Chapter 1: General Policy and Responsibilities

Hazard Control Selection and Management Requirements

Product ID: 671 | Revision ID: 2453 | Date published: 26 October 2022 | Date effective: 26 October 2022
URL: https://www-group.slac.stanford.edu/esh/eshmanual/references/eshReqControls.pdf

1 Purpose

This document defines how a risk-based approach is used to determine the need for controls on facilities, systems, or components to protect the public, workers, and the environment. For controls necessary to prevent or mitigate serious events, specific devices and procedures will be formally credited as part of the approved *safety envelope*. How these controls are selected, evaluated, and approved, and the process for maintaining and modifying controls, are described in these requirements[1].

As used here, *controls* and *hazard controls* mean those engineered, administrative, or personal protective elements that are used to protect against a hazard. Normal process or operational controls are not included in these requirements except to the extent that their use is directly tied to safety.

The concept of *credited control* is well established in the accelerator safety community. The concept of credited control is borrowed from DOE Order 420.2C, "Safety of Accelerator Facilities" (DOE O 420.2C), but this document neither extends the requirements of DOE O 420.2C to non-accelerator hazards nor modifies those requirements for accelerator hazards. The intent is to extend those robust principles to management of controls for non-accelerator hazards of similar risk.

2 Roles and Responsibilities

2.1 Associate Laboratory Director

- Ensures that technical systems under his or her directorate's management are properly analyzed to determine the type and level of controls necessary to control risk to an acceptable level
- Maintains an inventory of credited control systems managed by his or her directorate, and owners responsible for these systems

2.2 ESH Program Manager

- Ensures that hazard controls prescribed by specific environment, safety, and health (ESH) programs are consistently applied and risk-based in accordance with these requirements

[1] Specific technical programs have controls and control thresholds specified. This document does not supersede these specific requirements but outlines the framework for performing risk assessments, developing controls hierarchies, and managing controls.

- Reviews hazard analyses and advises line managers and responsible system owners on selection of controls to meet these requirements
- Commensurate with technical program requirements, performs hazard analyses and specifies safety credited and defense-in-depth controls
- Performs periodic assessments of installed credited control systems to ensure control system integrity
- Approves changes to credited control systems as maintaining equivalent safety as the initial configuration

2.3 Technical System Owner

- Ensures that hazards inherent in the operation of his or her technical system have been properly analyzed, and that risk-based controls have been specified in accordance with these requirements to mitigate those hazards
- Ensures the integrity of hazard control systems supporting his or her technical system
- Approves credited control systems and their management plans and interface control documents for her technical systems
- Designates, as appropriate, hazard control system owners to assist in discharging this responsibility

2.4 Hazard Control System Owner

- Manages the hazard control systems under his or her authority in accordance with these requirements
- Develops and ensures conformance with, as appropriate, the credited controls management plan for each credited control system for which he is responsible
- Develops interface control documents for the hazard control systems under his or her authority and concurs with those for systems on all sides of that interface
- Ensures that comments received during credited control systems reviews are addressed and resolved before putting the credited control system into service
- Maintains records of design, approval, acceptance, testing and verification for credited control systems

3 Requirements

3.1 Risk-based Selection of Hazard Controls

Controls must be specified using a risk-based approach in which ongoing operations and credible upsets are listed, the probability and consequences are predicted, and a resulting risk is found. Controls are used to mitigate risks. Risks may be personal (for example, injury or illness), environmental (for example, spill, contamination, release to the environment), regulatory (for example, exceedance of a published standard), programmatic (for example, interruption of a user program), financial, reputational, or a number of other potential negative consequences.

This document does not mandate a specific hazard analysis process, but rather specifies hazard analysis as the basis of selection of controls. Appendix A gives an example risk matrix; the specifics may vary according to the specific situation, but the important point is that the process must be defined, systematic, and documented[2].

When a review process identifies unacceptable risks, the hazards causing those risks must be eliminated or substituted to the extent feasible. If elimination and substitution are not sufficient to reduce the risk to an acceptable level, additional controls must be applied. The diagram below illustrates this hierarchy.

