) collaboration agreement was executed by and among four Class I railroads (CSXT, NSR, and UPRR submitting this PTCDP, and BNSF) wishing to achieve Positive Train Control (PTC) system interoperability through, in part, the development of an interoperable train control system which would enable locomotives of one participant to transition at track speed to the control of another participant.

I-ETMS was developed based on the following Principles of Interoperability, which represent a common set of agreements regarding the implementation of an ITC compliant PTC system and were reached through consensus among ITC members. The principles are intended to provide continuous guidance throughout the technical development of the PTC system. The Principles of Interoperability were written in such a way that they should not change significantly over time and act as a foundation for validating any future decisions regarding the interoperable nature of the PTC system. Each of the seven Principles of Interoperability is described in the sections that follow.

- ITC compliant Locomotive Segments shall utilize a single software executable.
- ITC complaint PTC systems will implement certain Concepts of Operations with common requirements for System Initialization, Wayside Beaconing, and Systems Management.
- ITC compliant PTC systems shall implement a common “look and feel” in regards to the Human-Machine Interface onboard the locomotive.
- ITC compliant PTC systems shall utilize common data definitions and information relationships for track, wayside, and locomotive assets.
- ITC compliant PTC systems shall utilize standardized Interface Protocols between the Wayside, Locomotive and Back Office Segments.
- ITC compliant PTC systems shall implement interoperable communication systems to enable the delivery of messages between assets owned by multiple railroads located in the Back Office, Locomotive, and Wayside Segments.
- Railroads that implement an ITC complaint PTC Systems shall share access to their 220 MHz Radio Base Stations with other railroads physically adjacent to their PTC operating territory.

3.6.1 Common Onboard Executable

- **Principle:** ITC Locomotive Segments shall utilize a single software executable.

- **Rationale:** A single executable helps to reduce the architectural complexity and the cost of an interoperable PTC system. ITC PTC equipped locomotives shall be capable of operating across multiple railroads.

- **Implications:** Onboard functional requirements for all railroads implementing the ITC PTC compliant systems must be incorporated into the single software executable. ITC Member railroads have chosen to implement the Common Onboard Executable through purchase of the Wabtec ETMS/I-ETMS system.

3.6.2 Common Concepts of Operation

- **Principle:** ITC complaint PTC systems will implement certain Concepts of Operations with common requirements for System Initialization, Wayside Beaconing, and Systems Management.

- **Rationale:** In order to make the ITC PTC System Interoperable a certain subset of functional and system requirements must be implemented in a common manner.

- **Implications:** Requirements to support the Common Concepts of Operation may be implemented through both proprietary and AAR standardized interfaces and components.

3.6.3 Common Human Machine Interface (HMI)

- **Principle:** ITC compliant PTC systems shall implement a common “look and feel” in regards to the Human-Machine Interface onboard the locomotive.

- **Rationale:** A common HMI reduces the training necessary for the locomotive engineer to operate the PTC System. No additional training should be necessary to operate an ITC compliant PTC system when a foreign locomotive is in the lead position.

- **Implications:** The Common Onboard executable shall implement a common HMI.

3.6.4 Common Data Model

- **Principle:** ITC compliant PTC systems shall utilize common data definitions and information relationships for track, wayside, and locomotive assets.

- **Rationale:** Leverage of a common data model reduces complexity and cost of the Common Onboard Executable. Maintenance of railroad geography and asset information is being implemented with railroad specific GIS and asset management systems. A Common Data Model standard supports the proprietary interface to the onboard track database.

- **Implications:** Railroads are responsible for configuration management of GIS & Asset information and the timely update of onboard track databases. ITC specific GIS survey standards and certain asset naming and addressing conventions will be implemented to support the Common Data Model.

3.6.5 Standard Interface Protocols

- **Principle:** ITC compliant PTC systems shall utilize standardized Interface Protocols between the Wayside, Locomotive and Back Office Segments.

- **Rationale:** An ITC compliant PTC System requires standardized interface protocols to enable information to be exchanged between the various systems utilized for interoperability between railroads.

- **Implications:** All railroads utilizing an ITC compliant PTC system will need to utilize the established interface protocols for connections between the various defined systems.

3.6.6 Interoperable Communications System

- **Principle:** ITC compliant PTC systems shall implement interoperable communication systems to enable the delivery of messages between assets owned by multiple railroads located in the Office, Locomotive, and Wayside Segments.

- **Rationale:** ITC compliant PTC Systems shall implement a Communication System capable of supporting Interoperable Application Interfaces, System Security, Systems Management, and railroad specific Business Applications.

- **Implications:** Implementation of an Interoperable Communication System implies:

    - Applications implement a standard application interface protocol using standard message structure and data formats.
    - Implementation of 220Mhz Radio and IP Networks

3.6.7 220 MHz Radio Base Station Sharing

- **Principle:** Railroads that implement ITC complaint PTC Systems shall share access to their 220 MHz Radio Base Stations with other railroads physically adjacent to their PTC operating territory.

- **Rationale:** The ITC standard 220 MHz Radio makes efficient use of scarce 220 MHz radio frequencies thru use of a shared nationwide radio control channel and use of nearest neighbor radio base stations.

- **Implications:** Reliability and cost of the ITC Communication System is improved. PTC message traffic from physically adjacent foreign railroads will utilize a railroad's base station and communications back-haul networks. Service level agreements may be required to make Radio Base Station Sharing operationally viable.

In the current ITC architecture, standard application-level specifications define the behavior of the interoperable office, locomotive, and wayside segments. Use of and compliance with these common behavioral specifications insure each interoperable system segment properly interprets and acts upon exchanged data messages.

I-ETMS common interface definitions include one or more radio protocols (220MHz) and hardware interfaces to radio equipment, a common standard messaging protocol (ITC Messaging), and standard data element and application message format and content definitions (I-ETMS interface control documents). These interface standards are comprised of message formatting, data integrity, use of a data dictionary, quality of service, and message data content. Use of and compliance with these common interface definitions insures the ability to exchange data messages between interoperable system components.

Testing of the interoperable specifications and interfaces will be conducted in accordance with a coordinated master test strategy. This strategy and approach will be utilized for testing of I-ETMS. While each organization will provide resources to the test effort, overall coordination of the test effort between organizations is the responsibility of each Railroad conducting its test program in accordance with the plan.

The purpose of the testing effort is to demonstrate that the I-ETMS system is in conformance with system requirements and business processes in both a laboratory and a field environment in order to obtain acceptance of the I-ETMS system and to facilitate PTCSP development and certification.

4 I-ETMS Applicable Categories of Railroad Operations - §236.1013 (a)(2)

This section provides a description of the railroad operation or categories of operations on which I-ETMS is designed to be used, including train movement density (passenger, freight), operating speeds (including a thorough explanation of intended compliance with §236.1007), track characteristics, and railroad operating rules as required by §236.1013 (a)(2).

I-ETMS design supports deployment across variations of the following operational characteristics:

- Methods of Operation and Operating Rules
- Train Types and Characteristics
- Operating Speeds
- Track Characteristics
- Train Frequency and Volume

The specific descriptions of railroad operations on which I-ETMS will be operated by deploying railroads is identified and described in each submitting road's Positive Train Control Implementation Plan (PTCIP) as filed with the FRA pursuant to 49 CFR 236.1011.

4.1 Methods of Operation and Operating Rules

I-ETMS is designed and developed to be overlaid upon a combination of methods of operation and other supplementary systems prevalent on North American heavy-rail freight and passenger railroads. The method of operation in effect on a main track is identified in the railroad's Timetable and the associated governing rules are described in its rulebook. Railroad timetables and rulebooks utilize unique nomenclature and rules in describing a particular method of operation; however, they are identified and briefly described below in generic fashion. A more detailed description of each method of operation, along with a description of how I-ETMS provides corresponding PTC functionality under that method of operation, appears in Section 5 - Concept of Operations.

Traffic Control. Trains may be authorized to occupy and move on a main track by the indications of a Traffic Control System. Trains and/or men and equipment may also be authorized to occupy a main track and move in both directions within specific limits by authority provided by mandatory directive. Traffic Control may be utilized in single or multiple main track territory. Automatic Cab Signals (ACS) or Automatic Train Control (ATC), which are not methods of operation, may be utilized where Traffic Control is in effect.

Current of Traffic. Trains may be authorized to occupy and move on a main track with the current of traffic by the indications of an Automatic Block Signal System. Trains and/or men and equipment may also be authorized to occupy a main track and move against the current of traffic or in both directions within specific limits by authority provided by mandatory directive. Current of Traffic is typically utilized in multiple main track territory. Automatic Cab Signals (ACS) or Automatic Train Control (ATC), which are not methods of operation, may be utilized where Current of Traffic is in effect.

Track Warrant Control. Trains and/or men and equipment are authorized to occupy and move on a main track by authority provided by mandatory directive. Track Warrant Control may be utilized in single or multiple main track territory. Automatic Block Signals (ABS), Automatic Cab Signals (ACS) or Automatic Train Control (ATC), which are not methods of operation, may be utilized where Track Warrant Control is in effect. Additional common implementations of track warrant control, as the term is utilized in this document, include Direct Traffic Control (DTC), Form D Control System (DCS), and Occupancy Control System (OCS).

Restricted Limits. Trains and/or men and equipment are authorized to use the main track not protecting against other trains or engines. All movements must be made at restricted speed.

Yard Limits. Trains and/or men and equipment are authorized to use the main track not protecting against other trains or engines where Traffic Control or Current of Traffic are not also in effect. Movements may be required to be made at restricted speed unless operating on a signal indication more favorable than “Proceed prepared to stop at next signal”. Where Traffic Control or Current of Traffic is also in effect, permission from the control operator is required in order to enter the main track or operate against the current of traffic. Automatic Block Signals (ABS), Automatic Cab Signals (ACS) or Automatic Train Control (ATC), which are not methods of operation, may be utilized where Yard Limits are in effect.

The I-ETMS track database identifies the method of operation in effect on each track segment as well as whether Automatic Block Signal (ABS) system, Automatic Cab Signals (ACS), Automatic Train Control (ATC), or Yard Limits are also in effect. From this profile in the track database, I-ETMS is able to determine the proper rules for enforcement of authority and speed limits on a track segment.

The I-ETMS track database and configuration files also include attributes which identify the application of certain railroad-specific rules for the method of operation in effect on the track segment. These attributes include:

- Maximum speed allowed under restricted speed rules;
- Conditions under and extent to which reverse moves are allowed;
- Signal indications.

4.2 Train Types and Characteristics

I-ETMS is designed and developed to support the prevalent types and characteristics of trains which operate on North American heavy-rail freight and passenger railroads. The system determines the type of train on which it is operative as indicated in the consist data provided by the operating road's dispatching system or as manually indicated by the train crew. Train types currently recognized by I-ETMS include Freight, Intermodal, Passenger, High-Speed Passenger, Tilt-Passenger, and Commuter. Train type is currently utilized by I-ETMS in the following functions:

- Permanent speed limit enforcement – Train type is utilized to retrieve the corresponding timetable speed limits contained in the I-ETMS track database.
- Temporary speed limit enforcement – Train type is utilized to determine the applicability of the bulletins and speed restrictions.
- Predictive braking algorithm – Train type is utilized to select and parameterize the algorithm utilized to perform all predictive braking calculations.
- Signal indication enforcement – Train type is utilized to determine the enforcement rules for any signals which include indications specific to a particular train type.

In addition to train type, the following train consist data is utilized by the I-ETMS predictive braking algorithm and other functions:

- Train length;
- Total train weight;
- Total axles;
- Loaded and empty car counts;
- Locomotive count, horsepower, and operative status;
- Presence of isolated or dead-in-tow locomotives
- Short- or long- hood forward configuration of lead unit;
- Presence and position of distributed power locomotives;
- Inoperative brake count;
- Consist or lading speed restrictions.

I-ETMS accepts values for each of the train consist parameters within a defined range. The acceptable range for each parameter is currently defined at the extreme limits of train consists found on North American heavy-rail freight and passenger railroads. However, the acceptable range for each parameter may be reduced to reflect the limits of operations actually tested.

4.3 Operating Speeds

I-ETMS is designed and developed to support operating speeds prevalent on North American heavy-rail freight and passenger railroads – up to 70mph and 125mph for freight trains and passenger trains, respectively. In order to support passenger train operation at speeds in excess of 90mph, the system will be designed and developed in accordance with Appendix C to 49 CFR Part 236 as required by 49 CFR 236.1007(b)(1).

Where the speed limit for freight trains is in excess of 50mph or in excess of 60mph for passenger trains, I-ETMS interfaces with and enforces the safety-critical functions provided by a block signal system or functional equivalent thereof as prescribed by 49 CFR Part 236 and in accordance with 49 CFR 236.1007(a). The configuration of a block signal system or functional equivalent in any such territory is described in the implementing railroad's PTCIP.

I-ETMS will prevent unauthorized or unintended entry of a train onto a PTC track from an auxiliary or non-PTC main track, in accordance with 49 CFR 236.1007(b)(2), when the Locomotive Segment has previously been initialized and the non-PTC track is described in the track database. Predictive warning and/or enforcement are provided such that the train will be automatically stopped prior to its entering or fouling a PTC track without authorization. Procedures for initializing the Locomotive Segment and mapping of non-PTC tracks will be described in the railroad PTCSP. The railroad PTCSP will also describe any equivalent measures utilized to comply with 49 CFR 236.1007(b)(2) where use of I-ETMS to provide this function is not feasible.

Any deviation from 49 CFR 236.1029(b) will be described in the PTCSP submitted by a railroad as required by 49 CFR 236.1007(b)(3) for operations at more than 90 miles per hour.

4.4 Track Characteristics

I-ETMS is designed and developed to support track characteristics prevalent on North American heavy-rail freight and passenger railroads. The track database design and navigation functions place no specific limitations on the number of tracks or track geometry; however, practical limitations on track gradient and curvature may be established during development in order to bound testing scope. For example, current plans include testing of the I-ETMS navigation and predictive braking algorithm functions on grades of up to +/- 3%. This limit may be adjusted upward or downward during initial system development, and may be further adjusted in future versions to accommodate new requirements or bound testing.

During initialization, the system will require input from the train crew to identify the track on which the train is located. Once the train has been resolved to track, I-ETMS navigation maintains on-track position through a combination of GPS, wheel tachometer feedback and dead-reckoning, switch position monitoring, and track database. It continuously monitors the correspondence of its navigational inputs and if any are inconsistent with the resolved train location, the train crew is alerted and the system enforces the train to a stop if corrective action is not taken.

A planned enhancement of I-ETMS includes integration of a high-precision location determination system which will obviate the manual track selection now required to disambiguate track selection.

Performance of the predictive braking algorithm on different track characteristics will be measured during the development and testing process through a combination of lab simulations, analysis, and field testing.

4.5 Train Volume and Frequency

I-ETMS is designed and developed to support train volumes and patterns prevalent on North American heavy-rail freight and passenger railroads.

The Locomotive Segment executes safety-critical PTC functions and it is dedicated to the processing requirement for the train on which it is initialized. Its processing load is sensitive to train volume or frequency on a line segment only to the extent the processing load of radio messages is determined by Wayside Interface Unit (WIU) density or number of mandatory directives issued to the train to move it over the line segment.

The WIU executes safety-critical PTC functions and it is dedicated to the processing requirements at the location at which it is installed. The WIU provides a periodic broadcast of wayside status that is nominally received and processed by all trains in proximity of and governed by devices monitored by the WIU. In such cases, the processing load of the WIU is unaffected by the volume or frequency of trains operating in its proximity. However, under conditions where communications between WIU and locomotives perform poorly, individual equipped I-ETMS trains may make requests to the WIU to broadcast wayside status messages at intervals more frequent than the periodic broadcast rate.

The Back Office Server (BOS) in the Office Segment executes office processing functions for all trains that occupy or may operate within specific geographic limits, typically one or more railroad subdivisions. The processing load demand of the BOS is a function of the aggregate volume of trains operating concurrently within the geographic limits along with their aggregate number of mandatory directive transactions. The Office Segment is designed such that the office processing load may be distributed across multiple BOS instances on the basis of geographic limits and train volume and frequency within those limits. It is incumbent upon the implementing

railroad to perform the engineering necessary to allocate geographic territories and train volumes to one or more BOS instances in order to meet its performance requirements.

The Communications Segment is designed to utilize the available network bandwidth according to priority of the PTC messages as well as inter-railroad office messages in a shared network infrastructure. It is incumbent upon the implementing railroad to perform the engineering necessary to provide communications systems coverage adequate to meet its performance requirements.

5 Concept of Operations - §236.1013 (a)(3)

This section provides the operational concepts document, including a list with complete descriptions of all functions which the PTC system will perform to enhance or preserve safety as required by §236.1013 (a)(3). This concept of operations is organized generally in accordance with Institute of Electrical and Electronics Engineers (IEEE) standard 1362-1998. It describes I-ETMS functionality, operation and characteristics generally from the user's perspective. A limited description of the internal workings of the system is included in some sections where it augments understanding of observable system behavior.

This concept of operations provides a description of the complete set of I-ETMS functions. I-ETMS onboard software will be a single, common computer "executable" which provides a composite set of train control functions supporting a composite set of railroad train control operational needs as determined by the participants in the ITC process. From the perspective of system design and implementation, there is no concept of "mandatory" or "optional" functions; all in-scope functions are embedded into the common "executable". The use by a railroad of any particular function is driven by entries in the track database, messaging generated by the railroad's non-PTC back office systems, and/or railroad-specific configuration items (refer to Section 3.6). A small and controlled number of versions of the I-ETMS software will be permitted from a policy and interoperability perspective by the railroads that deploy the system. Additionally, it includes a function that "enforces" compliance with the permitted software version policies of a particular railroad. However, on any particular railroad property and at any particular location, only a subset of the complete set of I-ETMS functions may be active. There are no "minimum" operational rules or special instructions that are documented. The set of I-ETMS functions active at any point in time is determined by factors which include:

- the location of the locomotive and/or track segments occupied by the train;
- the content of messages provided to I-ETMS by the railroad dispatching system or other external railroad back office systems;
- configurable I-ETMS system and operating parameters; and
- locomotive engineer input.

I-ETMS configurable operating parameters are adjustable, under configuration management, on either a system or per-railroad basis. These values are subject to change during and as a result of testing, and in order to ensure target safety levels are achieved during system operation. The respective PTCSPs submitted by each railroad implementing I-ETMS shall fully describe revenue service operation of the system and the configuration for each adjustable parameter.

Section 5 organization is as follows:

- Section 5.1 describes the regulatory requirements for PTC functionality.
- Section 5.2 provides an overview of I-ETMS functionality
- Section 5.3 briefly describes how interoperability is achieved.
- Section 5.4 briefly describes existing railroad non-PTC operations and the roles and responsibilities of key personnel in those operations.
- Section 5.5 provides an overview of key I-ETMS operational concepts.
- Section 5.6 describes planned railroad PTC operations with I-ETMS and the roles and responsibilities of key personnel in those operations.
- Section 5.7 identifies specific changes and effects on railroad operations caused by I-ETMS deployment, both during testing and revenue service operation.

5.1 Regulatory Requirements for PTC Functionality

49 CFR 236 Subpart I, requires PTC systems to fulfill specific functionality as specified in §236.1005. Table 4 below lists the requirements from the Subpart and labels each as "safety-critical" (SC) or "non safety-critical" (NSC) based on the functionality required to meet the requirement.

Table 4 – PTC System Functions

Ref #	PTC System Function (Defined in §236.1005, 49 CFR 236 Subpart I)	Safety Critical or Not
1	Prevent Train-to-Train Collisions: reliably and functionally prevent train-to-train collisions—including collisions between trains operating over rail-to-rail at-grade crossings in accordance with the following risk-based table or alternative arrangements providing an equivalent level of safety as specified in an FRA approved PTCSP.	Safety Critical
2	Prevent Overspeed Derailments: reliably and functionally prevent overspeed derailments, including derailments related to railroad civil engineering speed restrictions, slow orders, and excessive speeds over switches and through turnouts.	Safety Critical
3	Prevent Work Zone Incursions: reliably and functionally prevent incursions into established work zone limits without first receiving appropriate authority and verification from the dispatcher or roadway worker in charge.	Safety Critical
4	Prevent Movement through a main track switch or any switch on a siding where the allowable speed is in excess of 20 mph is in the Improper Position: reliably and functionally prevent a train from advancement through a switch whose position is unknown or improperly aligned for the train's route.	Safety Critical

Ref #	PTC System Function (Defined in §236.1005, 49 CFR 236 Subpart I)	Safety Critical or Not
5	Include Wayside and Cab Signal Systems: include safety-critical integration of all authorities and indications of wayside and cab signal systems, and other similar systems, in order to provide warning and enforcement.	Safety Critical
6	Protect Derail or Switch Protecting Main Line: provide an appropriate warning or enforcement when a derail or switch protecting access to the main line required by §236.1007, or otherwise provided for in the applicable PTCSP, is not in its derailing or protecting position, respectively.	Safety Critical
7	Protect Against Highway Rail Grade Crossing Malfunction: provide an appropriate warning or enforcement when 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.	Safety Critical
8	Protect After Arrival Mandatory Directive: provide an appropriate warning or enforcement when 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.	Safety Critical
9	Protect Movable Bridges: provide an appropriate warning or enforcement when any movable bridge within the route ahead is not in a position to allow permissive indication for a train movement pursuant to § 236.312.	Safety Critical
10	Integrate Hazard Detectors: provide an appropriate warning or enforcement for all hazard detectors integrated into a signal or train control system on or after October 16, 2008.	Safety Critical
11	Limit Passenger and Freight Train Speeds: limit the speed of passenger and freight trains to 59 miles per hour and 49 miles per hour, respectively, in areas without broken rail detection or equivalent safeguards.	Safety Critical
12	Record Safety-Critical Train Control Data to the locomotive event recorder.	Not Safety Critical
13	Crash Hardened Memory Module: record safety-critical train control data to a crash hardened memory module on locomotives manufactured and in service after October 1, 2009.	Not Safety Critical

5.2 I-ETMS Functional Overview

I-ETMS is a locomotive-centric, vital train control system designed to be overlaid on existing methods of operation to provide an improved level of railroad safety through enforcement of a train's authority limits, enforcement of speed limits, protection of established work zone limits, protection against train movement through improperly lined main track switches, and protection of any switch on a siding where the allowable speed is in excess of 20 mph without the benefit of the indications of a wayside or cab signal system or other similar appliance, method, device, or system of equivalent safety or which would create an unacceptable risk.

System-level requirements were derived from the top-level system requirements and objectives of the Rail Safety Improvement Act of 2008 (RSIA08) and 49 CFR 236 Subpart I and address ITC system functions with respect to railroad operations.

Table 5 is a summary of Safety Assurance Concepts and specific techniques utilized by I-ETMS to operate safely. Functionality defined for I-ETMS is included in Table 6 below and has been noted as either "safety-critical" (SC) or "non safety-critical" (NSC). The Safety Assurance Concepts being applied to prevent hazards are also identified in Table 6.

5.2.1 I-ETMS Functionality

Table 5 – Safety Assurance Concepts

Safety Assurance Concepts	Definition	Technique
Checked-Redundancy (IEEE 1483-2000, A.1.2.2)	The concept of Checked-Redundancy is typified by the use of two or more identical, independent hardware units, executing identical software and performing identical functions. A means is provided to periodically compare safety critical parameters and results of the independent redundant units, requiring agreement of compared parameters to assert or maintain a permissive output. If the units do not agree, safety critical functions and outputs default to a known safe state.	**Independent Processing** This technique uses identical processors with cross-checked software to protect against random failures. Software on each processor exchanges safety critical parameters for comparison. If software determines a parameter to be out of tolerance, a failure is declared and a safe response is taken. **Data Redundancy** Data Redundancy requires storing data in multiple independent locations and comparing the data to detect errors. Equivalently, the redundant data can drive redundant processes and comparison of the output identifies the existence of errors.
Diversity and Self-Checking (IEEE 1483-2000, A.1.2.4)	This concept requires that all critical functions be performed in diverse ways, using diverse software operations and/or diverse hardware channels, and that critical hardware be tested with self-checking routines. Permissive decisions are allowed only if the results of the diverse operations correspond and the self-checking reveals no failures.	**Algorithmic Diversity** Algorithmic Diversity sends the input data streams to different algorithms with different failure modes. The outputs of the algorithms are compared to determine if an error exists. Error detections result in flagging the output invalid and appropriate safe action is taken. Algorithmic Diversity protects against errors in algorithm definition and execution. **Data Source Diversity** Data Source Diversity uses multiple inputs with

Safety Assurance Concepts	Definition	Technique
		independent failure modes to determine parameters or states used in decision processes. Inconsistencies detected result in appropriate safe actions. Data Source Diversity protects against errors in a single data source. **Self-Checking Codes (IEC 61508-7, A.4.4)** This technique requires that transmitted safety critical data is monitored to ensure its integrity. Implementation examples of this safety assurance concept take the form of a Cyclic Redundancy Checks (CRC) or hash codes. Permissive decisions are allowed only if the calculated checking code agrees with the transmitted checking code. **Watchdog Timers / Avoidance of Action (IEC 61508-7, A.9.1 and A.9.2)** This concept has two related implementations. The use of hardware and software Watchdog Timers requires that timing elements with a separate time base (a hardware clock or a software process that references the system clock at intervals) are periodically triggered to monitor the computer's behavior and the plausibility of the program sequence. An upper limit is given for the watchdog timer. If the program sequence takes a longer time than expected, the timer causes the subsystem to terminate processing and transition to a safe state. Avoidance of Action requires that the system be designed to transfer to a more restrictive state unless keep-alive signals are received at specific modules within the system. **Defensive Programming / Reasonableness Checks / Range Checking (IEC 61508-7, C.2.5)** This concept requires that safety critical data is monitored to ensure that it is consistent compared with its previous values and also reasonable when compared with expected ranges and potentially other associated data. Permissive decisions are allowed only if the safety critical data is both consistent and reasonable. **Information Redundancy / Closed Loop Segment-to-Segment Cross Checking (IEC 61508-7, A.7.6)** Messages between segments require acknowledgment of successful receipt. **Information Redundancy / Data Association (Similar to IEC 61508-7, A.7.6)** Data transmissions incorporate elements that can be associated with other data at the destination to ensure correctness. **Information Hiding / Encapsulation (IEC 61508-7, C.2.8)** IEC 61508-7 describes this concept as follows: "Data that is globally accessible to all software components can be accidentally or incorrectly

Safety Assurance Concepts	Definition	Technique
		modified by any of these components. Any changes to these data structures may require detailed examination of the code and extensive modifications. Information hiding is a general approach for minimizing these difficulties. The key data structures are 'hidden' and can only be manipulated through a defined set of access procedures. This allows the internal structures to be modified or further procedures to be added without affecting the functional behavior of the remaining software. For example, a name directory might have access procedures insert, delete and find. The access procedures and internal data structures could be re-written (for example to use a different look-up method or to store the names on a hard disk) without affecting the logical behavior of the remaining software using these procedures." **Stale Data Rejection** Due to the nature of the processing and communication methods of PTC, it is possible for messages to be received late. When messages are received too late, the information could be stale or if received out of sequence, could even be incorrect. To prevent this all messages are time tagged, and if a message is received too late, after accounting for normal communications delay, the message will be overtly rejected and the receiver will take no other action based on stale data. A second aspect of this technique is used on periodic data. Parameters will remain valid for a defined period of time. If the parameter is not refreshed before it times out, the data will be marked invalid and will not be consumed by the system.
Intrinsic Fail-Safe Design (IEEE 1483-2000, A.1.2.1)	This concept addresses the design of fail-safe hardware circuits or systems employing discrete mechanical and/or electrical components. Verification of fail-safe operation for systems designed using this concept requires the application of Failure Modes and Effects Analysis (FMEA).	Failure of a safety critical function is either detectable or results in a safe system state. No single failure will prevent an unsafe event. Circuitry should use simple, analyzable components; no complex devices should be used. Non-Self reveling will be real-time testable to minimize exposure time. Redundant circuitry should be physically separated and isolated from each other. Combinations of critical signal states are deterministic; deviation from a valid state defaults to a safe state.

