DEVELOPMENT AND REALISATION OF THE ESS MACHINE PROTECTION CONCEPT

A. Nordt, R. Andersson, T. Korhonen, A. Monera Martinez, M. Zaera-Sanz, European Spallation Source ERIC, Lund, Sweden
A. Apollonio, R. Schmidt, CERN, Geneva, Switzerland
C. Hilbes, ZHAW, Winterthur, Switzerland

Abstract

The European Spallation Source ERIC (ESS) is facing extremely high beam availability requirements and is largely relying on custom-made, specialised, and expensive equipment for its operation. The average proton beam power of 5MW per pulse will be unprecedented and its uncontrolled release can lead to serious damage of the delicate equipment, causing long shutdown periods, inducing high financial losses and, as a main point, interfering drastically with international scientific research programs relying on ESS operation. Implementing a fit-for-purpose machine protection concept is one of the key challenges in order to mitigate these risks. The development and realisation of the measures needed to implement such concept to the correct level in case of a complex facility like the ESS, requires a systematic approach, and will be discussed in this paper.

ESS MACHINE PROTECTION

The European Spallation Source ERIC (ESS), currently under construction, consists of a 600m long high power proton Linac, accelerating proton pulses of 2.86ms length to the energy of 2GeV with a repetition rate of 14Hz. The proton pulses (5MW) then interact with a rotating tungsten target wheel. Neutrons are created due to the spallation process and further guided through 22 different neutron beam lines towards the experimental stations. It is expected to have the first protons on target mid 2019 [1].

As a user facility for neutron science, overall availability of the ESS needs to be defined from a user point of view. Hence, it should be characterized by the average neutron production during a certain time period. ESS availability is interpreted as the average proportion of beam production time during scheduled operation time. In general, the availability characteristics of a system are determined by its reliability, maintainability and inspectability. High operational availability is achieved by increasing the mean time between maintenance while avoiding large mean downtimes. A detailed discussion is presented in [2, 3].

In the context of ESS Machine Protection (MP), the term "machine" or Equipment Under Control (EUC) encompasses all elements in the Accelerator, Target Station and Neutron Science system segments - all being necessary for neutron beam production and its further use by the neutron science experiments.

Annika.Nordt@esss.se

ESS MP Design Approach

MP is concerned with operational goals of the ESS, that means, enabling neutron science and investment protection. It is not concerned with safety aspects that are regulated by legal authorities, such as personnel safety or public safety. Nevertheless, because of the high-risk potential associated with damage to the machine, elements related to MP will be implemented in accordance with functional safety standards [4, 5]. To keep the distinction between safety and protection requirements as transparent as possible, adequate definitions for MP have been introduced. The IEC 61511 is defining a Safety Integrity Level (SIL) [5], whilst we refer to the Protection Integrity Level (PIL) for MP instead [6, 7]. Protection Integrity describes the average probability of a protection system satisfactorily performing the required protection functions under all the stated conditions within a stated period of time.

ESS MP Goals and Top Level Requirements

The EUC is exposed to potential damage sources related to proton and neutron beam properties, related radiation, electrical power, vacuum, cooling, RF, etc. The severity of damage is defined with respect to neutron beam quality losses, quality loss duration and resource costs for the recovery of operational capabilities. The goals for MP are defined as follows [6]: MP shall, in that order, prevent and mitigate damage to the machine, be it beam-induced or from any other source, in any operating condition and lifecycle phase, in accordance with beam- and facility-related availability requirements. In addition, MP shall protect the machine from unnecessary beam-induced activation having a potential to cause long-term damage or increase maintenance times.