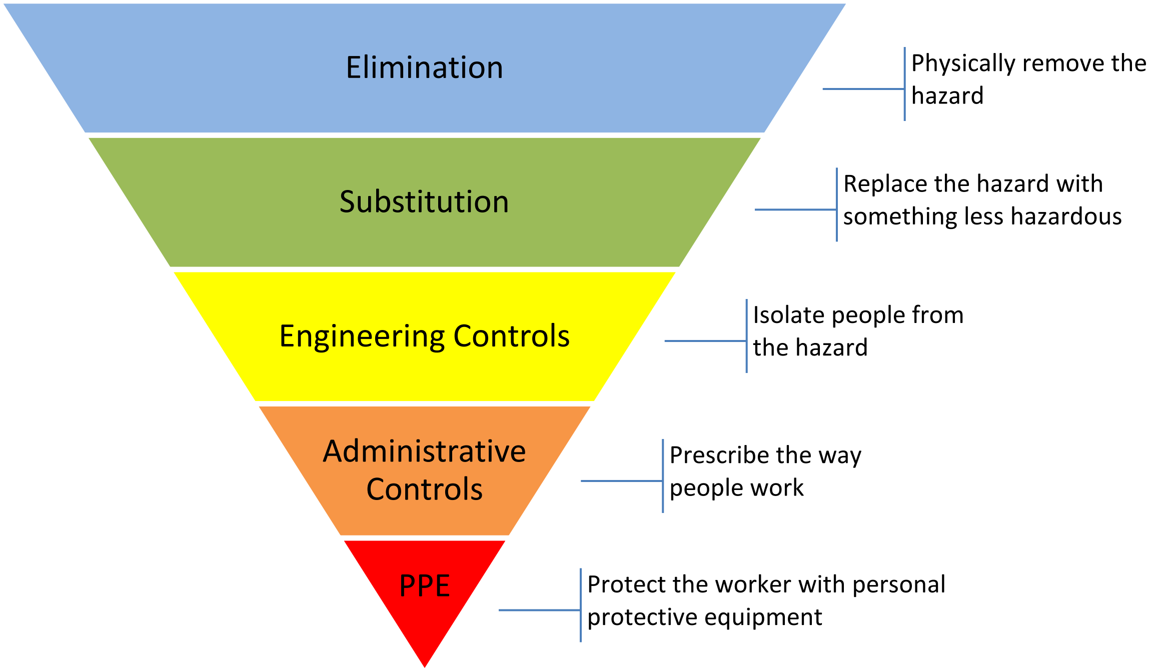
Elimination
Physically remove the hazard
Substitution
Replace the hazard with something less hazardous
Engineering Controls
Isolate people from the hazard
Administrative Controls
Prescribe the way people work
PPE
Protect the worker with personal protective equipment

Figure 1 Hazard Control Hierarchy

The selection of engineering, administrative, and personal protective controls depends upon the risk to workers, the public or the environment from the unmitigated hazard (that is, from failure of the controls). Controls must be assigned to reduce risk to an acceptable level at a minimum, with the desired point to drive the risk to a level that is *as low as reasonably practicable (ALARP)*[3]. In general, unacceptable risks (for example, high and medium as outlined in Appendix A) require the use of credited controls to reduce risks to an acceptable level, while acceptable risks (for example, low and extremely low) use defense-in-depth controls per the ALARP principle.

[2] Controls for some hazards are specified in the applicable institutional program requirements for managing that hazard. Use of the risk-based approach outlined may not result in selection of controls that are less rigorous than those prescribed by other requirements in the ESH Manual.

[3] *As low as reasonably practicable (ALARP)* is a general concept that is analogous to the term *as low as reasonably achievable (ALARA)* (widely used in radiation protection). It is a concept of driving safety beyond minimal protection. Although ALARA is not strictly used in reference to upset conditions, ALARP is applied to credible upset conditions and should serve as the management goal.

Categorization of risk (for example, as high, medium, low, or extremely low) is made through a hazard analysis process (for example, Appendix A).

- High risks generally require at a minimum multiple, independent, credited control systems ("defense in depth") to protect workers or the public from the risk.
- Medium risks should be mitigated using at least one credited (engineering and/or administrative) control system, supplemented by defense-in-depth controls, basic safety management programs and inherent robust design.
- Low risks may be further reduced using a combination of engineering, administrative, and personal protective defense-in-depth controls.
- If the unmitigated risk is extremely low then no additional controls are required but may be applied as best practice.

Selected credited and defense-in-depth controls must be approved by the line manager and, commensurate with technical program requirements and Chapter 1, "General Policy and Responsibilities", Section 2, the appropriate ESH safety officer.

Refer to other chapters in this ESH Manual and the SLAC Conduct of Engineering Policy or consult directorate safety coordinators or subject matter experts for additional guidance.