Table 6 – I-ETMS Functionality

Function	Functional Description	Safety Assurance Concepts
Power Up and Diagnostics (Safety Critical)	• I-ETMS Power Up and Diagnostics functionality includes internal system tests executed to ensure the system is functioning	• Diversity and Self Checking: The Locomotive Segment monitors itself for failed and incorrectly installed hardware.

Function	Functional Description	Safety Assurance Concepts
	as intended and ready to proceed to Initialization.	(Reference Section 3.4: The Locomotive Segment includes…)
Initialization (Safety Critical)	• Initialization occurs when a train crew arrives onboard or at the start of an I-ETMS equipped train's trip over an I-ETMS track segment. • Initialization with multiple railroads, if required, occurs during the Initialization process. • The I-ETMS Initialization process includes software version and configuration file verification, crew authorization, consist verification, Train ID verification, identification of intended route of a train based upon Train ID, and an I-ETMS Departure Test, if required.	• Diversity and Self Checking: The Locomotive Segment verifies that software and configuration files are valid as defined by the Office Segment. (Reference Section 3.2.1: The Office Segment will…) • Diversity and Self Checking: Crew's credentials are authenticated by an external back office system. (Reference Section 9.3: The locomotive I-ETMS…) • Diversity and Self Checking: Consist data is range checked. (Reference Section 4.2: In addition to train type…)
Consist (Safety Critical)	• Train consist information is displayed to the crew for viewing and modification prior to confirmation of accuracy.	• Diversity and Self Checking: Consist data is range checked. (Reference Section 4.2: In addition to train type…)
File Download (Safety Critical)	• Software, Configuration, and Track Files are capable of being downloaded from the Office Segment to the Locomotive Segment.	• Diversity and Self Checking: Software, Configuration, and Track files downloaded from the Office Segment to the Locomotive Segment contain a MD5 hash that is validated before use. (Reference Section 6.1: The Locomotive Segment receives…)
Departure Test (Safety Critical)	• The I-ETMS Departure Test includes the execution of a series of tests, including a penalty brake application, to ensure the system is operational prior to departure.	• Diversity and Self Checking: Locomotive Segment requires successful completion of a PTC initiated full service brake application to insure the Locomotive Segment can apply a penalty brake application. (Reference Section 5.6.2: I-ETMS provides the capability…)
I-ETMS System Synchronization (Safety Critical)	• Synchronization of data between the Office Segment and the dispatching system is managed with a message exchange protocol between systems to minimize synchronization problems and ensure detection of those synchronization problems that occur. Upon occurrence of a message exchange protocol violation or other anomaly which leaves the dispatching system or Office Segment incapable of positively assuring all data is synchronized, the Office Segment downgrades from its most permissive explicit control operating mode to a more restrictive non-explicit control operating mode. • The I-ETMS system detects data discrepancies between the Office Segment and the Locomotive Segment through "heartbeat" messaging protocol. Detection of an anomaly causes I-ETMS to attempt to resynchronize data and to disengage if the data anomaly could impact the train at its current location. • A configurable time tolerance threshold is set to allow for detection of a data	• Diversity and Self Checking: A closed loop process verifies the Office Segment possesses the current set of bulletins and authorities from the railroads back office systems. (Reference Section 5.5.7.3: Upon receipt of a valid heartbeat...) • Diversity and Self Checking: A closed loop process verifies the Locomotive Segment possesses the current set of bulletins and authorities from the Office Segment. (Reference Section 6.1: The Locomotive Segment receives…) • Diversity and Self Checking: Switch and signal data received peer-to-peer from the Wayside Segment remains valid for a limited time within the Locomotive Segment. (Reference Section 11.1: The Locomotive Segment track…)

Function	Functional Description	Safety Assurance Concepts
	synchronization failure between a Wayside Segment device and the Locomotive Segment. Failure to receive an update within the threshold period causes I-ETMS to assume the wayside device is in its most restrictive state.	
Location Determination & Navigation (Safety Critical)	• The I-ETMS Location Determination function resolves a train's location to mapped track. • I-ETMS Location Determination function provides a means of selecting the train's location when multiple track solutions may be available. • The I-ETMS Navigation function calculates the train's route when moving. • The I-ETMS system provides defined system and display behavior to safely handle situations where the Locomotive Segment is unable to locate the train on surveyed track.	• Checked Redundancy: The Locomotive Segment independently calculates a train location on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…)
Warning and Braking Calculation (Safety Critical)	• Locomotive Segment continuously monitors train speed and proximity to speed restrictions or authority limits (considered zero-speed restrictions) in advance of the train. • Locomotive Segment establishes a train's route and authorized speed profile. • Locomotive Segment uses train data and track profile data from the track data base to establish a conservative braking curve based on current train configuration, an "if brakes were applied now" brake profile. • Locomotive Segment accounts for any acceleration or deceleration and calculates an "if brakes were applied in XX seconds" brake profile which is combined with the predicted distance traveled in those XX seconds to provide the warning distance.	• Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…)
Territory Entrance Protection (Safety Critical)	• The I-ETMS system provides warning and enforcement protection at entrance to territory where I-ETMS is in effect. • Territory Entrance protection requires that the I-ETMS system be initialized and fully active sufficiently in advance of approaching the territory boundary.	• Diversity and Self Checking: A closed loop process verifies the Office Segment possesses the current set of bulletins and authorities from the railroads back office systems. (Reference Section 5.5.7.3: Upon receipt of a valid heartbeat...) • Diversity and Self Checking: A closed loop process verifies the Locomotive Segment possesses the current set of bulletins and authorities from the Office Segment. (Reference Section 6.1: The Locomotive Segment receives…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's

Function	Functional Description	Safety Assurance Concepts
		Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Protection of Movement Authority provided by Mandatory Directive in ABS or Non-ABS Territory (Safety Critical)	• The I-ETMS system protects train and engine movement in accordance with movement authority held by the train or engine and enforces on-track authority limits and any restrictive conditions imposed upon the authority. • The text of a movement authority is displayed by the Locomotive Segment upon request. • Movement authority provided by mandatory directive is delivered to the Locomotive Segment while the train or engine is en-route or after Initialization.	• Diversity and Self Checking: A closed loop process verifies the Office Segment possesses the current set of bulletins and authorities from the railroads back office systems. (Reference Section 5.5.7.3: Upon receipt of a valid heartbeat...) • Diversity and Self Checking: A closed loop process verifies the Locomotive Segment possesses the current set of bulletins and authorities from the Office Segment. (Reference Section 6.1: The Locomotive Segment receives…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Temporary Speed Restriction Protection (Safety Critical)	• Predictive enforcement of Temporary Speed Restrictions (TSR) by the I-ETMS system accounts for all attributes of a TSR including time in effect and applicability to entire train or head-end only. • The text of a TSR is displayed by the Locomotive Segment upon request. • TSR data is delivered to the Locomotive	• Diversity and Self Checking: A closed loop process verifies the Office Segment possesses the current set of bulletins and authorities from the railroads back office systems. (Reference Section 5.5.7.3: Upon receipt of a valid heartbeat...) • Diversity and Self Checking: A closed loop process verifies the Locomotive Segment

Function	Functional Description	Safety Assurance Concepts
	Segment while the train or engine is en-route or after Initialization.	possesses the current set of bulletins and authorities from the Office Segment. (Reference Section 6.1: The Locomotive Segment receives…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Work Zones Protection (Safety Critical)	• The I-ETMS system predictively protects temporal and spatial work zone limits with warning and ultimately enforcement upon failure to obtain permission before entering or moving within the limits of the work zone. • The I-ETMS system reactively enforces unauthorized train or engine movements within the limits of active work zones. • The presence and location of the work zone are continuously displayed to the train crew, even after the train crew has indicated authority to enter its limits. • The text of a Work Zone bulletin is displayed by the Locomotive Segment upon request. • Work Zone data is delivered to the Locomotive Segment while the train or engine is en-route or after Initialization.	• Diversity and Self Checking: A closed loop process verifies the Office Segment possesses the current set of bulletins and authorities from the railroads back office systems. (Reference Section 5.5.7.3: Upon receipt of a valid heartbeat...) • Diversity and Self Checking: A closed loop process verifies the Locomotive Segment possesses the current set of bulletins and authorities from the Office Segment. (Reference Section 6.1: The Locomotive Segment receives…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple,

Function	Functional Description	Safety Assurance Concepts
		analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Advisory or Cautionary Notices Protection (Safety Critical)	• Advisory or Cautionary Notices contain non-enforceable textual data provided by the dispatching system to advise train and engine crew members of changes in operating rules or practices, changes to the physical track structure or hazards that may exist along the wayside. • Advisory or Cautionary Notices are displayable by the Locomotive Segment upon request. • Advisory or Cautionary Notices are delivered to the Locomotive Segment while the train or engine is en-route or after Initialization.	• Diversity and Self Checking: A closed loop process verifies the Office Segment possesses the current set of bulletins and authorities from the railroads back office systems. (Reference Section 5.5.7.3: Upon receipt of a valid heartbeat...) • Diversity and Self Checking: A closed loop process verifies the Locomotive Segment possesses the current set of bulletins and authorities from the Office Segment. (Reference Section 6.1: The Locomotive Segment receives…)
Protection of Notice of Highway Crossing Warning System Malfunction (Safety Critical)	• The I-ETMS system protects the limits of a rail-highway crossing upon receipt of a mandatory directive that is associated with a failure or false activation of the crossing warning system. • As each train approaches and is within a defined threshold distance of the highway crossing, a manual input indicating that flagging protection has been establish may be provided, causing I-ETMS to allow that train to move through the crossing in accordance with the restrictions prescribed by the applicable operating rules. The restriction remains in effect for each subsequent train approaching the highway crossing. • The text of a Notice of Highway Crossing Warning System Malfunction is displayed by the Locomotive Segment upon request. • Notice of Highway Crossing Warning System Malfunction is delivered to the Locomotive Segment while the train or engine is en-route or after Initialization.	• Diversity and Self Checking: A closed loop process verifies the Office Segment possesses the current set of bulletins and authorities from the railroads back office systems. (Reference Section 5.5.7.3: Upon receipt of a valid heartbeat...) • Diversity and Self Checking: A closed loop process verifies the Locomotive Segment possesses the current set of bulletins and authorities from the Office Segment. (Reference Section 6.1: The Locomotive Segment receives…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Protection of Notice of Track Out of Service (Safety Critical)	• The I-ETMS system predictively protects the limits of an out of service track until such time as the track is restored to service and the corresponding Notice of Track Out of Service Bulletin is voided and delivered to the	• Diversity and Self Checking: A closed loop process verifies the Office Segment possesses the current set of bulletins and authorities from the railroads back office systems. (Reference Section 5.5.7.3: Upon

Function	Functional Description	Safety Assurance Concepts
	Locomotive Segment. • The text of a Notice of Track Out of Service Bulletin is displayed by the Locomotive Segment upon request. • Notice of Track Out of Service is delivered to the Locomotive Segment while the train or engine is en-route or after Initialization.	receipt of a valid heartbeat...) • Diversity and Self Checking: A closed loop process verifies the Locomotive Segment possesses the current set of bulletins and authorities from the Office Segment. (Reference Section 6.1: The Locomotive Segment receives…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Critical Alert Protection (Safety Critical)	• The I-ETMS system protects any enforceable limits contained in Critical Alert notifications, such as locations where severe weather or flooding may create hazardous conditions or when notification of equipment anomaly indicated by train defect detector is received. • The text of Critical Alerts is displayed by the Locomotive Segment upon request. • Critical Alert notifications may include enforceable limits or text only and are delivered to the Locomotive Segment while the train or engine is en-route or after initialization. When enforceable limits are included in the critical alert, I-ETMS will enforce them as specified. When no enforceable limits are included, the text of the critical alert may be displayed, but no enforceable conditions are specified.	• Diversity and Self Checking: A closed loop process verifies the Office Segment possesses the current set of bulletins and authorities from the railroads back office systems. (Reference Section 5.5.7.3: Upon receipt of a valid heartbeat...) • Diversity and Self Checking: A closed loop process verifies the Locomotive Segment possesses the current set of bulletins and authorities from the Office Segment. (Reference Section 6.1: The Locomotive Segment receives…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …)

Function	Functional Description	Safety Assurance Concepts
		• Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Permanent & Equipment Speed Enforcement (Safety Critical)	• The I-ETMS system provides enforcement of the following defined speed limits: permanent speed restrictions as contained in the Timetable or Special Instructions, including turnout speed restrictions; consist, equipment or lading speed restrictions, as delivered during Initialization or entered directly by the train crew. • The I-ETMS system predictively enforces permanent speed restrictions in advance of the train, with a warning consisting of a visual alert accompanied at the start by a momentary audible alert prior to enforcement. • The I-ETMS system reactively enforces over speed conditions by providing audible and visual alerts (no specific duration) during an over speed event until the enforcement threshold is reached or train speed is reduced to comply with the speed limit.	• Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Wayside Signal Indication Enforcement (Safety Critical)	• The I-ETMS system predictively enforces signal indications requiring a stop, and signal indications requiring reduced or restricted speed with a warning consisting of a visual alert accompanied at the start by a momentary audible alert prior to enforcement • The Wayside Segment will beacon switch and signal data to the Locomotive Segment peer-to-peer. • The Locomotive Segment may register for and receive switch position and signal indications (stop/not stop) from the Office Segment.	• Diversity and Self Checking: Switch and signal data received peer-to-peer from the Wayside Segment remains valid for a limited time within the Locomotive Segment. (Reference Section 11.1: The Locomotive Segment track…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Intrinsically Fail-Safe Design: Failures of the Wayside Segment's Interface result in a safe state. (Reference Section 11.1: The Locomotive Segment track…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes

Function	Functional Description	Safety Assurance Concepts
		redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Switch Protection (Safety Critical)	• In non-signaled territory, the I-ETMS system protects equipped train movement over monitored switches (switches that interface directly to a Wayside Interface Unit (WIU) device) and over unmonitored switches protected by signals by enforcing a stop before the train moves over a switch whose position is unknown or improperly lined for the movement to be made. In some cases, hand-operated switches in non-signaled territory will be interconnected with track circuits. When a track circuit indicates the conditions in the block are not favorable, all switches are assumed to be in improper position for train movement and enforcement of Restricted Speed throughout the block is provided accordingly. • In signaled territory, the I-ETMS system provides protection for monitored switches whose alignment is unknown, and for switches whose alignment is inconsistent with the train's current authority. • The Wayside Segment will beacon switch and signal data to the Locomotive Segment peer-to-peer. • The Locomotive Segment may register for and receive switch position and signal indications (stop/not stop) from the Office Segment.	• Diversity and Self Checking: Switch and signal data received peer-to-peer from the Wayside Segment remains valid for a limited time within the Locomotive Segment. (Reference Section 11.1: The Locomotive Segment track…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Intrinsically Fail-Safe Design: Failures of the Wayside Segment's Interface result in a safe state. (Reference Section 11.1: The Locomotive Segment track…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Track Circuit Enforcement (Safety Critical)	• The I-ETMS system predictively enforces the limits of track circuits which indicate a condition such as a broken rail or occupancy by another train. The I-ETMS system reactively enforces restricted speed within the limits of a track circuit indicating such a condition.	• Diversity and Self Checking: Switch and signal data received peer-to-peer from the Wayside Segment remains valid for a limited time within the Locomotive Segment. (Reference Section 11.1: The Locomotive Segment track…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Intrinsically Fail-Safe Design: Failures of the Wayside Segment's Interface result in a safe state. (Reference Section 11.1: The Locomotive Segment track…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to

Function	Functional Description	Safety Assurance Concepts
		prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Cab Signal Indication Enforcement (Safety Critical)	• Within CAB signal territory, the I-ETMS system predictively enforces CAB signal indications requiring reduced or restricted speed, with a warning consisting of a visual alert accompanied at the start by a momentary audible alert prior to enforcement. • The Locomotive Segment senses when the locomotive CAB signal system is cut-out, partially cut-out, or cut-in and operational for Automatic Cab Signal (ACS) or Automatic Train Control (ATC).	• Diversity and Self Checking: The Cab Signal input is received by redundant circuitry; each lane independently produces different parts of a message used by the redundant processors. (Reference Section 3.4.1.3: Where I-ETMS is integrated…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Reverse Movement Enforcement (Safety Critical)	• For a train making a reverse movement, the I-ETMS system provides enforcement of signal indications, authority limits, and permanent or temporary speed restrictions in accordance with the applicable railroad operating rules.	• Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …)

Function	Functional Description	Safety Assurance Concepts
		• Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Switching State Enforcement (Safety Critical)	• Switching State is a Locomotive operational state to allow the train to perform switching work on a controlled track in a practical manner without requiring the system to be completely disengaged or cut-out.	• Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Notification of Authority Violation by another Train (Non-Safety Critical)	• Violator report of authority violation is sent to the Office Segment. • Office Segment forwards the violation report to all Locomotives whose clearance includes the subdivision/district where the violation report originated. • Locomotive Segment warning to the violated train is provided for violations detected behind the violated train. • Locomotive Segment warning and braking are provided to the violated train for violations ahead of the violated train.	• (If violation is received by the Locomotive Segment it will be handled in a vital manner.) (Reference Section 5.6.1: Failure to invoke…) • Checked Redundancy: The Locomotive Segment independently calculates a train location, speed, braking distance, and next enforceable target on redundant processors and cross channel compares the results. (Reference Section 11.2: Each processor receives…) • Diversity and Self Checking: Locomotive's Brake Interface requires periodic data to prevent enforcement. (Reference Section 11.2: Communication between individual…) • Diversity and Self Checking: Locomotive's Brake Interface periodically self checks enforcement circuitry. (Reference Section 3.4.1.4: Penalty Brake Interface …) • Intrinsically Fail-Safe Design: The Locomotive's Brake Interface utilizes redundant, independent paths of simple, analyzable components to hold off penalty brake application. (Reference Section 3.4.1.4: The I-ETMS Brake Interface Module …)
Crew Authority	• Crew may request new, rollup, time	

Function	Functional Description	Safety Assurance Concepts
Requests (Non-Safety Critical)	extension, and release of authority limits.	
Cut-Out State (Non-Safety Critical)	• In the event of a critical failure, the Locomotive Segment is able to be electrically isolated until repaired or replaced.	
Territory Exit (Non-Safety Critical)	• The I-ETMS system provides notification at exit from territory where I-ETMS is in effect.	
Horn Activation (Non-Safety Critical)	• The Locomotive Segment provides automatic horn activation in the event that a locomotive engineer fails to sound the horn in approach to a public highway grade crossing when required.	
Parking Brake (Non-Safety Critical)	• The I-ETMS system parking brake function provides a means, which may be used in addition to other methods required by rule or law, to secure the locomotive and train from unintended movement. • When the parking brake function is invoked, the locomotive is monitored for movement and when nominal locomotive movement is detected for a period in excess of a threshold time, the Locomotive Segment commands a full-service penalty brake application.	
Train Handling and Energy Management Assistance (Non-Safety Critical)	• Through an optional interface with Energy Management software suites (e.g. NYAB LEADER® or GE's Trip Optimizer™), the I-ETMS system supports the display of an operating profile for fuel efficient operation of the train based upon terrain, train dynamics, speed restrictions, and the train's authority limits. • In prompting mode, the Locomotive Segment displays Energy Management information locomotive control setting prompts in designated sections of the display but takes no further action. • In cruise-control mode, the I-ETMS Locomotive displays Energy Management information in designated sections of the display and executes the locomotive control settings provided by EM in a manner that is independent from and in no way preempts the train control and enforcement functions provided by I-ETMS.	
Logging (Non-Safety Critical)	• The Office and Locomotive Segments log data into memory and supports log retrieval for analysis or playback. • An external event recorder as required by §236.1005(d) is included.	
File Upload (Non-Safety Critical)	• Locomotive Segment log files are uploaded to the Office Segment.	
Train Operation Exception Reporting (Non-Safety Critical)	• The Locomotive Segment monitors train speed, location, and locomotive control settings in order to detect exceptions to train-	

Function	Functional Description	Safety Assurance Concepts
	handling as defined by a railroad's air brake and train handling rules. • Train handling exceptions are configurable and are specific to a railroad's air brake and train handling rules.	
Switch Position Awareness (Non-Safety Critical)	• The Office Segment monitors WIU status reports and relays switch position to the dispatching system. • The Office Segment will assume a wayside device is in its most restrictive state when a data refresh does not occur within a defined tolerance.	
Crew Logoff (Non-Safety Critical)	• The crew logs off at the end of an I-ETMS equipped train's trip over an I-ETMS track segment. • The Crew Logoff function discards employee ID and PIN, clearance number, and Train ID at the end of an I-ETMS equipped train's trip. • The Locomotive system state is set to Cut Out which sends notification to the Office Segment indicating the Locomotive is no longer controlling.	

5.3 I-ETMS Support for Railroad Interoperability

I-ETMS interoperability is achieved through the specification and implementation of standard behavioral components which communicate with each other via standard interfaces. The Locomotive Segment communicates continuously and simultaneously with the Office Segment infrastructure that governs the I-ETMS-controlled track of each railroad which the equipped I-ETMS train will traverse during the trip of a particular train crew, regardless of locomotive owner or operator.

During Locomotive Segment initialization, the railroads over which the train will operate are selected from a list. The Locomotive Segment requests all applicable track segment data from the Office Segment of each selected railroad that encompasses the route that the crew will traverse during their normal tour of duty. Should the route change while the train is en route, additional track segment data will be served to the Locomotive Segment before that track segment is traversed. I-ETMS will prevent entry into any subdivision or district PTC track segment in the known route of the train that has not been initialized.

Once initialized; the Locomotive Segment communicates *continuously and concurrently* with the Office Segment of each railroad over which the train will operate; all data needed to cross a railroad boundary is thus onboard and current before the train actually reaches the boundary and no special "hand-off" processing is required at that time. This approach is premised on existing railroad operations – a train's movement may be simultaneously governed by mandatory directives, signal aspects, and rules from multiple railroads as it nears a transition point. For example, a train operating on a CLEAR signal indication on one railroad may be approaching the limits of another road

– where a temporary speed restriction is in effect. I-ETMS will display and provide predictive enforcement of the speed restriction before the train actually crosses an interline boundary.

Interoperability between the Locomotive Segment and the Wayside Segment for any combination of I-ETMS-equipped locomotive and track segment ownership is provided through use of a WIU behavior and communications/messaging protocol standard. This standard protocol combination is utilized by each I-ETMS-compatible WIU and Locomotive Segment, regardless of track segment operator, locomotive ownership, or wayside segment component manufacturers. Wayside devices, their location, and associated WIU information are identified in the track data for each track segment on which I-ETMS is operative.
The I-ETMS interoperability architecture is depicted in Figure 15.

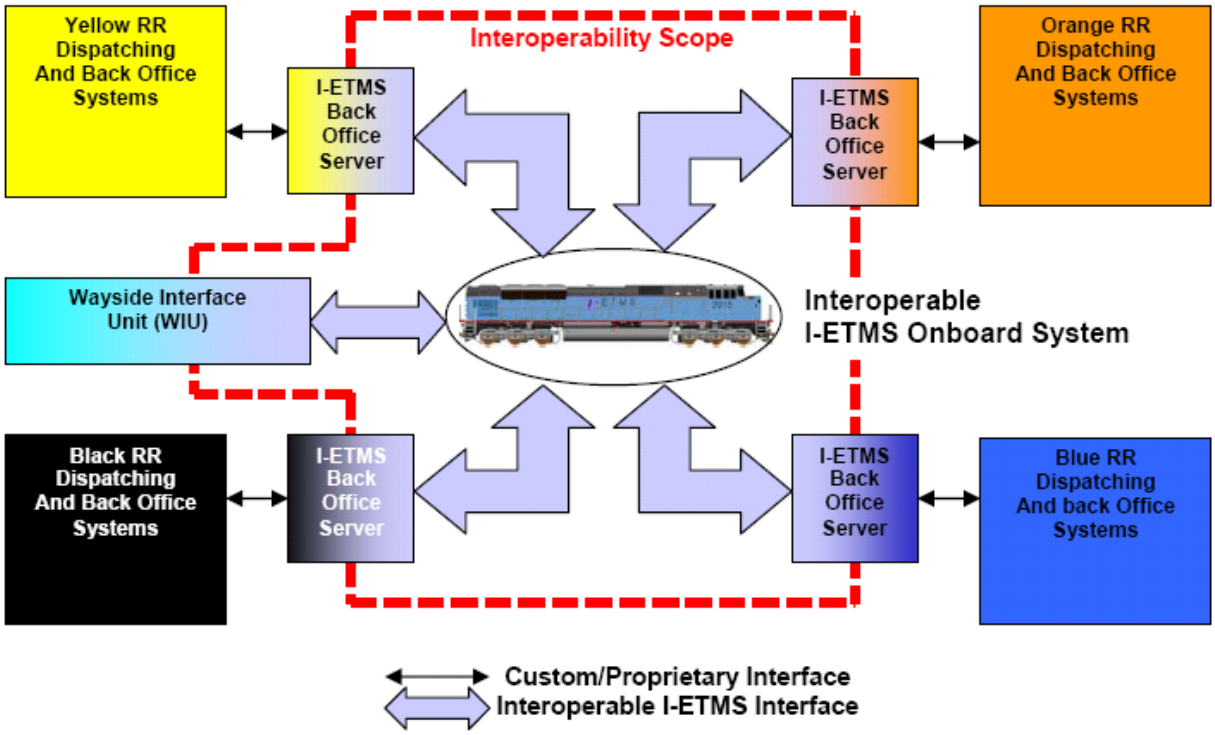

Figure 15 – I-ETMS Interoperability Architecture

Figure 16 depicts a typical I-ETMS interoperability scenario.

- The train crew, employed by the GREEN railroad, has previously completed initialization of the I-ETMS system on the BLUE locomotive for operation of RED subs A and B, BLUE subs A and B, and GREEN subs A and B;
- The BLUE locomotive continuously communicates with back office infrastructures of each railroad with which it initialized, regardless of its proximity to the respective subdivisions controlled by those back office infrastructures;
- Within a railroad, the operating data for various subdivisions may be hosted on multiple back office servers;
- The BLUE locomotive talks to all WIUs on its route, regardless of their affiliation with a particular railroad or subdivision.

