Prevention through Design Assessment Process

MSS Prevention through Design Panel

November 2019

Overview

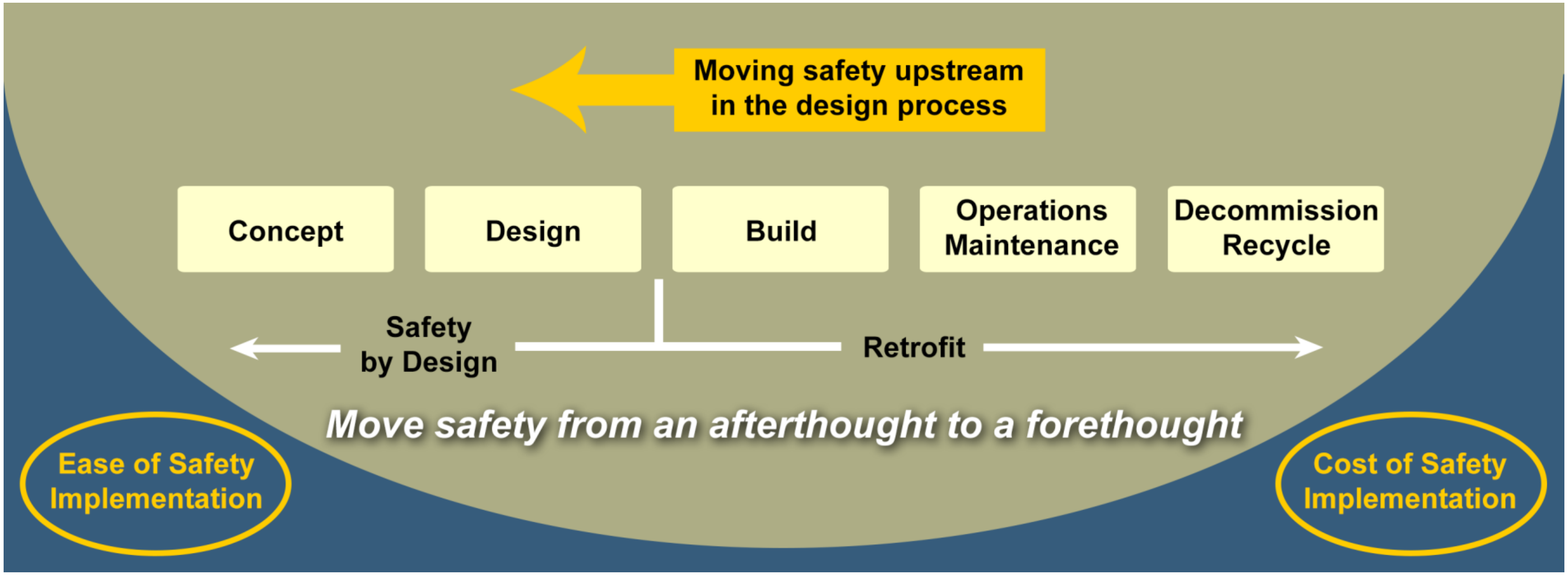
- Prevention through Design Concept
  - Benefits & Motivation
  - Background on Development
  - Relationship to Engineering Manual Risk Assessment (ERA)
- Prevention through Design (PtD) Assessment Tool
  - Hazard Identification
  - Risk Assessment and Mitigation
  - Residual Risk and Status

Prevention through Design Concept

- This concept emphasizes **eliminating hazards** and **controlling risks** to workers "at the source" or as early as possible in the life cycle of equipment, products, or workplaces
  - The process is also referred to as Safety by Design in industry
  - The more general term Prevention through Design was chosen for Fermilab since the same assessment process can also be used for non-safety risks (e.g. engineering, quality, cost, & schedule risks)

