Fermilab Engineering Manual Chapter 2, Alternate Prevention through Design Process Instructions

Revision History

Revision	Date Release	Description of Change
0	Nov 2019	Initial Document Release
1		
2		

Table of Contents

1. Acronyms

dBA	Decibels A weighted
ICW	Industrial Chilled Water
LCW	Low Conductivity Water
PtD	Prevention through Design
QAM	Quality Assurance Manual
RAW	Radioactive Water
SbD	Safety by Design
WBS	Work Breakdown Structure

2. References

1	Safety Through Design: Best Practices, edited by Wayne Christensen, Fred Manuele, NSC Press, 1999
2	Fermilab Quality Assurance Manual
3	
4	
5	
6	
7	
8	
9	

3. Purpose

The purpose of Prevention through Design (PtD), also called Safety by Design (SbD), is to minimize occupational hazards early in the design process. The emphasis is on eliminating hazards and controlling risks to workers “at the source” or as early as possible in the life cycle of equipment, products, or workplaces. PtD is a shift in approach for on-the-job safety. It involves evaluating potential risks associated with processes, equipment and structures. It takes into consideration the product life cycle phases from design through disposal. It increases the cost-effectiveness of enhancements to occupational safety and health.

4. Scope

The PtD process is applicable to all engineering design tasks performed at the Lab. PtD is often a required element for various design review phases which are conducted for projects across the Lab.

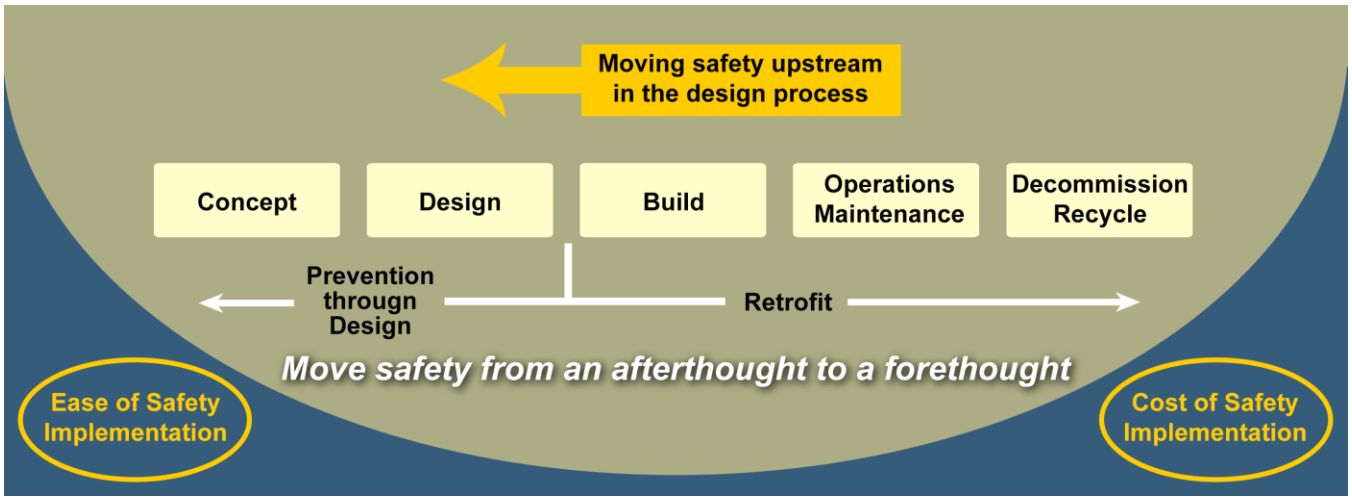
5. Overview

Prevention through Design is a process to integrate hazard identification and risk assessment early in the design process to eliminate or minimize risks throughout the life cycle of the system or structure. The process encourages engineers and designers to control risks to workers and the environment, to an acceptable level “at the source” or as early as possible in the life cycle of the equipment. The process reduces the reliance on the use of personal protective equipment which is the least effective method for protecting workers.

The benefits of controlling risks early in the design process include:

- Reduced hazards that prevent or reduce injuries or incidents
- Increase productivity
- Reduced operating costs
- Reduced retrofitting to correct design shortcomings
- Fewer delays due to accidents or unwanted outcomes
- Improved communications between engineers with interfaces between systems
- Improved specifications and interface documents

The PtD model is graphically shown below.