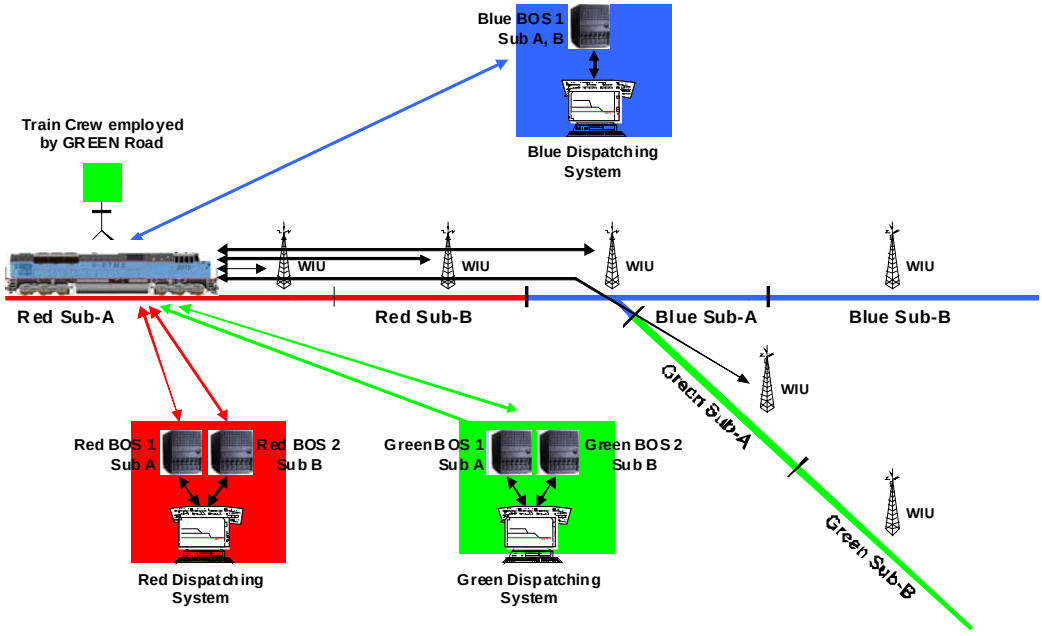

Figure 16 – I-ETMS Typical Interoperability Scenario

5.4 Existing Non-PTC Operations and Systems

This section describes railroad operations and systems that are conducted without I-ETMS. Railroad Train Dispatchers and Control Operators utilize computer-aided dispatching systems to supervise the movement of trains, engines, and employees on their respective rail networks. The current Methods of Operation rely on employees to observe and comply with signal indications, authority limits, and speed limits to provide a safe operating environment.

5.4.1 Operational Policies and Constraints

Railroad operations are governed by each road's respective Operating Rules, Special Instructions, General and Operations Bulletins, Air Brake and Train Handling Rules, and Timetables.

Timetables and General and Operations Bulletins are typically issued by and on the authority of the Operating Department.

5.4.2 Methods of Operation

North American railroads utilize four primary Methods of Operation: Traffic Control (TC), Current of Traffic (COT), Track Warrant Control (TWC), and Yard or Restricted Limits (YL or RL). The Method of Operation on a particular portion of the railroad and/or designated tracks is specified in the timetable. The I-ETMS system described in this document is intended to support these four primary Methods of Operation and accommodate certain variations in their implementation by railroads.

5.4.2.1 Traffic Control

On portions of the railroad, and on designated tracks so specified in the timetable, trains will be governed by block and interlocking signals, whose indications will supersede the superiority of trains for both opposing and following movements on the same track. Traffic Control (TC) may be used on single or multiple main tracks. Automatic Cab Signals (ACS) or Automatic Train Control (ATC), which are not Methods of Operation, may be used where TC is in effect.

Movement of trains or engines will be supervised by the train dispatcher who may also operate the signal office control machine. Trains or engines must not enter TC territory unless the governing signal displays a proceed indication, authority is obtained from the control operator, or the train crew has operated all wayside appliances and conformed to operating rules at a location between signals. The office control machine (subsystem of the dispatching system) is the interface to the field signal system. Switch and signal controls are generated by the office control machine in response to train dispatcher or dispatching system requests and transmitted to the field. Switch and signal indications are received from the field. Switch, signal, and track state derived from these controls and indications are displayed in the office and used by the movement planner to facilitate the movement of trains. Non-vital edit checking of signal control requests is performed in the office control machine. Vital checking of signal control requests is performed by the field signal system.

The train dispatcher or control operator may issue track authority to an employee authorizing occupancy of a track or tracks within specified limits of a Controlled Point or Manual Interlocking between specified times. Prior to issuing such authority, the train dispatcher or control operator will establish a block such that no controlled signal at the limits of the authority can be cleared. This prevents inadvertent authorization of a train into the limits of the authority. When such track authority is issued, the instructions must be copied by the requesting employee on the prescribed form, and repeated to the train dispatcher or control operator. Upon successful repeat, the train dispatcher or

control operator will give the OK time, at which time the track authority becomes effective. A track authority must be released to the train dispatcher or control operator when the employee is clear of the limits and will not require further authority.

The train dispatcher or control operator may grant track authority to a train, engine, or employee authorizing occupancy of a track or tracks within specified limits and between specified times. Within exclusive track authority limits, trains or engines may move in either direction at maximum authorized speed, subject to signal indication. Within joint track authority limits, trains or engines may move in either direction and all movements must be made at Restricted Speed. When track authority is granted, the instructions must be copied by the requesting employee on the prescribed form, and repeated to the train dispatcher or control operator. Upon successful repeat, the train dispatcher or control operator will give the OK time, at which time the track authority becomes effective. A track authority must be released to the train dispatcher or control operator when train, engine, or employee is clear of the limits and will not require further authority.

5.4.2.2 Current of Traffic

On portions of the railroad, and on designated tracks so specified in the timetable, trains will run with reference to other trains in the same direction by block and interlocking signals whose indications will supersede the superiority of trains. Current of Traffic (COT) is generally used on Double Track. Automatic Cab Signals or Automatic Train Control, which are not Methods of Operation, may be used where COT is in effect.

Movement of trains or engines will be supervised by the train dispatcher who may also operate the signal office control machine. Trains or engines must not enter COT territory unless the governing signal displays a proceed indication, authority is obtained from the control operator, or the train crew has operated all wayside appliances and conformed to operating rules at a location between signals. The office control machine provides an interface to the field signal system at selected interlocking locations. Switch, signal, and track indications outside of interlocking limits may not be available in the dispatching system. Switch and signal controls are generated by the office control machine in response to train dispatcher or dispatching system requests and transmitted to the field. Switch and signal indications are received from the field. Switch, signal and track state derived from these controls and indications are displayed in the office and used by the movement planner to facilitate the movement of trains. Non-vital edit checking of signal control requests is performed in the office control machine. Vital checking of signal control requests is performed by the field signal system.

The train dispatcher or control operator may grant track authority to an employee authorizing occupancy of a track or tracks within specified limits of a Manual Interlocking between specified times. When such track authority is granted, the instructions must be copied by the requesting employee on the prescribed form, and repeated to the train dispatcher or control operator. Upon successful repeat, the train dispatcher or control operator will give the OK time, at which time the track authority becomes effective. A

track authority must be released to the train dispatcher or control operator when the employee is clear of the limits and will not require further authority.

To authorize movement against the current of traffic or bi-directional movement, the train dispatcher may grant Track authority to a train, engine, or employee authorizing occupancy of a track or tracks within specified limits and between specified times. Within Exclusive Track authority limits, trains or engines may move in either direction at maximum authorized speed, subject to signal indication. Within Joint Track authority limits, trains or engines may move in either direction and all movements must be made at Restricted Speed. When Track authority is granted, the instructions must be copied by the requesting employee on the prescribed form, and repeated to the train dispatcher or control operator. Upon successful repeat, the train dispatcher or control operator will give the OK time, at which time the Track authority becomes effective. Track authority must be released to the train dispatcher or control operator when train, engine, or employee is clear of the limits and will not require further authority.

5.4.2.3 Track Warrant Control

The terms "Track Warrant Control" or "Track Warrant" and the acronym "TWC" are used generically in this document to refer to a Method of Operation where movement authority may be granted to train, engine, or employee only by the Train Dispatcher or Control Operator and conveyed by Mandatory Directive.

On portions of the railroad, and on designated tracks so specified in the timetable, trains, engines, or employees will be governed by Track Warrant authority for both opposing and following movements on the same track. A Track Warrant may authorize movement in one direction or both directions. Track Warrant Control (TWC) may be used on single or multiple main tracks. Track Warrant Control may be used with or without an Automatic Block Signal (ABS) system. Automatic Cab Signals or Automatic Train Control, which are not Methods of Operation, may be used where TWC/ABS is in effect.

Movement of trains or engines will be supervised by the train dispatcher. Trains or engines must not enter TWC territory unless authority is obtained from the train dispatcher. The train dispatcher may grant Exclusive or Joint Track Warrant authority to train, engine or employee authorizing occupancy of a track or tracks within specified limits. Within Exclusive Track Warrant limits, trains or engines may move in the authorized direction at maximum authorized speed, subject to signal indication in TWC/ABS territory. Within Joint Track Warrant limits, trains or engines may move in the authorized direction and all movements must be made at Restricted Speed.

The train dispatcher may verbally grant Track Warrant authority to a train, engine, or employee authorizing occupancy of a track or tracks within specified limits and between specified times. When Track Warrant authority is granted, the instructions must be copied by the requesting employee on the prescribed form, and repeated to the train dispatcher. Upon successful repeat, the train dispatcher will give the OK time, at which time the Track Warrant becomes effective. Track Warrant authority must be released to

the train dispatcher when train, engine, or employee is clear of the limits and will not require further authority.

5.4.2.4 Yard Limits / Restricted Limits

On portions of the railroad, and on a Main Track or other designated tracks so specified in the timetable, trains, engines, or employees will be governed by Yard Limits or Restricted Limits rules. Within Yard or Restricted Limits all movements must be made at Restricted Speed, unless railroad Operating Rules and/or signal indication permit a higher speed. Entry to Yard Limits may require verbal permission from the train dispatcher or control operator.

5.4.3 Track Bulletin System

The term "Track Bulletin" is used generically in this document to refer to a temporary speed restriction, work zone or miscellaneous restriction or message issued by Mandatory Directive.

The Track Bulletin system provides the train dispatcher with the capability to issue or void individual track bulletins which affect the movement of trains. Each Track Bulletin is assigned a unique identifier by the dispatching system. The dispatching system uses this identifier to track delivery of Track Bulletins to each affected train or cancellation of a Track Bulletin. Track bulletins fall into three general categories.

5.4.3.1 Temporary Speed Restrictions

These track bulletins are created in the dispatching system to advise train crews of those conditions which require a reduction of timetable train speeds. Temporary Speed Restrictions may be addressed to all trains. Temporary Speed Restrictions identify the spatial limits of the restriction, the maximum authorized speed, the tracks to which the restriction applies, the effective dates and times and whether the restriction applies to the whole train or to the head-end only.

5.4.3.2 Work Zones

These track bulletins are created in the dispatching system to identify specific locations where a train crew must obtain authorization from an Employee-In-Charge (EIC) in order to enter and proceed through the work zone limits. Work zones are bulletined in effect between specific milepost locations and times, and are used to protect Roadway Workers, large scale production gangs etc., performing maintenance, or working on or about the track. Authority to enter and move within the limits of a Work Zone may only be granted by the EIC specified in the track bulletin and must be repeated by the employee receiving authorization. The EIC may impose restrictions upon train movement within the limits of a Work Zone, such as a reduction in speed, or a requirement to stop at a particular location. Trains may not be permitted to make reverse movements within the limits of the work zone, depending upon the railroad rules in effect.

5.4.3.3 Miscellaneous Track Bulletins

These track bulletins are created in the dispatching system and identify conditions affecting operation of the train and safety of employees. Miscellaneous track bulletins may address any of the following:

- Bad footing on or about the right-of-way;
- Highway crossing warning system malfunctions;
- Switches or signals out of service
- Track(s) out of service;
- Suspension of signal system operation; or
- Other advisory information.

5.4.4 Cab Signals

On portions of the railroad and on designated tracks so specified in the timetable, Automatic Cab Signals (ACS) or Automatic Train Control (ATC), which are not Methods of Operation, are in service. ACS and ATC are train control systems which augment the underlying Method of Operation.

Where Cab Signals are in use, a Cab Signal aspect indicating the condition of the current block, and possibly blocks ahead, is continuously displayed by the Aspect Display Unit (ADU) in the cab of the locomotive or control car. Cab signal indications are in conformance with indications displayed by wayside signals, if also present. Upon downgrade of a Cab Signal aspect, an alert is provided which requires an acknowledgement in response; failure to do so within a prescribed time interval will result in a full-service penalty brake application.

ATC provides overspeed enforcement for Cab Signal indications requiring a reduction in train speed. Upon a Cab Signal downgrade from a more favorable indication, an acknowledgement must be provided and train speed must immediately be reduced to the speed prescribed by the new Cab Signal indication. Suppression braking may be required to reduce the speed of the train within the prescribed time interval to the new prescribed speed. Failure to reduce train speed within the prescribed time interval will result in a full-service penalty brake application.

5.4.5 Roles and Responsibilities of Personnel

The existing roles and responsibilities for persons who are involved in the operation or maintenance of the railroad are described in this section.

5.4.5.1 Train Crew

The general direction and government of a train is in the charge of the conductor and all persons employed on the train are subject to his/her instructions. Should there be any doubt as to authority or safety of proceeding, from any cause, he/she must consult the engineer and shall be equally responsible with the engineer for the safety and proper operation of the train, for holding printed or written record of all mandatory directives in

effect for the train, and for such use of signals and other precautions as the case may require.

The engineer is in charge of the engine and responsible for proper handling of the train or engine. In the absence of the conductor, the engineer is in charge of the train.

The conductor and engineer and anyone acting as pilot are responsible for the safety of the train and the observance of the rules, and under conditions not provided for by the rules, must take every precaution for protection.

5.4.5.2 Train Dispatcher

The train dispatcher is responsible for supervising the safe and efficient movement of trains, engines, roadway workers, or machines on a Main or other controlled track.

5.4.5.3 Roadway Workers

Roadway workers are responsible for inspection and maintenance of the railroad's physical plant. Maintenance of Way personnel perform construction, inspection and maintenance of the track structure. Roadway workers must obtain authority or other bulletined protection from the train dispatcher or control operator before occupying or fouling a Main track or other controlled track to perform work. The roadway worker in charge is also responsible for authorizing the safe movement of trains through the limits of work zones he or she controls.

5.4.5.4 Signal Personnel

Signal personnel perform design, construction, inspection and maintenance of the signal systems. Signal personnel may perform work along the railroad right-of-way under protection as described for Roadway Workers.

5.4.5.5 Mechanical Personnel

Mechanical personnel are responsible for inspection and maintenance of the railroad's rolling stock.

5.4.5.6 Telecommunications Personnel

Telecommunications personnel are responsible for operation, inspection and maintenance of the railroad's telecommunications facilities, such as wayside base station radios, towers, antennae, cables, and leased facilities. Telecommunications personnel require authority or protection as Roadway Workers if they will work on or about the track.

5.4.5.7 Other Office Technical Personnel

Other office technical personnel are responsible for the operation and maintenance of the railroad's computerized operating systems.

5.4.5.8 First-Line Supervisors

First-line supervisors are responsible for monitoring the job performance of the personnel under their direction.

5.5 I-ETMS Operational Concepts

Key and overarching I-ETMS operational concepts are described in this section.

5.5.1 Operational Policies and Constraints

Railroad operations are governed by a railroad's respective Operating Rules, Special Instructions, General Bulletins, Air Brake and Train Handling Rules, and Timetables.

Timetables and General Bulletins are typically issued by the Operating Rules Department on the authority of the Executive Vice President Operations.

Specific operating rules governing I-ETMS operation will be promulgated by railroads using the system in any of the documents identified above at such time as the system is certified for operation and deployed. Candidate topics for rules changes, as understood at this time, are identified in Section 5.7.

5.5.2 Underlying Methods of Operation

Railroads utilize four primary Methods of Operation: Traffic Control (TC), Current of Traffic (COT), Track Warrant Control (TWC), and Yard or Restricted Limits (YL or RL). The Method of Operation on a particular portion of the railroad and/or designated tracks is specified in the Timetable. I-ETMS is designed to be effectively overlaid on these Methods of Operation.

Operations under I-ETMS will continue to utilize these existing Methods of Operation to authorize the movement of trains, engines, employees, or machines on a Main Track or other controlled track. No changes to the existing Methods of Operation visible to train crews are anticipated, except as described in Section 5.7.

I-ETMS provides a high level of safety by supervising train movements in accordance with underlying Methods of Operation through continuous display of authority and speed limits, monitoring the train's movements with respect to these limits, and intervention by the display of warnings to the train crew and invocation of a full-service (or emergency) enforcement brake application when authority or speed limits are (or are predicted to be) violated (see Section 5.6.12.2).

Under existing Methods of Operation, train movement may at any time be governed by one or more speed limits prescribed by signal indication, permanent speed restriction, temporary speed restriction, consist or lading restriction, proximity to authority limit, or other dynamic condition. I-ETMS continuously enforces the *most restrictive* of all speed limits in effect at any time or location.

5.5.3 Locomotive Segment Operating States

The Locomotive Segment maintains an operating state determined by dynamic conditions. The operating states are identified below along with a brief description of I-ETMS functional capabilities that exist while in each state:

- ACTIVE – A state in which the Locomotive Segment is fully operational and providing all PTC functions.
- SWITCHING – A state in which the Locomotive Segment is fully operational and providing PTC functions in such manner as to provide flexibility for switching operations.
- DISENGAGED – A state in which the Locomotive Segment has initialized but will not provide predictive enforcement due to conditions including the following:
  - The Locomotive Segment has determined the train is not located in PTC territory;
  - The Locomotive Segment is unable to positively determine the train's location;
  - The Locomotive Segment has detected a possible discrepancy between its internal data stores and data in the office.
- INITIALIZING – A transitional state initiated by the crew in which the Locomotive Segment validates its configuration and the crew credentials and obtains essential information about the train.
- CUT-OUT - A state in which the Locomotive Segment has not yet initialized or cannot provide enforcement due to operation of the I-ETMS cut-out switch.
- SELF TEST - A state in which the Locomotive Segment performs a self-test of certain of its hardware and software components.
- FAILED – A state in which a hardware or software error has been detected.

5.5.4 Display of Information in the Locomotive Cab

When in its fully operational state, the Locomotive Segment continuously displays train location, speed, proximity to track features, speed limits, and any mandatory directives currently governing movement of the train within a 5-mile display horizon. Figure 9 and Figure 10 depict the use of both graphic and text means to display safety-critical information.

5.5.5 Track Database

The track database consists of a description of I-ETMS controlled tracks organized in railroad and subdivision/district hierarchy. The combination of the track database and the I-ETMS navigation function serves as the basis for most key display and enforcement functions. Primary elements of the track database include:

- Geographic location and characteristics of track(s);
- Permanent (civil) speed limits of track;
- Location and type of wayside signals or Cab Signal aspect change points;

- Location of all switches;
- Location, configuration, and fouling points of switches;
- Location of all switch clearance points (main and siding);
- Location of any inside switches equipped with switch circuit controllers;
- Location of all crossings;
- Location of mileposts, including integer mileposts;
- Location of station signs;
- Location of all signals;
- Location and attributes of highway crossings at grade; and
- Attributes relevant to the method of operation on track, e.g. signaled, cab signals present and integrated with I-ETMS, etc.

Distribution of the track database onboard in response to locomotive requests is provided by the Office Segment. The Locomotive Segment verifies correct track data versioning during initialization (see Section 5.6.1) and continuously during operation and requests any updates if a conflict between the versions maintained onboard and the Office Segment are detected. Railroads deploying the I-ETMS system are responsible for production and management of the I-ETMS track databases for their respective I-ETMS territories in accordance with AAR I-ETMS track database specifications [16]. Only one active I-ETMS track database will exist for any segment of track and that version of the track database is served to all equipped locomotives that request it, regardless of locomotive ownership.

5.5.6 Data Integrity and Authentication

I-ETMS relies on the exchange of data messages through public and private data radio networks in order to effect the movement of operating data between office and locomotive and wayside and locomotive. In order to protect the integrity and security of data exchanged through communication networks, I-ETMS includes codes embedded in each data message which allow the receiver to authenticate the sender of each message and detect any data errors possibly introduced in transit. The system discards any data message in which data errors are detected or for which the sender cannot be authenticated.

Data message authentication or integrity errors are not specifically indicated on the display; however, I-ETMS enforces restrictions on train movement when such errors result in application of fail-safe logic.

5.5.7 Interfaces and Data Synchronization

A key requirement for safe train movement under I-ETMS enforcement is the tight synchronization of operating data as it moves through the interfaces between internal and external components of I-ETMS. As a result, I-ETMS employs several mechanisms for detecting data synchronization problems to ensure safe operation as described in the following sections.

5.5.7.1 Wayside – Locomotive Segment

The status of each associated switch, signal, or wayside device that is transmitted by Wayside Interface Units (WIUs) to the Locomotive Segment is completely refreshed at a defined rate because changes may be highly dynamic and communications networks are capable of supporting high data transfer rates. A WIU broadcasts fresh data values on a periodic basis. These broadcasts may be configured to be continuous or on demand by the locomotive depending on the specific demands of the railroad where the system is deployed. The data broadcast rate will be designed and set to achieve target levels of safety and performance. By convention, a single refresh rate will be defined and utilized by all railroads that will deploy I-ETMS. Upon receipt of WIU data, the Locomotive Segment will authenticate and validate the fresh data utilizing the techniques described in Section 9.2.1. If valid, the Locomotive Segment discards older stored data, replacing it with the new data. Failure of the Locomotive Segment to receive fresh WIU data within a configured threshold time tolerance results in a data synchronization failure and causes the Locomotive Segment to assume the affected wayside device is in its most restrictive state. This threshold time tolerance will be established during design, development, and testing of I-ETMS to meet safety requirements. The wayside – locomotive interface is specified in AAR S-9352B [15].

5.5.7.2 Wayside – Office Segment

Wayside status data transmitted by WIUs may be forwarded by the Communications Segment to the Office Segment for relay to the dispatching system. This mechanism may be utilized to allow the dispatching system to monitor the position of switches in non-signaled territory much like they are in Traffic Control territory. Like the Locomotive Segment, the Office Segment will assume a wayside device is in its most restrictive state when a data refresh does not occur within a defined tolerance.

5.5.7.3 Office – Locomotive Segment

A “heartbeat” process is utilized to ensure synchronization of data between the Office Segment and the Locomotive Segment. The Office Segment transmits a heartbeat message to the Locomotive Segment on a configurable periodic basis (at a rate depending on proximity of the train to affected subdivisions/districts), containing “data digest” codes. These data digest codes are computed over all data for each subdivision/district that should be synchronized between the Office and the Locomotive Segment. Upon receipt of a valid heartbeat, the Locomotive Segment compares the data digest codes with those it has computed over its own data stores. When the codes match, the Locomotive Segment has positively determined its local store of operational data is current with the Office data store. Failure of the Locomotive Segment to receive a valid heartbeat within a threshold time tolerance, or a mismatch between the code calculated by the Locomotive Segment and that received in the heartbeat from the Office Segment causes the Locomotive Segment to restrict train movement on any affected subdivisions/districts until such time as data synchronization is positively re-established. This threshold time tolerance will be established during design, development, and testing of I-ETMS to meet safety requirements. By convention, a single set of heartbeat rates will be defined and utilized by all railroads that will deploy I-ETMS. The locomotive – office interface is specified in [14].

5.5.7.4 Dispatching System – Office Segment

Operational data for all trains operating on I-ETMS-controlled territories is conveyed from the dispatching system to the Back Office Server (BOS). This data consists primarily of mandatory directives and train sheet information generated by the dispatching system. In order to ensure that mandatory directives and other operational data remain synchronized between the two systems, each railroad implementing I-ETMS will develop a highly disciplined message exchange protocol to minimize synchronization problems and ensure positive detection of those that do occur. So long as this protocol between systems is maintained within defined performance parameters, the BOS is operating in an explicit control state allowing it to maintain its most permissive operating mode. In this explicit control mode, the Office Segment delivers all mandatory directives received from the dispatching system to the Locomotive Segment of each equipped train along with an indication of its fully-operational state.

When the message exchange protocol is violated or other anomaly occurs on a link that introduces the possibility of data loss and renders the dispatching system or Office Segment incapable of positively assuring that all data is synchronized, the Office downgrades from explicit control and enters a more restrictive "non-explicit control" operating mode. In the non-explicit control operating mode, the Office Segment only delivers those mandatory directives to trains which further restrict train movement (such as Track Warrant voids or new Track Bulletin items). The Office Segment withholds all mandatory directives which provide incremental increase in authority, such as new Track Warrants, or reduce or remove operating restrictions, such as Track Bulletin voids.

Events that cause the Office Segment to fall out of explicit control and downgrade to the non-explicit control operating mode include the following:

- Detected physical or logical break in the link between systems;
- Inactivity on the link exceeding a pre-configured threshold time;
- Timestamp in received message outside of tolerance from receiving system's current date/time;
- Missing or out of order message detected through sequence number processing;
- Invalid message format or syntax;
- Error detected in the transformation of mandatory directive received from dispatching system which could result in an unsafe overlap; or
- Office Segment re-start and prior to achieving synchronization at initialization.

The Office Segment may dynamically recover from the non-explicit control operating mode and re-enter the explicit control operating mode when the condition which caused the degradation is cleared. For example, a recovery of message timestamps to within tolerance or void of an authority which could not be processed may trigger an Office Segment operating mode upgrade. For those conditions which are not dynamically recoverable, the Office Segment must resynchronize all data with the dispatching

system in order to re-enter the explicit control operating mode. It remains in a degraded operating mode for the duration of a resynchronization. The Office Segment synchronization protocols must be designed to meet the performance requirements of the implementing railroad so that a re-synchronization will minimally impact currently-operating trains.

Office Segment operating mode transitions are not specifically indicated on the display; however, I-ETMS enforces restrictions on train movement for the duration of an operating mode downgrade resulting in application of fail-safe logic.

5.5.8 Handling of Time and Time Zones

I-ETMS utilizes UTC internally as provided by GPS and other sources to synchronize operation across its segments. The track database indicates the applicable time zone for each track segment and I-ETMS has the ability to convert between UTC and locally-adjusted time. A railroad implementing I-ETMS will include proper time formats and time zone qualification during specification of the interface between the Office Segment and its dispatching and other back office systems. This interface will include provision for the unambiguous conveyance of time attributes of mandatory directives. The system design includes elements to manage and limit clock drift and/or assume fail-safe behavior.

5.5.9 Impact on Roles and Responsibilities of Personnel

Changes to the roles and responsibilities of personnel affected by the deployment of the I-ETMS are described in this section. Railroads will develop training programs specific to each class of personnel (employee or contracted) on installation, operation, maintenance, or inspection procedures related to I-ETMS.

5.5.9.1 Train Crew

The introduction of I-ETMS does not change the duties of members of the train crew other than the responsibility of the Locomotive Engineer to initialize and operate the Locomotive Segment. I-ETMS provides functions which allow the conveyance of mandatory directives either in the background underneath the existing verbal conveyance process or in a standalone manner to supplant the verbal process. If and when the latter method of delivery is utilized, the impact to train crew members will be assessed and operating rules describing the procedures for mandatory directive conveyance will be modified (see Section 5.6.5.2.

Energy Management (EM) technology interfaced with I-ETMS provides guidance for more fuel efficient operation of the train. EM is further described in Section 5.6.16. Railroads will promulgate operating rules and procedures for operation of EM in Timetables, Special Instructions, or General Bulletins. Section 5.7 contains more information on the nature of rules to be promulgated.

5.5.9.2 Train Dispatcher or Control Operator

The introduction of I-ETMS does not impact the existing roles or responsibilities of the Train Dispatcher or Control Operator other than as follows:

- Handle and establish protection in accordance with §236.1029 in the event of an en-route failure of the Locomotive Segment apparatus on an equipped train; and
- Respond to alerts generated by I-ETMS and provided to the dispatching system, which provided notification of operational events such as emergency brake applications or authority violations by I-ETMS trains.

The provision of train sheet information and mandatory directives from the dispatching system to I-ETMS is transparent and does not require any specific actions by the Train Dispatcher or Control Operator. The system provides functions which allow the conveyance of mandatory directives either in the background underneath the existing verbal conveyance process or in a standalone manner to supplant the verbal process. Where the latter method of delivery is utilized, train dispatcher rules for mandatory directive conveyance will be modified (see Section 5.6.5.2).