These two goals can be achieved if MP fulfils the top-level functional and operational requirements being described in the following. MP shall detect all relevant off-nominal states that can lead to damage or unnecessary beam-induced activation and take all the necessary actions for its prevention and mitigation. Protection functions shall be implemented with timing and protection integrity levels in accordance with damage risk reduction requirements. The protection functions shall be implemented such that the probability of spurious trips is reduced. All information about detected off-nominal states, performed prevention and mitigation actions shall be recorded, allowing for an a-posteriori reconstruction and analysis. Operation during all foreseen lifecycle phases of the machine, for example assembly and

ISBN 978-3-95450-148-9

installation, commissioning, tuning, operation, fault-finding, maintenance, and dismantling shall be supported. Also all operating modes of the machine, for example proton beam up to intermediary targets, proton beam with reduced beam power or alternative beam envelopes, and proton beam with alternative duty cycles shall be supported. It is important that MP supports operation in case of degraded equipment under control and in case of degraded protection functions.

FUNCTIONAL ARCHITECTURE CONCEPT

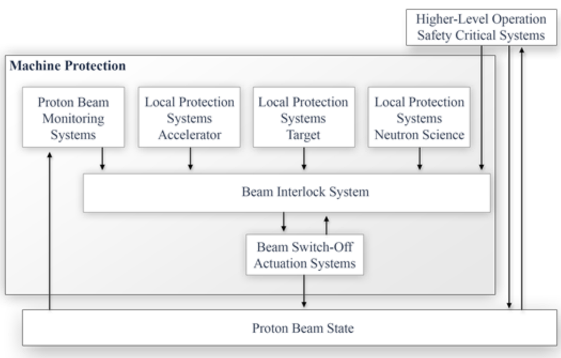

Figure 1: Functional architecture concept for ESS MP. Details are described in this section [6].

Off-Nominal States

The states that have to be monitored for off-nominal state detection can be grouped into four major parts.

Monitoring of the local state of the accelerator segment EUC. Accelerator EUC includes e.g. magnets, magnet power-supplies, RF generators, cavities, beam-choppers, proton source, vacuum valves, vacuum, and cryogenics. Respective local state variables would be vacuum valve positions, magnet coil temperatures, magnet power-supply output currents, etc.

Monitoring of the local state of the target segment EUC. Target EUC includes the target wheel, moderator, reflector, cooling system, etc. Respective local state variables would be target wheel rotation velocity and wheel temperature, etc.

Monitoring of the local state of the neutron science segment EUC. Neutron science EUC includes e.g. neutron choppers, light shutters, neutron guides, and experiment specific equipment. Respective local state variables would be neutron chopper velocity, and light shutter positions.

Monitoring of the proton beam state. State variables include beam current, beam shape, beam position, beam losses.

In principle, deviations of any of the mentioned state variables could lead to damage or to beam-induced activation.

Local Protection Systems (LPS)

These systems are in charge of monitoring specific EUC within a specific segment and detecting off-nominal local states that can lead to damage. They need to take the necessary actions to prevent damage to the monitored EUC in such a case. Depending on the EUC, off-nominal states might have an influence on the beam and cause beam-induced damage or beam losses leading to activation further downstream. For this reason, LPS are required to take any necessary action to switch off the beam. Starting beam operation while knowing that something is wrong should be avoided. This would unnecessarily increase the demand rate and protection integrity requirements for the Proton Beam Monitoring Systems. Therefore the LPS shall additionally confirm that everything in their segment is ready for beam production, if relevant (i.e. provide a beam permit signal).

Proton Beam Monitoring Systems (PBMS)

As the beam itself is a potential source of damage and the source for beam-induced activation, MP has to make sure that the beam parameters are as they should be. Detection of off-nominal beam states is allocated to the PBMS. It should be noted that proton beam monitoring could only help mitigate effects of already produced beam.

Beam Interlock System and Beam Switch-Off Actuation Systems

The Beam Interlock System (BIS) collects the signals from all LPS and PBMS and combines them into one global beam permit state. The BIS is controlling a set of beam switch-off actuation systems that will finally switch off beam. The actuation systems can be divided into two classes: those that are able to prevent new beam production and those that are able to mitigate the effects of beam that has been already produced and is injected into the Linac.

By switching off the magnetron of the proton source, new beam production can be prevented (it takes ~100µs until no further plasma is being created). The creation of trigger signals for new pulse generation can be stopped at the level of the timing system.

