Semiconductor Industry (ICRC Working Group) Response To US Occupational Safety and Health Administration (OSHA) Request for Information (RFI) Docket No. OSHA-2016-0013

The semiconductor industry has formed a Control of Hazardous Energy Working Group (WG) within Semiconductor Equipment and Material International's International Compliance and Regulatory Committee (SEMI ICRC). This feedback documents the results of those efforts. This ICRC Working Group has been integral to 2 previous publications related to the control of hazardous energy in the semiconductor industry:

1) SEMI White Paper on COHE LOTO for Semiconductor Manufacturing Equipment
   Ref Link: https://www.semi.org/en/semi-2016-white-paper-cohe-loto
   NOTE: LOTO = Lock Out and Tag Out. Tag Out, the use of a tag instead of a lock on an energy isolation device (permitted by OSHA, under some circumstances, for equipment made before a certain date), is not known by the WG to be used in the semiconductor industry. Applying a tag with a lock is part of "Lock Out".
2) ANSI Z244.1, Annex S - Application of this Standard to the Semiconductor Industry (Informative)

CoHE in the Semiconductor Industry

Semiconductor manufacturing uses various types of process and metrology equipment, much of which uses more than one type of hazardous energy. By consensus of the suppliers and users of this equipment, the industry relies primarily on SEMI S2 and other documents in the SEMI Standards "S" series to guide the safe design of equipment. The industry has a very strong safety record which demonstrates the effectiveness of the hazardous energy control design methodologies it uses.

The hazardous energies in the semiconductor industry include, but not limited to:

- **Distributed Electrical** (high voltages, high currents)
- **Stored Electrical** (capacitors, batteries)
- **Pressurized Liquids** (hydraulic, pumped)
- **Compressed Gases** (liquefied, pressurized)
- **Electromagnetic Radiation** (X-Ray, RF, IR, UV, lasers)
- **Static Magnetic Fields** (permanent magnets)
- **Gravitational Energy** (suspended, hinged loads)
- **Kinetic Energy** (moving robots, linear drives, gears)
- **Thermal / Cryogenic Energy** (hot, cold temperatures)
- **Chemical Energy** (heat of reaction, toxicity)
- **Stored Mechanical Energy** (springs, elastic seals)

Each of these hazardous energies can lead to harm to personnel, as well as significant equipment, facility, and environmental damages. The semiconductor industry, however, is very highly automated, so very few worker tasks are required during production. Most human interaction with the equipment occurs during scheduled or unscheduled downtime. When a task requiring worker intervention in an area in which the worker would be subject to an unacceptable risk of unexpected startup or re-energization is performed, the equipment must be placed in a state so as to prevent unexpected startup or re-energization.

When isolation and de-energization methods prohibit the completion of certain tasks, "alternative" Control of Hazardous Energy (CoHE) methods (*e.g.*, use of robot teach pendants) are allowed by industry standards to prevent unexpected startup of the equipment. In these special cases, the use of robust control circuit designs can provide a highly-reliable engineered solution to control these hazardous energies.

The semiconductor industry has adopted some of these functional safety design approaches (*e.g.*, using robot teach pendants and 3 position enable switches) when hazardous energies are required for certain specific tasks (*e.g.,* teaching robot end-effector positions) and the industry would welcome being permitted to use functional safety design approaches for maintenance and service tasks without being restricted by the current minor service exemption as outlined in:

1) OSHA CFR 1910.147(a)(2)(ii)(B) "Minor Service Exception"
2) **OSHA Directive CPL 02-00-147, February 11, 2008** The Control of Hazardous Energy – Enforcement Policy and Inspection Procedures

Semiconductor Industry Support of Options in ANSI Z244.1 (2016)

The semiconductor industry CoHE Working Group supports the use of Alternative Methods and Remote Lockout defined in the 2016 revision of ANSI Z244.1, a US industry consensus standard highlighting the best practices known today. The new standard also made a very strong statement against basing the permissible means of worker protection on the "Minor Service" exemption. The ANSI Z244.1 committee realized that work gets done based upon the tasks to be performed without regard to a characterization of whether the task is normal production operations, service, or maintenance. The following explanation appears in the Introduction to the revised standard:

The Service and Maintenance Construct

With the 2016 revision, the committee has rejected the normal production operations versus service and maintenance construct as an artificial distinction without real world application. More specifically, the committee realized that work gets done based upon the tasks to be performed without regard to a characterization of whether the task is normal production operations, service or maintenance. Hazards associated with the unexpected release of hazardous energy need to be addressed – regardless of any labels or characterization attached to it.

By placing different requirements based on when a task is performed (*e.g.,* during productive uptime, or during maintenance/service downtime), the focus turns to whether it meets the requirements of minor service or not rather than enabling the work to be done safely through the control of hazardous energy. These conversations are not productive if protecting workers by control of hazardous energy is determined based on a risk assessment – not on whether certain work meets the criteria for an exemption. OSHA should focus on the control of hazardous energy based on practicability justifications and risk assessment of the task being performed, regardless of "when" that task is being done (uptime or downtime).

Definitions Used In This Response

Actuator (of an EID or DEI) – The means by which an EID or DEI is commanded to isolate or de-isolate a hazardous energy. Actuators include:

1) Currently-OSHA-Compliant: knife switch handle attached to circuit breaker, manual valve handle
2) For use with alternate means of energy isolation: pneumatic supply to a valve; electric supply to a relay, contactor, or valve actuator

Alternate means – Alternate means of CoHE or alternate means of energy isolation.

Alternate means of CoHE – Using control circuits to reduce the risk of injury by the hazardous energy, by some means other than isolation. Alternate means of CoHE may include additional functions to

1) dissipate the residual hazardous energy,
2) verify the hazardous energy has been removed, or
3) provide continuous sensing and warning of the hazardous energy

Alternate means of energy isolation – Using control circuits to isolate the hazardous energy. Alternate means of energy isolation maybe provided by equipment that includes additional functions to:

1) dissipate the hazardous energy,
2) verify the hazardous energy has been removed, or
3) provide continuous sensing and warning of the hazardous energy

Device for Energy Isolation (DEI) – A device used for energy isolation function that is actuated by some method not conforming to the current OSHA regulations. An example of a DEI is a contactor:

1) through the contacts of which the electrical power supply to a machine passes and
2) the coil wire power of which passes through a key switch. (The key switch allows the key to be removed only while the switch is open.)

Energy Isolation Device (EID) – OSHA-compliant manual energy isolation device

Functional Safety –

1) The practice of using one or more safety related control functions within the machine design to reduce the risk presented by the machine to an acceptable performance level.
2) The state achieved when all of the equipment's safety functions successfully operate at, or above, their required performance levels.

NOTE: EN ISO 12100 defines the safety function as a function of a machine whose failure can result in an immediate increase of the risk. Whether and to what extent the risk on a machine must be reduced is determined from the risk assessment.

Remote Lockout – Using a control circuit to actuate a DEI, isolating a hazardous energy at a location other than near where the work will be done. Remote Lockout is done by the worker near where they would otherwise be exposed to the hazardous energy, not in the location of the DEI.

*Safety Interlocks (*within semiconductor manufacturing equipment) – Control circuits (not necessarily electrical) that operate automatically to reduce risk, such as by isolating or reducing hazardous energy before personnel are exposed. Amongst the industry specific requirements are that they be single fault tolerant (which requires them to be separate from any normal control circuits that they are backing up), they switch the ungrounded side of the circuit and that they require a manual reset action to restore the energy. Examples include:

1) door interlock that stops internal mechanical motion or chemical flow when opened;
2) an overtemperature interlock that prevents items from reaching a hazardous temperature, and
3) exhaust interlock that stops chemical dispense when safety exhaust drops below setpoint.

Safety interlocks generally do not provide a means of ensuring exclusive control over the hazardous energy. There are also safety interlocks that are enable circuits (for example, ones allowing chemical dispensing, but preventing two incompatible chemicals from being dispensed at the same time) that don't require a manual reset.

Safety Interlocks Versus Alternate Means: The semiconductor industry currently recognizes that properly designed control circuits (safety interlocks) may activate, if there is a foreseen equipment fault or human error, to prevent a hazardous situation or to reduce ones risk. These are intentionally added engineering controls to protect both the workers and the equipment. These safety interlocks are evaluated for design robustness, per SEMI S2.

Specifically, in SEMI S2, Section 11 "Safety Interlocks", performance requirements are outlined. These safety interlock control circuits are currently addressed separately from Section 17 Hazardous Energy Isolation. If Alternate means of CoHE are used, many of the same functional safety/control reliable principles apply.

Example: Hazardous Chemical Gas Box Door Interlock

Many pieces of semiconductor wafer processing equipment use door/guard interlocks to isolate hazardous energy if door/guard is opened. Once activated, the hazardous energy cannot be restarted until guard is closed and there is a manual reset. This is a precaution to address the reasonably foreseeable case of misuse of a worker not following proper Lockout procedures prior to opening. The semiconductor industry does not believe this type of safety interlock control circuit alone would still satisfy all proper CoHE steps and should not be considered as full CoHE/Lockout. (For all compressed gases, proper CoHE includes reduction of the pressure within wetted components to approximately the ambient pressure. For toxic, pyrophoric, and (in some cases) flammable gases, proper CoHE includes removal of the gas remaining after isolation and, in some cases, cycle purging (alternating between filling the wetted components with a non-reactive gas (typically nitrogen) and evacuating those components, typically ten to one hundred times).

The semiconductor industry discussed advantages of still having lockable isolation points to ensure exclusivity control by the worker during activities where CoHE is implemented for maintenance tasks. The requirements in Section 17 are currently under revision to add more clarification and details. References to new ANSI Z244.1 Annex B are being considered. We would like to have clear delineation of the design and verification requirements when control circuits used as remote lockout or alternate means of CoHE compared to when they are used for other layers of protection.

Chapter 8 of the ANSI Z244.1 2016 revision does an excellent job highlight the addition design and verification requirements needed if control circuits are to be used. Additionally, ANSI Z244.1 Annexes L - S provide illustrative examples of how various industries have employed various methods to provide persons with effective protection. These improvements to allow control circuits to effectively control the hazardous energy should enable companies to use modern technology and innovative solutions to improve the safety and productivity of operations in the workplace.

A key point here is that OSHA has specifically requested information in determining under what conditions control circuit type devices could safely be used for the control of hazardous energy. We believe it is important to point out that it is not just control "devices" that should be addressed. The entire control circuit (*e.g.,* electrical, pneumatic, hydraulic, mechanical, or some combination thereof) must be properly designed and validated. This type of "systems" approach is based on the same concepts as defined in many national and international design standards related functional safety performance requirements. Proper CoHE using Alternative Methods (per Chapter 8 of ANSI Z244.1) directs designers to consider the entire control circuit, not just individual control device(s).