Railroads will promulgate operating rules and procedures for Train Dispatcher or Control Operator's operation of I-ETMS in the Rules & Instructions for Train Dispatchers, Timetables, Special Instructions, or General Bulletins. Section 5.7 contains more information on the nature of rules to be promulgated.

5.5.9.3 Roadway Workers

The introduction of I-ETMS does not change the responsibilities of the Roadway Workers, other than as follows:

- Coordinate changes resulting from their work that might impact the I-ETMS track database.

Operation of the I-ETMS work zone function is described in Section 5.6.7.

5.5.9.4 Signal Personnel

The introduction of I-ETMS does not change the responsibilities of Signal Personnel, other than as follows:

- Perform the design, installation, operation, inspection and maintenance of wayside interface units and their interconnection with signal systems;
- Coordinate changes resulting from their work that impact the I-ETMS track database.

5.5.9.5 Mechanical Personnel

Mechanical personnel will be responsible for the installation, inspection and maintenance of the Locomotive Segment apparatus and locomotive communications subsystems.

5.5.9.6 Telecommunications Personnel

Telecommunications personnel will be responsible for the installation, inspection, operation and maintenance of the communications systems utilized by I-ETMS. This will include field infrastructure, such as radio base stations, antennae, and backhaul links, as well as office infrastructure, such as base station controllers and inter-railroad communication links.

5.5.9.7 Other Office Technical Personnel

Other office technical personnel will be responsible for the installation, operation and maintenance of the back office server infrastructure. Additionally, these personnel will be responsible for final production and configuration management of the I-ETMS track database.

5.5.9.8 First-Line Supervisors

First-line supervisors will be trained as to the PTC-related duties of the personnel under their direction.

5.6 Railroad Operation under I-ETMS

Specific operations representative of key I-ETMS functions are described in this section.

5.6.1 Locomotive Segment Initialization

Prior to operation of I-ETMS train control functions on an equipped locomotive, the Locomotive Segment must be initialized. At successful completion of the initialization process, the Locomotive Segment has verified the integrity of all onboard functions and received and verified the integrity of all operational data specific to the routes over which the train will operate on this particular train crew's trip. Initialization is invoked by the locomotive engineer while the locomotive is stopped and prior to commencing a trip. The following functions are performed during Locomotive Segment initialization:

- Entry by the locomotive engineer of employee security credentials and authentication thereof;
- Selection by the locomotive engineer of railroads over which the train will operate as indicated on initial terminal paperwork or instruction;
- Entry by the locomotive engineer of a Train Clearance identifier as indicated on initial terminal paperwork or instruction, for each railroad over which the train will be operated during the train crew's trip, which allows verification of a match between train crew, train symbol, and locomotive ID;
- Verification and/or download of consist and active track data from the Office Segments for each applicable railroad over which the train will operate;
- Check for the existence of and installation of new Locomotive Segment software; and
- Verification that a departure test has been successfully completed per the criteria in Section 5.6.2.

Failure to invoke the initialization process or failure of the initialization process itself prevents the Locomotive Segment from activating PTC functions. By rule, on and after December 31, 2015, a train that is required to operate under PTC control will not be allowed to enter PTC territory unless the train has been successfully initialized, subject to the exceptions identified in §236.1029.

5.6.2 Departure Test

I-ETMS provides the capability for an authorized employee to invoke a departure test of the Locomotive Segment. The departure test invokes a series of diagnostics used to determine if the system is working as intended. The departure test may be required in order to complete the initialization process (see below) or may be invoked at the employee's discretion. Performance of the departure test requires entry and authentication of security credentials by the employee performing the test in order to support electronic record-keeping and ensure the employee performing the departure test is qualified to do so.

Functions performed during the departure test include the following:

- Verification of the onboard display and input keys
- Verification of operation of the GPS receiver and other locomotive interfaces;
- Verification of communications system operation;
- Verification of the interface to the brake system by invoking a full-service brake application and measure of the reduction;
- Determination of whether the locomotive penalty reduction limiting feature is operative or not;
- Verification of the audible enunciator by sounding an audible alert;
- Verification of the horn interface.

I-ETMS requires that a departure test be completed during the initialization process if any of the following conditions exist:

- I-ETMS penalty brake cut out switch was moved to the "cut out" position since last successful departure test;
- Last departure test that was performed failed;
- Locomotive Segment equipment was power cycled or rebooted since last successful departure test;
- 24 hours has elapsed since the last successful departure test was performed.

Completion of a successful departure test is required in order for the Locomotive Segment to activate PTC functions as part of the initialization process described in Section 5.6.1.

5.6.3 Consist Data Management

I-ETMS provides a consist management function, which allows the train crew to review and accept or discard pending changes, or make manual edits to the consist parameters utilized in train braking and performance calculations. Management of the consist data utilized by I-ETMS is ultimately the responsibility of the train crew who maintains discretion as to what consist data is applied and when. Consist data that is reviewable and editable by the train crew includes the following:

- Lead locomotive hood orientation
- Locomotive count
- Trailing Tonnage
- Operative Brake Count
- Total axle count
- Train length
- Loaded Car Count
- Empty Car Count
- Equipment Speed Restriction

Consist data may be reviewed and pending changes accepted or discarded any time the function is invoked. However, the ability to make manual edits to the consist data is only available while the train is stopped. The consist data management function is invoked under any of the following conditions:

- **During Initialization** – During initialization of the Locomotive Segment (described in Section 5.6.1), the consist data for the train obtained by I-ETMS from railroad external back office systems, or default data in the absence of same, is automatically displayed for review, edit (if the train is stopped)and/or acceptance.
- **Consist Softkey** – I-ETMS provides a softkey, available when no other enforcement warning or prompt is present, which the train crew may use at their discretion to review and edit (if the train is stopped) the consist data.
- **Receipt of Consist Data from External Railroad Back Office System** – Upon receipt of consist data from an external railroad back office system, the I-ETMS locomotive segment will display an indication that consist data was received. Additionally, a softkey is provided which allows the train crew to activate the consist management function to review and accept, discard, or edit (if the train is stopped) the received consist data at their discretion. The conditions under which consist data is sent from external railroad back office systems to I-ETMS are strictly a function of the business rules in those railroad back office systems and will vary by railroad.
- **Exit from Switching State** – Upon exit from the Switching state (described in Section 5.6.5.6), the consist management function is automatically invoked, requiring the train crew to review and accept, discard, or edit (if the train is

stopped) the consist data. I-ETMS requires that the train crew provide a disposition of the consist data as part of the transition out of Switching State.

5.6.4 Train Navigation

On-track location determination is a foundational function of I-ETMS, supporting most other functions. There are two aspects to I-ETMS navigation – along-track position and cross-track selection in multiple-track territory or where diverging routes exist.

To begin navigation, I-ETMS first establishes an initial on-track position. Initial along-track position is established based on GPS position. The Locomotive Segment displays valid track options in proximity of the current GPS position and prompts for selection of the track occupied by the train. Once a track has been selected, along-track position is established on the selected track based on a mixture of GPS position fixes and wheel tachometer inputs.

I-ETMS supports a future enhancement to integrate a high-precision "positive" train location system which will obviate the requirement for manual track selection at initialization. Research and development on this high-precision navigation system is being led by the Transportation Technology Center, Inc.

After establishing initial track position, I-ETMS continuously navigates along-track using GPS augmented with differential correction (when available), wheel tachometer input, and matches against the track database. In the absence of GPS signal, the Locomotive Segment will dead-reckon until such time as the accumulated positional uncertainty as calculated by the navigation function reaches a defined threshold. This system-level threshold definition will be set at the point where along-track positional uncertainty is deemed operationally unacceptable. Along-track positional uncertainty is included in all I-ETMS safety-critical train control functions.

Navigation through control point and monitored switch locations is performed through the processing of switch position information provided by the Office Segment or through peer-to-peer communication with a WIU at a monitored switch. I-ETMS determines the exit route from a control point or monitored switch based on the switch status information. If switch position is not known by the Locomotive Segment (due to WIU or communications failure), I-ETMS requires manual selection of the position of the switch. After traversing the switch, if I-ETMS detects an on track position other than as determined through switch status information received from a WIU or provided manually, I-ETMS provides a prompt to verify track selection. Once the I-ETMS track selection is confirmed, the train continues navigation along the track. If the new track selection is not confirmed within a threshold time, I-ETMS invokes a full-service enforcement brake application and stops the train.

In the ACTIVE or SWITCHING states, I-ETMS continuously displays a graphical representation of the track configuration in proximity of the locomotive, and the along-track locations of the train's head and rear ends. Additionally, the milepost location of the train's head-end is displayed.

Train location data is transmitted by the Locomotive Segment to the Office Segment upon events that include the following:

- after a configurable elapsed period of time;
- locomotive starts from a stop;
- locomotive stops;
- passes over a switch;
- crosses a subdivision/district boundary;
- change of Locomotive Segment operating state;
- upon receipt of request from office segment.

It is important to note that I-ETMS-generated position reports are not utilized by any I-ETMS safety-critical train control functions. They are generated by trains and sent to the office segment for forwarding to other external railroad and business and operational systems.

5.6.5 Train Movement

Enforcement of equipped train movement in accordance with timetable restrictions and mandatory directives held by the train is a foundational function of I-ETMS. It is primarily through this function that the system provides protection against train-to-train collisions and movement through switches in improper position in signaled territory. The various operating limits and methods by which it enforces restrictions and authority limits are described in this section.

5.6.5.1 Movement Authority

I-ETMS enforces train or engine movement in accordance with movement authority held by an equipped train through display and enforcement of authority limits and conditions imposed upon the authority. Movement authority may be provided by mandatory directive or by signal indication, or a combination of both signal indication and mandatory directive, depending upon the Method of Operation. Enforcement of signal indications is performed through the processing of wayside or Cab Signal aspects as described in Sections 5.6.5.3 and 5.6.5.4. Wayside or cab signal aspects are not displayed by I-ETMS; only the enforceable authority or speed limits that result from signal indications are displayed. Movement authorities provided by Mandatory Directive are generated by the train dispatcher or control operator through the creation and edit of a Track Warrant on the dispatching system.

When within the limits of a movement authority, I-ETMS performs predictive enforcement to ensure that an equipped train does not exceed the limits of the authority. It will allow an equipped train to move from the limits of one movement authority into the limits of another conterminous movement authority of the same or different type without warning or enforcement. The system protects reverse movements as described in Section 5.6.5.5.

When an equipped train occupies uncontrolled track, I-ETMS performs predictive enforcement at the entrance to any adjoining controlled track when the train holds no movement authority on that controlled track in accordance with the Method of Operation in effect. It allows an equipped train to move from uncontrolled track onto controlled track when it holds movement authority on that controlled track.

5.6.5.2 Movement Authority Provided by Mandatory Directive

Railroads utilize various forms for issuance of movement authority by mandatory directive. Examples include *Track Warrants*, *Track & Time*, *Track Permit*, *Foul Time Permit, Track Authority, Form EC-1, or Form D.* Each of these forms may be utilized by a particular railroad under some or all of its methods of operation, e.g. Track Warrant Control (TWC), Traffic Control (TC), Current of Traffic (COT), or manual interlocking limits. As part of the railroad's development of the interface protocol between its dispatching system and the Office Segment, it will define message protocols to convey its forms of authorities and their attributes to the Office Segment and to ensure their integrity in transit. The general process utilized to convey movement authority provided by mandatory directive to a I-ETMS train is as follows:

1. The train dispatcher creates and edits the movement authority on the appropriate form in the dispatching system.
2. If the movement authority is to be issued verbally, the train dispatcher reads the movement authority to a train crew or roadway worker, verifies correct read-back, and completes the movement authority. The movement authority is now instantiated in and protected by the dispatching system and the train crew or roadway worker holds a written or printed copy of the authority. If electronic-only conveyance is invoked, the movement authority is instantiated and protected by the dispatching system at the time it is created.
3. The dispatching system transmits the movement authority data to the Office Segment Back Office Server. The movement authority data transmitted by the dispatching system to the Office Segment may include both human- and machine-readable versions of the movement authority in accordance with the railroad's dispatching system – office segment interface protocol. Upon receipt of a movement authority from the dispatching system, the following process ensues:

    - The BOS performs a check of the transformation of a digital authority from the format provided by the dispatching system to the format utilized by I-ETMS to ensure that no unsafe overlap with another authority has been introduced. This check may detect errors introduced as a result of the processing by either the dispatching system or BOS, or the message exchange between them.
    - If no unsafe overlap is detected, the BOS sends the authority in the original format as provided by the dispatching system, as well as the results of its own transformation.
    - The vital Locomotive Segment performs its own transformation of the authority and compares it against the transformation results provided by the BOS. It will only act on the digital authority if the transformations match.

- A match between the transformations (1) mitigates transformation errors performed by the non-vital BOS and (2) ensures that Locomotive Segment is acting on an authority which passed the BOS transformation overlap check.

4. When an equipped train is addressed in the movement authority, the Office Segment transmits the movement authority to the specified Locomotive Segment. The movement authority data transmitted to the locomotive includes an indication of whether the movement authority requires acknowledgment or not.
5. When the movement authority indicates an acknowledgement is required, such as in the case of electronic-only conveyance, the Locomotive Segment provides an alert, displays the movement authority, and requires acknowledgement prior to beginning enforcement of the movement authority, or allowing the train to occupy the limits of the authority. Once acknowledged (if required), the Locomotive Segment begins display and enforcement of the movement authority and notifies the Office Segment that the authority has been successfully delivered and acknowledged. When acknowledgment is not required (indicating the authority was verbally conveyed), the Locomotive Segment begins enforcement of the movement authority immediately upon receipt.
6. The Office Segment notifies the dispatching system that the authority has been successfully delivered and, if applicable, acknowledged.

Upon any failure of the I-ETMS movement authority delivery process, the Office Segment notifies the dispatching system, which in turn provides an alert to the train dispatcher. However, the primary method for detection and safe mitigation of a delivery failure is provided by data synchronization check processes, described in Section 5.5.7.

The I-ETMS electronic conveyance process may be invoked on a per-mandatory directive basis and the method selected is driven by the railroad dispatching system and/or Office Segment. Use of either voice or electronic delivery of mandatory directives as the primary method may be freely intermixed, from a system perspective. Thus, the selection of either method is a matter of individual railroad policy, without dependency on the policy of other railroads. Further, a railroad may intermix the use of either method within its own operation, based on geography, training, schedule for rules promulgation, etc.

At this time the crew will continue to obtain and acknowledge the required mandatory directive information via their paperwork and verbal communication with the dispatcher. The system design supports the electronic delivery and acknowledgment of mandatory directives, but additional approval will be sought before this feature is used.

5.6.5.2.1 Track Warrant Control

A Track Warrant issued to a train in TWC territory may authorize movement in one or both directions. I-ETMS enforces the movement of an equipped train within and about the limits of Track Warrant authority as described in Section 5.6.5.1. In addition to authority limits and direction of movement, a Track Warrant may contain other conditions or restrictions, which are enforced by I-ETMS as follows:

Void Track Warrant. Upon delivery and acknowledgement (if required) of a Track Warrant which voids another Track Warrant held by that train, the system automatically voids the existing specified Track Warrant and begins enforcement of train movement in accordance with the new Track Warrant.

Not in Effect Until Arrival Of. I-ETMS requires acknowledgement of the arrival of each train or engine specified in the Track Warrant. It will only allow the train or engine to occupy and move within the limits specified in the Track Warrant once the arrival of all engines specified has been acknowledged.

Do Not Foul Limits Ahead Of. I-ETMS requires acknowledgement of the arrival of each train or engine specified in the Track Warrant. It will only allow the train or engine to occupy and move within the limits specified in the track authority once the arrival of all engines specified has been acknowledged.

Joint with Train or Engine. I-ETMS enforces a stop at the limits specified in a Track Warrant as joint with other trains(s) or engine(s), until such time as the joint limits are acknowledged. A prompt to acknowledge the joint limits is provided when the train is within a pre-configured threshold distance of the limits. Once acknowledged, the system enforces restricted speed approaching and through the joint limits as described in Section 5.6.12.3 – Restricted Speed Enforcement.

Joint with Men or Equipment. I-ETMS enforces a stop at the limits specified in a Track Warrant as joint with roadway workers or equipment, until such time as the joint limits are acknowledged. A prompt to acknowledge the joint limits is provided when the train is within a pre-configured threshold distance of the limits. Once acknowledged, I-ETMS enforces restricted speed approaching and through the joint limits as described in Section 5.6.12.3 – Restricted Speed Enforcement.

Do Not Exceed. I-ETMS enforces any temporary speed restrictions imposed as a condition of a Track Warrant. See Section 5.6.6.3.

Stop Short. I-ETMS enforces a stop at a location specified in a track warrant where a stop is required as a condition prior to proceeding further toward the limit of the authority. The train may proceed only when the track warrant is modified to remove the stop short condition.

5.6.5.2.2 Traffic Control

Movement authority may be issued by mandatory directive by the train dispatcher to trains, engines, or roadway workers and equipment to move in either direction within the specified limits in Traffic Control territory. I-ETMS enforces the movement of an equipped train or engine within and about the limits of movement authority issued by mandatory directive in TC territory as described in Section 5.6.5.1. When movement authority issued by mandatory directive is joint with other trains, engines, roadway workers, or equipment, I-ETMS prompts for an acknowledgement of the joint limits when the train is within a pre-configured threshold distance of the limits and displays

and enforces these limits as described in Section 5.6.12.3 – Restricted Speed Enforcement upon receipt of acknowledgement.

5.6.5.2.3 Current of Traffic

Movement authority may be issued by mandatory directive by the train dispatcher to trains, engines, or roadway workers and equipment to move in either direction within the specified limits in Current of Traffic (COT) territory. I-ETMS enforces the movement of an equipped train or engine within and about the limits of movement authority issued by mandatory directive in COT territory as described in Section 5.6.5.1. When movement authority issued by mandatory directive is joint with other trains, engines, roadway workers, or equipment, I-ETMS prompts for an acknowledgement of the joint limits when the train is within a pre-configured threshold distance of the limits and displays and enforces these limits as described in Section 5.6.12.3 – Restricted Speed Enforcement upon receipt of acknowledgement.

5.6.5.2.4 Movement Authority Issued to Roadway Workers

The train dispatcher may create and issue movement authority by mandatory directive to a Roadway Worker. A movement authority issued by mandatory directive to Roadway Workers is transmitted by the dispatching system to the Office Segment, where it is stored and subject to transformation check as described in Section 5.6.5.2. Movement authority issued by mandatory directive to Roadway Workers is not electronically conveyed to Roadway Workers at this time.

5.6.5.2.5 Authority to Pass Signal Displaying STOP Indication

Authority to Pass Signal Displaying Stop Indication (ATP) is granted by the train dispatcher to authorize a train or engine to advance past a controlled signal displaying STOP indication. I-ETMS enforces such authorities and provides two methods for handling them.

The first method is utilized when movement past a signal displaying STOP indication is authorized by the train dispatcher and conveyed from the dispatching system to the Office Segment. The ATP is processed by I-ETMS and delivered to the train as described in Section 5.6.5.2. This process ensures that an electronic version of the ATP is made available to the Locomotive Segment.

The second method is utilized primarily under communications failure conditions, or when ATP is not required by operating rule, but under conditions not discernable by I-ETMS. After stopping within a preconfigured threshold distance in approach to a signal displaying STOP indication for a preconfigured period of time, a manual input may be made to the Locomotive Segment indicating that the train is authorized to pass the signal either because ATP has been received from the train dispatcher or control operator, or because such authority is not required.

Upon receipt of Authority To Pass Signal Displaying STOP Indication from the dispatching system via the Office Segment or a manual indication that the train is authorized to pass the signal, I-ETMS enforces movement of the train or engine at

Restricted Speed up to and past the signal displaying STOP indication to the next governing signal in advance or to the end of block system limits, whichever comes first. Where Cab Signals are in use and integrated with I-ETMS, the speed enforced beyond the absolute signal is determined by the Cab Signal indication.

5.6.5.2.6 Authority to Enter the Main Track between Signals

Authority to Enter the Main Track (EMT) is granted by the train dispatcher to authorize a train or engine to enter the Main (or other controlled) tracks in CTC or COT territory at a location between block signals and proceed in one direction. I-ETMS enforces such authorities and provides two methods for handling them.

The first method is utilized when entry to the main track is authorized by the train dispatcher and conveyed from the dispatching system to the Office Segment. The EMT is processed by I-ETMS and delivered to the train as described in Section 5.6.5.2. This process ensures that an electronic version of the EMT is made available to the Locomotive Segment.

The second method is utilized primarily under communications failure conditions, or when EMT is not required by operating rule, but under conditions not discernable by I-ETMS. After stopping within a preconfigured threshold distance of the clearance point of switch at the entry location for a preconfigured period of time, a manual input may be made to the Locomotive Segment indicating that the train is authorized to enter the main track either because EMT has been received from the train dispatcher or control operator, or because such authority is not required.

Upon receipt of Authority to Enter the Main Track from the dispatching system via the Office Segment or a manual indication that the train is authorized to enter the main track, I-ETMS enforces movement of the train or engine between the Main Track entrance location and the next governing signal in advance (or the end of block system limits) as follows:

- At Restricted Speed from location equipped with electric lock; or
- In accordance with the indication displayed by a signal in lieu of electric lock as described in Section 5.6.5.3, at location equipped with same. Alternatively, where a wayside equipment or communication failure exists, or when a proceed indication is not displayed by the signal in lieu of electric lock, the train crew may provide an indication that they are authorized to pass the signal only after a threshold time has elapsed since the train stopped within a threshold distance of the signal.

Where Cab Signals are integrated, I-ETMS will enforce train movement as described in Section 5.6.5.4. I-ETMS will additionally provide enforcement of the position of the entering switch, based on how it is monitored, as described in Sections 5.6.11.1 - 5.6.11.4.

5.6.5.3 Wayside Signals

I-ETMS enforces train and engine movements in accordance with wayside signal indications on those sections of the railroad that are equipped with wayside signals, Cab Signals or both. Where Cab Signals are not in use or where signal status is not obtained through an interface to the onboard Cab Signal system, the signal aspect data is received through an interface to the wayside signals and is processed by the Locomotive Segment. Where Cab Signals are in use in addition to wayside signals and integrated with I-ETMS, the Locomotive Segment will enforce train movement in accordance with Cab Signal Indications (described in Section 5.6.5.4), which are in conformance with wayside signal indications.

Various forms of hazard detectors may be integrated with a signal system, such as those which monitor movable bridge alignment, high-water conditions, slide fences, right-of-way encroachment, etc. I-ETMS integrates with these hazard detectors through the signal system and provides protection against the associated hazards through enforcement of signal indications.

As a train or engine navigates down the track in territory where wayside signals are monitored, the Locomotive Segment listens for and accepts signal state data periodically broadcasted from WIUs located at signal locations. The Locomotive Segment decodes the received signal state information and constructs enforceable operating limits in accordance with the corresponding indication for each signal. Because the Locomotive Segment independently monitors switch position, enforces the corresponding turnout speeds, and enforces track civil speed limits, the actual enforceable limits generated strictly from signal aspect data are simplified in comparison to the corresponding signal indication rules. The combination of switch position, speed, and simplified aspect enforcement results in compliance with the proper operating limits. Table 7 identifies the five simplified enforcement rules applied by I-ETMS that correspond to the range of possible signal indications. The mapping of signal aspects and indications to simplified enforcement rules occurs in the track database.

Table 7 – Signal Enforcement Rules

Rule	Enforcement Limits	Example Signal Indication
1	Stop at signal Upon a compliant stop, the train may be able to advance as described in Section 5.6.5.2.5	Stop before any part of train or engine passes signal.
2	Stop at signal Upon compliant speed reduction (see Section 5.6.5.3.2), train allowed to proceed at restricted speed to and beyond signal to next signal in advance.	Proceed at Restricted Speed.

Rule	Enforcement Limits	Example Signal Indication
3	Stop at next signal in advance	Proceed prepared to stop before any part of train or engine passes next signal.
4	Stop at 2nd signal in advance.	Proceed prepared to stop at second signal.
5	None	Proceed.

The assignment of signal enforcement rules to aspects displayed by a signal will depend on the type of signal. For example, the most restrictive aspect displayed by an absolute signal will be mapped to signal enforcement rule #1, which results in enforcement of a positive stop at the signal. Conversely, the most restrictive aspect displayed by an automatic or intermediate signal will be mapped to signal enforcement rule #2.

The Locomotive Segment may modify the enforcement criteria generated for a particular signal when the indication of a signal in advance so warrants. For example, where two successive signals display APPROACH, the stop limit generated at the location of the second signal will be relieved as a result of that signal displaying APPROACH (vs. STOP, RESTRICTING, or RESTRICTED PROCEED).

When the age of the last valid signal aspect data received from a signal WIU exceeds the time tolerance threshold, the Locomotive Segment assumes the signal is in its most restrictive state and enforces train movement accordingly.

5.6.5.3.1 Approach Lighting

I-ETMS fully accommodates existing approach lighting features incorporated in the signal system. Enforcement is forestalled for any signal in advance of an equipped train indicating DARK (via the broadcast message from its WIU) and any signals further in advance of that signal when the train is outside an approach lighting threshold location. However, if the signal continues to indicate DARK and is not otherwise displaying a proper aspect by the time the train has passed an approach lighting threshold location, the Locomotive Segment assumes the signal is in it most restrictive state, generates a stop or Restricted Speed restriction at the signal location (depending upon its type) and enforces train movement accordingly (see Section 5.6.5.3.3). The Locomotive Segment may actuate “advance” approach lighting via the Communications Segment. This feature allows the Locomotive Segment to initiate wayside status broadcast and obtain signal aspects prior to when they would otherwise be provided in accordance with conventional track circuit-based approach lighting.

5.6.5.3.2 Approaching and Operating on Signal Requiring Restricted Speed

The Locomotive Segment enforces a stop at any signal displaying an indication which requires restricted speed until such time as the train completes a compliant speed reduction as described in Section 5.6.12.3.

After passing a signal requiring movement at Restricted Speed, the Locomotive Segment graphically and textually displays the Restricted Speed restriction and performs reactive (overspeed) enforcement of the maximum speed allowed under the railroad's Restricted Speed rule in effect. While a train or engine is operating on a signal requiring Restricted Speed and the next signal in advance displays an indication more favorable than RESTRICTING, the Locomotive Segment continues to enforce train movement at Restricted Speed until the leading wheels of the locomotive pass the next signal.

5.6.5.3.3 Approaching and Operating on Signal with Indication Unknown to I-ETMS

The Locomotive Segment assumes a signal within the display/route horizon to be in an unknown state when no aspect data has been received from the signal, when the last aspect data received from the signal has exceeded the age tolerance threshold, or when the signal indicates DARK after the train has passed the defined approach lighting threshold location for the signal. To minimize unnecessary restriction of train movement due to varying RF coverage and propagation conditions, I-ETMS forestalls enforcement of a signal whose state is unknown until such time as the signal becomes the next signal in advance of the train. At that time, it assumes a signal whose state is unknown to display its most restrictive indication and enforces a stop or Restricted Speed at the signal, depending upon its type. Figure 17 depicts enforcement of a wayside signal in a state that is unknown to I-ETMS.

