Machine Protection Risk Management Lifecycle at the European Spallation Source ERIC

S. Kövecses[1], J. Gustafsson[1], M. Carroll[1], A. Nordt[1]

[1]European Spallation Source ERIC, Sweden

Machine Protection Risk Management Lifecycle

Reliability and availability requirements are taken into consideration before and during the design of the Machine Protection Systems at ESS. This is done by systematically identifying, assessing and mitigating damage risks to equipment.
The machine protection risk management lifecycle has the following phases:

1. Identification of concept and scope
2. Risk identification
3. Risk assessment
4. Risk mitigation
5. Requirement specification
6. Design and implementation
7. Verification and validation

1. Identification of concept and scope
During this phase it is determined which systems are included and will have a detailed Machine Protection analysis and which systems are excluded.

2. Risk identification
During the risk identification phase Damage Events (DE) are identified. The consequence is defined by estimating the impact of the damage event on cost and downtime. Depending on the consequence a Tolerable Occurrence Magnitude (TOM) is assigned to the damage event.

3. Risk assessment
During the risk assessment phase the hazards leading to a damage event are identified. Multiple hazards can lead to the same damage event. The Expected Occurrence (EO) rate of each hazard is estimated in this phase.

4. Risk mitigation
During this phase the mitigations are identified. The Overall Protection Function (OPF) defines **what** should be done to mitigate the hazard. Each overall protection function is assigned a Functional Integrity Magnitude (FIM) which defines the requirements on the mitigation.
In addition Protection Functions (PFs) are specified (**how** the risk is mitigated). This includes a functional specification, required Protection Integrity Level (PIL) and Maximum Reaction Time for each function.

The outcome from the risk identification, risk assessment and risk mitigations is documented in a machine protection analysis. The analysis is performed in workshops, with the related system owners, technical experts and system engineers.

5. Requirement specification
During this phase requirements are assigned to the different systems involved in the implementation of the protection functions.

6. Design and implementation
The systems are designed according to the requirements. In some cases it might not be possible to implement the protection functions as intended and the analysis has to be revaluated.

7. Verification and validation
The verification an validation is done according to a predefined plan. In some cases the requirement can't be fulfilled and then the analysis revaluated or design has to be changed.

Machine Protection Purpose

The purpose of Machine Protection at ESS is to support ESS availability requirements by preventing damage to equipment which could lead to long downtimes.

Example 1: Risk identification
In this example, the damage event (damage to a device) has been estimated to be 500k euro and its repair or replacement will cause 8 days of downtime.

- Cost 500k €
- 8 days of downtime

The "consequence matrix" below is used to determine the consequence category for the damage event as "significant".

Cost \ Downtime	< 1 h	1 h – 1 d	1 d – 14 d	14 d – 3 m	> 3 m
< 0.1 M€	Minor	Moderate	Significant	Significant	Severe
0.1 M€ – 1 M€	Moderate	Moderate	Significant	Significant	Severe
1 M€ – 5 M€	Significant	Significant	Significant	Severe	Severe
> 5 M€	Severe	Severe	Severe	Severe	Severe

To be able to bring the damage event into an acceptable green field in the risk matrix below, a Tolerable Occurrence Magnitude (TOM) 3 is selected.

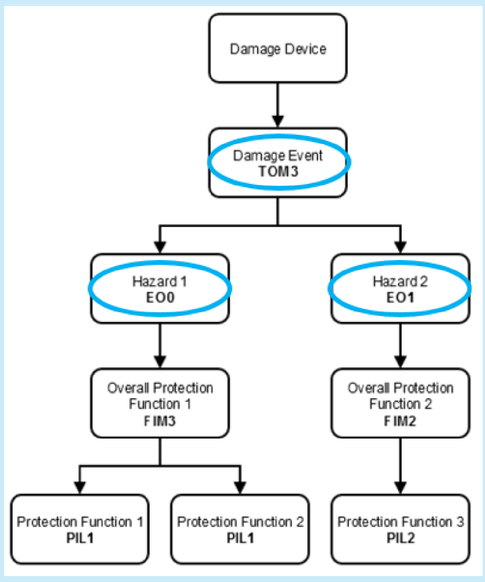
Tolerable Occurrence Magnitude \ Consequence	Minor	Moderate	Significant	Severe
TOM3				
TOM2				
TOM1				
TOM0				

Each Tolerable Occurrence Magnitude level corresponds to a maximum number of times the event is allowed to happen.