The Working Group, however, differs with the 2016 ANSI Z244.1 in one key point. We believe that any of the three types of worker protection (traditional lockout, alternative means of isolation, or alternative means of CoHE) should be permitted, as long as an acceptable level of risk is achieved.

The semiconductor industry is heavily anchored in the concept of "Hierarchy of Controls" as specifically spelled out in semiconductor industry consensus guidelines, which emphasize the preference of hazard elimination and of engineering controls over administrative controls. This concept is not new, and has a wide foundation across many key semiconductor industry related standards:

SEMI S2: Section 6.9	ISO 13849-1 Section 4.2 1
Machinery Directive, Annex 1.1.2	ANSI Z244.1 Section 8.1.2
ISO 12100 Figure 1, Figure 2	Other SEMI S-Guidelines

It is also recognized that OSHA promotes this same philosophy on the OSHA website:

- "***Recommended Practices for Safety and Health Programs***".
  Link: https://www.osha.gov/shpguidelines/hazard-prevention.html

Summary:

In summary, the semiconductor industry still strongly believes that properly designed alternative means offers a significant advantage over traditional Lockout, particularly in cases requiring more complex Lockout, which are prone to human error or misuse.. We strongly support OSHA's adoption of Alternate Methods and Remote Lockout as described in ANSI Z244.1 so better guidance and direction to properly designed Remote Lockout circuits (or other equivalent methods, such as trapped key systems) can be used to help make our work environment safer due to a workers' greater willingness to use such devices if they are easy, provide better efficiency, and less downtime,

In summary, the semiconductor industry still strongly believes that properly designed control circuits for the use of control of hazardous energy/Lockout offers significant advantages to address the problems we are seeing for the consistent use of Lockout to address many of the issues of relying on a human-error prone administrative control, including:

- Not locking out because it is inconvenient
- Locking out the adjacent identical tool at other than that at which work is to be done.
- Inadequate energy dissipation or removal verification compliance due to complexity or inconvenience

It is also recognized that, to implement other means of worker protection, there will very likely be a transition period where manual Lockout and control circuits will both be needed as the various facilities that use semiconductor manufacturing equipment update their safety programs to allow for the use of control circuits for energy isolation before they can be used.

RFI Question 1) *In what work processes should OSHA consider allowing the use of control circuit type devices for hazardous energy control?*

OSHA should consider allowing the use of control circuit type devices for hazardous energy control in all work processes.

Following the ANSI Z244.1 construct, work is work and hazards are hazards, so the semiconductor industry viewpoint is that work gets done based upon the tasks to be performed, without regard to a characterization of a task as normal production operations, service or maintenance. Hazards associated with the unexpected release of hazardous energy need to be addressed – regardless of any labels or characterization. (*e.g.,* Operation or Minor Service versus Service or Maintenance) attached to it.

The OSHA questions focus on only the control circuit device. The semiconductor industry recognizes the important understanding that proper risk management involves more than just individual control circuit devices. The entire control circuit must be evaluated for its performance, and we should not focus only on just the individual devices used, but rather, how they are put together properly to achieve the required performance of the entire control circuit.

We use the term alternate means of isolation to describe a means of addressing cases in which locations of the different hazardous energy isolation points are not where maintenance or service is to be done (*e.g.,* isolation points could be in a different room, or even a different floor, of the building). The semiconductor industry does believe that use of a designed (and verified/validated) alternate means to a proper performance standard such as:

- *ANSI Z244.1,or*
- *ISO 13849-1, ISO 13849-2*
- *IEC 62061*

should be allowed during maintenance and service work to greatly reduce human errors of complex Lockout tasks.

Example: Hazardous Chemical Gas Box Door

Semiconductor equipment can be designed with a lockable electro-mechanical switch next to gas box door which can be turned and locked in closed position. Turning the switch to the energy-isolating position and locking it would then initiate a sequence of pre-defined steps through control circuit logic (safety PLC) and diagnostics, to shut down multiple hazardous energies (*e.g.,* Chemical, Electrical, Mechanical) in the proper order, ensuring isolation, de-energizing of each hazardous energy, and then successfully verifying this (with feedback to worker) to bring system into safe condition for maintenance. Today – Complex Remote Lockout control circuits like this are rare, but there is strong motivation to bring such control circuit designs into use. It is in the use of these types of control circuits (*i.e.*, use of Engineering Controls versus Administrative Controls) in service and maintenance activity that the semiconductor industry sees large benefits in mitigating the risk of human error. For more details on example of a complex Lockout task – see answer to ***Question 3)***.

RFI Question 2) *What are the limitations to using control circuit type devices? Do they have specific weaknesses or failure points that make them unsuitable for hazardous energy control??*

The limitation of a control circuit type device that is of greatest concern is that a means of isolating hazardous energy incorporating such a device could fail in a manner it would appear, incorrectly, that the hazardous energy had been isolated.

For any given component, a particular failure mode can either "***Fail Safe***" (stops working but in safe condition - potentially indicating a problem when there is not one or interrupting a hazardous energy path when it was not directed to do so) or "**Fail to Danger**" (indicating there is no problem, when there may be one or not interrupting a hazardous energy path when it was directed to do so). It is very important to understand the potential failure modes within each device if they are to be used for CoHE/Remote Lockout.

If a component fails to danger, it is highly desirable to be able to detect that failure and take proper action before a worker is exposed to the relevant hazardous energy. Current technology allows, in most cases, for such monitoring and notification.

The highest risk scenario is the component failing to danger, but the failure going undetected. These undetected fails-to-danger must be prevented or, at a minimum, detected prior to someone becoming exposed to the hazardous energy. In some cases, the failure will not be detected until the verification step of the CoHE process.

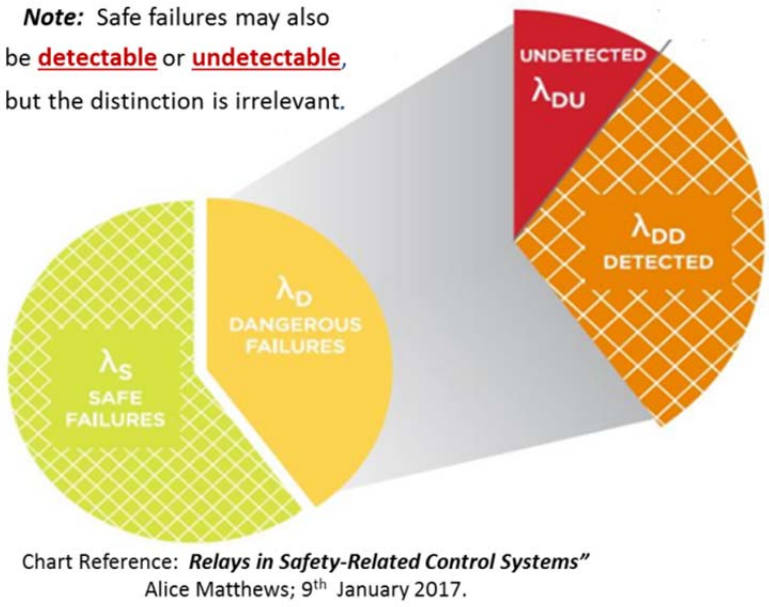


Figure 1: Breakdown of Types of Failures for Control Circuit Devices

Internet Link: https://www.electronicspecifier.com/power/relays-in-safety-related-control-systems

The good news is that there are individual, component level standards (for switches, relays, contactors, etc.) that can be used to evaluate each component's design robustness, which indicates the probability of each type of failure for such a device. Manufacturing and verifying compliance to these standards can be used to demonstrate a component's suitability and reliability for a particular application.

REF: The international standard ISO 13849-2: Safety of Machinery — Safety-Related Parts of Control Systems — Part 2: Validation. Components listed in Annex D - Table D.3 are considered to be "well-tried" if they are certified to the specific standards listed in Table D.3. .

Based on the foreseen failure modes and their frequencies and on the risk assessment, the control circuit can be designed with appropriate redundancy and self-checking.

RFI Question 3) *If OSHA were to allow the use of control circuit type devices or other methods to control hazardous energy, would your firm choose to use them? Why or why not? Do you anticipate that these devices would save your firm money? For example, would these devices simplify operations or maintenance? Are there fewer steps needed to implement the controls? How frequently do you employ some form of lockout/Tagout system in your facility??*

The SEMI ICRC CoHE working group is a collection of many firms. Individual companies would need to answer this question, but the following is our collective response.

In tasks where energy is required (*e.g.*, teaching a robot end-effector its positions) we already use control circuits (within the robots) to provide exclusivity of control and to limit the speed of motion and also the torque/force with which it could hit a worker in the danger zone. Additionally, these robot systems utilize a 3-position enable switch which allows for the limited speed/torque motion only when switch is engaged in the middle position. If it is pressed too tightly or dropped, motion stops.

In the white paper referenced on page 1, we define a complex Lockout of common wafer processing equipment which could greatly benefit from the use of properly design alternate means of energy isolation, as the lockout protocols for service and maintenance tasks need to be very complex. The entire wafer processing equipment is taken completely down/off very infrequently. To maximize throughput, semiconductor equipment is usually modular, so that one portion of the tool (process chamber) can be taken down for maintenance or service while other portions of the tool remain up and running.

When working on our industry's more complex equipment designs, it is not uncommon to need to lockout ten or more different hazardous energy sources. The energy sources typically found in semiconductor equipment include:

Distributed Electrical (high voltages, high currents)	Gravitational Energy (suspended, hinged loads)
Stored Electrical (capacitors, batteries)	Kinetic Energy (moving robots, linear drives, gears)
Pressurized Liquids (hydraulic, pumped)	Thermal / Cryogenic Energy (hot, cold temperatures)
Compressed Gases (liquefied, pressurized)	Chemical Energy (heat of reaction, fire)
Electromagnetic Radiation (X-Ray, RF, IR, UV, lasers)	Stored Mechanical Energy (springs, elastic seals)
Static Magnetic Fields (permanent magnets)	

Furthermore, there are some systems in which hazardous energies must be managed stepwise. Consider, for example, a piece of chemical process equipment in which the supplies of hazardous production materials (HPMs) must be isolated, but other hazardous energy sources, such as electrical power and purge fluids, must be used for removal of the residual HPMs. Such a case requires three degownings, three gownings, and six moves between building levels. Each typical degowning and each regowning includes shoe covering; head covering; face covering; torso, arms, and legs covering; and gloves. As semiconductor fabs usually install many pieces of like equipment side by side, the worker must be careful to identify and manage the hazardous energies of the correct one. The risk to personnel of having locked out the wrong equipment is managed by the verification step. Figure 2 provides an example of travel necessitated by use of direct lockout.)