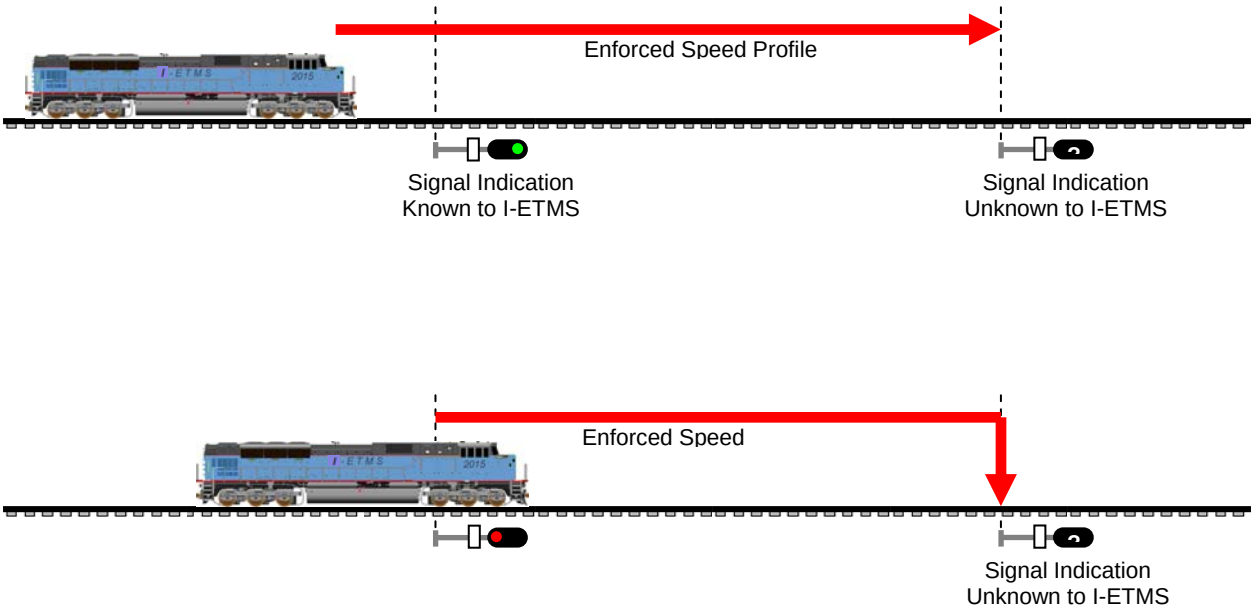

Figure 17 – Enforcement of Wayside Signal in State Unknown to I-ETMS

Where the signaling system includes lamp-out protection features, fewer actual dark signals will be encountered by trains. Additionally, any aspect downgrades at and on approach to a signal with a lamp-out condition will be fully realized and enforced by I-ETMS.

5.6.5.3.4 Wayside Signal Upgrades and Downgrades

I-ETMS allows a train operating on a signal whose indication does not require Restricted Speed to accept and operate on the indication displayed by the next signal in advance of the train prior to passing the signal. This capability allows upgrades or downgrades of the next signal in advance to be immediately realized by the train and enforced by I-ETMS accordingly.

5.6.5.4 Cab Signals

When interfaced to a 4-aspect cab signal system, the Locomotive Segment enforces train movement in accordance with Cab Signal indications on those sections of the railroad where 4-aspect Cab Signals are in use. In cases where the Locomotive Segment obtains the current Cab Signal aspect from the locomotive Cab Signal system, the Locomotive Segment processes it in the context of current train speed, train location, and train proximity to fixed signals, control points, or aspect change points in advance. In TC territory, the Locomotive Segment additionally obtains the status of switches and signals at control points (via a WIU or the Office Segment). The availability of positioning, train speed, and track feature data combined with the current Cab Signal indication allows I-ETMS to augment traditional Cab Signal functionality with positive (predictive) stop and overspeed enforcement.

The Locomotive Segment senses when the locomotive Cab Signal system is cut-in and operational and enforces train movement in accordance with Cab Signal indications when approaching or within Cab Signal territory. Upon a change of the Cab Signal aspect, I-ETMS enforces train movement in accordance with the new Cab Signal indication, which supersedes enforcement of the preceding Cab Signal indication.

The locomotive Cab Signal system remains fully operational concurrent with I-ETMS operation; the cab signal system displays aspects on the aspect display unit and it continues to enforce acknowledgement of Cab Signal downgrades. I-ETMS will enforce positive speed reduction or predictive stop at the locations prescribed by the current Cab Signal indication; no cab signal aspects are displayed by I-ETMS. It is able to perform this predictive enforcement because of its along-track navigational capability.

Because the Locomotive Segment independently monitors switch position and enforces the corresponding turnout speeds and enforces track civil speed limits, the actual enforceable limits generated strictly from Cab Signal aspects are simplified in comparison to railroad signal indication rules. I-ETMS is designed to integrate at the wayside, in the cab, or both. The combination of switch position, speed enforcement, and simplified aspect enforcement results in enforcement criteria equivalent to full Cab Signal indication enforcement.

5.6.5.4.1 Operation in Four-Aspect Cab Signal Territory

A Cab Signal aspect may be in conformance with multiple wayside signal indications, some more restrictive than others. In such cases, the Locomotive Segment generates enforcement criteria in accordance with the most restrictive conforming wayside signal indication. Use of a more permissive wayside indication to upgrade enforced targets

will require additional positive input, as provided by a WIU. Table 8 identifies the simplified operating limits enforced by I-ETMS corresponding to each Cab Signal Indication as currently defined in railroad operating rules.

Table 8 – Cab Signal Indication Enforcement

Cab Signal	Most Restrictive Corresponding Wayside Indication	I-ETMS Enforcement Criteria
CLEAR	Proceed.	None
ADVANCE APPROACH or APPROACH MEDIUM	Proceed prepared to stop at second signal.	Stop at 2nd signal or aspect change point in advance
APPROACH	Proceed preparing to stop at next signal. Train or engine exceeding Medium Speed must at once reduce to that speed.	Stop or Restricted Speed at next signal or aspect change point in advance, depending upon status and/or type of signal (see Section 5.6.5.4.1.1)
RESTRICTING	Proceed at Restricted Speed.	Maximum speed allowed under railroad restricted speed rules. Stop or Restricted Speed at next signal or aspect change point in advance, depending upon status and/or type of signal (see Section 5.6.5.4.1.1)

5.6.5.4.1.1 Enforcement at Next Signal in Advance

I-ETMS may enforce additional conditions at the next signal or aspect change point in advance of a train depending upon the current Cab Signal indication and type or status of the next signal. These enforceable conditions may supersede or be in addition to conditions described in Table 8. Table 9 identifies the conditions enforced by the Locomotive Segment for the next signal in advance.

Table 9 – Enforcement at Next Signal In Advance

Type and Status of Next Signal In Advance	Current Cab Signal	I-ETMS Enforcement Criteria
Absolute signal displaying STOP Indication	Any	Stop before any part of train or engine passes signal.

Type and Status of Next Signal In Advance	Current Cab Signal	I-ETMS Enforcement Criteria
Absolute signal with status UNKNOWN to I-ETMS		Once stopped, the train may be able to advance as described in Section 5.6.5.2.5.
Absolute signal displaying proceed indication	CLEAR	None
	ADVANCE APPROACH or APPROACH MEDIUM	
	APPROACH	Stop at signal Upon compliant speed reduction (see Section 5.6.12.3), Restricted Speed to signal.
	RESTRICTING	
Intermediate signal	CLEAR	None
	ADVANCE APPROACH or APPROACH MEDIUM	
	APPROACH	Stop at signal Upon compliant speed reduction (see Section 5.6.12.3), Restricted Speed to signal.
	RESTRICTING	

When approaching the next signal in advance requiring a stop or Restricted Speed, the Cab Signal indication will typically be in conformance (e.g. APPROACH or RESTRICTING) and prescribe a stop at the signal. However, I-ETMS always enforces the most restrictive condition of either the current Cab Signal indication or type/status of the next signal in advance regardless of whether the Cab Signal indication is in conformance or not. For example, if the Cab Signal is CLEAR and the next signal in advance is an absolute signal with status unknown to I-ETMS, the Locomotive Segment enforces a stop at the signal. Conversely, if the current Cab Signal is APPROACH and the next signal in advance is an absolute signal displaying a proceed indication, the Locomotive Segment still enforces a stop at the signal, subject to the conditions of a compliant speed reduction as described in Section 5.6.12.3.

The status of an absolute signal in advance of the train may be determined through control point status information provided to I-ETMS via the dispatching system or via WIU communication.

5.6.5.4.1.2 Cab Signal Downgrade to RESTRICTING

As noted in Table 8 when the Cab Signal is RESTRICTING, the Locomotive Segment enforces train or engine movement at the maximum speed permitted under the

railroad's Restricted Speed rules and graphically and textually displays the Restricted Speed restriction. However, actions taken by I-ETMS at the time the Cab Signal downgrades to RESTRICTING, other than within a drop-out zone as described in Section 5.6.5.4.1.4, depend on train speed at the time the downgrade occurs. When train speed does not exceed the maximum speed allowed under Restricted Speed rules plus an overspeed tolerance at the time the downgrade occurs, the Locomotive Segment enforces train or engine movement at the maximum speed allowed under the railroad's Restricted Speed rule.

When train speed exceeds the maximum speed allowed under the railroad's Restricted Speed rule plus the overspeed tolerance at the time a downgrade occurs, I-ETMS places a Restricted Speed restriction at a calculated location in advance of the train in lieu of immediately applying a reactive (overspeed) full-service enforcement brake application. The calculated location of the restriction limit includes a configured reaction time and predicted stopping distance of the train, as depicted in Figure 18. This feature allows a speed reduction consistent with good train handling to manage in-train forces, in lieu of an unanticipated full-service penalty brake application for an unexpected downgrade. However, failure to make a compliant speed reduction prior to entering the limits of the Restricted Speed restriction will result in a full-service enforcement brake application nonetheless, as described in Section 5.6.12.3.

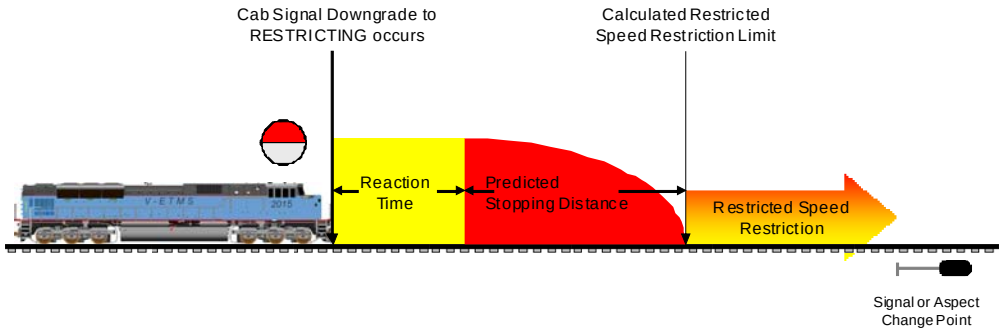

Figure 18 – Calculation of Restriction Location on Cab Signal Downgrade to RESTRICTING

5.6.5.4.1.3 Cab Signal Upgrade from RESTRICTING

When the Cab Signal upgrades from RESTRICTING to an aspect more favorable than RESTRICTING, the Locomotive Segment enforces train movement at Restricted Speed until the train moves a distance equal to its length, or passes the next governing signal or aspect change point, whichever occurs first.

5.6.5.4.1.4 Cab Signal Drop-Out Zones

Locations exist along the track where Cab Signal information is known to be absent from the rails due to the arrangement of Cab Signal feeds to the track. The limits of these "drop-out zones", typically located within interlocking or control point limits where crossovers or cut sections exist, are defined in the track database. The Cab Signal

aspect for a train entering the limits of a drop-out zone will temporarily downgrade to RESTRICTING (if the aspect was more favorable than RESTRICTING previously) while the locomotive is within the limits of the drop-out zone.

When a locomotive enters the limits of a drop-out zone, the Locomotive Segment maintains enforcement of train movement in accordance with the Cab Signal indication prior to the drop-out and forestalls enforcement of the RESTRICTING Cab Signal aspect while the train occupies the drop-out zone limits. When the locomotive exits the limits of the drop-out zone, if the Cab Signal indication does not change to a more favorable indication, the Locomotive Segment enforces train movement as described in Section 5.6.5.4.1.2.

5.6.5.5 Reverse Movement

The Locomotive Segment provides enforcement of authority and speed limits during reverse movements utilizing the rear of the train (defined as offset from controlling locomotive location by train length as maintained in the Locomotive Segment consist data) as the leading end. I-ETMS will protect and provide enforcement for reverse movements based on railroad-specific configuration parameters which are set in accordance with the railroad's operating rules within limits of unidirectional movement authority (as provided by signal indication or authority provided by mandatory directive).

The Locomotive Segment enforces train movement at Restricted Speed during reverse movements. Additionally, enforcement of signal indications in the reverse direction is provided as well.

5.6.5.6 Switching State

I-ETMS allows the selection of a "Switching" state which modifies certain aspects of the I-ETMS enforcement function in such manner as to allow the train to perform switching work on a controlled track in a practical manner without requiring the system to be completely disengaged or cut-out. The number of manual consist edits and the impact of conservatism in the predictive enforcement algorithm might otherwise cause the performance of switching moves under I-ETMS control to be extremely onerous or even impossible.

In Switching state, I-ETMS will enforce bi-directional operation at Restricted Speed within the limits of the train's current authority (provided by signal indication or mandatory directive) and assumes that the train consists of only the controlling locomotive. The following prompts will be displayed and acted upon only once after entering the Switching state:

- Confirm authority to enter work zone;
- Indicate position of unmonitored switch;
- Confirm authority to pass signal displaying STOP indication;
- Confirm authority to enter the main track between block signals;
- Confirm proper flagging present at highway crossing;

- Confirm knowledge of joint authority limits;
- Confirm arrival of train or engines.

The enforceable conditions resulting from the response to any of these prompts is "latched" for the duration of the operational instance of Switching state; no subsequent prompt of each type is displayed in Switching state after the initial prompt. However, the presence of conditions related to a prompt, e.g. presence and limits of a work zone switch position, remain on the display.

The following non-enforcement-related functions are also suppressed while in the Switching state:

- Initialization
- Departure test
- Notification of departure from I-ETMS territory
- Train handling exception detection
- Horn protection
- Energy management

Upon exit from Switching state, the Locomotive Segment will reinstate all enforcement and non-enforcement-related functions, prompting, and will prompt for any consist changes that have occurred.

Switching state may only be invoked or exited by the locomotive engineer while the train or engine is stopped. Use of Switching state is optional and if invoked will be further governed by railroad Operating Rules, Timetable, Special Instructions or Operating Bulletin.

5.6.5.7 Entry to I-ETMS Territory

The Locomotive Segment enforces entry by a train into I-ETMS controlled territory from territory not controlled by I-ETMS. Entry point locations include those locations where a Main Track in I-ETMS territory adjoins one in non-I-ETMS territory or where an uncontrolled auxiliary track adjoins I-ETMS territory at a switch.

Once the Locomotive Segment has been successfully initialized, a train or engine without corresponding authority to enter I-ETMS controlled territory will be subject to predictive warning and enforcement to protect against unauthorized entry. I-ETMS allows a train or engine with authority, whose limits include the entry point into I-ETMS controlled territory, to pass through that entry point and enter I-ETMS territory.

In Track Warrant Control territory where I-ETMS is in use, a valid Track Warrant whose limits include the entry point location must be held by a train or engine to permit entry into I-ETMS territory.

In signaled I-ETMS territory, the method utilized for entry enforcement depends on the Method of Operation in the territory and the specific configuration at the entry point. Table 10 identifies the system requirements for entry to signaled I-ETMS territory.

Table 10 – Requirements for Entry to Signaled I-ETMS Territory

Method of Operation -> Entry Point Configuration	TWC/ABS	COT	TC
Controlled Signal	Track Warrant authority and Permissive signal indication or Authority to Pass Signal Displaying STOP Indication (as described in Section 5.6.5.2.5)	Permissive signal indication or Authority to Pass Signal Displaying STOP Indication (as described in Section 5.6.5.2.5) to move with the current of traffic; Movement Authority provided by mandatory directive to move against the current of traffic or in either direction.	Permissive signal indication or Authority to Pass Signal Displaying STOP Indication (as described in Section 5.6.5.2.5)
Hand-Operated Switch with Electric Lock	Track Warrant authority	Authority to Enter the Main Track (as described in Section 5.6.5.2.6) to move with the current of traffic. Movement authority issued by mandatory directive authorizing movement in either direction.	Authority to Enter the Main Track (as described in Section 5.6.5.2.6) to move with the current of traffic. Movement authority issued by mandatory directive authorizing movement in either direction.
Hand-Operated Switch with Signal in Lieu of Electric Lock	Track Warrant authority		

5.6.5.8 Exit from I-ETMS Territory

The Locomotive Segment displays a warning when a train or engine approaches an exit point from I-ETMS controlled territory. No specific enforcement of exit from I-ETMS territory to non-I-ETMS territory is provided, except as provided due to the enforcement of a signal governing the route, Cab Signal, track warrant limit, or speed restriction located at an exit location. Upon leaving I-ETMS controlled territory, the Locomotive

Segment automatically downgrades its operating mode and no longer enforces train or engine movement, except in approach to I-ETMS territory as described in Section 5.6.5.7. I-ETMS provides both visual and audible indications when the Locomotive Segment operating mode changes.

5.6.5.9 Yard Limits and Restricted Limits

The Locomotive Segment enforces train and engine movements on those portions of the railroad and on tracks so specified in the timetable as governed by Yard Limits or Restricted Limits and designated as I-ETMS-controlled territory.

Where Main Track within Yard Limits is not signaled or designated as Restricted Limits, the Locomotive Segment enforces train and engine movements at the maximum permitted speed under Restricted Speed rules, and displays graphically and textually that Restricted Speed is in effect.

Where Main Track within Yard Limits is signaled, the Locomotive Segment enforces train and engine movements in accordance with wayside or Cab Signal indications as described in Sections 5.6.5.3 and 5.6.5.4. I-ETMS may enforce train and engine movements at Restricted Speed unless operating on a signal more favorable than APPROACH.

5.6.5.10 Movement of Unequipped or Uninitialized Trains in I-ETMS Territory

Crewed or remotely-controlled locomotives assigned to yard, terminal or switching duty where I-ETMS is deployed may not be equipped with the Locomotive Segment apparatus or may not be initialized. However, these locomotives may make yard, local, hostling service, or industrial moves or be part of work trains which require them to enter the limits of I-ETMS territory and operate for short distances, provided that any such moves will be conducted in accordance with the final Subpart I regulation.

5.6.6 Speed Limits and Restrictions

The Locomotive Segment concurrently enforces speed restrictions from several sources and of several types in I-ETMS-controlled territory. It is through this function primarily that I-ETMS prevents train derailments due to overspeed conditions. The most restrictive of all applicable speed restrictions at a location dictates the speed enforced.

5.6.6.1 Permanent Speed Restrictions

The Locomotive Segment enforces train and engine movements in compliance with permanent speed restrictions, established by Timetable, Special Instructions, or General Order. Permanent speed restrictions are derived by I-ETMS from the track database and include civil and switch turnout speed limits. Additionally, civil speed limits based on the following criteria will be enforced, if they are so indicated in the track database:

- Train speed class (general freight, intermodal, passenger, high-speed passenger, etc.);

- Direction of train movement;
- Train weight;
- Tons per operative brake;
- Axle count; or
- Head-end versus entire train

The Locomotive Segment performs both predictive and reactive warning and enforcement of trains approaching or operating within the limits of permanent speed restrictions, as described in Section 5.6.12.

5.6.6.2 Temporary Speed Restrictions

The Locomotive Segment enforces train and engine movements in compliance with temporary speed restrictions (TSR), as established by track bulletin. TSRs are conveyed from the dispatching system to the Office Segment, which in turn delivers them to affected trains. TSRs may be delivered to a train during initialization of the Locomotive Segment, or while the train is en-route after initialization.

The Locomotive Segment takes into account all attributes of a TSR in the enforcement thereof, including time(s) in effect and applicability to the entire train or head end only. Additionally, the text of a TSR bulletin item is displayable upon request.

The Locomotive Segment performs both predictive and reactive warning and enforcement of trains or engines approaching or operating within TSRs as described in Section 5.6.12.

5.6.6.3 Track Warrant Speed Restriction

The Locomotive Segment enforces train and engine movements in compliance with a speed restriction conveyed as a condition of a Track Warrant. Track Warrants are conveyed from the dispatching system to the Office Segment, which in turn delivers them to the Locomotive Segment of the addressed train. The Locomotive Segment performs both predictive and reactive warning and enforcement of trains or engines approaching or operating within speed restrictions conveyed as a condition of a Track Warrant, as described in Section 5.6.12.

5.6.6.4 Consist or Lading Speed Restriction

The Locomotive Segment enforces train and engine movements in compliance with consist or lading speed restrictions, as established by Timetable, Special Instructions, or General Order. Consist or lading speed restrictions result from the limits placed on particular equipment or from the arrangement of equipment in the train. Consist and lading speed restrictions may be conveyed from the dispatching system to the Office Segment as part of train data, which in turn delivers them to affected trains. Consist and lading speed restrictions may be delivered to a train during initialization of the Locomotive Segment, or after initialization as a result of train consist changes while en-route. Consist or lading speed restrictions may also be applied through manual entry while the train is stopped.

5.6.7 Work Zones

The Locomotive Segment enforces train or engine movements while closely approaching and/or within work zones conveyed via track bulletin. It is through this function primarily that I-ETMS prevents unauthorized train incursions into the limits of work zones or unauthorized train movements within the limits of a work zone by separate and diverse functions. First, the Locomotive Segment provides enforcement for the limits of the work zone. Secondly, I-ETMS will present prompts based on conditions described below to ascertain whether verbal permission from the Employee In Charge (EIC) has been received per the railroad operating rules pertaining to work zones. As a third level of protection, the visual display of the defined limits remains even after the prompts related to the work zone are acknowledged.

When a train or engine approaches and is within a configured threshold approach distance from active work zone limits or a work zone is issued for the track the train currently occupies, the Locomotive Segment prompts for an indication that verbal permission has been received from the EIC of the work zone to enter and proceed through the limits. Until the prompt is acknowledged indicating that verbal permission has been received to proceed through the work zone limits, the Locomotive Segment performs predictive warning and enforcement of a stop at the near limit of the work zone. When the prompt is acknowledged, signifying that verbal permission has been received (within the threshold approach distance and prior to application of a predictive enforcement brake application), the Locomotive Segment relieves enforcement of the stop at the near limit, allowing the train or engine to enter and operate through the limits of the work zone.

When a train or engine begins to move after stopping within the limits of an active work zone (having previously entered the limits), the Locomotive Segment provides a Work Zone warning and prompt requiring acknowledgement that verbal permission has been received from the EIC authorizing continued movement. If acknowledgement is not provided in response to the Work Zone prompt within a configurable time, the Locomotive Segment invokes a full-service enforcement brake application and stops the train in a fail safe manner. If the Work Zone prompt is acknowledged within a pre-configured time after beginning movement, the Locomotive Segment removes the Work Zone prompt and permits the train to continue movement through the Work Zone. I-ETMS will protect and provide enforcement for a change of direction within the limits of a work zone based on railroad-specific configuration parameters which are set in accordance with the railroad's operating rules.

When a train or engine is occupying the limits of a work zone when the Work Zone becomes active (based on time specified in the work zone track bulletin), the Locomotive Segment displays a Work Zone warning, and prompt requiring an acknowledgement that verbal permission has been received from the EIC to proceed through the limits, as described above. When time limits of a work zone have expired, the Locomotive Segment ceases to enforce train and engine movements through the work zone limits. If a full-service enforcement brake application was invoked due to enforcement of work zone limits just prior to the expiration of the limits, the Locomotive

Segment ceases enforcement of the work zone limits when the train comes to a complete stop.

The combination of (1) predictive and reactive enforcement, (2) the requirement for the train crew to provide an indication of their train's authorization to enter in order to remove that enforcement, and (3) the continuous display of work zone presence and limits provides three levels of protection against the risk of an unintended incursion into a work zone.

5.6.8 Malfunctioning Highway Grade Crossing Warning Systems

The Locomotive Segment enforces train operation through highway grade crossings where a crossing warning system malfunction has been indicated by track bulletin. Such track bulletins are issued by the train dispatcher and provided by the dispatching system to the Office Segment, which distributes them to all affected trains during Locomotive Segment initialization or en-route as they are created. The Locomotive Segment will display and enforce a stop at the location of a crossing for which a track bulletin indicating Activation Failure has been issued, and a 15mph speed head-end only restriction at the location of a crossing for which a track bulletin indicating False/Partial Activation or the existence of some other anomalous condition (broken crossbucks or stop sign, cars standing in close proximity to crossing, etc.) has been issued.

As the train or engine approaches and is within a configurable threshold distance of a crossing with a bulletined malfunction, the Locomotive Segment will display a prompt for the train crew to indicate whether they have received authorization to proceed through the crossing at normal speed. The train crew may provide such an indication when they have received instructions from an authorized or designated employee that alternative means of protection authorizing operation in accordance with 49 CFR 234 Appendix B has been provided.

In the absence of such instructions, a train which has stopped within a configurable distance short of a crossing with a bulletined Activation Failure, to allow a crew member to dismount and flag highway traffic to a stop, is then released to proceed through the crossing. Similarly, in the absence of such instructions, a train approaching a crossing with a bulletined False/Partial Activation will be enforced to proceed through the crossing not exceeding 15 mph.

Upon receipt of acknowledgement that the train is authorized to proceed through the crossing because alternative protection has been established at the crossing, the Locomotive Segment removes enforcement of any stop or reduced speed limit at the crossing, allowing the train to proceed in accordance with railroad Operating Rules. This acknowledgement releases enforcement only for the particular movement through the crossing of the train on which the acknowledgement was provided. The crossing malfunction bulletin remains fully in effect and enforceable for all subsequent movement of trains through the crossing until such time as the bulletin is cancelled by the train dispatcher or control operator.

5.6.9 Tracks Out of Service

The Locomotive Segment prevents a train from entering the limits of a track that has been bulletined as out of service. These track bulletins are provided by the dispatching system to the Office Segment, which distributes them to all affected trains during Locomotive Segment initialization or en-route as they are created. The Locomotive Segment will provide predictive enforcement of a stop at the limits of a track out of service until such time as the track is placed back in service and the corresponding track bulletin is voided.

5.6.10 Miscellaneous Track Bulletins

The Locomotive Segments displays the text conveyed by miscellaneous track bulletins upon request. Miscellaneous track bulletins are used to convey conditions not indicated by the track bulletins described above and may or may not convey enforceable operating limits to the Locomotive Segment. A miscellaneous track bulletin may address conditions such as severe weather, detector alert, encroachment into a train's authority limits by another train, or any other condition to which the train crew should be cognizant that is not otherwise protected by I-ETMS. When the miscellaneous track bulletin contains enforceable restrictions, the Locomotive Segment enforces train movement at the prescribed speed within the limits of the alert or may require a stop at or within the limits of the alert. A miscellaneous track bulletin requiring a stop may include a grace period, allowing the locomotive engineer of a train occupying the limits of the critical alert to move the train to a safe location, not fouling highway crossings at grade or bridges, prior to any enforcement action.

Miscellaneous track bulletins which do not contain enforceable criteria may describe conditions such as bad footing, security alerts, or company events.

5.6.11 Route Integrity Protection

The Locomotive Segment continuously monitors the state of wayside devices ahead of the train which provide information related to the integrity of the train's route ahead. Such devices may include switches in signaled territory, monitored hand operated switches in non-signaled territory, and other miscellaneous monitored devices. It is through these functions primarily that I-ETMS prevents the movement of trains through switches in improper position or under conditions indicated by hazard detector. Where WIUs are deployed, a single WIU may monitor and report the state of one or more attached devices, such as switches, signals, or hazard detectors.

5.6.11.1 Switches Monitored by WIU

I-ETMS ensures safe train movement through switches monitored by WIU by monitoring the status broadcasts provided by the radio-equipped WIUs directly connected to the switches. It enforces a stop at the location of a switch not known to be in a position safe for train movement. Typical applications of switch WIUs include, but are not limited to, power-operated main track switches in signaled territory and main track switches in non-signaled territory.