Prevention through Design Model

Same model holds true for non-safety risks as well

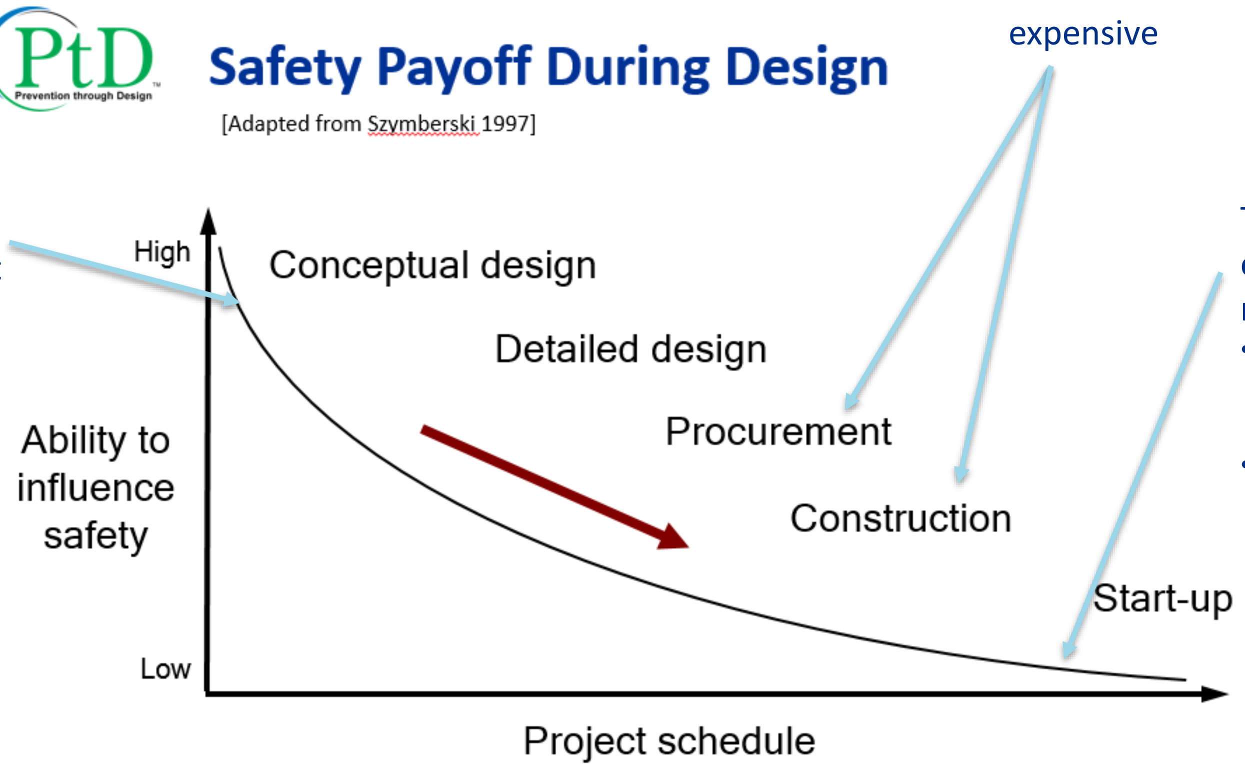


Safety by Design Model adapted from “Safety Through Design”, Wayne Christensen, NSC Press, 1999.

Prevention through Design Model

Adding or modifying design features after procurement placed or construction starts is often very expensive

Design phase is when an engineer or technical reviewer can most effectively influence a design or fabrication plan