3.1.1 Selection of Defense-in-depth Controls

Defense-in-depth engineered, administrative, and personal protective equipment controls must be selected based upon the specific hazards being protected against.

1. Engineered controls are preferred and must be implemented unless infeasible.
2. Administrative controls are the next most preferable level of control.
3. Personal protective equipment controls may only be used to supplement engineering and administrative controls or used temporarily during the period when engineering and/or administrative controls are being implemented.

3.1.2 Selection of Credited Controls

Once the need for a level of credited control is determined, it necessitates following a disciplined process to select the set of equipment items (*credited engineered controls*), administrative controls (*credited administrative controls*) and/or personal protective equipment (*credited PPE controls*) needed to accomplish the required safety function. The selection of credited controls often involves choices between multiple items that could function to control a particular hazard.

When selecting credited engineered controls, it is necessary to identify any dependencies for each system being considered. For example, if a given system is a credited engineered control but it depends on another system to enable it to function as required, then at least some aspect of that other system becomes a part of the credited engineered control. Structures, systems, and components that directly support the function of credited engineered controls (or credited administrative controls) need to be identified and their safety functions defined in the hazard analysis.

The selection criteria listed below must be followed to the greatest extent practical when designating credited controls. There will be situations where some of the criteria may not be appropriate for a given situation. Engineering judgment must be applied in these cases to determine the best items for selection.

1. Engineered controls are preferred and must be implemented unless infeasible.
2. Administrative controls are the next most preferable level of control.
3. Personal protective equipment controls may only be used to supplement engineering and administrative controls or used temporarily during the period when engineering and/or administrative controls are being implemented.
4. When either an active or passive device can be credited to ensure the safety function, the passive device should be selected. *This selection is based on the inherently higher reliability of passive devices.*
5. When a choice exists between controls that would prevent an event and controls that could mitigate the consequences of the event, the preventive controls should be selected. *This selection is based on the inherent value of preventing accidents as opposed to mitigating their effects.*
6. Only those items essential to mitigate risk to an acceptable level should be selected as credited controls. The number of credited controls should, in general, be minimized and include only a limited subset of the total number of controls employed for overall facility operation. *This guidance allows a high degree of operational attention (for example, monitoring, surveillance, maintenance, control of documentation) to be devoted to the credited controls.* To support this selection criterion, credited controls that protect against multiple events or receptors are preferred.
7. Where two levels of control are selected, the controls should be independent such that the failure of one level of control does not cause failure of the other. *This "defense in depth" criterion ensures that multiple levels of control are not compromised by a single point failure.*

3.2 Management of Controls

Credited and defense-in-depth engineering, administrative, and personal protective equipment controls must be managed per best practice (for example, manufacturer recommendations) and requirements given elsewhere in this manual. The technical system owner is responsible for the integrity of hazard controls necessary to safely operate the system.

3.2.1 Management of Defense-in-depth Controls

At a minimum, defense-in-depth controls should be managed to include the following elements:

1. **Competence.** Individuals who analyze, specify, design, operate, and maintain defense-in-depth controls must be competent in the tasks they perform.
2. **Configuration management.** Changes to defense-in-depth controls may only be made after assurance that the level of safety required is maintained by the change.

   Whenever a defense-in-depth control system interacts (for example, signals, dependencies) with a credited control system, or interacts with any system such that the interaction crosses system boundaries or technical system ownership, that interaction must be documented[4]. The documentation

[4] This document is the *interface control document* when the interface is with a credited control system, see Section 3.2.2.

must specify the information that each system is receiving from the other, what the expected actions of each system in relation to that information are, and who is responsible for maintaining each side of that interface. The documentation is approved by the owner of the technical system having the hazards being controlled and contains concurring signatures of the hazard control system owners of the systems on all sides of that interface. That interface becomes a configuration-controlled element.

3. **Verification.** Defense-in-depth controls must be periodically evaluated to ensure that they continue to be effective. This evaluation may be through inspection, measurement, or other means.
4. **Recordkeeping.** When required, records of design, approval, acceptance, testing, and verification of defense-in-depth controls must be maintained in a retrievable fashion. Who maintains these records is generally specified in the institutional program managing the specific hazard for which the defense-in-depth control is used.

3.2.2 Management of Credited Controls

The technical system owner must ensure that the credited control system, whether engineering, administrative, personal protective equipment, or a combination, is managed to include the following elements[5]. To accomplish this, a credited control system management plan specifying procedures for fulfilling these elements should be established.