- TOM3 = 1/5000 y^{-1}
- TOM2 = 1/500 y^{-1}
- TOM1 = 1/50 y^{-1}
- TOM0 = 1/5 y^{-1}

I.e. the more severe the consequence the less often is the damage event allowed to happen.

Example 2: Risk assessment
In Example 1, the damage event was classified as TOM3.



There are two separate hazards (Hazard 1 and Hazard 2) which can lead to this damage event.

"Hazard 1" is expected to happen regularly during normal operations. That corresponds to expected occurrence of EO0 according to the table below.

Expected Occurrence (EO)	Description
EO0	The hazard is expected to happen during normal operation.
EO1	The hazard is expected to happen during the facility lifetime
EO2	The hazard is unexpected during facility lifetime

Machine Protection Concept

The key concept of Machine Protection at ESS is to monitor the state of the machine and stop beam operation if a state that can cause damage is detected. The sensors used to detect the state of the machine and the logic interpreting them are distributed over multiple systems.

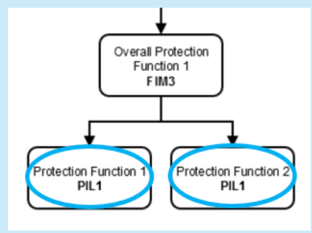
Example 3: Risk mitigation
In the Example 2, the expected occurrence rate was estimated to a EO0.

The tolerable occurrence rate (TOM) and expected occurrence rate (EO) for the damage event have been defined. Since the expected occurrence rate is higher than the tolerable occurrence rate a mitigation has to be made, this mitigation is called an Overall Protection Function (OPF). Depending on the occurrence rate difference the overall protection function gets different requirements represented by the Functional Integrity Magnitude (FIM).

To define the functional integrity magnitude for "OPF1" the following calculation is used:

TOM3 – EO0 = 3 – 0 = FIM3.

The FIM3 should be reached by the protection functions implementing the overall protection function.



Two protection functions able to mitigate the hazard were identified and classified as protection integrity level (PIL) 1 functions.

PIL	SIL (IEC 61508)	Required PFH	Required PFD
PIL0	N/A	<= 1 * 10^{-4}	<= 1
PIL1	SIL1	<= 1 * 10^{-5}	<= 1 * 10^{-1}
PIL2	SIL2	<= 1 * 10^{-6}	<= 1 * 10^{-2}
PIL3	SIL3	<= 1 * 10^{-7}	<= 1 * 10^{-3}
N/A	SIL4	<= 1 * 10^{-8}	<= 1 * 10^{-4}

The protection integrity level is the required reliability level of a protection function. It is defined by

- probability of failure per hour (PFH) or probability of failure on demand (PFD)
- the architectural constraints (Safe Failure Fraction (SFF) and Hardware Fault Tolerance (HFT))

PIL1 + PIL1 + one redundant element correspond to:
1 + 1 + 1 = FIM3

The European Spallation Source ERIC (ESS) is a research facility under construction outside Lund Sweden. Protons will be accelerated through a 600 m long linear accelerator and hit a rotating solid tungsten target. When the protons hit the target neutrons will be created through the spallation process. The neutrons will be moderated and directed towards the 22 instruments were research samples are investigated. ESS will be a high intensity pulsed neutron source with pulse lengths up to 2.86 ms.

europeanspallationsource.se

EUROPEAN SPALLATION SOURCE

ACCELERATOR RELIABILITY WORKSHOP ARW 2022