Prevention through Design Model adapted from "Safety Through Design", Wayne Christensen, NSC Press, 1999 [4]

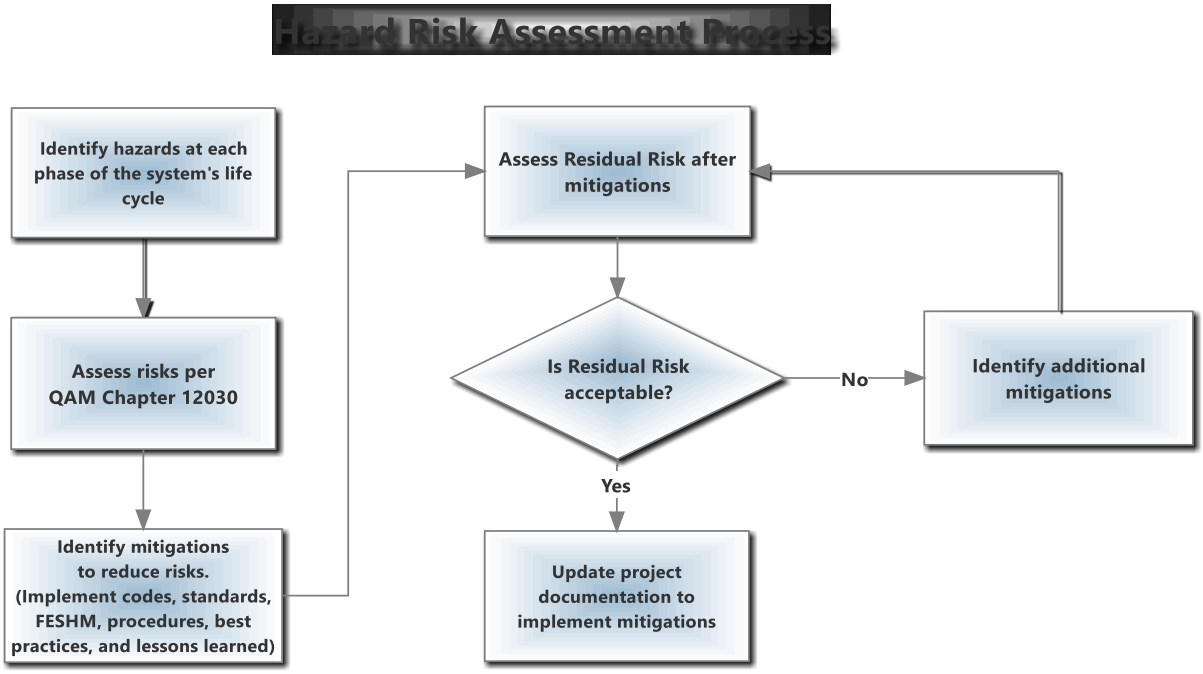
The PtD process moves safety upstream in the design process making it a forethought instead of an afterthought. This enables safety to be integrated into the design reducing costly redesign after system implementation.

6. Hazard Risk Assessment

A hazard risk assessment is the combination of identifying and analyzing potential or future events that may negatively impact individuals, property, and/or the environment and making judgements on the tolerability of the risk while considering influencing factors. The risk assessment analyzes what can go wrong, how likely it is to happen, what the potential consequences are, and how tolerable the identified risk is. As part of this process, the resulting determination of risk may be expressed either quantitatively or qualitatively. The PtD hazard risk assessment is an integral part of the overall risk management strategy.

6.1. PtD Hazard Risk Assessment Process

The PtD hazards risk assessment process flowchart is shown below. The process consists of 1) identifying hazards that may impact people, equipment, and/or the environment; 2) assessing those risks in accordance with the Fermilab Quality Assurance Manual (QAM) Chapter 12030 [2]; 3) identifying mitigations to reduce risks; 4) assessing the residual risk after mitigations; and 5) updating project documentation to implement mitigations.



6.2. Hazard Identification

The first step in the PtD hazard risk assessment is to identify both the visible and implied hazards that may threaten people, equipment, and/or the environment. A hazard is a potential condition, event, or circumstance that can lead to an unplanned or undesirable event. It may exist as a single condition or in combination with other hazards and conditions to become an actual functional failure or accident.