1. **Competence.** Individuals who analyze, specify, design, operate, and maintain credited control systems must be competent in the tasks they perform.
2. **Specificity.** The elements that collectively make up the credited control system must be specified.
3. **Monitoring.** When credited controls provide feedback (for example, alarm status) indicating that the specified protection is being provided, the status of that feedback must be monitored to detect out-of-tolerance conditions and to direct appropriate responses.
4. **Fail-safe.** Credited controls must be configured, when practical, so that in the event of component failure due to internal or external events (including loss of power), the action is to maintain the protective nature of the control. Some credited controls may not be configured to be fail-safe. In these cases there must be sufficient redundancy of protection ("defense in depth") that a single failure will not lead to unacceptable risk.
5. **Responsibility.** Each credited control system must have a specified responsible owner who has the authority and responsibility for assuring that the system is managed per these requirements.
6. **Configuration management.** Before being placed into service, each new credited control system must be reviewed independently from the line organization responsible for it. All review comments must be addressed and resolved[6]. Once all comments have been resolved, the credited control system must be formally accepted by the hazard control system owner, and this acceptance concurred with by line management. For some credited control systems, approval by the appropriate ESH safety officer is also required (see Chapter 1, "General Policy and Responsibilities", Section 2).

[5] These requirements are specified here at the highest level. The intent of these requirements is to ensure that controls are managed equivalently, not identically. The credited controls specified for different hazards may have different specific ways of addressing these fundamental requirements. Thresholds applicable to different hazards are specified in the institutional program for managing those hazards, and the credited control system management plan is reviewed and approved according to the processes outlined in that institutional program.

[6] The control system responsible owner ensures that the comments have been resolved satisfactorily.

Changes to a credited control system may only be made after a thorough review process to ensure that the level of safety required is maintained by the change. Changes may only be made after approval by the responsible owner or designee. There may be separate configuration management processes for permanent changes and for temporary changes. Compensatory actions that ensure maintenance of safety must be specified and concurred with by line management and appropriate ESH program manager.

Whenever a credited control system interacts (for example, signals, dependencies) with another credited or defense-in-depth control system, an *interface control document (ICD)* must be prepared detailing that interaction. The ICD specifies the information that each system is receiving from the other, what the expected actions of each system in relation to that information are, and who is responsible for maintaining all sides of that interface. The ICD is approved by the owner of the technical system having the hazards being controlled and contains concurring signatures of the hazard control system owners of the systems on all sides of that interface. That interface becomes a configuration-controlled element.

7. **Testing and Verification.** Credited control systems must be initially, and periodically thereafter, tested and verified to be operating properly. Testing intervals are specified in the credited controls system management plan. Procedures for the initial and periodic test and verification procedures must be specified and managed through a formal change control process.
8. **Recordkeeping.** Records of design, approval, acceptance, testing and verification must be maintained in a retrievable fashion. The hazard control system owner ensures that these records are maintained.

4 Training

Minimum training requirements are as dictated by the hazard that the control system addresses. Additional training may be specified by the credited control system management plan.

5 Definitions

competent. Possessing qualifications (for example, education, training, certification/licensing) and demonstrated ability to successfully perform the assigned task

control system. A collection of controls that together provide the specified protection from a given hazard. Control systems may be *defense-in-depth* or *credited*.

- *credited control.* An *engineered*, *administrative,* or *personal protective equipment control* that has been formally designated through hazard analysis to be essential for providing protection of the public, workers, or the environment from unacceptable risk. Failure of a credited control may result in death, major (unrecoverable) injury, illness, or impact to the environment, or may have off-site consequences. Generally speaking, credited controls are the primary protection between the hazard and the unacceptable risk.
- *defense-in-depth control.* An *engineered*, *administrative*, or *personal protective equipment* control that has been designated for providing protection of the public, workers, or the environment that is not a *credited control*. These controls provide protection beyond that afforded by credited controls alone to mitigate hazards that are categorized as posing a lower level of risk compared to those hazards that require mitigation by credited controls. Such controls provide extra layers of protection that ensure the effectiveness of the overall hazard mitigation. Failure of a defense-in-depth control may result in minor

(recoverable) injury, illness, or impact to the environment, and is unlikely to have off-site consequences