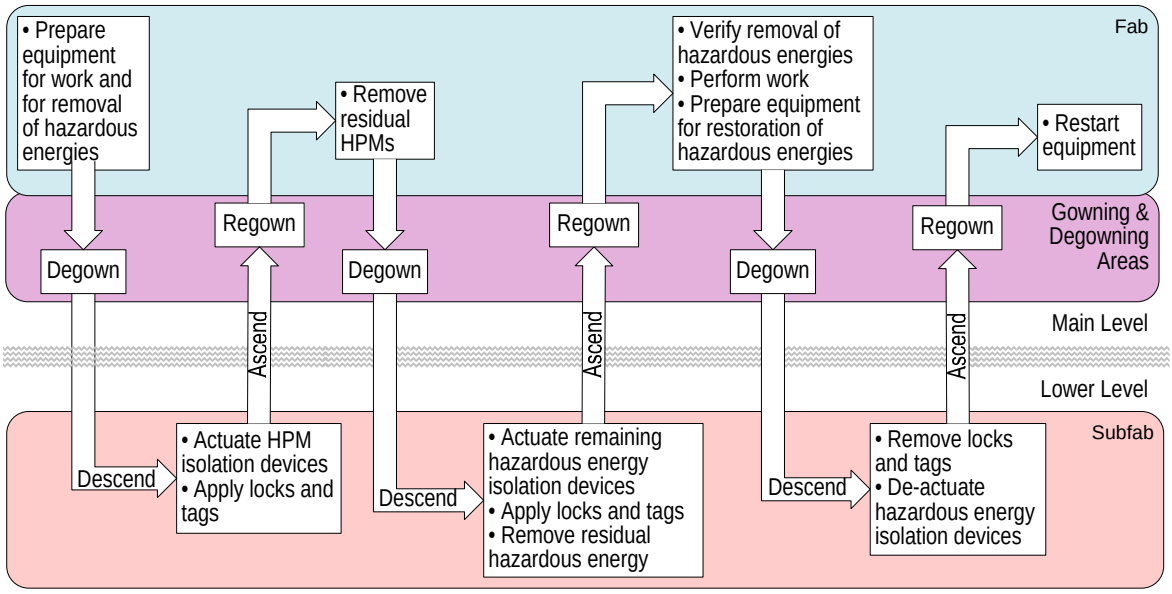


Figure 2: Example of Complex Conventional (Direct) Lockout.

While these steps are straight forward, and can be followed in sequence successfully, they are tedious, time-consuming, and prone to human error. Workers are also discouraged by the fact that a mistake resulting in locking out an adjacent system results in the loss of expensive product.

Alternate means can reduce downtime and increase safety. Among the advantages of automating the isolation of hazardous energies, is the improvement of reliability that is foreseen to result from relying on a machine, rather than a human, to execute a complex series of energy isolation steps and energy removal verification steps in the correct order. It is also a challenge for humans, in a typical semiconductor factory, to maintain their focus on hazardous energy isolation, particularly if the process takes more than a few minutes, as the complex, multi-floor processes do.

Our industry does anticipate that these devices would greatly simplify maintenance and service tasks due to fewer steps needed by the worker to implement proper Lockout.

RFI Question 4) *Are there any specific conditions under which the use of control circuit type devices would not be advisable?*

Based on ANSI Z244.1 Section 8.1.2 and Table 1 – The Hazard Control Hierarchy, which highlights that Engineering Controls being preferred over Administrative Controls), our industry we would like allow the use of alternate means . This is especially important in addressing the more complex Lockout tasks which are deemed to be prone to human error.

RFI Question 5) *When the Lockout/Tagout standard was originally drafted, OSHA rejected the use of control circuit type devices for hazardous energy control due to concerns that the safety functions of these devices could fail as a result of component failure, program errors, magnetic field interference, electrical surges, or improper use or maintenance. Have new technological advances to control circuit type devices resolved these concerns? How so?*

When OSHA wrote the current LOTO standard, the current standards for functional safety and electronic safety devices had not been written, and the components to meet those standards had not yet been designed. The new emphasis by International standards such as ISO 13849-1 and -2, to ensure designers evaluate and understand a specific component's failure modes and requiring the following of Basic and Well-Tried Safety Principles help ensure the design meets the performance requirements of the application (Performance Level). This fact, coupled with the advancement of the components within the control circuits which are highly reliable and tested and verified to specific standards ("Well-Tried" Components). Using these types of certified devices

1) **Input Devices** (e.g., door switches, pressure switches, over-temperature switches),
2) **Logic Devices** (e.g., Safety PLC's, relays), and
3) **Output Devices** (e.g., auxiliary contactors with forcibly guided (mechanically linked) contacts

will significantly help to minimize or eliminate potential failures to danger.

In the same example of a functional safety standard, ISO 13849-1 Annex F also looks at Common Cause Failures (CCF) which could affect the redundancy elements within a control circuit (all its devices). It considers protection against common cause failures caused by electromagnetic disturbances (EMC)/ Such protection can be provided in accordance with appropriate standards, including EMC Radiation and Immunity standards (EMC Directive), and current electrical design standards from our industry (*e.g.*, SEMI S2, SEMI S22, IEC 60204-33). Again – the key is to understand the control circuit's failure modes clearly and to select well-tried devices, and design in proper diagnostics or redundancy to ensure a fault does not result in unexpected start up or exposure to the hazardous energies we are trying to control. The design of the circuit depends on the hazard scenario. Based on the hazard scenario a risk assessment will determine the required performance level which the control circuit must meet to prevent a failures to danger above the specified frequencies:

Performance Level	MIN 1/ Avg PFH_D	MAX 1/ Avg PFH_D	Max Tolerance: 1 Dangerous Failure per ?? Hours	Max Tolerance: 1 Dangerous Failure per ?? Years	Range of Dangerous Failures	SIL
a	100,000	10,000	10,000 hrs	1.14	> 1 year and ≤ 11.4 years	*NA*
b	333,333	100,000	100,000 hrs	11.42	> 11.4 years and ≤ 38 years	1
c	1,000,000	333,333	333,333 hours	38.05	> 38 years and ≤ 114 years	1
d	10,000,000	1,000,000	1 million hours	114.16	> 114 years and ≤ 1,140 years	2
e	100,000,000	10,000,000	10 million hours	1,141.55	> 1,140 years to ≤ 11,400 years	3

These failures rates are still significantly less frequent when compared to published industrial human error rates in ISO/TR 14121-2

The EMC testing required for components should be based on the assessed risk and the resulting required reliability of those components.

In summary – if the designers of control circuits follow the guidance in an appropriate published consensus standard, we believe we can adequately resolve the initial concerns OSHA had back in 1989.

RFI Question 6) Are there issues with physical feedback for control circuit type devices?

Changing from using "hands-on" means of isolation to using "control circuit type devices" does entail changing from using observation and interpretation by a human to using sensing and interpretation by a machine. However, such a change comprises a change from an administrative control to an engineering control, which is generally viewed as favorable change in safety engineering. For some means of isolation, such as insertion of a blanking flange, human observation and interpretation, when it is performed diligently, is quite reliable. However, that's not a means of isolation likely to be performed by a "control circuit type device", nor is it commonly applied in the semiconductor industry.

There are similar "issues with physical feedback" with many of the currently-permitted means of lockout. Such issues can, however, be addressed by having the control circuit incorporate an appropriate sensor. In some cases, a "control circuit type device" may be more able to verify isolation than is a human. For example, a control circuit could include a valve position sensor to verify that a valve had closed, even if there's no way for a human to determine the position of the valve without exposure to its wetted surfaces.

The risk of a valve not closing because of such things as being contaminated does need to be managed by the verification step, but that is equally true of manually-actuated isolation valves.

The key is properly design and verify the design. The semiconductor industry has highlighted, in the recent SEMI S30 (Safety Guideline for energetic materials) publication, is that, in at least some cases, verification of the absence of the hazardous energy must be through an appropriate measurement, not through a measurement of the means by which devices controlling that energy are actuated.

Example of an "issue with physical feedback" that pertains to use of either direct mechanical or "control circuit" Lockout: Pneumatic pressure is commonly used to drive open a pressurized chemical valve (*e.g.,* a normally closed, spring return valve). The removal of this pneumatic pressure results in the mechanical spring closing of the chemical valve, and isolating the source upstream of the valve, from the rest of the downstream piping.

The "Hazardous Energy" is not the pneumatic energy that drives the pneumatic valves, but the hazardous pressurized chemical gases, liquids, or vapors that may flow through and downstream of these chemical valves. Lockout of the pneumatic drive pressure and verification that the drive pressure has been removed provides a potentially false sense of security that the chemical valve is in fact closed, when, in fact, it may not be:

There are several failure modes (common to energy isolation devices operated directly and those operated by a control system). For example, a valve can fail to stop flow because:

1) abnormally high pressure on its inlet,
2) a spring fails to close the valve, or
3) its seat is deformed, nicked, or contaminated by particles.

Unless you are specifically verifying both the isolation and de-energization of the chemical line pressures (not just the pneumatic line pressures) you simply are not in "Control of Hazardous Energy" for the chemical lines. For some hazardous chemicals, one needs positive verification of the chemical valve is closed, and that there is no failure to danger (*e.g.,* no chemical leak by of valve seat, or no spring failure)

Much of our response focuses on ISO 13849-1 guidance, but other appropriate safety standards can also be used. Not all devices which might be used in a control circuit have feedback capability. Based on a given performance level you need (see, *e.g.*, ISO 13849 Annex 1) the designer will need to select properly rated components that can ensure he meets or exceeds the required performance level.

In addition you have to select proper logic devices, such as a safety PLC compliant to IEC 61508,) to interpret the feedback signals and take proper actions. Just because something is a control circuit does not mean it's acceptable – it must be a properly designed and tested control circuit.

RFI Question 7) *What are the safety and health issues involving maintenance, installation, and use of control circuit type devices? Have you found that alternative safety measures themselves cause any new or unexpected hazards or safety problems? Please provide any examples if you have them.*

There are no obvious differences between the health and safety risks of installing or maintaining DEIs that are actuated by control systems and the risks of installing EIDs that are actuated manually. The risks of use of the types of device do differ: Devices actuated manually typically have fewer failure modes, but there's a greater risk of human error. Devices actuated by control systems have more failure modes (because there are more ways the actuation can fail), but better means of detection of failure and less risk from human error.

There are risks pertaining to the work of converting energy isolation devices, in a machine that is in service, from manual actuation to actuation by a control circuit. However, such risks are limitted by:

1) the number of times such a task would be performed,
2) economic disincentives to making such a change on existing equipment (as opposed to implementing such a change in future equipment), and
3) the fact that, in many cases, there would be no need to insert an DEI in an energy path because either:
   a) the actuators on some EIDs can be changed without changing the portion through which the energy passes or
   b) the equipment already contains a device (for example, a contactor that is part of a safety interlock which removes power from a heater when unacceptable temperature is sensed) that interrupts the energy path and is actuated by a control circuit).