When identifying hazards, it is also necessary to identify who or what is at risk from the hazard and the potential consequences to them if the hazard is realized. The hazard identification process needs to consider the equipment life cycle phases. The various life cycle phases include fabrication, installation, commissioning, operations, equipment shutdown, maintenance, trouble-shooting, repairs/replacement, decommissioning, and disposal or recycling.

6.2.1. Life Cycle Phases

Equipment hazards can change depending on the equipment life cycle phase. For example, rigging hazards may only exist during the fabrication, shipping, installation, replacement and disposal life cycles; where a thermal burn hazard may only exist during the commissioning, operation, maintenance and repair life cycles. The following are example hazard categories and types of hazards that should be considered during the PtD hazard assessment for each life cycle phase. The list is not intended to be exhaustive, but rather a starting place for thought.

Hazard Categories	Hazards
Electrical	Exposed energized equipment (Isolation from electrical connections, Lock Out Tag Out) Equipment grounding Shorts / arcing / sparking Improper wiring (Overloading) Contaminants (Metal shavings, water, ice, condensation) Wet locations Unexpected startup / motion (Lock Out Tag Out) Overvoltage / overcurrent (Circuit Protection) Power interruption
Material handling	Stacking Storing Movement to or from storage Instability (Center of gravity labeled) Vehicle motion Fort lift movement (Equipment labeled with weight) Excessive weight (Equipment labeled with weight, engineered lifts) Crane movement (Special or complex rigging, lifting fixtures)
Mechanical	Crushing Cutting / severing / drawing-in / trapping / entanglement (machine guarding of moving components) Pinch point (machine guarding of moving components) Stabbing / puncture Impact Unexpected startup / motion (Lock Out Tag Out) Head bump on overhead objects Equipment instability (magnet or equipment stands)

Hazard Categories	Hazards
Slips / trips / falls	Slip (smooth / painted surfaces) Trip (piping or electrical conduits along floor) Elevated work fall hazard (ladder or lift usage, gauges and instrumentation at eye level) Equipment instability Equipment accessibility Falling material or objects (guards around openings)
Cold / Heat	Burns / scalds Radiant heat Severe heat Severe cold Cryogenics (dewars) Inadequate heating / cooling
Fluid / pressure	High pressure gasses (air, N2, He, Ar) High pressure coolants (ICW, LCW, RAW) Hydraulic fluids Vacuum (control over remotely actuated valves) Implosion / explosion
Radiation	X-Ray sources RF and microwave emissions Infrared radiation Electromagnetic sources (high magnetic fields) Radiological sources Radiological contamination
Lasers	Eye exposure Skin exposure Ignition sources (Class 4 lasers) Toxic gas (used within the laser or generated by laser operations)
Noise / vibration	Noise sound levels > 85 dBA Noise sound levels > 140 dBA (continuous, intermittent, impact) Equipment damage Interference with communications Personnel fatigue Material strength
Ergonomics	Excessive force / exertion Posture / repetition (duration of tasks) Lifting / bending / twisting
Chemical, hazardous or toxic substances	Chemical irritants Chemical exposure Chemical emissions or releases (environmental) Chemical toxicity Chemical production (hydrogen) Incompatible chemicals Chemical gasses

Hazard Categories	Hazards
Environmental / industrial hygiene	Hazardous and mixed waste Carcinogens (Be, silica, wood dust, asbestos, solvents) Asphyxiants (LN2, LHe, LAr) Irritants Poisons Solvents Toxic metals (lead, cadmium, chromium, mercury) Ozone depleting substances (SF6) Emissions Effluent / effluent handling Wastewater contamination (RAW) Corrosion Contamination
Fire / explosions	Uncontrolled ignition sources Sparks (welding) Flames (welding, soldering) Hot surfaces on equipment / components Flammable gas / liquid / vapor Improper chemical use Inadequate egress / evacuation routes Exposed electrical arcs (welding) Spontaneous combustion (pyrophoric materials)
Ingress / egress	Inadequate lighting Inadequate means of egress Material storage interference Blocked exit
Ventilation / confined space	Confined space (minimize to the extent possible) Excess ventilation Inadequate fresh air Loss of exhaust Air contaminants Recirculating air Airflow direction
Waste	Radiological waste Chemical waste Defective or replacement parts (disposal, mixed waste, hazardous waste) Material movement / transport (drum, carboy, bottle) Processing (water, chemicals, solvents)
Operational / Troubleshooting / Maintenance / Repairs	Inadequate instrumentation (ability to monitor and troubleshoot systems) Instrumentation accessibility (gauges and panels at eye level from floor) Maintenance accessibility (sufficient access to equipment and utilities)