As a train navigates down the track, the Locomotive Segment listens for and accepts switch position data periodically broadcasted by radio-equipped WIUs that monitor the position of switches in advance of the train. The Locomotive Segment requires continuous refresh of valid switch position data for each switch within the display/route horizon in order to maintain the switch position (and resulting enforcement criteria). When the age of the last valid switch position data broadcast from a switch WIU exceeds a defined time tolerance threshold, I-ETMS assumes the switch position is unknown and handles it as described in Section 5.6.11.4.

Switch status information broadcast by a WIU may also be relayed to the dispatching system. With this "switch position awareness", the dispatching system can generate track bulletins or alert the train dispatcher of open switches in non-signaled territory, which in turn can provide protection to unequipped trains.

5.6.11.2 Switches Monitored by Track Circuit

I-ETMS ensures safe train movement through switches interlocked with a track circuit by monitoring the status broadcasts provided by the radio-equipped WIUs which monitor the track circuit. Typical applications of switches interlocked with a track circuit include, but are not limited to, main track switches in non-signaled territory.

As a train navigates down the track, the Locomotive Segment listens for and accepts status data periodically broadcasted by radio-equipped WIUs connected to track circuits in advance of the train. Any switch interlocked with the track circuit that is not in position for safe main track movement will cause the track circuit to indicate its most restrictive state. I-ETMS will display and enforce restricted speed throughout the limits of the track circuit and also require the train crew to identify or acknowledge the position of each switch monitored by the track circuit as described in Section 5.6.11.4.

5.6.11.3 Switches Monitored by Signal System

I-ETMS ensures safe train movement through switches interlocked with a signal system by monitoring the status broadcasts provided by the radio-equipped WIUs which directly monitor signals or by the monitoring of cab signal aspects, where the cab signal system is integrated with I-ETMS. Typical applications of switches monitored by a signal system include, but are not limited to, main track switches in signaled territory.

Switches in signaled territory are interconnected with the signal system and any switch in an improper condition for movement of a train on the Main Track over the switch results in a restrictive wayside and/or Cab Signal aspect on any signal governing the block in which the switch is located. When a wayside or Cab Signal indicates a block is unoccupied, all interlocked switches within the block are assumed to be in a position safe for train movement on the main track. When a wayside or Cab Signal does not indicate the conditions are favorable in the block, all switches are assumed to be in unknown position and enforcement of restricted speed through the block is provided accordingly. Additionally the train crew is required to identify or acknowledge the position of each switch monitored by the track circuit as described in Section 5.6.11.4.

5.6.11.4 Switch Position Unknown to I-ETMS

The position of a switch may be unknown to I-ETMS because it is either not monitored by any WIU or interlocked with a track circuit or signal system, or, because of a failure of a monitoring WIU, track circuit, signal, or I-ETMS communications system. When a train is approaching and within a configured threshold distance short of a switch in unknown position and a predictive enforcement full-service enforcement brake application has not been applied, the Locomotive Segment provides a warning and prompts for an indication of the position of the switch. Confirmation must be made indicating the switch is in a position safe for continued movement (including operation of any electric lock) when making a trailing point move through the switch, but must indicate the actual switch position when making a facing point move. The Locomotive Segment continues to enforce a stop at the switch until it receives a response that would allow safe movement over the switch.

5.6.11.5 Other Monitored Devices

I-ETMS may monitor the status of other devices, including hazard detectors, not directly integrated with a signal system which indicates the integrity of the route ahead, such as track circuits for detection of broken rail, slide fences, bridge alignment detectors, or any other hazard detector interlocked with the signal system or connected to a WIU. Through monitoring of these devices in manners similar to switches as described in Sections 5.6.11.1 and 5.6.11.3, the Locomotive Segment may enforce a stop or Restricted Speed operation in accordance with monitored device state.

5.6.12 Warning and Enforcement

When I-ETMS predicts that train movement has or otherwise would exceed any authority or speed limit, it invokes an enforcement brake application. It also provides warning where possible prior to invoking a full-service enforcement brake application so that immediate action may be taken to properly control train movement and avoid a full-service enforcement brake application. Where a restriction includes time attributes for when it is in effect, it becomes enforceable at a pre-configured time prior to the time it is to be in effect. If enforcement braking is in effect for a restriction at the time it expires, the restriction remains enforceable until such time as an affected train is brought to a stop. The various methods by which I-ETMS invokes warning and enforcement are described in this section.

5.6.12.1 Reactive (Overspeed) Warning and Enforcement

I-ETMS continuously monitors train compliance with any and all speed restrictions in effect at the train's current location. When the speed of the train exceeds the most restrictive speed limit in effect at the train's location but is within an overspeed tolerance, the Locomotive Segment displays an overspeed warning and sounds an alert. The warning persists as long as train speed remains in excess of the most restrictive speed limit and within the overspeed tolerance.

If the train speed exceeds the most restrictive speed limit in effect plus the overspeed tolerance, the Locomotive Segment invokes a full-service enforcement brake application

and displays the reason. The full-service enforcement brake application is maintained until the train is stopped.

A planned future enhancement is to provide the ability for I-ETMS to allow the locomotive engineer of a passenger train to perform a running release of the enforcement brake application once the overspeed condition is cleared.

I-ETMS takes into consideration whether the speed limit is applicable to the whole train or head-end only in the performance of reactive warning and enforcement.

5.6.12.2 Predictive Warning and Enforcement

I-ETMS continuously monitors train speed and proximity to speed restrictions or authority limits (which are considered zero-speed restrictions) in advance of the train. When it predicts that the train is within warning distance of an authority or speed restriction limit, a warning is displayed and an audible alert is sounded. Warning distance is the dynamically calculated sum of the predicted distance traveled by the train during a configured warning interval plus the stopping (or reducing) distance under full-service enforcement brake application required to prevent the train from exceeding an authority limit or other stop target, or entering the limits of speed restriction at a speed exceeding a pre-configured threshold over the limit.

While within warning distance, but not within stopping (or reducing) distance, the Locomotive Segment displays the predicted time until the full-service enforcement brake application will be applied. When action is taken to properly control movement of the train such that the train falls outside warning distance, I-ETMS ceases the warning. The time to enforcement may thus decrease, increase, or remain constant depending upon the dynamic actions, if any, taken in response to the warning.

If the action taken to control movement of the train is not sufficient to bring the train's operation in compliance with the speed or stop limit in advance, as predicted by I-ETMS prior to the location where a full-service enforcement brake application is required to prevent the train from exceeding the limit, I-ETMS will invoke a full-service enforcement brake application. The full-service enforcement brake application is maintained until the train is stopped. Figure 19 depicts the relationship between warning interval, stopping (or reducing) distance, and warning distance.

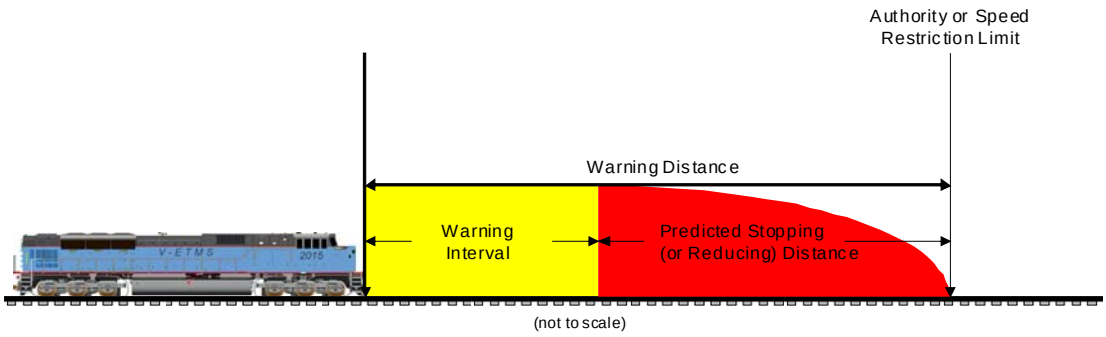

Figure 19 – Predictive Braking Calculations

I-ETMS prediction algorithms include the following factors:

- Current train speed;
- Proximity to limit of authority or restriction in advance;
- Track profile between train and limit of authority or restriction in advance;
- Locomotive control settings;
- Current state of brake system; and
- Train length, weight, and braking characteristics as defined by train consist data.

I-ETMS continuously displays textual warning distance and stopping distance from the current train location.

I-ETMS will additionally invoke an emergency enforcement brake application under certain conditions and subsequent to the full-service enforcement brake application if it is predicted to be insufficient to otherwise prevent the train from exceeding the authority or speed restriction limit for which enforcement braking was initially invoked. An I-ETMS equipped locomotive will require a penalty reduction limiting capability to preserve sufficient brake pipe pressure in order for this function to be useful. Conditions under which the emergency enforcement brake application would be invoked include the following:

- A full-service brake application has been active for at least some threshold time;
- the connection to the braking system for commanding emergency braking is cut in;
- the connection to the braking system for commanding emergency brake is not failed;
- the front brake pipe pressure is above a certain threshold;
- the current speed is within certain thresholds; and
- the train is still predicted to otherwise overrun the target.

At this time, the exact specification of these conditions is under research and development through an FRA-sponsored program being conducted at the Transportation Technology Center, Inc.

5.6.12.3 Restricted Speed Enforcement

I-ETMS enforces train and engine movement at Restricted Speed imposed by wayside signal indication, Cab Signal indication, movement authority condition, when the controlling locomotive is not at the leading end of the movement, or where required by rule or law. Enforcement of train movement in compliance with Restricted Speed has several facets.

When within the limits of a Restricted Speed restriction, the Locomotive Segment displays an indication that Restricted Speed is in effect and reactively enforces the configured maximum speed permitted under Restricted Speed rules for the railroad where the restriction is in effect, subject to overspeed tolerance as described in Section 5.6.12.1.

When approaching a Restricted Speed restriction, I-ETMS provides predictive enforcement of a stop at the limit of the restriction until such time as the train makes a "compliant speed reduction." A compliant speed reduction requires the speed of the train to be reduced below the maximum speed permitted under the railroad's Restricted Speed rule and the train to be within a threshold distance short of the limit of the Restricted Speed Restriction. At this point, the system recognizes a compliant speed reduction, removes the stop target, and enforces train movement in accordance with the configured Restricted Speed ceiling up to and within the limits of the Restricted Speed restriction. It should be noted that when making a compliant speed reduction, the speed of the train may likely be required to be at or below the Restricted Speed ceiling well before the train is within the threshold distance, to avoid predictive enforcement of the stop at the limit of the restriction. A compliant speed reduction is depicted in Figure 20. In this example, the maximum speed under the restricted speed rule is 20 mph.

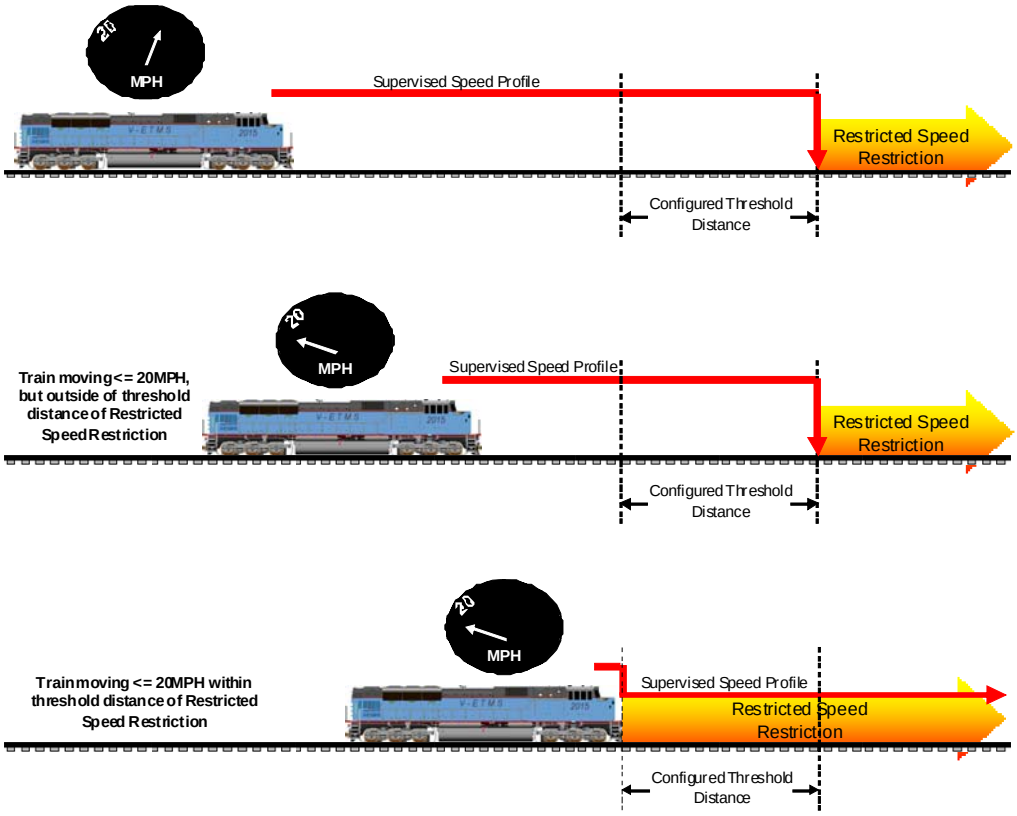

Figure 20 – Compliant Speed Reduction Approaching Restricted Speed Restriction

A train that fails to make a compliant speed reduction in approach to a Restricted Speed restriction will be subject to a predictive full-service enforcement brake application by I-ETMS sufficient to stop it prior to entering the limits of the Restricted Speed restriction.

5.6.13 Parking Brake

I-ETMS provides a "parking brake" function which may be used in addition to other means required by rule or law to secure the locomotive and train from movement. When a locomotive is stopped with the reverser handle centered, the Locomotive Segment provides a softkey to enable or disable the parking brake function. When the parking brake is enabled, the Locomotive Segment monitors the locomotive for movement, and, if locomotive movement is detected for a period in excess of a threshold time (5 seconds), I-ETMS invokes a full-service enforcement brake application. The parking brake function remains active until disabled.

5.6.14 Train Handling Exception Monitoring

I-ETMS monitors train speed, location, and locomotive control settings in order to detect potential exceptions to the train-handling practices as specified in the railroad's air brake and train-handling rules. When an exception is detected, I-ETMS displays an alert of the exception, if no other I-ETMS warning or alert is active due to enforcement

of operating limits. The alert is provided simply as advice and I-ETMS takes no specific action to enforce train handling rules, unless the exception is coincident with or results in a situation requiring enforcement. Table 11 lists some examples of train handling exceptions and the potential criteria used by I-ETMS to detect them. Train handling exceptions are logged and forwarded to the Office Segment for further processing.

Table 11 – Example Train Handling Exceptions and Criteria

Exception	Criteria
Power Braking	Locomotive Throttle >= 6 Brake Pipe Pressure < 76psi Speed > 20 MPH For >= 30 seconds
Brake Pipe Continuity	Front brake pipe pressure > 76 psi EOT pressure 10 psi < front brake Pipe For >= 60 seconds
Independent Brake Operation	Front brake pipe pressure < 82 psi Locomotive brake cylinder pressure > 10 psi Speed > 15 MPH For >= 30 seconds
Stopped with Brake Released	Speed = 0 MPH Brake Pipe > 84 psi For >= 300 seconds
Excessive Tractive Effort While Starting Train	Locomotive Throttle >= 6 Speed < 5 MPH
Engineer-Induced Emergency Brake Application	Emergency Brake application Speed > 8MPH and < 70MPH PCS closed
I-ETMS-Induced Enforcement Brake Application	Full-service enforcement brake application invoked by I-ETMS

When a train handling exception alert is displayed, the alert may be acknowledged to clear it from the display. The alert will otherwise be automatically cleared from the screen after a configured time has elapsed since it was first displayed if not previously acknowledged.

Additionally, a notification of the train handling exception is transmitted by the Locomotive Segment to the Office Segment. From there, the notification may be logged and distributed further to railroad information systems for record-keeping and possible follow-up.

I-ETMS provides several configuration parameters which allow the definition of train-handling exceptions on a per-railroad basis and in accordance with the train-handling rules of that railroad. It monitors train-handling against the exceptions applicable to the railroad that employs (or contracts for) the train crew, reflecting the general reciprocity of train-handling rules negotiated amongst the railroads.

5.6.15 Horn Protection

I-ETMS provides a configurable capability to sound the horn as a fallback to the engineer under conditions whereby the train is within a threshold time/distance from a highway crossing and the locomotive horn has not otherwise been manually sequenced. It will continuously sound the horn until such time as the locomotive engineer manually actuates the horn controls. Horn protection is actuated or suppressed at certain crossings as indicated in the I-ETMS track database which is constructed by the railroad in accordance with quiet zone ordinances. I-ETMS horn protection operates provided that the locomotive appurtenances, including the horn, are properly functioning to permit sounding the horn. I-ETMS never prevents use of the locomotive horn by the train crew.

5.6.16 Energy Management

I-ETMS provides an interface to an external Energy Management (EM) subsystem, such as New York Air Brake's LEADER™ or General Electric's Trip Optimizer™, which provides aid in the operation of the train in accordance with railroad schedule and fuel use performance objectives. I-ETMS provides track data, train consist data, location data, certain locomotive sensor readings, and the current enforceable operating profile (based on all existing enforcement targets) via this interface to the EM subsystem. The EM subsystem in turn calculates and returns, via the interface, the locomotive control settings required to meet the performance targets. I-ETMS may act on this information in one of two manners.

In a prompting mode, it displays the predicted speed and in-train forces calculated by the EM subsystem, along with a prompt indicating the desired locomotive control settings. No further action is taken with regard to the information provided by the EM subsystem. I-ETMS controls the display and display of train control information and prompts always takes precedence over EM displays.

In a cruise-control mode, it displays the predicted speed, in-train forces, and locomotive control settings calculated by the EM subsystem as in prompting mode. It additionally forwards the locomotive control settings via a Throttle/Brake Interface (TBI) to the locomotive control system for execution. The TBI provides an interface between I-ETMS and the locomotive control system, but is independent from and in no way preempts the train control and enforcement functions provided by I-ETMS. I-ETMS will suppress the forwarding of locomotive control settings to the TBI when it is not able to provide an accurate enforcement profile to the EM subsystem.

The EM subsystem is not a train control system, and is designed and implemented in such a manner as to preclude interference with I-ETMS train control functions. The operating profile calculated by the EM subsystem is presented in designated sections of the I-ETMS display. When the EM subsystem is operative, its operating profile is incorporated onto the I-ETMS train control display. An example screen is depicted in Figure 11.

The EM subsystem may also incorporate train pacing information as provided by the dispatching system in the calculation of its operating profile. Train pacing information from the dispatching system consists of a downstream target locations and arrival, dwell and/or departure times. Railroad dispatching systems will have the capability to provide more sophisticated downstream target locations for consumption by the EM subsystem and other trip optimization applications to provide broader operating efficiencies to the railroad.

5.6.17 I-ETMS Equipment Failures and Effects

I-ETMS operation depends upon the proper functioning of the components that make up its Locomotive, Office, Wayside, and Communications Segments. While it incorporates hardware and software components designed for reliable operation to minimize failures and their impact to operations, system design must include attributes which ensure safety is maintained when component failures occur. In some cases, redundant components may be deployed to increase reliability. This section provides a preliminary overview of the impact of failures on train crews and other operating personnel and is not intended as a failure modes and effects analysis or verification and validation of same. Additional information on actions to be taken until repairs are completed will be provided in each railroad's PTC Safety Plan in accordance with 236.1029(a).

Hardware and software failures manifest themselves and impact I-ETMS operations in different ways. Table 12 identifies the effect(s) observed upon failure of I-ETMS equipment. A complete description of the configuration and function of each subsystem and component may be found in Section 3.

Table 12 – Equipment Failures and Effects

Segment	Component Failed	Effect(s) Observed by Locomotive Engineer
Locomotive	Train Management Computer (TMC)	CDU displays failure of TMC Immediate full-service enforcement brake application as a result of fail-safe brake interface
	Computer Display Unit (CDU)	CDU blanks or indicates failure
	GPS Receiver	I-ETMS transitions from Active to Disengaged state when dead-reckoning capability exhausted.
	Cab Signal System	I-ETMS displays and enforces the most restrictive Cab Signal, i.e. RESTRICTING due to Cab Signal system cut-out or lack of receipt of Cab Signal aspect
	Peer-to-Peer Radio Subsystem (WIU communications)	I-ETMS displays and enforces all wayside signals and switches in their most restrictive state due to failure of TMC to receive state data from WIU

Segment	Component Failed	Effect(s) Observed by Locomotive Engineer
	Office Radio Subsystem (Office Segment Communications)	I-ETMS displays and enforces restrictive conditions as a result of failure of TMC to receive “heartbeat” from the Office Segment (see Section 5.5.7.3)
Wayside	Wayside Interface Unit (WIU)	I-ETMS displays and enforces wayside signal or switch in its most restrictive state due to failure of TMC to receive state data from WIU. Office Segment informs dispatching system that WIU is not reporting and that monitored switch position is not known.
	Peer-to-Peer Radio Subsystem (Locomotive)	I-ETMS displays and enforces affected wayside signal or switch in its most restrictive state due to failure of TMC to receive state data from WIU
	Signal Appliance	I-ETMS displays and enforces affected wayside signal or switch in its most restrictive state due to indication from WIU that signal appliance is failed
	Base Station Radio Subsystem (Office-Locomotive Communications)	I-ETMS displays and enforces restrictive conditions as a result of failure of TMC to receive “heartbeat” from the Office Segment (see Section 5.5.7.3)
Office	Back-Office Server Subsystem	Locomotive Segment displays and enforces restrictive conditions as a result of TMC failure to receive “heartbeat” from the Office Segment (see Section 5.5.7.3)
	Dispatching System	Locomotive Segment displays and enforces restrictive conditions as a result of TMC failure to receive any authority data and “heartbeat” indication that the Office Segment is operating in degraded mode

Failure of the Locomotive Segment may result in the need to cut-out I-ETMS on the affected locomotive in order to resume operation of the affected train. Railroads will promulgate rules in accordance with FRA regulations under which the Locomotive Segment may be cut-out and train operated under restrictions imposed by those rules. In ACS or ATC territory, failure of the Cab Signal system may necessitate cutting out the I-ETMS system as well.

Failure of Wayside equipment supporting I-ETMS operations will restrict train movements in proximity to, and past the affected wayside location. I-ETMS provides methods to advance the train past a failed wayside location without the need to cut-out

Locomotive Segment equipment, albeit in accordance with restrictions imposed by the system depending upon the type of wayside device.

Failure of the Office Segment, dispatching system, or office network subsystems will result in widespread restriction of all equipped trains operating in the subdivisions or districts governed by the affected system(s). However, high-availability design of the Office Segment and dispatching system, which eliminates single points of failure, will minimize the exposure to such events.

5.7 Summary of Operational Impacts

A summary of operational and organizational impacts resulting from the development, testing, and potential deployment of I-ETMS is described in this section. The exact nature of impacts and required changes to operating rules is dependent upon the existing rules maintained by the railroad implementing I-ETMS and the manner in which it chooses to implement the changes.

5.7.1 Operation of I-ETMS Locomotive Segment Equipment

Procedures, operating rules and practices for initialization, activation, and operation of I-ETMS, similar to those rules applicable to Cab Signal operation will be incorporated into the deploying railroad Operating Rules, System Special Instructions, and/or General Orders when the system is placed in revenue service. Additionally, rules will be promulgated in accordance with §236.1029 defining the procedures to be followed by train crews and the train dispatcher or control operator when a I-ETMS train experiences an en-route failure of the PTC system.

5.7.2 Conveyance of Mandatory Directives

I-ETMS supports electronic conveyance of mandatory directives either in a standalone manner to supplant the verbal process or in combination with the existing verbal conveyance process. In the standalone manner, I-ETMS may be utilized as the primary method of conveyance, receipt, acceptance, and acknowledgement of authorities or bulletin items will be made via the onboard display in lieu of the verbal conveyance by voice radio, however additional approval will be sought before these features are used. I-ETMS's electronic conveyance function and the dispatching systems are both expected to include all safety interlocks necessary to ensure that communications failures do not result in a hazardous condition.

Until additional approval is requested and granted for utilization of the standalone manner, crews will continue to obtain and acknowledge the required mandatory directive information via their paperwork and verbal communication with the dispatcher.

The primary method for conveyance of mandatory directives from the train dispatcher or control operator to an EIC will remain verbal.

5.7.3 Next Governing Signal

I-ETMS allows a train to operate in accordance with the indication of the next signal in advance prior to passing it when the train is currently operating on a signal more favorable than RESTRICTING, RESTRICTED PROCEED or STOP, and train movement is not otherwise restricted by rule or law requiring movement at Restricted Speed. Where I-ETMS directly monitors wayside signals, it may be able to realize and enforce the indication displayed by the next signal in advance prior to the location where the train crew is able to observe the signal, depending upon distance and line of sight to the signal.

5.7.4 Cab Signal Speed Control and Positive Stop Enforcement

In I-ETMS-controlled territory where Cab Signals are monitored and movement of trains is enforced by I-ETMS accordingly, traditional automatic Cab Signal operation is augmented with continuous speed control and positive enforcement of a stop at locations requiring a stop.

5.7.5 Predictive Enforcement

The current nature of predictive braking algorithms and the data they utilize may require that a level of conservatism be built-in to ensure target safety performance levels with great confidence. It is expected this conservatism will negatively impact train-handling and overall train velocity, and thus reduce capacity on I-ETMS-controlled territories and its cost-effectiveness. Ongoing monitoring and data collection of train performance during pilot, and any revenue demonstration phases of the project will be conducted to determine impacts while concurrently seeking ways to improve performance.

5.7.6 Energy Management and Train Handling Exception Monitoring

Energy Management and train handling exception monitoring are non-train control functions and their operation and use will be governed by rules promulgated in the air brake and train handling rules of the railroad.

5.7.7 Organizational Impact

Railroads and their PTC system suppliers will define and document processes for development, implementation, and operation of positive train control systems, as well as the roles and responsibilities of railroad and supplier personnel.

Revenue service operation and maintenance of I-ETMS will be described in each railroad's PTC Safety Plan (PTCSP). Railroad Operating Department, Mechanical and Engineering Department, and Information Technologies Department personnel will all play a role in the operation and maintenance of the system.

Maintenance of the system becomes the responsibility of the operating railroads as it is implemented and deployed. The configuration management plan for the system will be described in the respective PTCSPs. Maintenance procedures are described in the System Operations & Maintenance Manual and each operating railroad is responsible for maintenance of the system to ensure continued safe operations.

I-ETMS overlays rather than replaces the current Methods of Operation; and as a result, major changes to existing railroad operating rules and practices to provide for I-ETMS operations are not anticipated. Rules governing initialization, departure tests, operations with I-ETMS, and procedures to Cut-In and Cut-Out I-ETMS will be prescribed in each railroad's operating rules, Special Instructions and/or Operations Bulletins.

5.7.8 Impacts during Development and Testing

I-ETMS field testing is conducted under the supervision of authorized railroad employees and an FRA Test Monitor(s) when specified by FRA. Full test documentation, including detailed test procedures and measures that will be taken to protect trains and on-track equipment, will be provided by the railroad to the FRA Test Monitor for review and approval prior to conducting the actual test or tests, in accordance with the test requirements established by FRA.

I-ETMS test trains will operate in accordance with all applicable rules, regulations, or law. Field tests are to be conducted in such a manner as to ensure the safety of train movement and personnel, both for the test train(s), other trains, and employees in the immediate vicinity of the test area. Relief from compliance with specific operating rules or Special Instructions, such as the use of cell phones in the control compartment of a locomotive will be provided during authorized test activities.