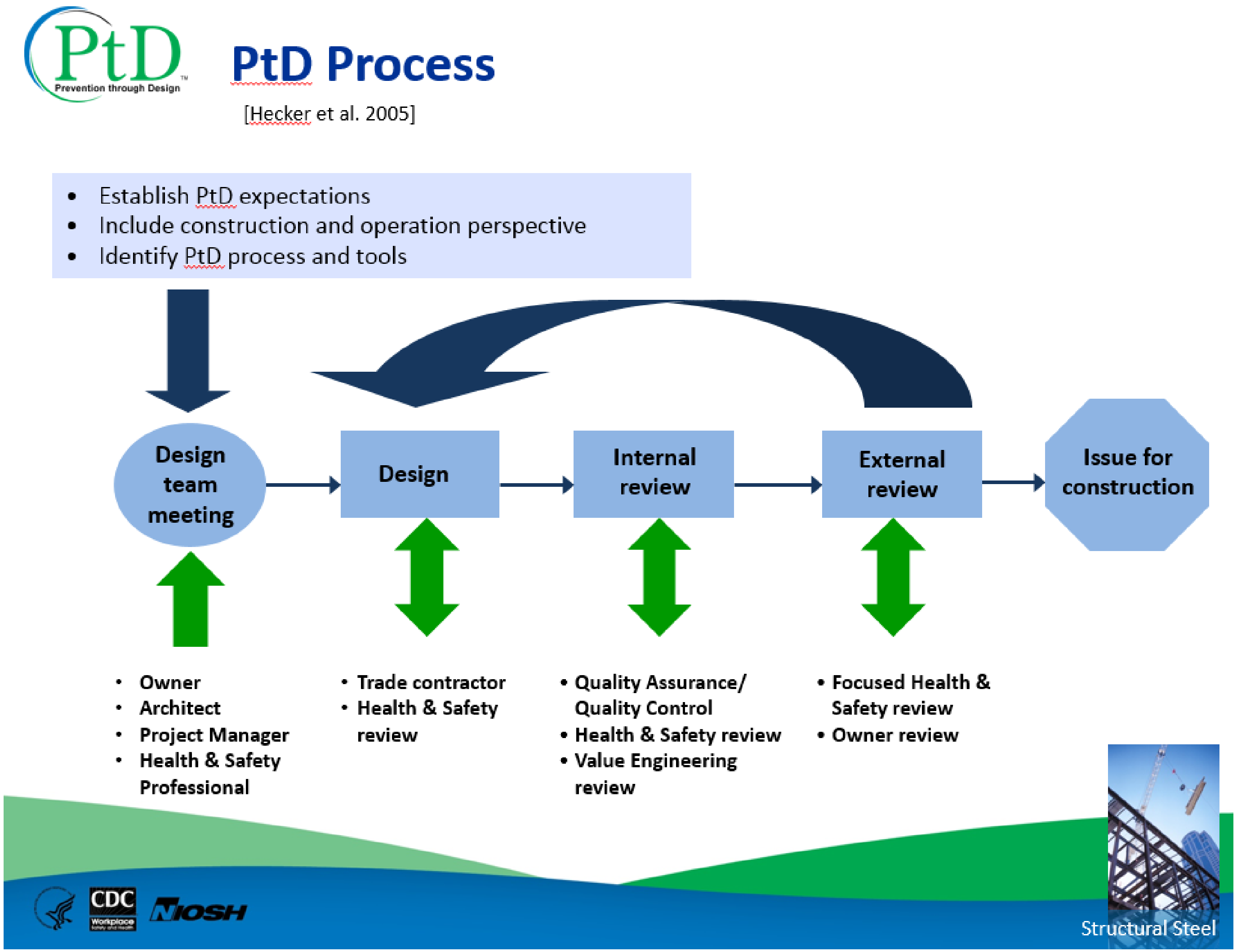


Typical point at which engineering note gets reviewed at Fermilab.

- Not a lot a safety reviewer can do besides approve or reject
- Might be overwhelming volume of documentation to review at once under time pressure

https://www.cdc.gov/niosh/docs/2013-136/

Prevention through Design Model



https://www.cdc.gov/niosh/docs/2013-136/

Benefits to Prevention though Design

- As engineers we want:
  - Reduced hazards ⟶ fewer injuries or incidents
  - Increased productivity ⟶ less rework required
  - Fewer delays due to accidents or unwanted outcomes

- PtD Assessment Tool can assist with these outcomes and
  - Improved communication between engineers
  - Improved specifications and interface documents
  - Improved communication of risks with management

Benefits to Prevention though Design

- PtD assessment tool provides a simple method to track identified risks and the status of risk mitigation plans
  - Similar in function to a project risk register, but on the individual engineer level
  - Project managers can easily search through PtD assessments for key risks to include in a project level risk register

- Technical & Safety Reviews
  - Almost every technical review has a charge question related to identifying risks & the status of their mitigation
    - Frequently a difficult charge question to answer, since risks and mitigations are scattered all over the documentation supplied at the review
  - PtD assessment is a convenient way to present identified risks and mitigation plans to reviewers
    - PtD assessment can be easily updated based on feedback from a review so that comments and recommendations are not forgotten

Benefits to Prevention though Design

- Transferring Responsibility
  - An up-to-date PtD assessment is a quick and robust method of transferring knowledge of risks and mitigations when a task is transferred from one engineer to another

- Conducive to Graded Approach
  - Left to judgement of engineer and management as to level of detail to apply
  - Small simple projects may only have a few risks. Large complex projects may have many. The assessment tool readily scales to the project

- Reducing paperwork
  - Making a design change late in the engineering process will often require a number of documents to get updated. Locating all of the spots where documents need updating can be quite tedious and time consuming.
  - The goal of Prevention through Design is to minimize the probability that changes will need to be made late in the engineering process (or even later!)

Background on Development

- MSS has been looking at ways to move elements of safety reviews earlier in the engineering process to increase efficiency & effectiveness

- Independently, PIP-II developed a Safety by Design assessment tool to identify, track, and mitigate safety risks
  - Effort led by John Anderson

- MSS refocused one of it's subject panels on Prevention through Design
  - Generalizing the PIP-II Safety by Design program for labwide use was selected as a key objective for the panel

- A self-assessment was performed on PIP-II Safety by Design program
  - Using self-assessment feedback, the generalized PtD Assessment tool was created

- Now collecting additional engineering community feedback prior to official roll-out
  - Goal is to meet with all engineering departments to introduce PtD assessment concept & collect feedback

- The plan is to include this PtD assessment tool as a link on the Engineering Manual Resource page
  - New Engineering Manual Resource page currently under development