6.3. Severity or Consequences

The next step is to assess the severity or consequence using the criteria found in the Fermilab QAM Chapter 12030 Table 1 repeated below [2]. When selecting the severity, use past experience and best engineering practices. Consider the worst potential consequence that is likely to occur because of the deficiency. The initial severity or consequence should be estimated without considering mitigations.

Fermilab QAM 12030TA Table 1

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.

6.4. Probability of Occurrence

Estimate the probability of occurrence using the criteria found in the Fermilab QAM Chapter 12030 Table 2 repeated below [2]. When selecting the probability of occurrence, use past experience and best engineering practices. The probability of occurrence should be based on an assessment of such factors as location, exposure in terms of cycles or hours of operation, and the affected population. Other circumstantial factors that should be considered include the number of workers exposed, frequency of exposure or duration of employee overexposure to contaminants, employee proximity to the hazardous conditions, use of appropriate personal protective equipment (PPE), medical surveillance program, and other pertinent working conditions. The initial probability of occurrence should be estimated without considering mitigations.

Fermilab QAM 12030TA Table 2

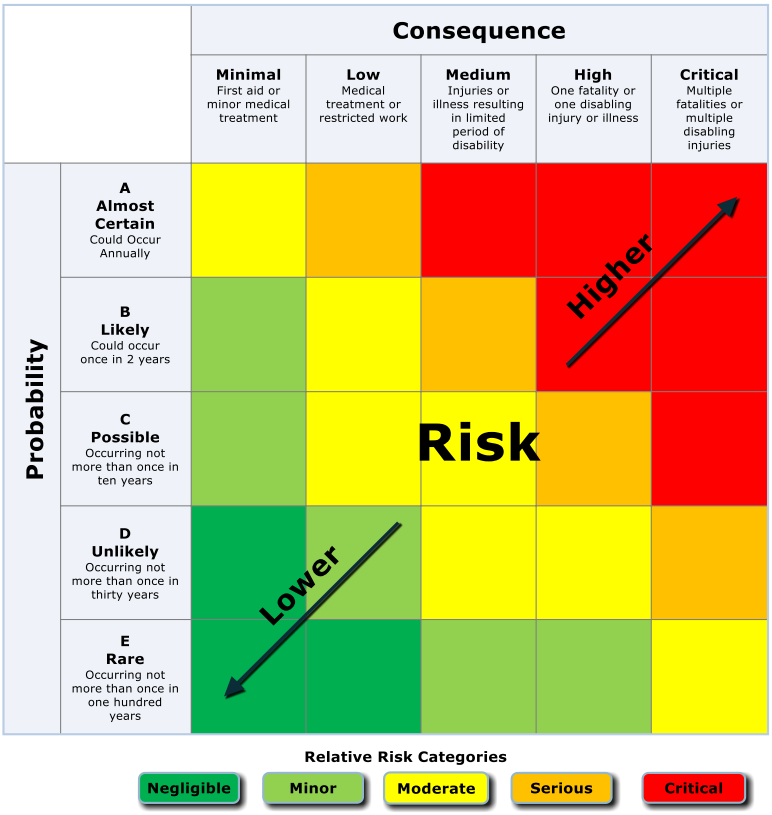
MISHAP PROBABILITY TABLE	
PROBABILITY	**DESCRIPTION**
A - Almost Certain	Could occur annually
B - Likely	Could occur once in two years
C - Possible	Occurring not more than once in ten years
D - Unlikely	Occurring not more than once in thirty years
E - Rare	Occurring not more than once in one hundred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

6.5. Risk

Risk is an estimate of the probability of a hazard-related incident or exposure occurring and the severity or consequence of harm or damage that could occur. Simply stated, risk is the product of severity and probability resulting in a Quantitative Risk Score as shown in the figure below.