By activating the LEBT chopper to deflect beam onto the LEBT absorber (rise time: 300ns), the effects of already produced beam can be mitigated. It should be noted that the LEBT absorber allows only a few nominal pulses to be dumped before it gets damaged itself. Also the MEBT chopper can be activated to deflect beam onto the MEBT absorber (rise time: 10ns). However, the MEBT absorber allows only for a partial beam pulse dump before it is damaged (~200µs). Furthermore it is possible to control the RF supply to the RFQ in order to stop beam from getting further accelerated (~20µs).

ISBN 978-3-95450-148-9

CHALLENGING ESS MACHINE PROTECTION REQUIREMENTS

During a preliminary risk and hazard analysis for the accelerator EUC, a total of 166 different protection functions (PF) have been identified [8]. The most stringent requirements resulting from this analysis will be described in more detail in the following.

The proton beam shall be stopped within 4 to 5µs when detecting non-nominal beam states in the low-energy part of the Linac. This short reaction time is resulting from the time needed to melt copper or steel at (low) beam energies of 1 to 3.6MeV which is around 10 to 20µs in case of perpendicular impact of a beam with 2mm size (see Tab. 1). In order to stop beam before melting starts, the overall reaction time has been set to 4 to 5µs for the low energy part of Linac (i.e. first 50m of the Linac). The reaction time shall include the detection of beam losses, the processing of this information and the stop of beam operation. Several systems are needed to assure this requirement is being fulfilled. The only Beam Instrumentation Systems, which can detect critical beam losses in the low energy part of the Linac, are the Beam Current Monitors (BCMs) and Beam Position Monitors (BPMs). Beam Loss Monitors (BLMs) are sensitive only for energies above 80MeV. The BCMs are designed such that a response time of 1µs can be achieved. The BCM response time includes the detection of beam losses, the comparison to a pre-defined beam loss threshold and the propagation of a digital signal towards the BIS, indicating that beam operation is permitted or that beam operation shall be stopped upon the detection of beam losses, which exceed the pre-defined thresholds. The BIS is then triggering the different beam switch-off actuation systems simultaneously within ~2 to 3µs. However, as it can be seen from the description above, only the LEBT chopper is able to stop the proton beam in less than 1µs and is able to absorb at least one nominal beam pulse of 2.86ms length without being damaged. Tab. 1 shows the different reaction times needed for different proton beam energies.

Table 1: Times needed to stop beam operation based on the time needed to melt steel or copper upon perpendicular impact of proton beam (with a size of 2mm).

Beam Energy	Melting Time	Beam Stop Time
1 - 3.6 MeV	10 - 20 µs	4 - 5 µs
3.6 - 90 MeV	20 - 200 µs	5 - 20 µs
90 - 216 MeV	200 - 400 µs	20 - 40 µs
> 216 MeV	> 400 µs	> 40 µs

A PIL2 for the protection functions with most severe impact on the overall ESS operational availability has been defined [8]. Since a protection function includes sensor systems, such as BCMs, BLMs, different LPS, etc., the BIS and the beam switch-off actuation systems, an allocation of the tolerable failure limits corresponding to a PIL has been proposed:

- 35% of the total PIL for BIS input systems,
- 15% of the total PIL for the BIS,
- 50% of the total PIL for the beam switch-off actuation systems.

The PIL2 overall requirement is then resulting in a tolerable failure rate of $1.5x10^{-7}$ – $1.5x10^{-8}$/h for the BIS which actually corresponds to the tolerable failure rate limit related to a PIL3 (see Fig. 2 and Tab. 2). The allocation mentioned above can be understood such, that e.g. the likelihood of the BIS to fail shall be only 15% out of the total PIL2, indicating that the BIS shall fulfil the most challenging requirement in terms of tolerable failure rates.