Relationship to Engineering Manual Risk Assessment

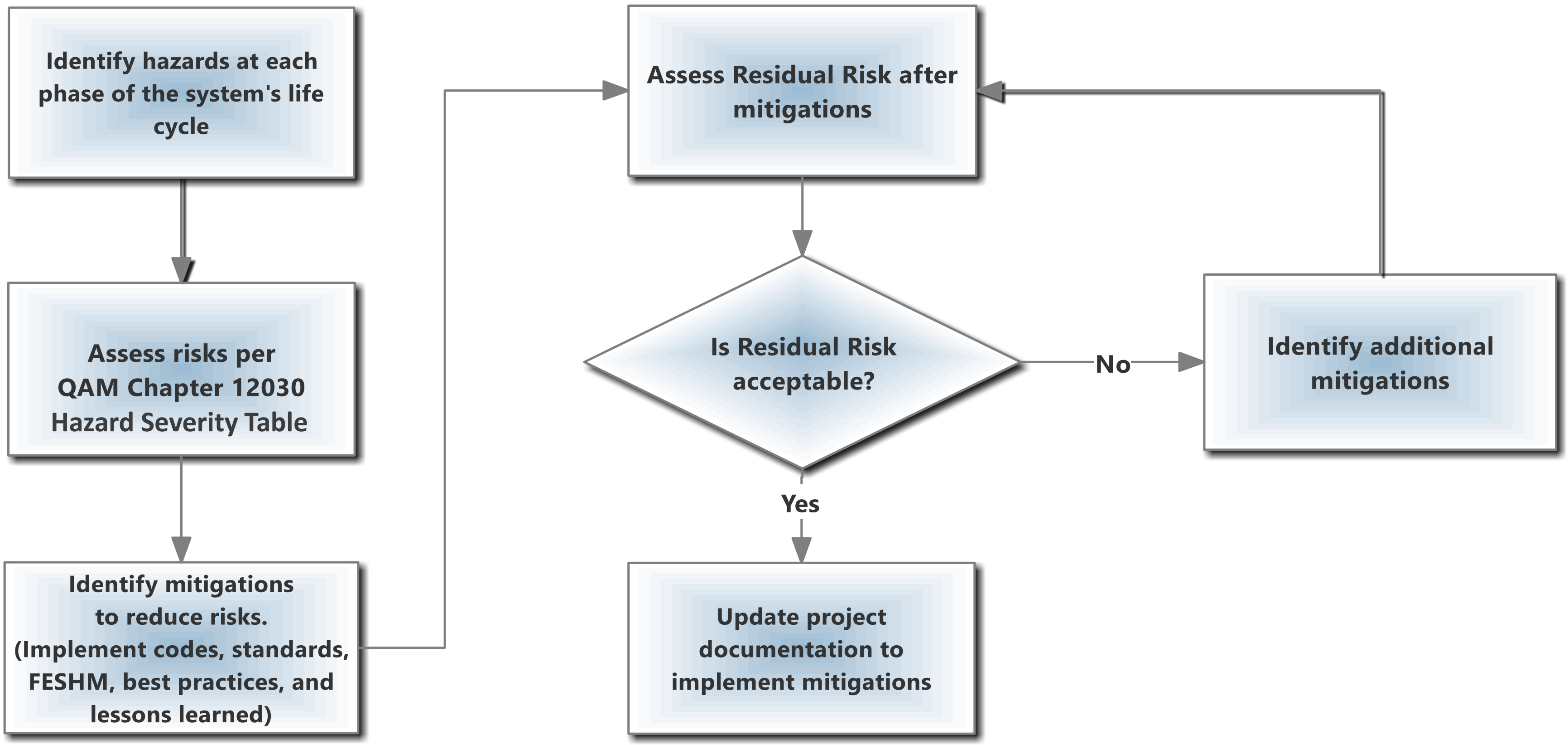
- Step 1: Engineering Manual Risk Assessment (ERA)
  - “This process helps the lead engineer and department head **evaluate project risks and determine the appropriate level of documentation and review a project needs**”
  - Typically performed only once at start of project
  - Does not track specific risks or their mitigations (other than general level of review)
- Step 2: Prevention through Design (PtD) Assessment
  - **A standardized method for engineers to assess, track, and mitigate the specific risks associated with their assigned tasks.**
  - Typically updated at every review called out by Engineering Manual and other technical reviews determined by the engineer's department and/or project