Key to addressing the second part of Question 7 is "management of change".

Our equipment is not stagnant, and the equipment design (but generally not a specific piece of equipment) is frequently upgraded numerous times a year to improve performance. Such changes to the equipment can affect the risks of other tasks and changes to tasks can affect the hazardous energy exposures and other risks of maintenance and service. Therefore, if any changes are made to tasks or equipment, the affected set of risk assessments should be reviewed and, if appropriate, updated.

As for changes to the "control circuit type devices", SEMI recently published an update of SEMI S22, including management of changes for safety controllers.

A substantial part of implementing any change to equipment, including a change to its safety features, is that personnel dealing with the equipment need to be trained on the changes to the equipment and to the procedures, including the procedures for management of risks posed by hazardous energies. As the hazardous energy control systems get more complex, we need to do additional training so that the personnel are able to continue to perform this function.

Based on available information, both incident data and anecdotal, the benefits of having the energy isolation and de-energization happen more automatically and with less effort will likely provide much more frequent risk reduction due to better compliance with Lockout/CoHE instructions, but there is a trade-off between the burdens of implementation and the improved risk management.

The primary safety and health issues during maintenance and service which utilize control circuit devices to control the hazardous energies is the existence of new "hidden hazards" as a result of a change to the design or procedure which go unchecked. The same issue is also with conventional Lockout.

Following the CoHE Guidance from our semiconductor industry white paper, use of an alternate means still requires an accurate assessment and documentation of the risks during the task. Assessing risk includes estimating the severity and frequency of harm that results from a hazard per the semiconductor industry's consensus method defined within SEMI S10. The acceptability of risk is determined by our industry consensus guideline (SEMI S2), and by individual company policies.

In some cases, the risk assessment will find that an acceptable level of risk cannot be achieved by conventional lockout OR other methods. In such cases, either the equipment or the task must be modified to make it possible to reduce the risk to an acceptable level.

It really goes back to the importance of the risk assessment, and the need to do it on each tool. An alternate means design on one system may not work well enough on another due to the different chemicals involved, which require different pump/purging routines to safety clear the lines (de-energize). The alternate means must match the tool configuration it is installed on.

RFI Question 8) *Do control circuit type devices address over-voltage or under-voltage conditions that may signal power-off, power-on, or false negatives on error checking?*

Some control circuit type devices do address those concerns and assuring that they are used where necessary is part of appropriate safety circuit design and validation procedures.

Our semiconductor industry has electrical performance requirements which address suitability of use for the devices used in our safety interlock control circuits. Over-voltage or under-voltage conditions (Semi F47) are just a few of the environmental and foreseeable design scenarios which may occur.

During our semiconductor equipment evaluations, which are conducted by qualified third parties, look at non-standard conditions and evaluate these conditions such as these listed above to ensure a properly designed alternate means and prevent undetected failures to danger.

Furthermore, due to the very high costs of loss of product, the power quality in semiconductor manufacturing facilities is generally significantly better and more highly monitored than for standard industry. We have a test protocol for voltage sags (SEMI F47) to ensure that the equipment can continue to operate normally and safely during many common power fluctuations.

RFI Question 9) *How do control circuit systems detect if a component of a control circuit device breaks, bends, or otherwise goes out of specification? How do the systems signal this to the exposed employee? Could these types of failures create a hazard while the system continues to signal that conditions are safe?*

The level of design robustness depends on the hazardous energy(s) being controlled and the foreseeable hazard scenario if they are not controlled. Again we will use an example based on the requirements of ISO 13849-1, but equivalent safety standards (*e.g.*, ANSI Z244.1) could be used.

Example 1: Some hazard scenarios are found to require performance level **PL_r – c**. Such a circuit can achieve its performance level based on reliability of the devices selected (Well-tried per tables in ISO 13849-2) and the control circuit following basic safety principles. This type of design is allowed based on having a very good understanding of all the failures to danger.

Example 2: Some hazard scenarios are found to require **PL_r – d. Such a circuit can achieve its performance level based** on design redundancy instead of component reliability, especially if there is NOT a very good understanding of all the failures to danger. In this type of design there are 2 control circuits with equivalent devices in parallel so that if on device fails, the other can still take proper action. It is very important in parallel systems control circuit design to prove it is robust against common cause failures which could take out both channels.

Some examples of design features to prevent common cause failures in redundant control circuit designs are:

- Physical separation between control circuit signal paths
- Design Diversity - different technologies/design or physical principles are used, 1st channel electronic or programmable electronic and 2nd channel electromechanical hardwired
- Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
- For each part of safety related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design
- Training of designers to understand the causes and consequences of common cause failures
- For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate EMC standards
- Consideration of other relevant environmental influences such as, temperature, shock, vibration, humidity, etc.

Typically, a control circuit can be made to detect failures by testing the performance of a DEI by actuating it and sensing whether the energy has been isolated. A sensor failure can be detected by using multiple sensors and continuously comparing the input from them. The detection of such a failure could be communicated through the human machine interface (HMI) display screen or through an audible or visible warning device.

It is possible for a failure to occur and not be detected, but that's also true of a manually-actuated EID. In either case, the verification step of a procedure manages the risk to personnel.

The second and third sentences of Question 9 suggest that there are to be performance criteria imposed on the use of "control circuit devices" that are not imposed on the currently-OSHA-permitted means of lockout. Were such requirements added, it would be easier to meet them with an automated control system than with the presently-OSHA-accepted lockout technology.

In many ways, a thorough implementation through control circuits allows for the machine to check for these concerns much more thoroughly and reliably than relying on a person doing anything to address these concerns. The possibilities that could be included in such a "prepare for maintenance" routine include:

- Automating the verification step that the hazardous energy diminishes when the device used to block the hazardous energy is actuated
- Automating any complex isolation and energy dissipation steps required to make the work area safe, and clearly flagging when this does not occur correctly
- If appropriate and available, monitoring for the possibility of energy leaking past the EID and activating visual or auditory alarms

In summary, it all goes back to following the appropriate design standards for function safety control circuits to ensure highly reliable, fault tolerant, and fail safe control of hazardous energy.

RFI Question 10) *What level of redundancy is necessary in determining whether a control circuit type device could be used instead of an EID?*

There is no level of redundancy that is appropriate in all cases. Redundancy is only one of the ways to achieve reliability. The required level of reliability is determined in the risk assessment and the way to achieve it is selected in the design process. Whether the proposed design provides the required level of reliability is determined in design validation. As with the previous answer (***Question 9***), the level of design robustness depends on the hazardous energy(s) being controlled and the foreseeable hazard scenario if they are not controlled.

The key point the semiconductor industry would like to re-iterate is that the solution depends on more than the control circuit type of device. Yes, the selection of each device within the control circuit is important, but it also requires the additional evaluation of the performance of the entire control circuit itself: examples include:

- Device selection (based on criteria identified in, for example, ANSI Z244.1 and ISO 13849 Annex 1)
- What level (e.g., detection of 60%, 90%, or 99% of dangerous failures) of diagnostics is used?
- Are parallel channels required or can single channels be used?
- What other design principles must be followed?

Some examples of proven design principles for redundant (parallel) circuits:

- Use of positively mechanically linked contacts for, e.g., monitoring function in Category 2, 3, and 4 systems (see, for example, EN 50205, IEC 60947-4-1:2001, Annex F, IEC 60947-5-1:2003 + A1:2009, Annex L).
- To avoid short circuits between two adjacent conductors, use cable with shielding connected to the protective bonding circuit on each separate conductor, or in flat cables, use one earthed conductor between each signal conductor.
- Use of sufficient distance between position terminals, components and wiring to avoid unintended connections
- Limiting voltage, current, energy or frequency to restrict movement or reduced speed, to avoid an unsafe state
- Avoid undefined states in the control system. Design and construct the control system so that, during normal operation and all expected operating conditions, its state, (i.e., its output(s)), can be predicted.
- Over-dimensioning - De-rate components when used in safety circuits by the following means:
  - current passed through switched contacts should be less than half their rated current;
  - switching frequency of components should be less than half their rated value;
  - total number of expected switching operations should be no more than 10 % of the device's electrical durability. This is greatly helped by having completely separate circuits for normal control versus safety functions.
- Balance should be made between complexity to reach a better control, and simplification in order to have better reliability.

In summary, it all goes back to following the appropriate design standards for function safety control circuits to ensure highly reliable control of hazardous energy.

RFI Question 11) *Lockout/tagout on EIDs ensures that machines will not restart while an employee is in a hazardous area. How do control circuit type devices similarly account for employees working in areas where they are exposed to hazardous machine energy?*

The protection described in Question 11 is afforded by the exclusivity of the control, not by how the control is actuated. In currently-OSHA-permitted lockout, each of the potentially-exposed personnel places a lock, to which only that person has a key, on an EID. Therefore, for the hazardous energy to be re-enabled, each of the potentially exposed personnel must (by removing his lock) consent to the energy being re-enabled. We agree that such exclusivity of control (if worker A locks out a hazardous energy source, then worker A must also unlock it) needs to be provided whether the means of performing energy isolation entails actuating an EID manually or actuating a DEI through a control circuit.

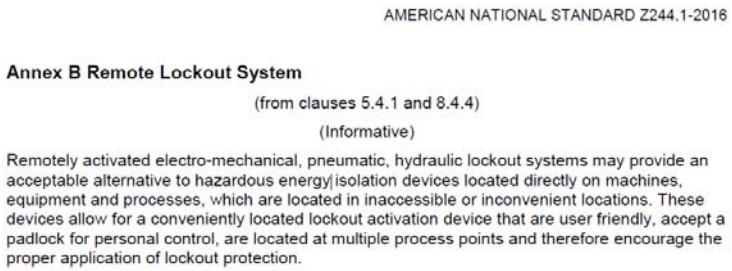
There are several ways similar performance can be provided by a system using a control circuit to perform energy isolation. For example, a key switch can be provided as an input to the control circuit, configured so that the key can then be removed only when the hazardous energy is isolated. A worker isolating the hazardous energy could keep the key in his possession, or place it in a lockable box and place a lock, to which only he has a key, on the box. The latter allows other workers to place their locks on the box, as well, providing a means of requiring that each of them consent to restoring the hazardous energy.