Absolute Block may be imposed upon the test train during actual I-ETMS braking tests. In such case, the Absolute Block established by the train dispatcher will include both opposing and following trains on the same track during the test.

Training for train and engine crews operating I-ETMS test trains during field tests will be provided by the railroad I-ETMS project teams. Job briefings will be conducted with the train dispatcher, train and engine crew, and other affected employees each day of testing, and prior to each test to be conducted to ensure that each affected employee clearly understands the movements to be made.

A training program will be developed by each railroad's Operating Practices Department prior to the commencement of formal I-ETMS qualification tests.

6 Safety Architecture - §236.1013 (a)(4)

This section includes a description of the manner in which the system architecture satisfies the safety requirements as required by 49 CFR 236 Subpart I §236.1013 (a)(4).

Safety critical functions are identified in Section 5 – Concept of Operations of this document.

6.1 Locomotive Segment

I-ETMS is being developed as a locomotive centric system. Fundamental to safety, the system will default to a restrictive state unless positive indications allowing movement are received. As described in Section 3, the TMC accommodates three independent processors that independently drive a vital brake interface. Each processor cross channel compares information with the adjacent processors to insure random hardware failures do not prevent safe action. Failed processors default to a requested enforcing state; the brake interface card votes two of three processors to take action. This is described in Section 11.2.

The Locomotive Segment receives information from the Office Segment, the Wayside Segment, and from the locomotive itself. Safety critical messages from the Office Segment are protected with a 32 bit CRC, encrypted with hashing codes for authentication, encoded with data to verify source and destination, validated for timeliness, and information is range checked. Closed loop interaction with the Office Segment insures messages have been successfully received. Subsequent periodic closed loop polls ensure Office and Locomotive remain in sync. Each processor independently decodes the Office Segment messages for target generation and determines if brake applications should be held off.

Wayside data received by the Locomotive Segment also is protected with a 32 bit CRC, encrypted with hashing codes for authentication, encoded with data to verify source, validated for timeliness, and information is range checked. Data is broadcasted at a periodic rate, so each wayside status has known “time to live.” The Locomotive Segment (more specifically, individual processors) failing to receive updated status will default the target at the particular location to the most restrictive state. Again each processor independently decodes the Wayside Segment messages for target generation and determines if brake applications should be held off.

The Locomotive Segment will accept individual sensor inputs and broadcast them to the three individual processors. Each processor will independently verify all available sensor inputs and filter them into a single PTC value for use on that processor. The aforementioned cross channel compare will detect any anomalies.

6.2 Office Segment

The Office Segment reconstructs railroad dispatching system messages into a common format. This reconstruction is compared against the original message to ensure

correctness through the use of a diverse algorithm. The Office Segment also performs a simplified transformation check to supplement the dispatching system verification. Otherwise the Office acts as a router between railroad office systems and the Locomotive Segment.

In addition to supporting synchronization between the Office and Locomotive Segment, the Office Segment also performs a synchronization check with the dispatching system to ensure the Locomotive Segment is synchronized with the dispatching.

6.3 Wayside Segment

The Wayside Segment will be developed, installed, and verified in a manner consistent with vital signal design.

6.4 Communication Segment

The PTC system has been designed so that segment communication is not critical for safety. Information is protected by CRC and the Locomotive Segment accounts for any loss of information by defaulting to the most restrictive state.

6.5 Safety Requirements

Safety related requirements are being established by two means:

1. By the identification of requirements needed for the implementation of safety critical functions, and;

2. By the identification of requirements needed for mitigation of hazards identified through the formal safety process.

All requirements are documented within Requisite Pro and are formally traced to lower level requirements. Requirements identified as safety related are tagged with a safety critical attribute that is inherited by all lower level requirements.

Safety critical functions and the safety process have been identified in Section 5 and Section 10.2 of this document respectively.

6.6 System Safety Process

The system safety process described in Section 6.6 identifies several of the tools that will be used to evaluate the system against potential hazards. Hazards will be identified through various analyses (e.g., PHA), documented to show failures and mitigations (e.g., FTA), tracked using a Hazard Log and closed when acceptable (HRI). Any additional analyses determined to be required will be included as part of the PTCSP submission. The elimination or reduction of identified hazards corresponds to MIL-STD-882C reference [4]. The process for testing safety requirements is included in a Verification Plan.

6.7 General Onboard Processing

As described in detail in Section 3.4.1, the I-ETMS system utilizes three identical train control processors operating identical software. Each train control processor utilizes a dedicated communication bus to a corresponding microcontroller on the brake interface card. Each microcontroller is segregated and monitored by independent watchdog devices. Loss of communications from a train control processor will default the individual brake interface channel into a penalty enforcing state. The brake interface card is designed so that two of the three channels are required to stop penalty brake application to prevent the brakes from being applied. The brake interface card has been designed to actively test in real time all the critical circuitry required to perform a penalty brake application. A Failure Mode and Effects Analysis (FMEA) has been conducted on the brake interface card which is considered AREMA Class II hardware (Class I excluding the microcontrollers). The train control processors also cross channel compare some data to insure both static expectations and dynamic targets are within tolerances. Two train control processors can vote the third train control processor out (default to an enforcing, single channel, state). This architecture protects the system from any random hardware failures.

6.8 Locomotive Segment Interface Failures

All interfaces in the Locomotive Segment require formal failure analysis to show adequate mitigation has been established to prevent identified failures.

6.9 Systemic Errors

The triplex processor card hardware will run common code. Common requirement base and code allows for better review and testing of the system (as compared to a dissimilar approach). Systemic errors will be shown to be minimized through formal validation of requirements and operational testing (lab and field) via a master test strategy. Requirements will also be validated, verified and traced to specific test procedures.

6.10 Fault Tolerant

The architecture is fault tolerant to any single processing card failure. Individual inputs may be fault tolerant depending on redundancy and potential use of safe defaults. The Segment level requirements are completed and formal design decomposition has begun to illustrate this feature. Lower level design documentation will be included as part of the PTCSP process and will document how inputs are fault tolerant.

7 Preliminary Human Factors Analysis - §236.1013 (a)(5)

This section describes the initial analysis techniques used to assess the impact of human factors in relation to train operation with the HMI for I-ETMS. This examination focused attention on the system's impact on train crew performance and system safety. The overall goal of this preliminary analysis is to demonstrate how the HMI has been designed to maximize system safety while minimizing locomotive crew workload. This analysis complies with the requirements of 49 CFR §236.1013(a)(5) and also provides a description of the extent to which the HMI design follows accepted human factors design guidelines that are likely to detect and mitigate potential human error during the operation of the I-ETMS system.

7.1 Human Machine Interface

The HMI of the I-ETMS system is an extension of an existing, approved train control system currently in operation at the BNSF. As part of the approval process, BNSF conducted Human Factors Analysis, Workload Study, HMI Design Analysis, and 49 CFR §236 Appendix E Analysis against the original ETMS® HMI (BNSF PSP, Appendix U). Applicable aspects from these analyses include situational awareness, predictability and consistency, user's memory load and information processing, glare, luminance, and contrast, general screen layout, and character color, spacing, and location.

Results from these studies also included recommendations regarding operating philosophy, engineer training, and display organization/presentation. Any changes made to the HMI stemming from these recommendations, as well as reasons for declining the incorporation of other of the recommendations, are documented in the approved BNSF PSP. The elements of these analyses are consistent with and applicable to I-ETMS except as detailed in the following sections.

Upon completion of the I-ETMS HMI design, a detailed evaluation of any modifications to the approved ETMS HMI will be performed. Changes will be documented and appropriate analysis will be conducted to evaluate effects on previously performed Human Factors Analysis, Workload Study, and HMI Design Analysis. The final HFA required to be submitted with the PTCSP will address any remaining or additional issues, including those introduced by updates that were made to the layout of the HMI to support the I-ETMS design. The following sections identify the high-level differences between the ETMS and I-ETMS implementations.

7.1.1 Crew Reliance

I-ETMS system is a vital system, which allows the crew to rely on the information being presented. The PTCSP will provide a sensitivity analysis specifically related to crew reliance. Train crew rules and procedures will be established to address suspected display anomalies. Crews will be trained on these procedures.

7.1.2 Computer Display Unit

The Computer Display Units (CDU) installed in the cab will support each crew member in the locomotive receiving the same I-ETMS information displayed in the same manner enabling them to execute any functions necessary to each crew member's duties as presently specified by 49 CFR §236.1029(f).

A CDU-I with key functionality will be available only to the locomotive engineer. The CDU-I has eight programmable soft key labels across the top or bottom of the display. Functional keys are identified by blue labels. Navigation keys are identified by green labels, e.g. menu keys. Keys used by the locomotive engineer for acceptance or rejection of system prompts are labeled in yellow. Red labels identify a pending prompt requiring engineer interaction or indicating the arrival of trains for a conditional authority. The keys that are available while stopped or moving are dependent on the I-ETMS system state and whether or not any braking or warning messages are being displayed. When a warning or braking banner is displayed on the CDU-I the menu keys are removed. Menu keys are the keys that are available on the Main menu and Menu 1, i.e. Menu1, Main, Mandatory Directives, Consist, Target Prompt, Switching Mode On, Switching Mode Off, Init, Depart Test, Select Location, Cut Out, Cut In, Park On, Park Off, and Crew Logoff. Therefore, these functions are not available to the locomotive engineer when the warning or braking banner is displayed.

The system is designed to support a CDU-NI that will display the same information as the primary display, without the ability for crew interaction.

I-ETMS includes processes for ensuring mandatory directive data is in sync between the dispatching system and the Locomotive Segment. In addition, the PTC system validates the integrity of each message received both onboard and in the back office. Out-of-sync conditions or message integrity failures will cause I-ETMS to enter the most restrictive state without the need for human intervention to detect the failed condition. Therefore the CDU does not need to be used as a means to compare the information that is received verbally or on paperwork to the data being used by the PTC system.

There is no visible change to the display layout between the two devices. The CDU-NI is to be a read only display and will not provide soft keys for user input. Key presses on the CDU-NI would have no effect on the system, so there is no need to mitigate any hazards associated with simultaneous key inputs. The use of an additional display to satisfy the current requirements of 236.1029(f) would not require any additional audible device; a single Sonalert® would continue to provide audible alerts related to I-ETMS.

7.1.3 Delivery of Mandatory Directives

I-ETMS supports both the current verbal process for delivery and acknowledgement of Mandatory Directives as well as an alternative electronic delivery and acknowledgement process. Specific onboard responses and crew responsibility are dependent upon individual railroad Operating Rules and Practices. Prior to utilizing the electronic delivery and acknowledgement feature, a railroad will submit a PTCSP or a request for amendment of its PTCSP that shows that the reading and acknowledging of mandatory directives via the PTC display by the locomotive engineer while the train is in motion can be done in a manner consistent with 49 CFR §236.1029(f).

The utilization of I-ETMS as a supplement to verbal delivery of mandatory directives is consistent with current operation; where a member of the crew will receive the mandatory directive verbally, transcribe it on the prescribed form, and repeat it to the train dispatcher or control operator. Upon successful repeat of the Mandatory Directive, the train dispatcher or control operator will activate the Mandatory Directive. In combination with the verbal process, I-ETMS will receive an electronic copy of the same mandatory directive (as entered by the train dispatcher or control operator) and acknowledge receipt at the application level. The crew is not required to acknowledge receipt of the electronic copy of the Mandatory Directive but a textual representation of the Mandatory Directive is available for review if selected on the CDU-I. Operating rules and practices remain consistent with current railroad operation. Should a discrepancy exist between the Mandatory Directive copied by the crew and the electronic copy, train and engine crew members will be instructed to immediately stop further movement until such time as they have reached an understanding of the movements to be made and any conditions imposed upon their movement with the train dispatcher or control operator.

The alternative process – electronic delivery and acknowledgment - would relieve the crew of the requirements to transcribe and repeat the Mandatory Directive to the train dispatcher or control operator and would allow the crew to review, and accept or reject a movement authority electronically. Mandatory Directives conveying movement authority are electronically delivered to the Locomotive Segment. I-ETMS acknowledges successful receipt of the Mandatory Directive at the application level, and prompts the crew to review and accept or reject the movement authority. Upon review and acceptance by a member of the crew, the movement authority is now enforceable. Upon review and rejection by a member of the crew, the movement authority is deleted on the Locomotive Segment and the crew must contact the train dispatcher or control operator for further instructions. Temporary Speed Restrictions, Work Zones, and Miscellaneous Track Bulletins are immediately placed in effect upon successful receipt by the Locomotive Segment even though crew review and acknowledgement is required. Should a failure of the Locomotive Segment occur, the crew will be required to stop further movement until such time as each applicable Mandatory Directive has been verbally copied from and repeated to the train dispatcher or control operator.

7.1.4 Energy Management

The I-ETMS display has been redesigned to shift textual stopping and warning distance and current head end location slightly to the right (see Figure 9 and Figure 10) to provide a small area for display of optional EM data. I-ETMS currently supports two separate, vendor-specific EM applications; however each will utilize a common set of display elements and interfaces to I-ETMS. I-ETMS hosts the EM application on a processor that is independent from the three train control processors. An Interface Control Document (ICD) has been developed to coordinate sharing of train data and display data between the two systems. Vendors of future EM applications will have to abide by this ICD or request changes to support their products.

The I-ETMS system displays train control and EM data on a prioritized basis, with train control warnings and enforcements assigned the highest priority. The EM application may only request the display of its associated data. When the Energy Management application is not in use, the display area designated for EM will remain unused. EM data may be present on the CDU graphical track line or on a display that is independent of I-ETMS, depending upon the requirements of an individual railroad.

Figure 11shows the display additions from an EM application. Immediately below the train profile, in-train forces and brake cylinder pressure graphs are depicted. When higher priority I-ETMS prompts and warnings are not displayed, EM advisory messages may be displayed. EM advisories are displayed on a gray background and follow consistent human factors principles. I-ETMS may display predicted speeds within the track grade as determined by the EM application.

The design approach for EM advisories is consistent with the approach used for train control advisories, prompts, and warnings. The background color of EM advisories will be unique to avoid confusion with train control advisories. EM application data uses I-ETMS character size and spacing. Phrases are simple and concise to minimize head down time and cognitive processing. Upon completion of the I-ETMS HMI design, a detailed evaluation of any modifications to the approved ETMS HMI will be performed. Changes will be documented and appropriate analysis will be conducted to evaluate effects on previously performed Human Factors Analysis, Workload Study, and HMI Design Analysis.

The graphical representations of in-train forces and brake cylinder pressure are simple and minimize head down time and cognitive processing. Graphs are consistent with those displayed in existing LEADER implementations and in locomotive engineer training simulators. Predicted speeds provided by an Energy Management system are displayed in a manner consistent with I-ETMS milepost data. The design of I-ETMS graphical displays insures that application data provided by an Energy Management system is adequately spaced to promote readability.

Individual railroads implementing EM applications on the I-ETMS platform will develop and provide comprehensive instruction on the proper operation of these systems.

7.2 Impact of Interoperability

I-ETMS processes track data, movement authority data, applicable speed restriction data, and configuration file data to create a route over which movement authority limits and speed restrictions are enforced. This processing of information is done within the context of the specific Method of Operation that is in effect on a particular railroad district, subdivision, or track segment. I-ETMS software capabilities will be designed to determine the applicable priority for proper handling of multiple enforceable targets at any given time. I-ETMS will be designed to be adaptable to and function as intended with a variety of known Methods of Operation as documented in Section 5 - Concept of Operations. As a result, the overall look and function of the HMI remains consistent across all I-ETMS applicable categories of railroad operations as described in Section 4.

8 Applicability of the Requirements of Subparts A Through G of 236 - §236.1013 (a)(6)

This section consists of an analysis of the applicability to the PTC system of the requirements of subparts A through G of Part 236 that may no longer apply or are satisfied by the PTC system using an alternative method, and an explanation of the manner in which those requirements are otherwise fulfilled.

Each citation of a rule or regulation is accompanied by a justification of why the rule or regulation does not apply or how the rule or regulation is being satisfied. The production I-ETMS system is compliant with all requirements contained within Part 236 Subparts A-G with the following noted exceptions and justifications.

8.1 §236.76 Tagging of wires and interference of wires or tags with signal apparatus

I-ETMS hardware consists of computers, computer peripherals, and communication devices. Onboard the locomotive and at the wayside locations, production equipment will not be tagged where there are individual wires in preformed cables or sealed connectors, connectors between circuit boards within devices, wires inside radios, and individual antenna coax internal Line Replaceable Unit (LRU) interconnects. Such items are under control of supplying vendors and are not directly accessed by railroad personnel. To the greatest extent possible, individual wires are grouped into cables, which are appropriately labeled, and attached to keyed connectors to facilitate quick and accurate installation. Where discrete wiring is necessary, and within LRUs that railroad personnel are required to access, the intent is to fully comply with this requirement.

8.2 §236.109 Time releases, timing relays and timing devices

I-ETMS hardware consists of computers, computer peripherals, and communication devices that incorporate numerous state-of-the-art timing devices. These timing devices contain no moving parts and are far more reliable than the devices for which the regulation was written to address. Timer anomalies will affect communication capability and is a self revealing failure. In addition, the enforcement card incorporates two independent timers that are periodically self-tested.

8.3 §236.552 Insulation resistance; requirement

I-ETMS hardware consists of computers, computer peripherals, and communication devices that could be damaged during resistance testing. Unexpected failures of locomotive wiring that results in a failure of the Locomotive Segment will not jeopardize the safety of the train operations or the safety of surrounding equipment/personnel. A train remains subject to the provisions of the existing operating rules with or without I-ETMS operating onboard.

Insulation testing is intended to be performed on the wiring that connects the I-ETMS brake interface to the locomotive air brake computer. Test points are established in the operations and maintenance manual for I-ETMS. The railroad is requesting relief from meggering sensitive data cables (i.e. data buses, data bus ribbon cables, Ethernet cables, etc.) that can cause harm to the computing equipment and are not necessarily exclusively responsible for safety-critical functions (e.g. braking the train).

8.4 §236.566 Locomotive of each train operating in train stop, train control or cab signal territory; equipped

Requirements are now governed by 49 CFR 236.1006.

8.5 §236.567 Restrictions imposed when device fails and/or is cut out en route

Requirements are now governed by 49 CFR 236.1029.

8.6 §236.586 Daily or after trip test

The testing of the electronic systems of I-ETMS is performed automatically during the initialization tests prior to an equipped train's departure. Failure or disarrangement of I-ETMS components is detected at this time. The departure test electronically records the results and requires successful pass criteria before the system can be initialized and engaged to be used in service.

8.7 §236.587 Departure test

I-ETMS provides the capability for the train crew or other qualified personnel to invoke a departure test as required by this regulation or railroad rule. Additionally, I-ETMS will require successful completion of a departure test under conditions described in Section 5.6.2 as part of the initialization process.

9 Service Restoration & Mitigation Plans and Security Measures - §236.1013 (a)(7)

This section contains the plan for a prioritized service restoration and mitigation plan and a description of the necessary security measures for the system as per §236.1013 (a)(7). The comprehensive and railroad-specific details of each shall be provided in each Railroad's PTCSP.

The Railroad's service restoration and mitigation plan will address restoration of communications services in the event of their loss or disruption. The service restoration plan will speak to the various segments of communications services including wired public and private networks and wireless public and private networks. The plan will cover various mechanisms specific to each segment to mitigate service interruptions. In the PTCDP, guidelines are provided for implementing railroads as they deploy I-ETMS. Railroad-specific details and a railroad's actual service and mitigation plan will be provided by each Railroad in its PTCSP. As the system for which this plan is required is still under development and testing, most aspects of the plan are yet undetermined.

This section of the PTCDP also provides a high level description of the security measures for the protection of I-ETMS as required by §236.1033. The security measures address train-borne, wayside, and centrally located train control subsystems and/or components as applicable. Security measures have been designed to limit unauthorized access to and prevent tampering with or overriding the safety functions of the system. Each of the system segments is protected utilizing physical security measures, operational procedures, and security policies. Railroad-specific security tools, I-ETMS security design and implementation details, as well as test results for conformance testing in accordance with a master test strategy will be provided by each Railroad in its PTCSP.

9.1 Service Restoration and Mitigation Plan

PTC service interruptions and issues will be promptly identified and routed to departmental or service support groups based on status information obtained through persistent system monitoring. Railroads today have existing departmental and service support groups responsible and experienced in monitoring and troubleshooting mission critical software, devices, and networks. The support scenarios introduced by the PTC system increase the number of critical software, devices, and networks to be managed and supported by railroad support groups that fit each road's organizational structure. However, fundamental monitoring and problem resolution techniques to detect problems and restore service are not new and are presently required either by regulation or corporate departmental internal controls.

Railroads will mitigate failures in service by streamlining problem detection, problem solving processes, automating analysis of device health, and inter-support group communication. For example, management systems can be integrated with trouble

ticketing systems so as problems are detected, trouble tickets are generated for the correct support group to respond and resolve. Automating system monitoring will also enable some predictive failure of devices so that PTC assets which show early signs of failure can be replaced or repaired before they fail. Detecting early failures in this way also allows any service interruptions associated with a preventative activity to be scheduled for minimal operational impact. A proposed Interoperable Systems Management System is being designed to provide for improved inter-railroad communication when problems occur that affect the operations of multiple railroads. Sharing device status information with other railroads will allow for early operational responses to unplanned service disruptions caused by weather or other natural disasters that railroads regularly overcome.

Ultimately, the establishment of a comprehensive service restoration and mitigation plan can only be completed upon successful testing of the I-ETMS system. It is expected that system testing will validate the I-ETMS design and its ability to tolerate intermittent outages in the Communications Segment. This will provide a railroad planning to deploy I-ETMS the necessary criteria to support a comprehensive assessment of its wired and wireless networks to formulate an effective service restoration and mitigation plan. The process of developing a plan will include an assessment of the assets being protected and possible threats to those assets, an evaluation of existing mitigation techniques including operational policies and procedures and physical deterrents, building scenarios to identify support and mitigation strategies, and determining priorities for service restoration. Any railroad filing a PTCSP associated with the I-ETMS system will include full details of its plan as required by §236.1033 (f).

9.1.1 Railroad Wired Networks

Railroad wired networks are comprised of private and public infrastructure. Typically, the public infrastructure consists of leased circuits which are used to extend or augment the private infrastructure. While these wired networks are characteristically robust and reliable, planned and unplanned service interruptions may occur. Railroads implement automated monitoring and alert systems to proactively identify service interruptions and alert personnel to disruptions so remedial action may be taken. Generally, interruptions to service are identified in the field and communicated to a central support staff center for triage and disbursement to the appropriate party either within the company or externally for public infrastructure issues.

To determine “what happens when,” a fault tree and triage plan will be developed as the system is tested and implemented as part of the support and maintenance documentation for the Communications Segment. When determining the extent to which alternate data paths or expedited restoration services should be developed for a given service, it is important to quantify the potential service disruption which may be experienced by the I-ETMS system. Depending on the potential impact of any particular outage, redundant circuits are typically provided to minimize service interruptions. This does not imply that redundancy of all wired circuits is required to maintain reliable service, but that it is one way to mitigate a potential disruption. For example, a wired network may provide a single path of connectivity in the network and ultimately to the

wireless network in support of I-ETMS system communications between the Office Segment and Locomotive Segment. However, for a given area of railroad right of way serviced by a wired network, there may be alternate wireless coverage paths such as public cellular or 802.11. In these cases, the availability of alternate wireless paths might obviate the need for redundant wired paths to mitigate a service interruption.

9.1.2 Railroad Wireless Networks

Railroad wireless paths may consist of 802.11, public cellular, private data radio, satellite, or other available technologies. Similar to wired networks, these wireless networks are comprised of private and public infrastructure. In most cases, the Railroad's private wireless network is managed and monitored in a similar fashion to the wired network through the use of automated tools and alerts. Since all wireless paths are subject to service interruptions, planned or unplanned, it is imperative that railroads deploying I-ETMS conduct wireless coverage analysis of the available paths in areas of I-ETMS deployment to assess the need for alternate paths and appropriate service disruption mitigation techniques.

While the I-ETMS system is designed to tolerate intermittent message transmission via the railroad provided Communications Segment, the acceptable outage duration in any given area will be dependent on the operational characteristics of the particular track segment. Again, as in the case of wired networks, the railroad must evaluate the availability of each of the deployed wireless network paths in I-ETMS territory to assess the impact of potential service interruptions.

In many cases where more than one wireless path is available and those paths are serviced by independent wired networks or networks with sufficient service support techniques, no additional measures will be required to support the operational demands of the I-ETMS system.

9.2 Security

Optimum protection of the PTC system comes from an integrated approach employing mutually supporting elements of physical security measures, operational procedures and security policies. I-ETMS has design criteria for security, implementation efficiency, versatility, and simplicity.

Specific security measures have been designed to prevent unauthorized access to and/or spoofing of safety-critical messages wherever these messages are communicated via radio, Internet or public switched network. Accordingly, all encryption will be accomplished with Advanced Encryption Standard (AES), a cipher approved by the National Security Agency for top secret information. AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes). I-ETMS will utilize multiple security measures to provide security for the system: encryption, user authentication, HMAC keys, timestamps, X.509 certificates, CRCs, EMP headers, and other means to insure safe and secure methods for transmitting data. Additionally, the system will be protected by implementing railroads utilizing physical and operational security measures such as

locks, video and network surveillance, alarms, personnel, operating rules and policies, etc.

9.2.1 Security Objectives for I-ETMS

Each railroad is responsible for implementing such measures to accomplish the following security objectives:

- Deterrence: security measures are established to either induce potential intruders to seek alternative targets rather than I-ETMS components or to discourage an offense altogether
- Detection: security measures are installed to monitor for unauthorized intrusion; and where feasible, provide intruder annunciation or report
- Delay: security measures are installed to delay an intruder's access to a I-ETMS physical asset and possibly provide time for incident response
- Assessment: the process of evaluating the legitimacy of an event and the procedures required to respond
- Communication: the process by which intrusions or breaches are made known to stakeholders
- Response: immediate measures taken to assess, interrupt and/or apprehend an intruder
- Intelligence: measures designed to collect, process, analyze, evaluate and interpret information on potential threats
- Audit: the review and inspection of security measures to evaluate effectiveness.

9.3 Locomotive Segment Security Measures

The TMC includes a tamper sensor that allows for detection of removed modules or disconnected I/O cables. A tamper detection bar, shown in Figure 21 below, has been designed to attach to the front bottom edge of the TMC. This bar holds the EBI, IOC, and DIO connectors in place and also prohibits the removal of any modules in the TMC. The bar is held in place by three screws on the front bottom edge of the TMC near the slot 1, slot 5, and slot 10 positions. The bar also has a feature that allows for installation of a plastic or lead tamper evident seal. In order to remove the bar, the seal must be broken and the screws must be removed. When the bar is in place, a switch inside the TMC is activated to indicate the system is intact. Once removed, that switch opens and a system fault is raised.