Prevention through Design Assessment Tool Example

	Hazard Identification				Risk			Mitigations	Residual Risk			Status		
Identifier	*Potential Hazard Description*	*Life Cycle Stage*	*Who is at risk?*	*What is at risk?*	*Pre-Mitigation Severity*	*Pre-Mitigation Probability*	*Pre-Mitigation Risk Score*	*Mitigations*	*Post-Mitigation Severity*	*Post-Mitigation Probability*	*Post-Mitigation Risk Score*	*Mitigation Action*	*Status of Implementation*	*Comments*
	Overexposure to radiation from machine operations	Operations	Personnel on access in beamline enclosure		Critical	A - Almost Certain	1 - Critical	Global requirement to supply a radiation safety interlock system. Technical specification for system to be compliant with FRCM Chapter 10.	Critical	E - Rare	3 - Moderate	Integrate into Design	In Process	
	Injury or fatality due to catastrophic failure of a cryomodule	Operations	Personnel on access in beamline enclosure		Critical	C - Possible	1 - Critical	General Functional Requirement to abide by all FESHM and FRCM requirements. Specific pressure and cryogenic safety chapters from the FESHM are referenced in the FRS.	Critical	E - Rare	3 - Moderate	Integrate into QA Plan	Implemented	
	Insufficient space for radiological frisking equipment limits emergency egress path	Operations	Personnel on Access		High	C - Possible	2 - Serious	Conventional Facilities Technical Specification updated to define necessary space for enclosure frisking equipment	High	E - Rare	4 - Minor	Update Specifications and Interfaces	In Process	
	Strain injury during LCW pump installation / replacement	Multiple	Contractors and Maintenance personnel		High	B - Likely	1 - Critical	Conventional Facilities Technical Specification to design in an A-Frame lifting fixture rated for 1 ton to facilitate pump installation / removal	Low	D - Unlikely	4 - Minor	Integrate into Design	Implemented	
	Environmental impact from antifreeze in cooling water system	Disposal or Recycling		Cooling ponds and waters of the state	Low	C - Possible	3 - Moderate	Technical Specification to use propylene glycol for an antifreeze in cooling water system	Minimal	C - Possible	4 - Minor	No Action Required	Not Implemented	Determined antifreeze in cooling water is unnecessary

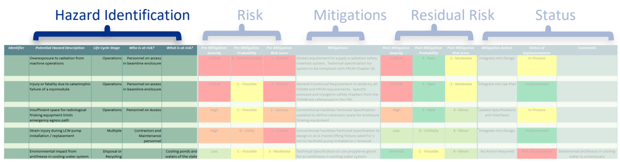
- Spreadsheet intended as an organization and tracking tool
- Living document through-out the design process

PtD Assessment Process Flowchart



Details covered on following slides

Hazard Identification Examples



Details Filled in by Engineer

Potential Hazard Description	*Life Cycle Stage*	*Who is at risk?*	*What is at risk?*
Overexposure to radiation from machine operations	Operations	Personnel on access in beamline enclosure	
Injury or fatality due to catastrophic failure of a cryomodule	Operations	Personnel on access in beamline enclosure	
Insufficient space for radiological frisking equipment limits emergency egress path	Operations	Personnel on Access	
Strain injury during LCW pump installation / replacement	Multiple	Contractors and Maintenance personnel	
Environmental impact from antifreeze in cooling water system	Disposal or Recycling		Cooling ponds and waters of the state

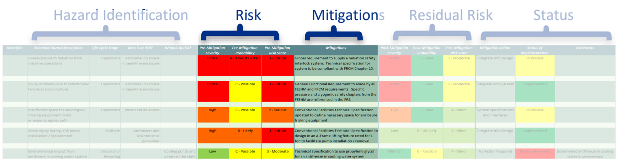
Pull down menu options next slide

Fermilab

Hazard Identification by Life Cycle Stage

- Life cycle stages (cradle to grave)
  - Fabrication
  - Inspection
  - Shipping
  - Installation
  - Testing
  - Commissioning
  - Operations
  - Equipment Shutdown (Lock Out / Tag Out)
  - Maintenance
  - Trouble-shooting
  - Repairs/Replacement
  - Decommissioning
  - Disposal or Recycling

Risk Assessment and Mitigations



Select from Pull-down Menu · Calculated · Details Filled in by Engineer

Pre-Mitigation Severity	*Pre-Mitigation Probability*	*Pre-Mitigation Risk Score*	*Mitigations*
Critical	A - Almost Certain	1 - Critical	Global requirement to supply a radiation safety interlock system. Technical specification for system to be compliant with FRCM Chapter 10.
Critical	C - Possible	1 - Critical	General Functional Requirement to abide by all FESHM and FRCM requirements. Specific pressure and cryogenic safety chapters from the FESHM are referenced in the FRS.
High	C - Possible	2 - Serious	Conventional Facilities Technical Specification updated to define necessary space for enclosure frisking equipment
High	B - Likely	1 - Critical	Conventional Facilities Technical Specification to design in an A-Frame lifting fixture rated for 1 ton to facilitate pump installation / removal
Low	C - Possible	3 - Moderate	Technical Specification to use propylene glycol for an antifreeze in cooling water system