Refer to our answer to Question 5 for failure to danger rates for Performance Levels versus the human error rate tables- - helping to justify the importance of engineering controls over administrative controls that rely on human being “perfect”…

RFI Question 12) *How do control circuit type devices permit an employee to maintain control over his/her own safety?*

Providing each worker a way to “maintain control of his/her safety” is not fundamentally different for DEIs actuated by control circuits and EIDs actuated manually. The input to the control circuit can be designed so that each of the exposed workers can place an individual lock on either the input device or a suitable group lockout device that controls a single lock on the input device. For example, the input device that commands a control system to isolate hazardous energies could be a key-operated switch from which the key can be removed only when the switch is set in the position that results in energy isolation. The first worker to work on the equipment could remove that key, place it in a lockable box, and put a personal lock on the box. Each additional worker would then place a personal lock on that box. To remove the energy isolation, each worker would need to remove his/her personal lock, then one of the workers could remove the key from the box and change the position of the switch, directing the control system to remove the energy isolation. Please note that this scenario is provided as an example of how exclusivity of control could be provided with energy isolation being done through a control system. Our strong preference is that OSHA provide performance requirements, not specify the way that an equipment supplier provide the required performance.

The preferred control circuits designs to control hazardous energy in the semiconductor industry are lockable (see our answer to ***Question 1)*** This way the control circuit would perform the complex Lockout sequences but the worker could still have a lock to prevent unexpected start up – this is the best use of technology and exclusive control of the conventional Lockout method. REF: ANSI Z244.1 for example of simple Remote Lockout System.



AMERICAN NATIONAL STANDARD Z244.1-2016

Annex B Remote Lockout System

(from clauses 5.4.1 and 8.4.4)

(Informative)

Remotely activated electro-mechanical, pneumatic, hydraulic lockout systems may provide an acceptable alternative to hazardous energy isolation devices located directly on machines, equipment and processes, which are located in inaccessible or inconvenient locations. These devices allow for a conveniently located lockout activation device that are user friendly, accept a padlock for personal control, are located at multiple process points and therefore encourage the proper application of lockout protection.

RFI Question 13) *How do control circuit type devices permit employees to verify that energy has been controlled before beginning work in danger zones? How do the devices account for exposed employees before equipment is restarted?*

How the absence of hazardous energy can be verified by a worker does not depend on how the EID has been actuated. Also, verification could be performed by the control circuit.

Again there are many different solutions to this and it is (as mentioned previously) more than "devices" but rather it's a complete system of devices (safety function). This question is really includes 2 separate and distinct questions:

The answer to the first part will depend on both the hazardous energy being controlled and the equipment design. There are many different ways to apply the verification process before beginning work. There are already electrical isolation devices with visual feedback to inform if hazardous voltage has been safely removed by the control circuit.

See example below of one such system (isolation device, monitoring devices, logic controller and visual door mounted output monitor). The semiconductor industry does not show preferential treatment of one company over another, it just that this example as a video link to help explain the device and its internal checking for verifying the absence of AC and DC voltage phase to phase and phase to ground. It has a very high safety integrity level (SIL 3, 1 dangerous failure > 1,100 years) per IEC 61508-1.

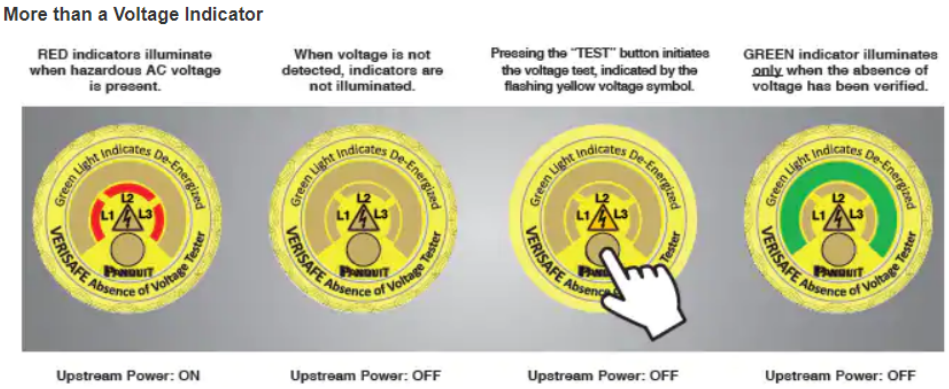


Figure 3: Example of Permanently Mounted Absence of Voltage Tester (AVT)

- LINK: https://www.youtube.com/watch?v=tV4x5dIb8wk
- LINK: https://www.youtube.com/watch?v=u4LibH5U9hg

Similar systems can be envisioned for non-electrical hazardous energies.

There's no obvious connection between how the energy is isolated and how the absence of personnel from certain locations is verified before restoring the energy. The personnel who are to direct a control system to remove energy isolation can verify the absence of personnel the same way they could verify the absence of personnel before reversing the manual activation of an EID.

The second part: ***How do the devices account for exposed employees before equipment is restarted?***" is somewhat confusing as there should not be any "exposed" employees if the alternate means was designed and implemented correctly. The equipment should only be allowed to restart if there are no other employees in "danger area". More information is required to answer the second part of this question further.

This concern is also addressed by providing proper exclusivity of control, so that each of the exposed personnel must act before a hazardous energy is restored.

RFI Question 14) *Control circuit type devices have a number of claimed benefits compared to energy isolating devices, including workers' greater willingness to use such devices, better efficiency, less downtime, and the lack of a requirement to clear programming on computer controlled devices. Are there any other benefits to using control circuit type devices? Are there certain situations where these devices are especially advantageous? For example, where machine tasks require frequent repetitive access, is the process faster and/or less physically demanding than applying mechanical lock(s)?*

The semiconductor industry sees the biggest benefit being fewer accidents due to reasonably foreseeable misuse. Per ISO 12100 Section 5.4 (c) Hazard Identification, examples of "reasonably foreseeable misuse" include:

- Behavior resulting from lack of concentration or carelessness,
- Behavior resulting from taking the line of least resistance in carrying out a task, and
- Behavior resulting from pressures to keep machinery running in all circumstances

Of all the examples given in the beginning part of this question lead to proper control of hazardous energy, which leads to safer workplace.

- Do our workers make Lockout mistakes?
- Do our workers sometimes take shortcuts with Lockout?
- Are we pressured by our customers and our local management to get our "tools" back up and running as quickly as possible?

I think we can say "YES" and this meets the definition, and it is definitely one area where we may need to consider certain improvements to our Lockout / CoHE equipment designs. Incidents happen when complex Lockout tasks are done wrong (human error) or shortcuts are taken, or pressures to get the equipment back up and running as soon as possible. But, if workers' greater willingness to use such devices, and alternate means allow for better efficiency, and less downtime, this all leads to a safer workplace.

Figure 4 shows some of the typical and relevant features of a piece of semiconductor manufacturing equipment (SME). This drawing does not represent a particular, real piece of equipment. It is a composite of several typical features and was created for the purpose of illustrating how CoHE is provided in such equipment. In order to fit the drawing on a single page, many process control components have been omitted.

In this equipment, a container of wafers is placed in the load station. Under the control of its internal logic, the equipment opens the door between the load station and transfer chamber. The parts handler then extracts a wafer from the container and moves it into the transfer chamber. The door closes and the vacuum pump empties the transfer chamber. When the required pressure is reached, the door to the process chamber opens and the parts handler moves the wafer to the wafer chuck. The door closes and the process steps begin. The heater in the wafer chuck raises the wafer to the appropriate temperature, process gases and inert gases are supplied at the top of the process chamber, as is microwave energy. Process byproducts and excess gases are removed by the vacuum pump, so that the required pressure is maintained. The cooling plate removes the excess heat from the process chamber. At the end of the process, the vacuum pump empties the process chamber. The wafer is then moved back to the transfer chamber, where it is cooled, then moved to the load station. This sequence is repeated for each wafer in the container. In normal operation, this whole sequence occurs without human participation.

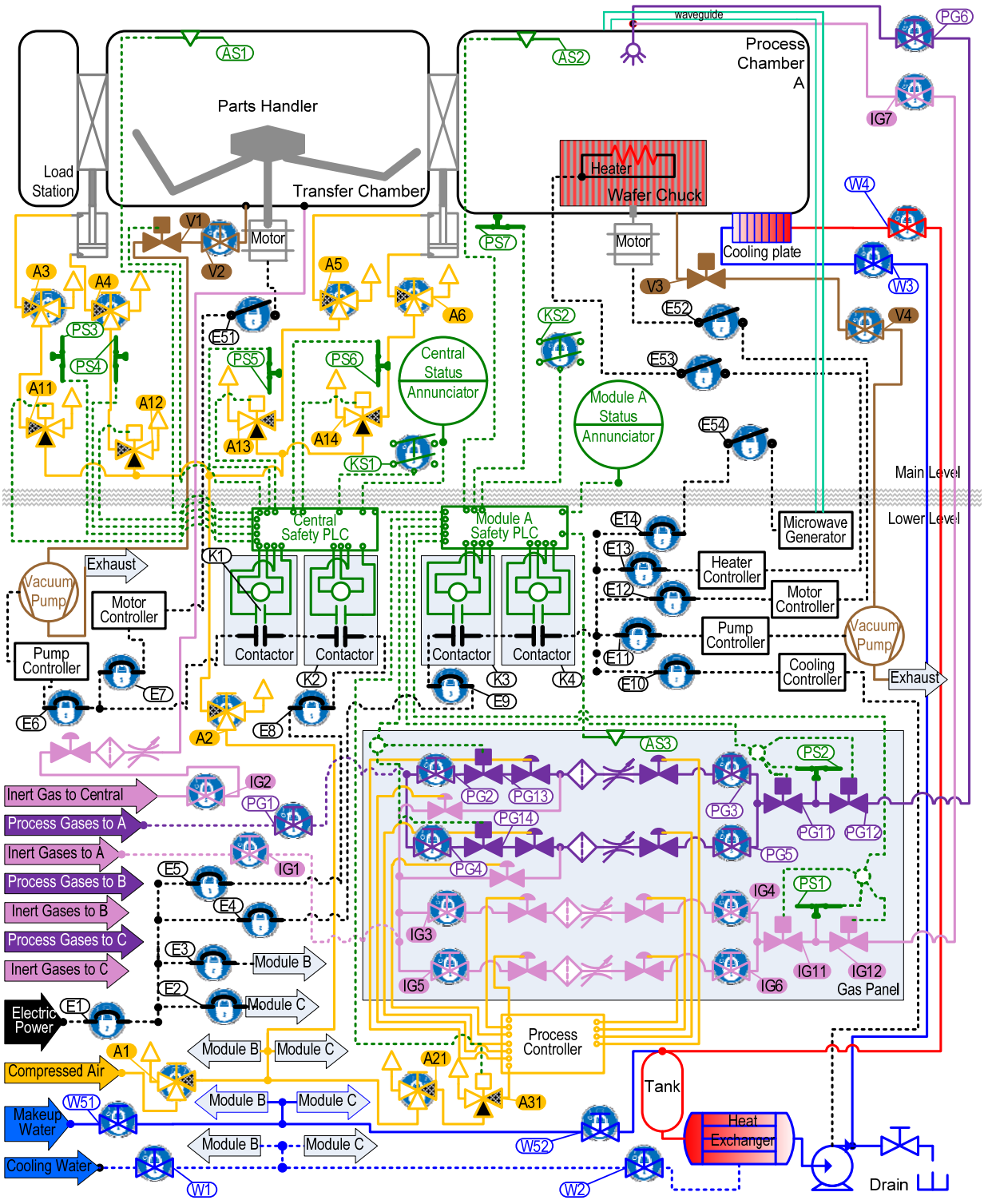


Figure 4: Simplified, generic example of semiconductor manufacturing equipment

Note: Solid lines represent single paths, such as a conductor or a pipe; dashed lines represent multiple paths, such as a multi-conductor cable or the supply and return hoses in a cooling loop.