The possible risk scores are best shown in a risk matrix. The risk matrix graphically shows the activities with highest and lowest risks binned by risk categories of Critical, Serious, Moderate, Minor, or Negligible. Critical and Serious risks may be rolled-up to the Risk Register by the relevant Manager for additional management-level tracking.

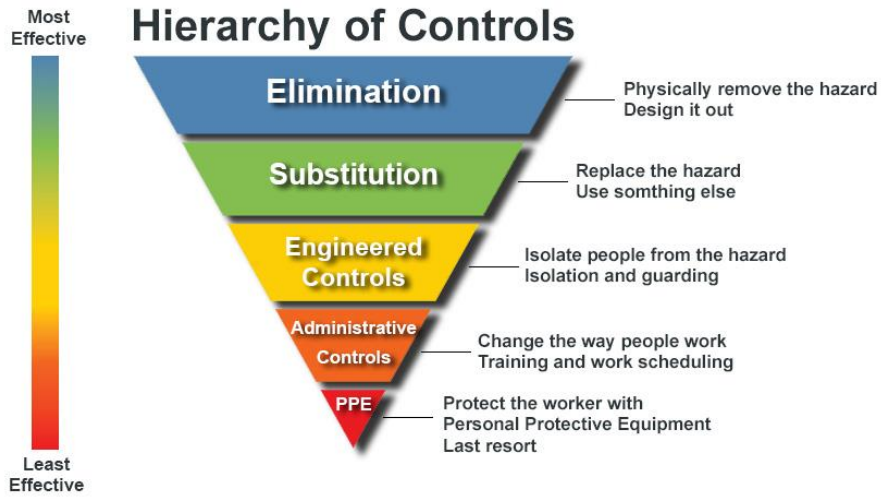
Risk Matrix



6.6. Risk Mitigation

When the initial risk assessment indicates mitigations are necessary, risk elimination, substitution, avoidance, reduction or control measures can be selected and implemented to achieve an acceptable risk level for each identified hazard. Using the risk category definitions, risk mitigation activities can be prioritized so that appropriate resource allocations can be made.

When selecting risk mitigations, the Hierarchy of Controls, as shown below, should be used as the basis for which remedial actions are made in the order of their effectiveness. When possible, eliminating a hazard should be the first choice and the use of PPE should be used as a last resort. New technologies could be explored that would enhance safety or quality. PtD is intended to reduce the reliance on and use of Administrative Controls and PPE.



6.7. Residual Risk

The residual risk is assessed after the planned remedial actions are identified to determine whether the remaining risk is acceptable. If the residual risk is still unacceptable, additional risk mitigation strategies shall be implemented until the residual risk is deemed acceptable. Risk mitigations identified should improve safety and or quality. However, it's possible for a risk mitigation to improve safety yet not change the overall post-mitigation risk score.

6.8. Risk Assessment Codes & Actions

The following table provides the recommended actions based on the risk assessment code calculated by the PtD spreadsheet:

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

6.9. 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.

Incorporated into Design: The hazard or consequence is mitigated by incorporating features into the design. A typical example would be incorporating a relief valve on a pressure vessel with supporting calculations to demonstrate that the pressure vessel cannot be overpressurized.

Incorporated into QA Plan: The hazard or consequence is mitigated by incorporate features into the QA plan. A typical example would be 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. A typical example would be a written LOTO procedure for maintenance on a pump or compressor. These are the least effective controls as described in Section 6.6.

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.