Quantify Risks

Risk is typically Measured As Severity times Probability

- QAM 12030 Technical Appendix A has matrices to assist with identifying both severity and probability

Fermilab QAM 12030 Hazard Severity Table

HAZARD SEVERITY					
SEVERITY	**PEOPLE**	**ENVIRONMENT**	**COMPLIANCE**	**PROPERTY**	**PROCESS/PROJECT**
CRITICAL	Multiple deaths from injury or illness; multiple cases of injuries involving permanent disability; or chronic irreversible illnesses.	Permanent loss of a public resource (e.g. drinking water, air, stream, or river).	Willful disregard for the rules and regulations.	Loss of multiple facilities or program components; (>$5,000,000 total cost*)	Total breakdown identified resulting in loss/shut down of a process or project.
HIGH	One death from injury or illness; one case of injury involving permanent disability; or chronic irreversible illnesses.	Long-term loss of a public resource (e.g., drinking water, air, stream, or river).	Major noncompliance that exposes the Lab to significant potential fines and penalties.	Loss of a facility or critical program component; (>$5,000,000 total cost*)	Major breakdown identified resulting in the failure to attain the budget, schedule, key performance indicators or customer expectations.
MEDIUM	Injuries or temporary, reversible illnesses resulting in hospitalization of a variable but limited period of disability.	Seriously impair the functioning of a public resource.	Significant noncompliance that requires reporting to DOE or other authorities.	Major property damage or critical program component; ($1,000,000 - $5,000,000 total cost*)	Significant compromise to the attainment of the budget, schedule, key performance indicators or customer expectations which exposes process/project to potential failure if gap cannot be immediately resolved.
LOW	Injuries or temporary, reversible illnesses not resulting in hospitalization with lost time.	Isolated and minor, but measurable, impact(s) on some component(s) of a public resource.	Programmatic noncompliance with the Lab's Work Smart set.	Minor property damage or critical program component; ($50,000 - $1,000,000 total cost*)	Minor breakdown or gap identified which does not result in significant compromise to the attainment of the budget, schedule, key performance indicators or customer expectations; gaps can be resolved.
MINIMAL	Injuries or temporary illnesses requiring only minor supportive treatment and no lost time.	No measureable impact on component(s) of a public resource	Specific instance of a noncompliance with the Lab's Work Smart set.	Standard property damage or critical program component; (<$50,000 total cost*)	Minor gaps identified which do not compromise the attainment of the budget, schedule, key performance indicators or customer expectations; gaps can easily be resolved.

Hazard Severity

- Estimate the Hazard Severity using the table
  - Consider the worst potential consequence that is likely to occur without any mitigations, then reconsider the risk after the mitigation plan has been implemented

- Engineers need to use their judgment when selecting severity
  - Not all hazards will neatly fall into a single spot on the QAM 12030 hazard severity table
  - Consult with management when uncertain about what severity level to select
  - **Risk scoring is only a helpful guide. The key point is to ensure that all risks have been identified and mitigation plans reduce risk to acceptable levels**

Fermilab QAM 12030 Mishap Probability Table

PROBABILITY	DESCRIPTION
A - Almost Certain	Could occur annually
B - Likely	Could occur once in two years
C - Possible	Occurring not more than once in ten years
D - Unlikely	Occurring not more than once in thirty years
E - Rare	Occurring not more than once in one hundred years.