Table 1: CoHE features of Figure 4

E51 through E53	Lockable switch	Switch that can be locked in only the open position. Isolates the electric power feed, preventing exposure to the electrical energy and to unexpected energization of the load. For the motors and the heater, these devices are placed in the fab (for convenience of access) in the energy path between the drivers and the loads. The lockout device may be part of the switch or part of the assembly in which the switch is mounted.
E54	Lockable switch	Switch that can be locked in only the open position. Isolates the electric power feed, preventing exposure to microwave energy that could result from the unexpected energization of the microwave generator. Because of the difficulty of providing an isolation device for the waveguide, the power supply to the microwave generator is routed up to the fab to the switch and back down to the subfab. The lockout device may be part of the switch or part of the assembly in which the switch is mounted.
IG1 through IG7	Lockable manual inert gas valve	Can be used to isolate the flow of an inert gas, such as helium, argon, and nitrogen. Handle can be locked only to prevent the valve being moved from the closed position to the open position.
IG11 and IG12	Remote inert gas valve.	This is a normally-closed valve: unless it is actuated, it is closed. Controlled by a safety PLC and used for remote lockout and for alternative methods, such as interlocks.
KS1 and KS2	Keyed Switch	A keyed or otherwise lockable input to a safety PLC. It is the means by which the remote lockout is activated.
PG1 through PG7	Lockable manual process gas valve	Can be used to isolate the flow of a process gas that is not inert, such as by being flammable, oxidizing, or toxic. Typical examples in the semiconductor industry are hydrogen, oxygen, and phosphine. Handle can be locked only to prevent the valve being moved from the closed position to the open position.
IPG11 and PG12	Remote process gas valve.	This is a normally-closed valve: unless it is actuated, it is closed. Controlled by a safety PLC and used for remote lockout and for alternative methods, such as interlocks.
IPG13 and PG14	Remote process gas valve.	This is a normally-closed valve: unless it is actuated, it is closed. Controlled by a safety PLC and used for alternative methods, such as interlocks.
PS1 and PS2	Pressure switch	Monitors the pressure between two remote gas valves. If the space between the valves is evacuated before the second valve is closed, a leak through either valve will result in a pressure increase in the space between them, indicating that at least one of the valves is no longer providing isolation. The safety PLC monitors the pressure switch and, if it detects such a valve failure, notifies the personnel relying on the protection of the remote valves.
PS3 through PS6	Pressure switch	Monitors the pressure between lockable manual and remote air valves. If the space between the valves is vented before the second valve is closed, a leak through the upstream valve will result in a pressure increase in the space between them, indicating that the remote valves is no longer providing isolation and that the manual valve is connected to the drive cylinder. If the manual valve is set to vent, the pressure switch may not indicate a failure of the remote valve, but that failure cannot cause the drive cylinder to move.
PS7	Pressure switch	Monitors the pressure in the process chamber. Through the safety PLC and PG11 and PG12, allows process gas flow only if the pressure in the chamber is below the switch setpoint. This is used to protect against delivering process gas to the process chamber under several foreseen conditions, including: an open lid (backs up the protection by AS2), leak from the chamber to the room, and loss of process pressure control (prevents reaching a high enough pressure in the chamber that an uncontrolled reaction could cause injury).
V1 and V2	Lockable manual vacuum valve	Used to prevent pumping on the chamber. Can be locked only in the closed position.
W1 and W2	Lockable manual water valve	Isolate the equipment from the facility cooling water loop. Can be locked only in the closed position.
W3 and W4	Lockable manual water valve	Isolate the cooling plate from the equipment cooling water loop. Can be locked only in the closed position.
W51 and W52	Lockable manual water valve	Isolate the equipment from the facility makeup water supply. Can be locked only in the closed position.

Maintenance (done to keep equipment operating properly) and service (done to repair equipment that has malfunctioned), however, do require humans. The following table lists several common maintenance and service tasks, the portions of the equipment to which human access is necessary, the hazardous energies present, and examples of how CoHE is provided to protect the personnel. The means of CoHE are presented in three different columns: direct lockout, remote lockout, and alternative methods.

Table 2: CoHE means for sample tasks in Figure 4

Task	Access To	Hazardous Energy	Direct Lockout required	Remote Lockout permitted	Alternative Methods
		Methods:	Lockout device (LD) and energy isolating device (EID), are in the same location with a direct mechanical linkage between them	LD and EID may be in different locations and may be connected by a control system with adequate control reliability.	Means of CoHE that do *not* include isolation of the hazardous energy, by either direct or remote lockout
Remove broken wafer	transfer chamber	Mechanical: motion of parts handler	E51 in fab or E7 in subfab	KS1 opens K1 and K2	AS1 opens K1 and K2
		Mechanical: Closing of door to load station	A4	KS1 deactivates A12	AS1 deactivates A12
		Mechanical: Closing of door to process chamber	A6	KS1 deactivates A14	AS1 deactivates A14
		Chemical: opening of door to process chamber	A5	KS1 deactivates A13	AS1 deactivates A13
		Inert gas feed to transfer chamber	Not needed, as the flow rate is too low to cause asphyxiation in a well ventilated room with the lid open and the space is not accessible with the lid closed		
		Entrapment: Vacuum pump starts	V2	V2 (note 1)	AS1 closes V2

Task	Access To	Hazardous Energy	Direct Lockout required	Remote Lockout permitted	Alternative Methods
Adjusting the path of the parts handler	transfer chamber	Mechanical: motion of parts handler	Not applicable, as this task can be done only if the parts handler is moving by itself while being observed directly.		Limiting the speed and force of the parts handler motion and providing a control to the person performing the task that must be actuated continuously for the parts handler to move.
		Mechanical: Closing of door to load station	A4	KS1 deactivates A12	AS1 deactivates A12
		Mechanical: Closing of door to process chamber	A6	KS1 deactivates A14	AS1 deactivates A14
		Inert gas feed to transfer chamber	Not needed, as the flow rate is too low to cause asphyxiation in a well ventilated room with the lid open and the space is not accessible with the lid closed		
		Entrapment: Vacuum pump starts	V2	V2 (note 1)	AS1 closes V2
		Chemical: exposure to process gases	PG6 in fab or PG3 and PG 5 in the subfab	KS2 closes PG11 and PG12	AS2 or PS7 closes PG11 and PG12
		Chemical: exposure to process residue	There's no available isolating device, so alternative methods must be used.) are needed		automated purging and cleaning processes, work practices, supplemental ventilation, or PPE
		Thermal: chuck is heated to 1000 ºC	E53 in fab or E13 in subfab (notes 2 and 5)	KS2 opens K3 and K4 (notes 2 and 5)	AS2 opens K3 and K4 (notes 2 and 5)
		Thermal: cooling plate	Not needed, as the heat transfer fluid is water, as is the utility to which it transfers heat, so the minimum temperature does not comprise a touch hazard.		
		Chemical: exposure to process residue	There's no available isolating device, so alternative methods are needed		automated purging and cleaning processes, work practices, supplemental ventilation, or PPE
		Electromagnetic: exposure to microwave energy	E54 in fab or E14 in subfab. (note 3)	KS2 opens K3 and K4.	AS2 or PS7 opens K3 and K4

Task	Access To	Hazardous Energy	Direct Lockout required	Remote Lockout permitted	Alternative Methods
Remove broken wafer	Process chamber	Mechanical: motion of parts handler	Not needed, as long as the door to the transfer chamber is closed and prevented from opening.		
		Mechanical: Closing of door to transfer chamber	A6	KS2 deactivates A14	AS2 deactivates A14
		Mechanical: opening of door to transfer chamber	A5	KS2 deactivates A13	AS2 deactivates A13
		Mechanical: movement of wafer chuck	E52 in fab or E12 in subfab	KS2 opens K3 and K4	AS2 opens K3 and K4
		Thermal: chuck is heated to 1000 ºC	E53 in fab or E13 in subfab (note 2)	KS2 opens K3 and K4 (note 2)	AS2 opens K3 and K4 (note 2)
		Thermal: cooling plate	Not needed, as the heat transfer fluid is water, as is the utility to which it transfers heat, so the minimum temperature does not comprise a touch hazard.		
		Chemical: exposure to process gases	PG6 in fab or PG3 and PG 5 in the subfab	KS2 closes PG11 and PG12	AS2 or PS7 closes PG11 and PG12
		Chemical: exposure to process residue	There's no available isolating device, so alternative methods must be used.		automated purging and cleaning processes, work practices, supplemental ventilation, or PPE
		Electromagnetic: exposure to microwave energy	E54 in fab or E14 in subfab. (note 3)	KS2 opens K3 and K4.	AS2 or PS7 opens K3 and K4
Replace filters in process gas lines	Gas panel	Chemical: exposure to process gas flows	PG2 and PG4	PG2 and PG4 (note 1)	AS3 closes PG2 and PG4
		Mechanical: exposure to process gas pressure	PG2 and PG4	PG2 and PG4 (note 1)	AS3 closes PG2 and PG4
		Chemical: exposure to process gas remaining in piping	There's no available isolating device, so alternative methods must be used.		automated purging and cleaning processes, work practices, supplemental ventilation, or PPE
Replace filters in inert gas lines	Gas panel	Chemical: exposure to process gas flows	IG3 and IG5	IG3 and IG5 (note 1)	AS3 deactivates A31
		Chemical: exposure to process gas remaining in piping	None (note 4)		
		Mechanical: exposure to inert gas pressure	IG3 and IG5	IG3 and IG5 (note 1)	AS3 deactivates A31
Replace parts handler motor controller	Electrical rack in subfab	Electricity	E7	E7 (note 1)	Finger-safe electrical connector

Notes: Table 2: CoHE means for sample tasks

1) As the work is to be done near (most importantly, on the same floor as) the energy isolating device, there's no great advantage to performing lockout from somewhere else.
2) Removing electrical power from the heater addresses contact with the electricity and the addition of heat, but it does not cause instantaneous cooling to a touch-safe temperature. Therefore, administrative controls (labeling and procedure) are needed to allow the chuck to cool before beginning work in the process chamber.
3) Installing a disconnecting device in the waveguide would require a large amount of space and could degrade performance and disassembling a waveguide is time consuming and, in some cases, presents access challenges, so E54 is provided to enable direct lockout in the fab.
4) Risk assessment found that the risk of this exposure is acceptable.
5) Protection from the thermal hazard of the chuck during work in the transfer chamber with the door between the chambers open is needed only if there is a credible expectation of contact with the hot parts. In most systems, there is no credible risk of accidental contact by personnel; in some systems, it is not geometrically possible to reach through the door between the chambers from the transfer chamber to the wafer chuck.