6.10. Status of Implementation

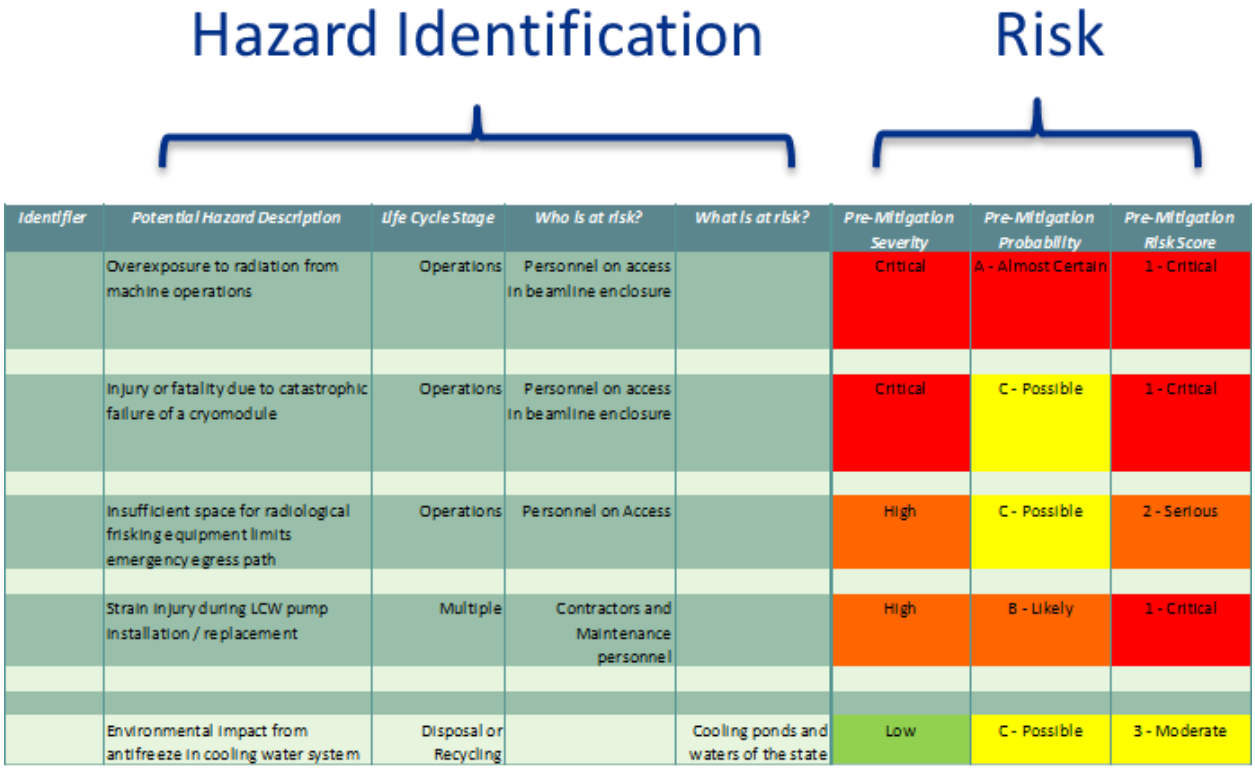
Implemented: Incorporated into the physical device. Incorporation into a reviewed and approved document also qualifies as implemented

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 as described in 6.8 Mitigation Actions.

7. Prevention through Design Spreadsheet

The PtD spreadsheet shown below [8], is used to identify hazards, assess risk in accordance with Fermilab QAM Chapter 12030, identify mitigative controls, assess residual risk, and track the status of control implementation. The PtD spreadsheet is intended to be a living document that is updated as necessary to add additional hazards and track implementation progress. Example entries are provided in the spreadsheet to assist the user with completing the spreadsheet.



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
	Overexposure to radiation from machine operations	Operations	Personnel on access in beamline enclosure		Critical	A - Almost Certain	1 - Critical
	Injury or fatality due to catastrophic failure of a cryomodule	Operations	Personnel on access in beamline enclosure		Critical	C - Possible	1 - Critical
	Insufficient space for radiological frisking equipment limits emergency egress path	Operations	Personnel on Access		High	C - Possible	2 - Serious
	Strain injury during LCW pump installation / replacement	Multiple	Contractors and Maintenance personnel		High	B - Likely	1 - Critical
	Environmental impact from antifreeze in cooling water system	Disposal or Recycling		Cooling ponds and waters of the state	Low	C - Possible	3 - Moderate

Mitigations	Post-Mitigation Severity	Post-Mitigation Probability	Post-Mitigation Risk Score	Mitigation Action	Status of Implementation	Comments
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	
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	
Conventional Facilities Technical Specification updated to define necessary space for enclosure frisking equipment	High	E - Rare	4 - Minor	Update Specifications and Interfaces	In Process	
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	
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