- Estimate the mishap probability
  - Use your judgement

- Spreadsheet calculates Risk Score

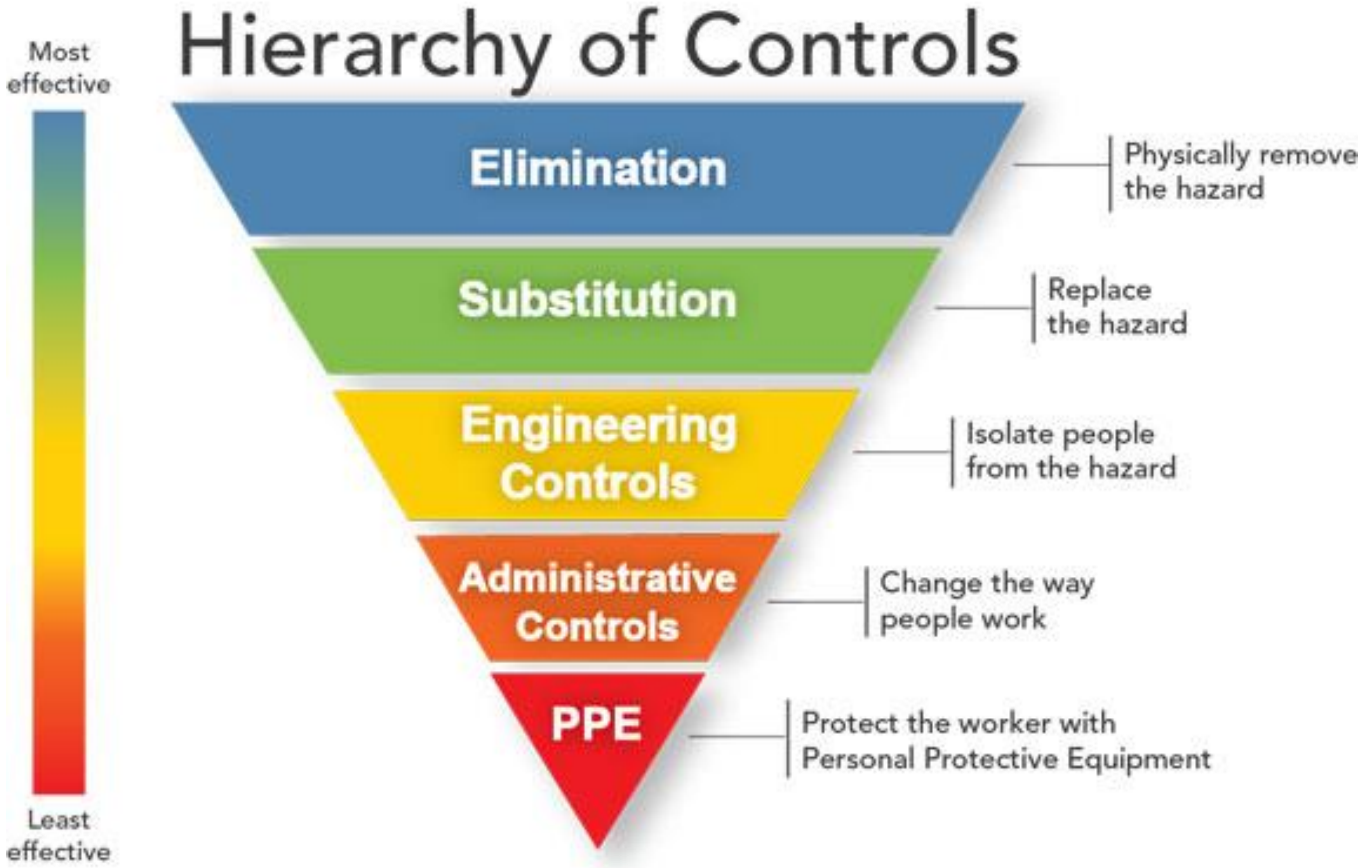
Risk Assessment Codes and Actions

Risk Code	Actions
1 - Very High	Unacceptable. Operation not permissible. Immediate action necessary.
2 - High	Mitigation action(s) to be given a high priority.
3 - Moderate	Mitigation action(s) to be taken at an appropriate time. - Can be considered an acceptable risk.
4 - Low	Mitigation action(s) discretionary.
5 - Negligible	No action necessary.

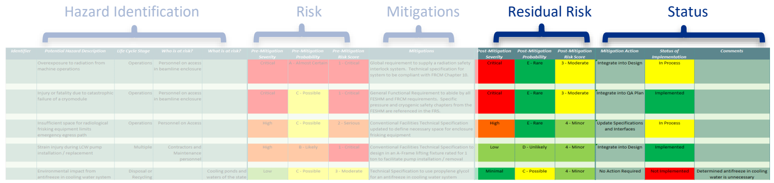
Prevention through Design is intended to drive risks lower.

Identify Mitigations

- What can be done to reduce the severity or likelihood?



Residual Risk and Status



Select from Pull-down Menu

Calculated

Select from Pull-down Menu

Details Filled in by Engineer

Post-Mitigation Severity	Post-Mitigation Probability	Post-Mitigation Risk Score	Mitigation Action	Status of Implementation	Comments
Critical	E - Rare	3 - Moderate	Integrate into Design	In Process	
Critical	E - Rare	3 - Moderate	Integrate into QA Plan	Implemented	
High	E - Rare	4 - Minor	Update Specifications and Interfaces	In Process	
Low	D - Unlikely	4 - Minor	Integrate into Design	Implemented	
Minimal	C - Possible	4 - Minor	No Action Required	Not Implemented	Determined antifreeze in cooling water is unnecessary