RFI Question 15) *What other methods or devices, if any, are being used with control circuit type devices to control the release of hazardous energy, especially in cases where the control circuit devices are only used to prevent machine start-up? Are there control circuit type devices that require additional methods or devices to fully control the release of hazardous energy? What improvements to safety or health does the use of these devices or methods provide?*

We are not sure we understand this question. It is possible in certain situations that more than one alternate means is needed.

A simple example would be using a Remote Lockout design to isolate multiple high temperature heaters (>1,000 degrees C) on a given process chamber. When the Remote Lockout is switched off and Locked, it initiates a sequence of safety functions so that various 24 VDC relays cannot command the power contactors which distribute power to the different heaters to close, thereby removing power to heaters. Permanently mounted absence of voltage systems can be used to verify each heater is off, isolated and de-energized. By this sequence, the hazardous electrical energy has been removed and is prevented from being started again by the process controller. However, additional hazardous energy remains. The heaters do not cool down instantaneously, some take over an hour to reach safe touch levels. In this case the alternate means used to turn off the heaters and prevent restarting of them is not enough – thermal burn risks still exist. To satisfy the risk assessment, an additional alternate means of CoHE can be added to hold the process chambers access door closed magnetically until the internal temperature (from all the heaters) reaches safe touch levels.

The key point is that each hazard scenario must be properly assessed to ensure that after alternate means is used the risk is reduced to acceptable level. If not further action is required.

In some cases, the risk assessment will find that an acceptable level of risk cannot be achieved by lockout plus alternative methods (if the hazardous energy is not needed) or alternative methods alone (if the hazardous energy is needed). In such cases, either the equipment or the task must be modified to make it possible to reduce the risk to an acceptable level. Changes to the equipment can affect the risks of other tasks (including normal operation) and changes to tasks can affect the hazardous energy exposures and other risks of maintenance and service. Therefore, if any changes are made to tasks or equipment, the affected set of risk assessments should be reviewed and, if appropriate, updated.

An example of this risk evaluation process is given in SEMI CoHE White Paper and shown below.

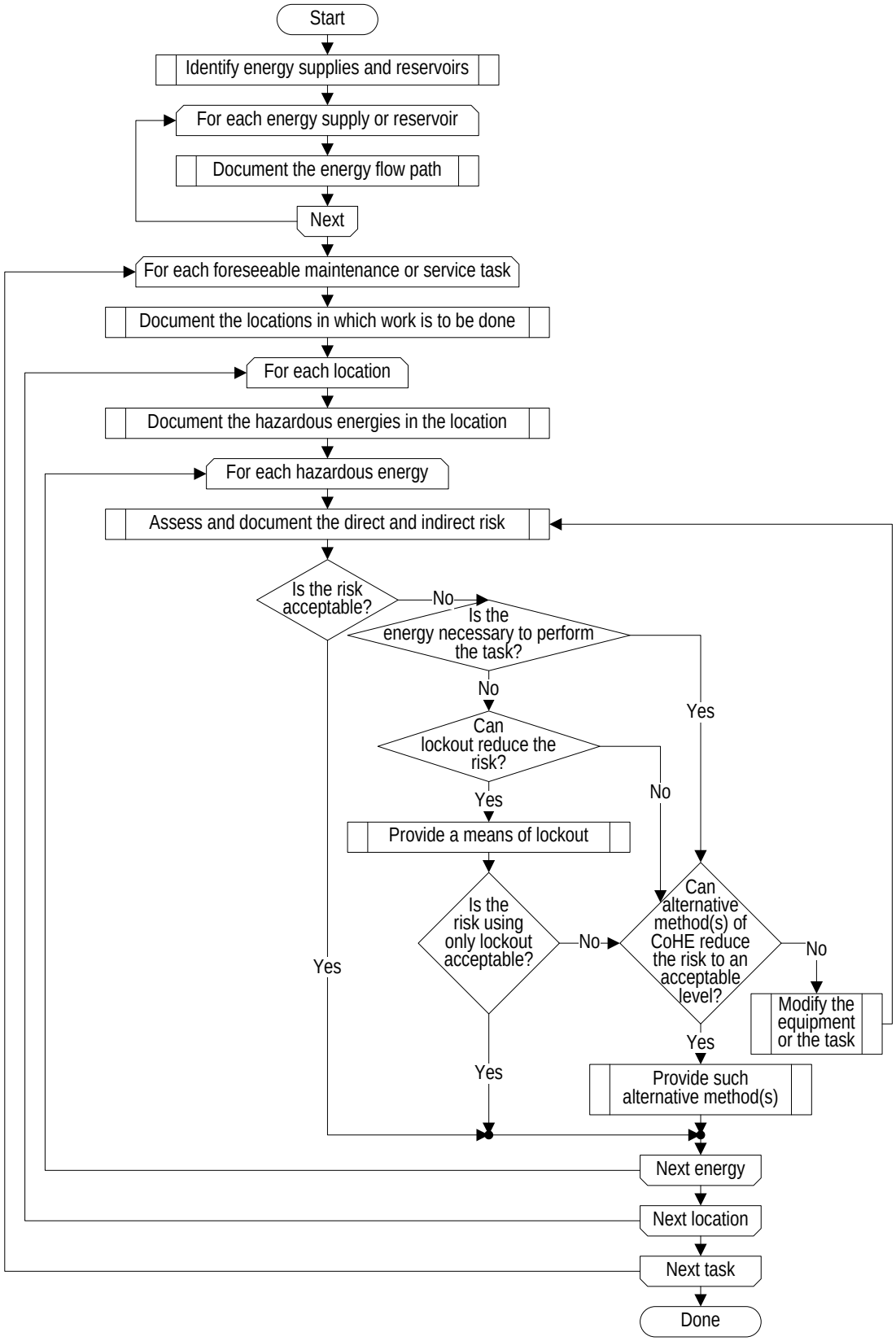


Figure 5: CoHE Method Assignment Process

RFI Question 16) *What are the unit costs for installing and using control circuit type devices or other alternative methods of hazardous energy control? Are the costs of installing and using control circuit type devices or other alternative methods of controlling hazardous energy dependent on the capacity or efficiency of the devices? If so, please include details on the effects of capacity on these unit costs including the capacity of any equipment you use in your facility. Are these devices generally integrated into newly purchased machinery, or are they purchased and installed separately? What steps need to be taken, and how long do those steps take, for these systems to be engaged in a manner that fully protects workers from the release of hazardous energy?*

The SEMI ICRC working group intentionally stays away from any quantitative discussions related to cost. Individual companies would need to answer this question, but as a collective we feel it is not within our scope to do so.

In general, it is known that the effort to design and build integrated control circuits for the control of hazardous energies is not trivial. There are knowledge and skill requirements for the design engineers, as well as the additional engineering efforts to ensure proper compliance to the functional safety standards. Yes there is a cost, and it is probably higher than just designing conventional Lockout.

Still the benefits mentioned previously in ***Question 14)*** in many situations outweigh the upfront additional costs.

There are cases, such as those that could make use of an EID already installed, in which retrofitting might not be so burdensome as to outweigh the benefits. For example, if a piece of equipment includes (in a safety interlock circuit that is managed by a safety controller) contactors that remove power from heaters, it might be possible to add a means of remote lockout by adding a lockable input switch to the safety controller and modifying that controller's software.

Typically these types of alternate means are difficult to retrofit to existing equipment designs. The industry sees the use of alternate means being most applicable to new system designs.

Some of the upfront additional costs of design and parts would likely be offset by reduced warranty and service costs due to complex preparation process being completed more reliably. This is in additional to the "benefit" of increased employee safety by having hazardous energy control completed correctly and completely with a higher reliability.

RFI Question 17) *What additional actions is your firm taking to protect workers when they are servicing machinery with control circuit type devices in order to meet OSHA's Lockout/Tagout standard requirements? For example, does your firm purchase and use physical devices that you feel do not enhance worker protections but nonetheless are required by the OSHA standard? What are these items and how much do they cost? Please explain why you feel these items do not enhance worker protections.*

SEMI is not a firm/company but has a wide range of diverse organizations (*e.g.,* end users, equipment suppliers, chemical suppliers, abatement suppliers, 3rd party evaluators, and independent consultants) as members. The responses herein from the working group reflect the consensus views resulting from discussion of OSHA's questions.

Lockout hardware that isn't used doesn't enhance protection and that the perceived burden of using traditional lockout reduces its use, even if the equipment is available. Furthermore, not all "enhancement" is mandated by reasonable safety engineering. If the risk without lockout is acceptable, why impose the additional burden?

RFI Question 18) *The American National Standards Institute (ANSI), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC) all have standards that may be applicable to control circuit type devices. Should OSHA consider adopting portions of any ANSI, ISO, or IEC standard that specifies requirements for control circuit devices as part of an updated OSHA standard? Are there recommendations in the consensus standards that you choose not to follow? If so, please explain why. Are there any requirements in these standards that would impose significant cost burdens if OSHA were to include those requirements in a revised Logout/Tagout standard? Are there provisions of one consensus standard when compared to the others that you perceive as having lower costs to implement and use on a day-to-day basis while providing protection to workers that is equal to or greater than that provided by the other standards? If so, please explain.*

There are many questions here. The most important question, we believe, is:

"***Should OSHA consider adopting portions of any ANSI, ISO, or IEC standard that specifies requirements for control circuit devices as part of an updated OSHA standard?"***

We believe that the industry consensus standards should be followed. We support OSHA permitting, but not mandating, the use of ANSI Z244.1. Similar to ANSI Z244.1 Committee position, the semiconductor industry does not think OSHA should be concerned with the specifying the requirements for providing alternate means – There are already industry consensus standards which do this well.

One way to address the concern of the burden of adopting a consensus standard is for OSHA to permit use of such a standard as an alternative to the currently-OSHA-permitted method

We believe OSHA should simply reference (but not incorporate the substance of) these detailed consensus standards as permissible ways to show conformity for proper control circuit designs, but OSHA should not, itself, publish its own version of requirements. If OSHA were to (as suggested) adopt portions of any ANSI, ISO, or IEC standard, this will lead to problems. You need the whole standard – that is why it is there. Adopting only portions of a standard will lead to incomplete designs.