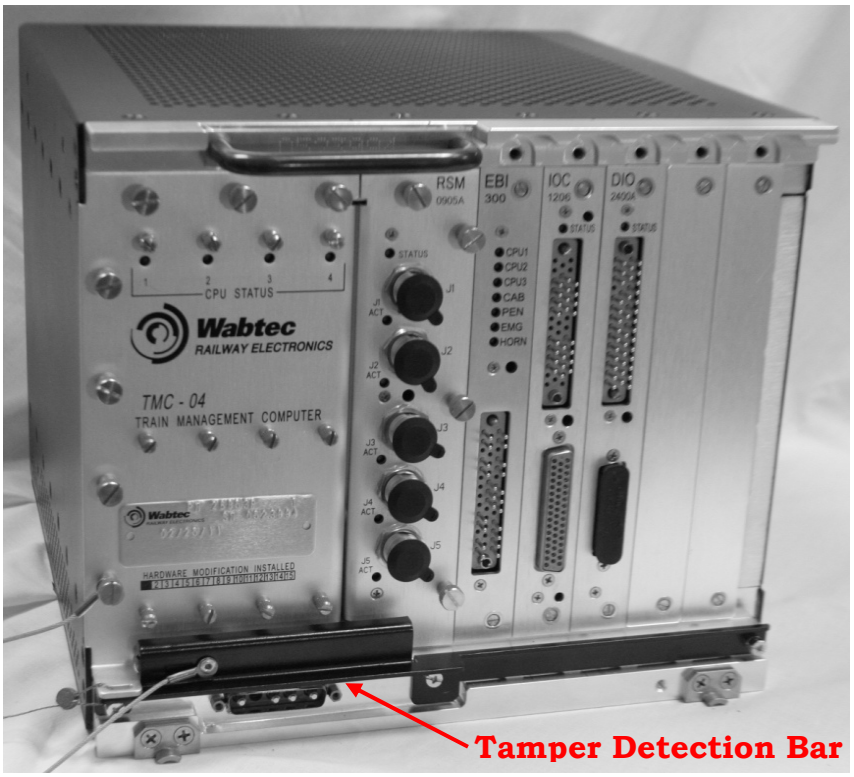

Figure 21 – TMC Tamper Detection Bar

The locomotive I-ETMS application is secured against unauthorized access via the application software. User authentication is required to access the system and perform operational and configuration functions. This authentication requires the user to enter valid credentials in the form of user ID and password. Interoperability is handled through authentication via the employing railroad for authorization. Security of messaging between the Locomotive Segment and other segments is discussed in the Communications Segment Security Measures section below.

9.4 Wayside Segment Security Measures

The I-ETMS wayside equipment is mounted within signal enclosures that are physically secured. This physical security includes locks or other mechanical means of preventing unauthorized access consistent with 49 CFR 236 Subpart A §236.3 and 49 CFR 234 Subpart D §234.211. These security measures help to secure the equipment from physical tampering as access is restricted to authorized railroad employees, consistent with existing operating practices. I-ETMS is also secured against unauthorized access via the application software. User authentication is required to access the system and perform operational and configuration functions. This authentication requires the user to enter valid credentials in the form of user ID and password. Any WIU settings that can affect the safety, vitality, or critical performance of the system is password protected and requires local presence to take effect, unless covered by another methodology. Security of messaging between the wayside segment and other segments is discussed in the Communications Segment Security Measures section below.

9.5 Office Segment Security Measures

The I-ETMS office equipment is located within secure railroad facilities (e.g. Information Technology Data Centers) that are physically secured by locks or other electronic security means of preventing unauthorized access. Only authorized railroad employees are allowed access to the facilities which house the office equipment. Access to the hardware or software for configuration is limited to only those with a need to perform the duties of their positions and is validated through user authentication. This authentication requires the user to enter valid credentials in the form of user ID and password. Further security against unauthorized network access is provided based on best practices (e.g. network intrusion detection, anti-virus protection, firewalls, etc.) as implemented by the operating railroad and a host of internal controls, such as the four COBIT (Control Objectives for Information and related Technology) domains. Security of messaging between the office segment and other segments is discussed in the Communications Segment Security Measures section below.

9.6 Communications Segment Security Measures

The security design of the Communications Segment also pervades the other three segments of I-ETMS and is built upon the requirements of 49 CFR 236 Subpart I §236.1033. I-ETMS uses a keyed Hash Message Authentication Code (HMAC) to provide cryptographic message integrity and authentication as required by 49 CFR 236 Subpart I §236.1033 (a). An interoperable Key Exchange Service will be utilized to manage HMAC keys. HMAC is applied by I-ETMS to safety critical data in messages between the Locomotive, Wayside, and Office segments. This provides a high level of security through the detection of latent, corrupted/manipulated, or “spoofed” messages. Authentication and validation between the locomotive and other segments occurs when the HMAC included in the message (from the WIU or BOS) matches the HMAC independently calculated by the Locomotive Segment. I-ETMS discards any messages that do not pass HMAC validation. The use of unique keys allows a receiver to validate both the integrity of the received message as well as the identity of the sender. The content of the message over which the HMAC is generated includes a field that contains the time a message was sent to provide mitigation for message replay. To create the HMAC Hash, each PTC asset will have a unique key installed during provisioning. Because each PTC asset has its own unique HMAC key, the veracity of the sender is implicit in the HMAC contained in the message. The HMAC keys are protected by encryption using X.509 certificates. The X.509 Certification Authorities protection measures are the responsibility of each road to implement its own controls to protect its internal Certification Authority.

Mutual cross domain certificates will be used to establish trust for communications between the back office segments of the railroads. The cross certificates will be issued by railroad CAs and will be physically installed on the corresponding CA of the other railroad to initiate trust. The cross certificate will be used to verify the signing authority of the other railroad.

I-ETMS is designed to operate as a vital overlay system such that it fails in a defined safe state. It is important to distinguish the difference in impact on the PTC messaging system in terms of the role the communication system plays in delivering a message versus the security or integrity of that message. While message *integrity* is essential to the safe operation of the system, message *delivery* does not affect safe operation. The reliable operation of communication services does impact the delivery of messages and is required to maintain an operational state of the system. However, if a message fails to be received due to loss of communication service or if messages are received latently, the system is designed to operate safely and to fail to a safe state. A service restoration plan which is prioritized based on projected impact to operational availability is essential to reliable operation of I-ETMS.

Each Railroad already employs various methods and technologies to protect its own assets and networks, including firewalls, intrusion detection, vulnerability assessments, and audits, etc. The processes and procedures a railroad utilizes to protect its network from intrusion which protect its financial and operational data as required by Sarbanes Oxley and Control Objectives for Information and related Technology (COBIT) “Delivery and Support” controls are the same controls in place to protect the network which I-ETMS will utilize.

10 I-ETMS Target Safety Levels - §236.1013 (a)(8)

This section describes a description of target safety levels (e.g., MTTHE for major subsystems as defined in subpart H), including requirements for system availability and a description of all backup methods of operation and any critical assumptions associated with the target levels as required by 49 CFR 236 Subpart I §236.1013 (a)(8).

10.1 System Safety under Normal Operations

I-ETMS is a vital overlay train control system that works in conjunction with existing Methods of Operation to protect against authority limit violations or over-speed conditions. I-ETMS provides an additional level of protection through an overlay approach that utilizes existing methods of railroad operations, train dispatch systems, field signal systems, and any other system supporting train operations as the primary means of control. Upon en-route occurrence of a failure and/or deactivation of the Locomotive Segment, an affected train will proceed in accordance with the underlying Method of Operation subject to operating restrictions imposed by regulation or railroad operating rules.

10.2 System Safety Processes

The safety assessment process provides a methodology for assurance that all relevant failure conditions are identified and that all significant combinations of failures which could cause those failure conditions have been considered. The system safety assessment process begins with the concept design from which the safety requirements for the system will be derived. As the system design evolves, changes may be made and the modified design will be reassessed. The process will be iterative in nature and will end with the verification that the design meets the safety requirements.

In general, the safety process is a set of four major activities repeated for each iteration of the development effort: hazard identification, assessment, mitigation, and verification. These activities are integrated with the development activities of requirements analysis, functional analysis, and synthesis for a given iteration. Ensuring that the mitigation strategies from any iteration are correctly applied in the next iteration is the goal of safety validation.

For the I-ETMS project, five (5) major iterations in the development cycle have been identified. These have been identified as “Levels”. Level 1 is the system level and encompasses the entire PTC implementation called “I-ETMS”. Level 2 decomposes the PTC system into several segments which include the Locomotive Segment and the Office Segment. Level 3 identifies components that make up a segment and Level 4 identifies the modules that make up components. The final level, Level 5, identifies the units that comprise a module.

To demonstrate that I-ETMS is designed to eliminate and/or mitigate potential identified hazards to an acceptable level, the following System Safety Analysis activities are being conducted against the its functions as described in Section 5 - Concept of Operations and specification documents:

- A Preliminary Hazard Assessment (PHA)
- A Hazard Log
- A Fault Tree Analysis
- A Failure Modes and Effects Analysis (FMEA) of the I-ETMS Brake Interface Module

The detailed results and conclusions regarding the categorization, elimination, and/or mitigation to an acceptable level, of identified hazards shall be documented and provided in the PTCSP. Suppliers and railroads implementing I-ETMS will collaborate on the analysis of common hazards and their mitigations. This information is expected to satisfy the criteria called out in 49 CFR Appendix C to part 236, paragraph (b) and items 2(i-v).

10.2.1 Preliminary Hazard Assessment

As part of the System Safety Process, System Safety Analysis begins with a Preliminary Hazard Assessment (PHA). The PHA is conducted against the I-ETMS functions as described in the Section 5 - Concept of Operations. For the PHA, one or more Wabtec and/or railroad employees who are qualified by training and/or experience to perform system safety engineering tasks hypothesize possible failure modes of each system function. Each of these failures is associated with an effect and a severity of that effect. These effects and severities are established at a railroad level. In many cases, I-ETMS functional failures require additional failures to occur first for the railroad level incident to be observed. Data is reviewed for consistency and correctness and frozen as the PHA to be included in the PTCSP. The PHA data is transferred to the Hazard Log for tracking and maintenance. As new functions are introduced to the I-ETMS system, addendums will be made to the Hazard Log; there is no intent to make further updates to the PHA.

10.2.2 Hazard Log

A hazard log form has been developed to track both common and railroad-specific I-ETMS issues. This log is a living document that will be updated throughout the life of the I-ETMS system. Upon a hazard log's creation, failure information is collected along with effect.

To affirm that I-ETMS has been designed in a safe manner, acceptable target safety levels have been defined by railroads planning to implement the system. These target safety levels, along with a predicted severity of identified hazards are aligned to create a Hazard Risk Index, detailed in Section 10.2.3. The Hazard Risk Index mandated by the railroad is used to correlate a hazard's failure to an integrity goal. This goal will be noted within the hazard log. Existing and mitigated hazard references and frequencies will be included to substantiate this claim.

10.2.3 Hazard Risk Index

The Hazard Risk Index is a tool used to establish a required level of integrity based on the predicted severity of identified hazards. The matrix in Figure 22 shows the Hazard Risk Index used for I-ETMS.

Severity → / Probability ↓	I Catastrophic	II Critical	III Marginal	IV Negligible
A Frequent	UN	UN	UN	AC
B Probable	UN	UN	UN	AC
C Occasional	UN	UN	AC/WR	AC
D Remote	UN	AC/WR	AC	AC
E Improbable	AC/WR	AC	AC	AC

Integrity Goal Definitions :

UN - Unacceptable

AC/WR - Acceptable with review by the railroad's chief safety officer or designated representative

AC - Acceptable without review

Figure 22 – Hazard Risk Index

The Hazard Risk Index correlates the predicted severity and probability of occurrence of identified hazards to a risk integrity goal. The matrix is used in the Hazard Risk Assessment process to establish initial hazard risk, and to set priorities for resolutions that eliminate, minimize, or control the identified hazards. Hazard Risk Assessment is the process of combining the hazard severity and hazard probability to determine which identified hazards are acceptable as is, acceptable with proper documentation, acceptable with sufficient mitigation, or unacceptable.

10.2.4 Hazard Assessment Criteria

The acceptance criteria will be based on the potential impact of the hazard on personnel, facilities, equipment, operations, the public, or environment, as well as on the product itself. Other factors specific to the product may also be used to assess risk. For a vital overlay PTC system, §236 Subpart I mandates that sufficient documentation demonstrate that the PTC system, as built, fulfills the safety assurance principles set forth in Appendix C to Part §236. If an identified hazard cannot be eliminated, the process shall be to reduce the associated risk to an acceptable level through design and proper implementation using Safety Assurance Concepts. The criteria used to assess the Hazard Severity and the Hazard Probability is defined in the following paragraphs.

Hazard Severity is defined as a subjective measure of the worst credible mishap resulting from personnel error, environmental conditions, design inadequacies, and/or procedural deficiencies for system, subsystem, or component failure or malfunction, and shall be categorized as follows:

I. Catastrophic

- Deaths, system loss or severe environmental damage

II. Critical

- Severe injury, severe occupational illness, major system or environmental damage

III. Marginal

- Minor injury, minor occupational illness, or minor system or environmental damage

IV. Negligible

- Less than minor injury, occupational illness, or less than minor system or environmental damage

Hazard Probability is defined as the probability that a specific hazard will occur during the planned life-cycle of the system element, subsystem, or component. Hazard probability can be described subjectively in potential occurrences per unit of time, events, population, items, or activity, and shall be ranked as follows:

A. Frequent

- P (incident) > 1E-3 per operating hour
- Classification associated with a hazardous event that is likely to occur often in the life of the system, subsystem, or component. The probability of occurrence is greater than 1E-3 per system operating hour. Likely to occur frequently in an individual item; may be continuously experienced in fleet/inventory.

B. Probable

- 1E-3 per operating hour >= P (incident) > 1E-5 per operating hour
- Classification associated with a hazardous event that will occur several times in life of the system, subsystem, or component. The probability of occurrence is between 1E-3 and 1E-5 per system operating hour. Will occur several times in life of an item; will occur frequently in fleet/inventory.

C. Occasional

- 1E-5 per operating hour >= P (incident) > 1E-7 per operating hour
- Classification associated with a hazardous event that is likely to occur sometime in the life of the system, subsystem, or component. The probability of occurrence is between 1E-5 and 1E-7 per system operating hour. Likely to occur sometime in the life of an item; will occur several times in fleet/inventory.

D. Remote

- 1E-7 per operating hour>= P (incident) > 1E-9 per operating hour
- Classification associated with a hazardous event that is unlikely, but possible to occur in life of the system, subsystem, or component. The probability of occurrence is between 1E-7 and 1E-9 per system operating hour. Unlikely but possible to occur in life of an item; unlikely but can be expected to occur in fleet/inventory.

E. Improbable

- P (incident) <= 1E-9 per operating hour
- Classification associated with a hazardous event that is so unlikely to occur that it can be assumed it will not be experienced in the life of the system, subsystem, or component. The probability of occurrence is less than 1E-9 per system operating hour. Very unlikely; it can be assumed occurrence may not be experienced; unlikely to occur, but possible in fleet.
- The E (Improbable) category is not interpreted as zero probability, thus zero risk. The E (Improbable) category includes all items that are judged to have low or extremely low probability of occurrence. There is no zero probability category included in the ranking matrix.

10.2.5 Hazard Log Documentation

A hazard log to be included in the PTCSP will document the integrity goal in all cases. The identified hazards will be associated with mitigations which will also be documented in the hazard log detail. Mitigations may include a specific requirement or, if not a requirement, other specified nomenclature may apply (e.g. Training). Each mitigated hazard is evaluated based upon the entered frequency and hazard goal to assign a Risk status to it.

To identify potential hazards and associated severities, personnel (railroads and suppliers in combination) who are qualified by training and/or experience to perform system safety engineering tasks hypothesize possible failure modes of each function. Each of these failures is associated with an effect and a severity of that effect. Once hazards and associated severities are identified, failure rates for existing railroad failures will be established and provided by a group of knowledgeable railroad personnel. This group is to be a composite of experienced railroad personnel from varied areas to include Technical Research, Engineer Training, Operating Practices, Rules, Dispatching, Mechanical, and Human Factors, who can effectively determine or estimate the yearly occurrence of all but the most difficult or unusual hazards. This group is asked to provide or estimate yearly occurrences of a list of identified events (e.g. train separation or unauthorized occupancy/movement). Yearly occurrences obtained are converted to a failure rate (failures/hour) by using a weighted average of FRA reported Train Miles and an average Train Speed. In many cases, the failure rate data is identified as a conservative assumption. The intent is to select a conservative value (i.e. a higher probability of failure) based on known information. As no varying time dependences for exposure times exist, a one-hour exposure will be used. This will allow all the rates to be entered as probabilities for quantitative analysis; a practice that is to be used throughout. Details will be included within the Fault Tree section of the PTCSP.

10.2.6 Fault Tree Analysis

Fault Tree Analysis (FTA) for I-ETMS develops from the top down, by taking two initial, top-level catastrophic events, Collision and Derailment, and logically decomposing each event into layers of lower, more specific contributing factors. The system is analyzed in the context of its environment and operation to find credible ways in which the undesired events (Collision or Derailment) may occur. The fault tree will be composed of many intermediate layers representing a decomposition of an event into faults or combinations of faults required to create the event. I-ETMS failures decompose to the functional levels that were produced by the PHA effort. Continued decomposition of the top level events occurs until a logical terminal event, or basic event is obtained and failure rate data can be established. These basic events are items for which failure rate data is either available through industry or real world data sheets or it can be logically estimated. Low level basic events are described and failure rates justified in the PTCSP.

Basic events are populated with applicable failure rate data or probability of occurrence data to obtain a top level probability of the hazardous event (Collision or Derailment). Once applicable failure rate data is associated with basic events, fault tree evaluation and further analysis will be performed. This analysis utilizes the commercial, industry accepted fault tree tool, CAFTA®. This tool allows the trees to be entered graphically and manipulated to produce readable outputs. More importantly, the tool accounts for all mathematical computations at each level of the tree using the data input.

The results of the quantitative fault tree analysis will be evaluated for acceptability by the railroads and any applicable suppliers. Hazard mitigation will be updated within the hazard log.

10.3 Segment Mean Time to Hazardous Event (MTTHE)

The Hazard Risk Index found in Figure 22 indicates that I-ETMS system level hazards classified as catastrophic should not occur at rate greater than 1E-9 per operating hour. Preliminary fault tree analyses, based on the system architecture identified in Sections 3 and 6, have been created and cut sets generated. The cut sets show that both the Locomotive and Wayside Segments can directly influence catastrophic hazards. An equal allocation of failure rate to the Locomotive and Wayside Segments indicates each segment must exhibit a MTTHE greater than 2E9 hours. Hazards associated with the Communication and Office Segments are mitigated by the consuming Locomotive Segment. The protection provided by the Locomotive Segment allows the Communication and Office Segments to have a MTTHE as low as 1E5 hours. Table 13 below summarizes these MTTHE numbers which will be verified through the formal safety process and results will be disclosed in the PTCSP.

Table 13 – MTTHE Summary

System/Segment	MTTHE
System – Catastrophic Hazards	1E9 hours

System/Segment	MTTHE
Locomotive Segment	2E9 hours
Office Segment	1E5 hours
Wayside Segment	2E9 hours
Communication Segment	1E5 hours

10.4 System Availability / Backup Modes

Since no system can provide 100% availability, the fallback mode of operation to mitigate system failures will be defined in accordance with 49 CFR 236.1029 to allow for the continuing operations of the rail network. This description includes the I-ETMS operational concepts which provide fallback modes for abnormal operating conditions.

I-ETMS is a vital overlay that works in conjunction with existing Methods of Operations to protect against the consequences of human error. This approach provides an additional level of protection for train operations while retaining the existing Methods of Operation as the primary means of control. Upon en-route occurrence of a failure and/or deactivation of the Locomotive Segment, an affected train will proceed in accordance with the underlying Method Of Operation subject to operating restrictions imposed by regulation (49 CFR 236.1029) and railroad operating rules.

Procedures will be defined to report and repair equipment problems in situations where the Locomotive Segment fails a departure test or fails into an unrecoverable state (i.e., train unable to move due to I-ETMS penalty application). Such procedures will be in accordance with 49 CFR 236 Subpart I.

In the event that the Locomotive Segment should fail to an unrecoverable state while in use, the system has been designed to provide the ability to be manually “Cut-out” which allows a train to safely transition to fallback operation. The Locomotive Segment is currently specified to achieve 99.9% availability.

Reliability estimates for the proposed Locomotive Segment equipment indicate approximately 65,000 hours MTBF for Wabtec-provided equipment, but due to design, the system may maintain its full operating state when failure of a redundant component occurs. While considering degraded modes of operation, the projected system-level MTBF is 120,000 hours for a critical failure that would either prevent a train start or cause a road failure.

11 I-ETMS Enforcement - §236.1013 (a)(9) & (11)

This section provides a description of how I-ETMS will enforce authorities, signal indications, and conditions monitored by hazard detectors as required by 49 CFR 236 Subpart I §236.1013 (a)(9) and (a)(11).

11.1 Target Generation

Authority for movement of a train or engine provided by mandatory directive is securely delivered by the railroad's dispatching system to the Office Segment. The Office Segment securely delivers the authority to the Locomotive Segment of the appropriate I-ETMS equipped locomotive. Closed-loop processes are utilized by the I-ETMS application to detect anomalies in the exchange of data between the Office and Locomotive Segments and assure that a safe state is maintained in the presence of those anomalies. Additionally, the synchronization of data maintained by the Office and Locomotive Segments is periodically validated to detect any latent errors.

Authority for movement may also be derived by I-ETMS from signal indication (provided by WIU) in Traffic Control or Current of Traffic territory.

The Locomotive Segment uses the movement authorities to establish a permissive route between two or more locations subject to permanent speed restrictions as contained in the track data base and any other restrictions conveyed to the train. I-ETMS generates zero-speed targets on controlled track outside the movement authority limits. Additional targets may be generated from speed restrictions provided by other railroad office systems and overlaid on these movement authorities. Such targets include Restricted Speed restrictions, Temporary Speed restrictions, and consist, lading or equipment speed restrictions, and zero MPH speed targets as generated by the Locomotive Segment for conditions including Work Zones, and non-communicating monitored wayside switches, signals, or other devices.

The Locomotive Segment track database contains wayside switch, signal, and device information required for the Locomotive Segment to communicate with individual wayside locations and to receive switch, signal, or device status from these locations in a wayside status message. Wayside status messages may be securely received onboard directly from the wayside or indirectly via the Office Segment. Wayside status messages are transmitted by the wayside at a periodic rate and each message contains a "creation time" indication to allow I-ETMS to determine the "freshness" of its data. A wayside status message, whose age has exceeded a pre-defined tolerance, or failure to receive a wayside status message, results in the generation of a target that is equivalent to the most restrictive indication for that switch, signal, or device. Receipt of valid wayside status messages may result in the generation of reduced speed, restricted speed, or stop targets by the Locomotive Segment.

I-ETMS provides protection for conditions monitored by hazard detectors, either when integrated with a signal system or in a stand-alone configuration. When integrated with a signal system, hazardous conditions monitored by the detector (or the lack thereof) are manifested through signal indications. Hazard detectors not integrated with the signal system and directly monitored by WIU are capable of communicating with the Locomotive Segment. Similar to monitored switches, each standalone hazard detector becomes an entry in the track data base. A locomotive in approach to a communicating hazard detector must stop or proceed at restricted speed so long as a valid "permissive" wayside status message from the device has not been received. Failure to receive wayside status messages within an acceptable age tolerance results in the generation of a target consistent with the most restrictive conditions conveyable for that device.

All speed targets are overlaid on each other to create the most restrictive speed profile for the train's route. I-ETMS supports up to 128 levels of targets that can be overlaid.

11.2 Enforcement Braking

I-ETMS utilizes a cross channel comparison of redundant processors, a minimum of two, to account for safety; a third processor may be added for additional system availability. Each processor independently makes a determination if enforcement braking is required.

Each processor receives all target data as well as any required data about the train. An onboard track data base supplies track characteristics and wayside apparatus details. Based on this data, the processor establishes a train's route and authorized speed profile. Train data and track profile data from the track data base are used to establish a conservative braking curve based on current train configuration, an "if brakes were applied now" brake profile. The processor accounts for any acceleration or deceleration, again using the current train configuration, estimates a new predicted track position and speed, and re-calculates an "if brakes were applied in XX seconds" braking curve. This predictive process is repeated as the processor continuously extends the locomotive's predicted position to a pre-determined warning time interval down the track. Warning and Braking curves are compared against the train's authorized speed profile to generate and display warnings and ultimately invoke a penalty brake application. Each of the three processors asynchronously repeats this overall process once a second independent from the other processors. The application, compiler, operating system, and processor are the same. The triplex design protects against random hardware failures. The operating system is safety critical certifiable (per DO-178B level A). Maintaining this common approach to the individual slices allows for better testing and configuration management.

Communication between individual train control processors and the Brake Interface Module is conducted using “closed loop” safety principles. Each processor is required to transmit an encoded message to the Brake Interface Module at a periodic rate to forestall enforcement. Each processer has three means of creating an enforcement request from the point of view of the Brake Interface Module. First, a train control processor may request a penalty brake application via its dedicated serial interface. The Brake Interface Module will set an enforcement request for that train control processor. Second, if the Brake Interface Module fails to receive a valid encoded message from the train control processor within a predetermined time period a hardware watchdog circuit will set an enforcement request for that train control processor. Finally, a failed train control processor will be detected by the Brake Interface Module and set an enforcement request for that train control processor. Failure may be established by the processor itself or by consensus of the two remaining processors in a three processor configuration.

The Brake Interface Module using a three processor configuration compares the three processors’ enforcement messages as shown in Figure 23 below. Any two processors indicating enforcement will cause the Brake Interface Module to invoke a penalty brake application. Independent circuitry switches the high side and low side of an internal, isolated power source that is used to supply voltage to the interface of a Magnet Valve or EAB. Current flowing through the closed loop will hold off penalty brake application. No single point failure will prevent brake application.

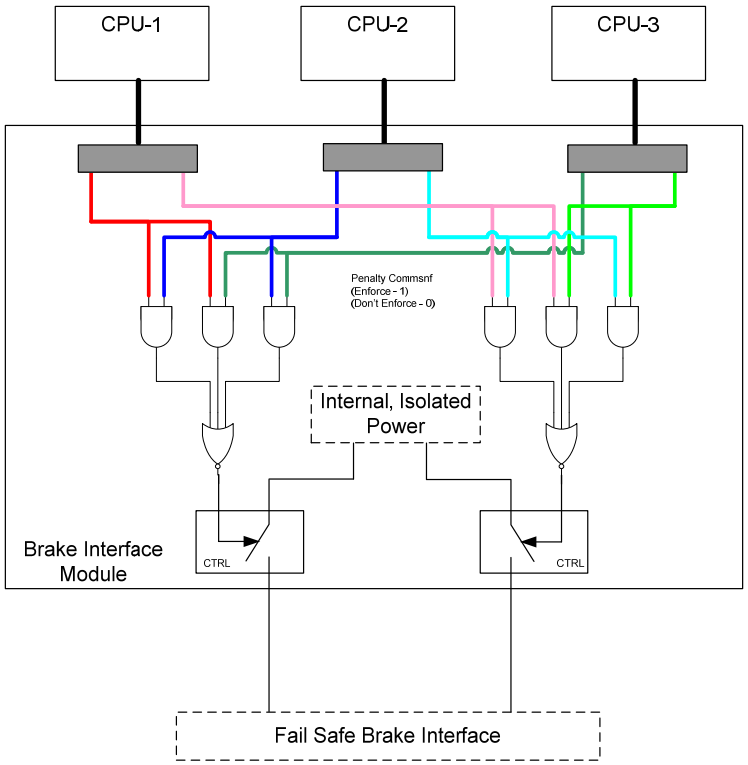

Figure 23 – Simplified Overview of Brake Interface Module

12 En-route Failure Deviations - §236.1013 (a)(10)

Upon en-route occurrence of a failure and/or deactivation of the Locomotive Segment, an affected train will proceed in accordance with the underlying Method Of Operation subject to operating restrictions imposed by regulation (49 CFR 236.1029) and railroad operating rules. No deviations from the applicable rules are anticipated at this time.