Mitigation Actions

- **Integrated in Specs and Interfaces:** The hazard or consequence is mitigated by including provisions in the specification or interface documents that mitigate or eliminate the hazard or consequence.
  - Typical example: Specifying that a pressure vessel is purchased with the appropriate stamp or certification mark per the pressure vessel code.
- **Incorporated into Design:** The hazard or consequence is mitigated by incorporating features into the design.
  - Typical example: Incorporating a relief valve on a pressure vessel with supporting calculations to demonstrate that the pressure vessel cannot be over pressurized.
- **Incorporated into QA Plan**: The hazard or consequence is mitigated by incorporating features into the QA plan.
  - Typical example: Ensuring that welders and their weld procedures are qualified by the applicable code and FESHM chapter.
- **Incorporated into Administrative Controls and PPE**: The hazard or consequence is mitigated by incorporating features into a safety-related procedure, which may include Personal Protective Equipment.
  - Typical example: Written LOTO procedure for maintenance on a pump or compressor. These are the least effective controls as shown on the Hierarchy of Controls inverted pyramid
- **No Action Required**: Evaluation of risk concluded with opinion that no action is required. Justification for the decision (or reference to the justification) is included in the PtD assessment spreadsheet.

Status of Implementation

- **Implemented**: Incorporated into the physical device. Incorporation into a reviewed and approved document also qualifies as implemented
- **In-process:** Incorporated into documentation. The device may not yet be fabricated. Or the associated documents may not yet be reviewed and approved
- **Not implemented:** Mitigation plan has not yet been implemented. Or the risk requires no action.

Collecting PtD Examples Labwide

- The intent is apply the PtD assessment tool across the diverse array of design activities that take place across Fermilab
  - Panel is collecting one or two examples from each engineering group to demonstrate the broad applicability of the tool

- Discussion:

	Hazard Identification				Risk			Mitigations	Residual Risk			Status		
Identifier	*Potential Hazard Description*	*Life Cycle Stage*	*Who is at risk?*	*What is at risk?*	*Pre-Mitigation Severity*	*Pre-Mitigation Probability*	*Pre-Mitigation Risk Score*	*Mitigations*	*Post-Mitigation Severity*	*Post-Mitigation Probability*	*Post-Mitigation Risk Score*	*Mitigation Action*	*Status of Implementation*	*Comments*
	Overexposure to radiation from machine operations	Operations	Personnel on access in beamline enclosure		Critical	A - Almost Certain	1 - Critical	Global requirement to supply a radiation safety interlock system. Technical specification for system to be compliant with FRCM Chapter 10.	Critical	E - Rare	3 - Moderate	Integrate into Design	In Process	
	Injury or fatality due to catastrophic failure of a cryomodule	Operations	Personnel on access in beamline enclosure		Critical	C - Possible	1 - Critical	General Functional Requirement to abide by all FESHM and FRCM requirements. Specific pressure and cryogenic safety chapters from the FESHM are referenced in the FRS.	Critical	E - Rare	3 - Moderate	Integrate into QA Plan	Implemented	
	Insufficient space for radiological frisking equipment limits emergency egress path	Operations	Personnel on Access		High	C - Possible	2 - Serious	Conventional Facilities Technical Specification updated to define necessary space for enclosure frisking equipment	High	E - Rare	4 - Minor	Update Specifications and Interfaces	In Process	
	Strain injury during LCW pump installation / replacement	Multiple	Contractors and Maintenance personnel		High	B - Likely	1 - Critical	Conventional Facilities Technical Specification to design in an A-Frame lifting fixture rated for 1 ton to facilitate pump installation / removal	Low	D - Unlikely	4 - Minor	Integrate into Design	Implemented	
	Environmental impact from antifreeze in cooling water system	Disposal or Recycling		Cooling ponds and waters of the state	Low	C - Possible	3 - Moderate	Technical Specification to use propylene glycol for an antifreeze in cooling water system	Minimal	C - Possible	4 - Minor	No Action Required	Not Implemented	Determined antifreeze in cooling water is unnecessary

Summary

- Prevention through Design Assessment Tool
  - Assists with identifying hazards and mitigations to minimize risk early in the design process
  - Documents the hazard assessment, risks and controls
  - Tracks progress on implementation of mitigations
  - High level hazards may be rolled up into the project risk registry
  - One of the deliverables presented at each technical review phase
  - Spreadsheet is intended to be a living document where hazards and mitigations can be added to or updated as necessary

Contributors

- John Anderson (PIP-II ES&H)
- Tom DiGrazia (Quality Section)
- Joe Hurd (APS-TD Cryo)
- Dave Mertz (ESS Chair, ES&H)
- Matt Slabaugh (AD/MS)
- Bill Soyars (CSS Chair, APS-TD Cryo)
- Mike White (MSS Chair, APS-TD Cryo)*

*Primary contact for feedback about PtD Assessment Tool

Backup slides

Risk Matrix (safety)