The semiconductor industry has its own "consensus" SEMI Safety Guidelines. We also refer to some national and international consensus standards for understanding the specific design and testing details. If OSHA makes strict and prescriptive rules on how to control hazardous energy it will fail to keep up to date, becoming outdated and putting us into a similar situation we are in today. The means of how to control hazardous energy should be left to industry consensus standards committees to keep them current.

Just as the ANSI Z244.1 Committee proposes, the semiconductor industry also believes OSHA's role as it related to control of hazardous energy legislation should focus on the minimum of **what should be done** and not the more prescriptive of **how it should be done.**

RFI Question 19) *ISO categorizes "the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions" into one of five levels, called performance levels. These performance levels "are defined in terms of probability of dangerous failures per hour." Should OSHA consider requiring a specific performance level in determining whether a control circuit type device could be a safe alternative to an EID.*

Specifying a minimum performance level (ISO 13849-1) goes against the entire concept of risk assessment. Some hazardous energy scenarios may be perfectly acceptable with less and this would require additional unnecessary control circuit features. Other hazardous energy scenarios may need much more that a so called minimum performance level, which would lead to a false sense of security, if only the minimum level was designed.

As an example, the international robotic standard (ISO 10218-1) and the US national consensus robotic standard (ANSI RIA 15.06) does specify a minimum performance requirement (CAT3 = Category 3 architecture which means redundant channels with diagnostic monitoring on the outputs) and a Required Performance Level (PL_r = d) which includes a maximum of 1 dangerous failure every 114 years for continuously operating systems. In certain instances, this level of performance is not needed for some semiconductor industry robots with lower force and speed than the fastest industrial robots. Thus, it is imposing undue, additional requirements on equipment manufacturers (situation specific). We do not recommend this approach of having OSHA requiring a specific performance level in determining whether a control circuit type device could be an acceptable alternative to the currently-OSHA-permitted means of managing risk to personnel.

RFI Question 20) *Can System Isolation Equipment, as discussed in the UL consensus standard UL6420 Standard for Equipment Used for System Isolation and Rated as a Single Unit provide protection equal to that obtained through lockout/tagout?*

The level of protection obtained through direct, conventional Lockout is still a function of whether or not the procedure for doing Lockout is written correctly and each step is followed correctly. When you ask about "equal protection" you are in effect asking about equivalent residual risk. Even a conventional Lockout tasks are not zero risk. If it is done properly, we believe as an industry there is low risk of harm due to unexpected startup of hazardous energies – but it is not zero. However, Lockout, as we know, can be and sometimes are done incorrectly – especially for very complex Lockout of multiple energy sources, on multiple floors/rooms. Here the level of risk must take into account *reasonably foreseeable misuse*. (for definition see answer to ***Question 14***).

The Semiconductor industry guidelines are heavily based on the principles of risk assessment. We believe this statement in the Foreword section from Z244.1 is helpful in distinguishing the term "equal protection" and describes a better approach on how to compare different solutions, on risk assessment:

> The standard recognizes that zero risk is only a theoretical possibility, but is not an operative reality - zero risk does not exist. The concept of feasible risk reduction to achieve acceptable or tolerable risk is emphasized whether using conventional lockout, tagout or alternative methods. With regard to hazardous energy control the term "safe" suggests the absence of risk. More accurately, "safe" should be viewed as the acceptability of risk to those who may be exposed. There are numerous terms that reflect the circumstances under which servicing and maintenance is done routinely today. Terms such as AFARP (as far as reasonably practical), ALARA (as low as reasonably achievable), or ALARP (as low as reasonably practicable) convey a more realistic approach to risk reduction and in particular the use of alternative methods.

UL 6420 systems are definitely an option to be used for proper Remote Lockout applications. These systems are rated as a single unit, but they are a system, a control circuit made up of individual devices that must be evaluated independently and as a system. Currently there are systems for electrical Lockout, and separate devices for pneumatic and hydraulic. Looking forward, a "system" that can do all 3 with a single Lockout point would be even more desirable in certain applications. UL 6420 may be an appropriate tool for selection of means of isolating electrical energy. I point out, however, that it would be highly undesirable to make this the only way to qualify a remote lockout, as it applies to only supplies of electrical energy. It does not address stored energy or other types of energy, such as thermal and chemical.

The key point here is the term equal protection should not be used.to We cannot expect one solution to fit all applications. Each hazard scenario during a given Lockout task must be looked at independently, following the flowchart as provided in our answer to ***Question 15).*** The risk assessment is absolutely critical to justify whether or not you have proper protection.

RFI Question 21) *The ANSI/ASSE Z244.1 consensus standard encourages the use of risk assessment and hazard control hierarchy as alternative methods of hazardous energy control. Should OSHA consider incorporating these methods in any new standard with respect to the use of control circuit type devices?*

YES. We have discussed the importance of "Risk Assessment" and the importance of "Engineering Controls being preferred over Administrative Controls" in almost all of our answers so far. This supports our industry voice on the importance of OSHA doing this.

RFI Question 22) *Do you currently utilize the services of a specialized safety engineer or employment safety administrator to test for competency and/or ensure that the hazardous energy control system is operational? If so, how many hours does this individual spend on these tasks? Do you anticipate you would need to make use of these services if OSHA revised the Lockout/Tagout requirements to align with the consensus standards? Based on data from the Bureau of Labor Statistics, OSHA estimates that an occupational health? A safety specialist makes $33.14 an hour or $68,930 annually plus benefits. If you have used the services of such specialists, how does this compare with your experience?*

The SEMI ICRC working group intentionally stays away from any quantitative discussions related to cost. Individual companies would need to answer this question, but as a collective we feel it is not within our scope to do so.

SEMI is not a firm/company but has a wide range of diverse organizations (*e.g.*, end users, equipment suppliers, chemical suppliers, abatement suppliers, 3rd party evaluators, and independent consultants) as members. The consensus resulting from discussion of this question is that typical industry practice is for equipment suppliers to have safety staffs and to have independent review of safety features prior to industry introduction of new equipment designs. The independent review of the safety features of the equipment, demonstrated in the form of a report to the industry safety standard SEMI S2, is a very common purchase specification requirement for most new equipment.

As mentioned in our answer for ***Question 18),*** we believe OSHA's role as it related to control of hazardous energy legislation should focus on performance criteria and not the more prescriptive aspects of how the required performance be provided.

ANSI Z244.1 guidance requires the review by a qualified person when necessary. The alternate means approach requires should be reviewed throughout the design process. Equipment designers should document this, and be able to provide as evident of due diligence in proper control system design. We would welcome further discussions on this on the most efficient and effective way to do this going forward.

8.2.14 Review by a Qualified Person

Where necessary, an alternative method shall be reviewed by a qualified person.

NOTE: The persons developing the alternative method should use due diligence throughout the process in order to achieve a high level of confidence in the results. Confidence can be improved by consulting others who possess the appropriate knowledge and expertise, and by having other qualified persons review the design.

and Reference ANSI definition:

3.7 Qualified Person

A person who, as a result of training and experience, understands and demonstrates competence with the design, construction, operation or maintenance of the system and the associated hazards. Also sometimes referred to as a competent person.

Whether a change by OSHA to align with a consensus standard would result in additional need for such services would depend on the internal capabilities of each company, which consensus standard were to be adopted, and whether OSHA were to continue to allow the use of the traditional means of compliance.

RFI Question 23) *How much training do you currently provide on Lockout/Tagout requirements? How long does training on this subject take and how often do employees receive training on the subject? If OSHA were to revise the Lockout/Tagout standard to permit use of control circuit type devices in some circumstances, would newly hired workers require more training or less than under the current standard? What format do you use to provide training on the Lockout/Tagout standard at your facility (i.e., small group classroom session, self-guided computer modules, etc.)? If you have used third-party training vendors to provide similar training, what are the costs? If training is provided in-house, what sort of employee provides the training (i.e., a first-line supervisor, a safety and health specialist, etc.)?*

The SEMI ICRC working group will not discuss the cost of compliance, and we have variances on how Lockout training is performed throughout the industry.

The formats for performing training in our industry are outlined in SEMI S19-0311: Safety Guideline for Training of Mfg Equip. Installation, Maintenance and Service Personnel (re-approved 0816) and should be followed as a minimum.

Individual companies would need to answer this question, but as a collective we feel that in general, the cost are design and hazard specific and it would be difficult to do a cost/benefit analysis with taking into account multiple variables (the most important being shortened downtime of complex Lockout tasks and less downtime do to any incidents as a result of human errors.

Training would still be required and competency testing should be completed. For much of the equipment in the semiconductor industry, equipment-specific training of user personnel is provided by equipment suppliers.

Whether a change by OSHA would result in additional need for training would depend on the internal practices of each company, and whether OSHA were to continue to allow the use of the traditional means of compliance.

RFI Question 24) *Should OSHA consider making revisions to the Lockout/Tagout standard that address advances to robotics technology with respect to hazardous energy control? If so, what revisions should OSHA consider?*

In principle, “yes” to the first question. Industrial robotics and the safety measures that pertain to them have both evolved substantially since the current regulations were promulgated and it is likely that similar, and perhaps better, means of risk management are available.

RFI Question 25) No Response

RFI Question 26) No Response

RFI Question 27) No Response

RFI Question 28) *Are you currently using some form of lockout/tagout to control hazardous energy in robots? What steps do you take? How long do those steps take? Do you use any specially purchased equipment or materials for this process? How frequently do you take steps to control hazardous energy releases in your industrial robots? How does the process compare to the steps undertaken to comply with OSHA’s Lockout/Tagout standard? How many labor hours do these additional steps require? Do these steps require any additional equipment? If so, what does this equipment cost?*

Yes. Only in teach or manual mode is Lockout not employed. No data on additional time as its dependent on the equipment.

RFI Question 29) No Response

RFI Question 30) No Response

RFI Question 31) No Response

RFI Question 32) No Response

RFI Question 33) *In addition, are there any reasons that the benefits of reducing exposure to hazardous energy might be different in small firms than in larger firms? Are there any reasons why the costs for controlling hazardous energy would be higher for small employers than they would be for larger employers? Are there provisions that would be especially costly to small employers? Please describe any specific concerns related to potential impacts on small entities that you believe warrant special attention from OSHA. Please describe alternatives that might serve to minimize those impacts while meeting the requirements of the Occupational Safety and Health Act of 1970, 29 U.S.C. 651 et seq.?*

There's no obvious reason that economy of scale wouldn't pertain to a change in hazardous energy risk management practices. However, any increase in cost to a smaller entity could be avoided if OSHA were to modify the regulations in a manner that added means of compliance, rather than replaced the current means. That would enable each business to decide whether to change its practices.