- *engineered control.* Hardware or structural items (for example, structures, systems, and/or components) that are required to ensure a required safety function is accomplished. They are characterized by not requiring cooperation from the workers to be effective. Common engineering controls include protective ventilation systems, shielding, interlocks, gas detection systems, and secondary containment.
- *administrative control.* A procedure or other requirement that specifies certain human action(s) take place that ensure the safe operation of the facility for workers and the public. They include training, procedures, maintenance activities, work scheduling, and work rules. Workers must properly execute administrative controls for them to be effective.
- *personal protective equipment control.* Personal protective equipment such as gloves, hearing protectors, protective clothing, and respirators. These do not remove the hazard, but rather separate the worker from it. Effectiveness of personal protective equipment relies wholly on the workers' proper use of it.

hazard analysis. A rigorous process of analyzing the probability and consequences from a condition or event and determining the potential impact. There are several formalized and well documented hazard analysis processes. This standard does not mandate a specific hazard analysis process, but rather specifies hazard analysis as the basis of selection of controls.

risk. The combination of the probability of an event and the consequence from that event that determines the potential impact of the event. Risk is determined from analysis of the probability and consequence using some rigorous and defined hazard analysis process.

- *high risk.* The combination of event probability and unmitigated consequences warrants special design and operational consideration.
- *medium risk.* A level of control is expected or addressed with the inherent robustness of the design. The unmitigated impact is credibly above acceptable limits for normal operation.
- *low risk.* Regulatory limits are met, but risks could be reasonably reduced further.
- *extremely low risk.* Probability and/or consequence are such that the impact is acceptable without further controls.

safety envelope. The set of engineered and administrative bounding conditions within which a system or process may be safely operated with acceptable risk. The safety envelope is comprised of control systems (defense-in-depth and credited) and operating parameters. The safety envelope is generally established through a hazard analysis process. For accelerators, the term *accelerator safety envelope* has a specific meaning and specific requirements imposed by DOE O 420.2C. The accelerator safety envelope is a special case of safety envelope.

6 Forms

The following forms and systems are required by these requirements:

- None

7 Recordkeeping

The following recordkeeping requirements apply for these requirements:

- Associate laboratory directors ensure an inventory of credited control systems managed by their directorates, and owners responsible for these systems, is maintained
- Technical system owners are responsible for credited control systems and their management plans and interface control documents
- Hazard control system owners maintain records of design, approval, acceptance, testing and verification for credited control systems; for defense-in-depth controls who maintains these records is generally specified in the institutional program managing the specific hazard for which the defense-in-depth control is used

8 References

SLAC Environment, Safety, and Health Manual (SLAC-I-720-0A29Z-001)

- Chapter 1, "General Policy and Responsibilities"
  - General Policy and Responsibilities: ESH Project Review Procedure (SLAC-I-720-0A24C-001)

Other SLAC Documents

- SLAC Conduct of Engineering Policy (ENG-2018-018)
- Conduct of Accelerator Facility Operations (CACM-2019-059)

Other Documents

- Site Compliance Plan for Department of Energy Order 420.2C, "Safety of Accelerator Facilities" (DOE O 420.2C SCP)

Appendix A: Example Risk Analysis

Table 1 Hazard Probability of Occurrence Levels

Category	Description
High	Event is likely to occur several times in a year
Medium	Event is likely to occur annually
Low	Event is likely to occur during the life of the facility or operation
Extremely low	Occurrence is unlikely or the event is not expected to occur during the life of the facility or operation
Incredible	Probability of occurrence is so small that a reasonable scenario is inconceivable. These events are not analyzed further.

Table 2 Hazard Consequence Rating Levels

Consequence Level	Maximum Consequence*
High	Serious impact on-site or off-site. May cause deaths or loss of the facility/operation. Major impact on the environment. Significant regulatory or contractual violation.
Medium	Major impact on-site or off-site. May cause severe injuries or severe occupational illness to personnel or major damage to a facility or moderate impact on the environment. Capable of returning to operation. May result in regulatory or contractual violation.
Low	Minor on-site with negligible off-site impact. May cause minor injury or minor occupational illness or minor impact on the environment. De minimis regulatory or contractual violation.
Extremely low	Will not result in a significant injury or occupation illness or provide a significant impact on the environment

*The consequences listed are examples. Depending upon the hazard analyzed there may be other consequences (for example, financial or reputational) that should also be considered.

Table 3 Risk Matrix

Probability Consequence	Extremely Low	Low	Medium	High
High	🟦	🟨	🟥	🟥
Medium	🟩	🟦	🟨	🟥
Low	🟩	🟩	🟦	🟨
Extremely low	🟩	🟩	🟩	🟦

Risk Level		
🟥	High	Unacceptable
🟨	Medium	Unacceptable
🟦	Low	Acceptable
🟩	Extremely low	Acceptable