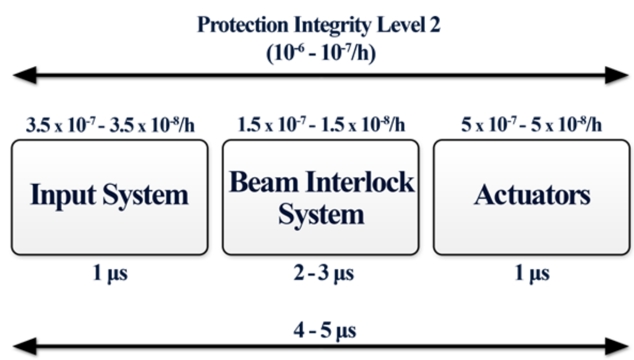

Figure 2: Shown is the PIL2 requirement and resulting tolerable failure rates allocated to different systems. The fastest reaction time and its allocation to the different systems are shown as well.

A first Failure Mode, Effects and Diagnostics Analysis (FMEDA) for the BIS prototype indicates that the required tolerable failure rates can be achieved [9]. It should be noted that only random hardware failures are analysed, whereas configuration errors, software, firmware and other failures are not considered in an FMEDA and need to be evaluated using other methods. A more detailed description of the BIS design can be found in [10].

Table 2: Different Rates of Tolerable Failures Per Hour [4, 5]

PIL (Protection Integrity Level)	Tolerable Failure Rates/h
1	10^{-5} – 10^{-6}
2	10^{-6} – 10^{-7}
3	10^{-7} – 10^{-8}
4	10^{-8} – 10^{-9}

ISBN 978-3-95450-148-9

THE MACHINE PROTECTION MANDATE AT THE ESS

ESS MP addresses stakeholder concerns and functions that cut across different ESS divisions and systems. Hence, a cross-divisional organizational unit is established for the overall coordination and decision-making on MP concerns, the ESS MP Committee (MPC). The MPC coordinates MP related activities with the relevant ESS divisions, working groups, in-kind contributors and experts of the ESS equipment and operation teams. One of the major tasks of this committee is to coordinate the identification, assessment and documentation of relevant risks, hazards, failure scenarios of the EUC. The committee is furthermore in charge of coordinating the coherent development (including design, integration, commissioning) of the EUC and its future changes or upgrades in regard to MP, but also the coordination of the ESS operation concerning MP.

The MPC formally approves overall MP decisions, including approval of overall MP requirements and protection functions, the overall technical decisions, the delegation of tasks (system development, commissioning, operation, etc.) to the divisions, and the overall development approaches for EUC local protection systems. In addition, the MPC defines boundary conditions for operation (proton beam power, repetition rate, etc.) and authorities/procedures for short-term interventions (e.g. overnight relaxation of operational boundaries).

The MPC is composed of representatives from all ESS divisions who are stakeholders in MP, with decision-making authority for their division. Currently it includes representatives of the Accelerator division, Target division, Integrated Control Systems division, Neutron Scattering Science division, and Operations division.

The MPC receives its mandate from the overall ESS management. Complementary to the MPC and its mainly formally approving character is the MP Panel (MPP), a discussion forum that meets regularly in order to gather relevant MP information and communicate MP issues into the organization [6, 11].

CONCLUSION

The European Spallation Source ERIC (ESS) is facing very challenging requirements for beam availability and systems reliability. At the same time the beam power is unprecedented (5MW) introducing a high risk potential for damaging delicate equipment. If the beam is for example not within the right beam parameter space, melting of copper or stainless steel can occur within a few microseconds only, potentially leading to long downtimes and costly repair actions, impacting significantly on the research mission of ESS. It is thus important to develop a fit-for-purpose machine protection concept, ensuring the high availability goals but also providing proper protection integrity. Such a concept cannot be developed and implemented by building sophisticated and dedicated protection systems only. It is equally vital to be able to raise awareness of the potential risks and to have a decision making body for machine protection relevant issues in place, being supported by the upper management.

The impact of certain decisions, when designing (local or single) systems, on the global performance level of a complex facility like ESS is often underestimated and not addressed in time, increasing the damage potential even further. At ESS, some effort has been taken in order to face these challenges and reduce the risks hopefully as good as possible.

REFERENCES

[1] J. Yeck, "Neutron facility: European Spallation Source is on track", *Nature*, vol. 519, no. 7543, p. 291, Mar. 2015.

[2] E. Bargalló et al., "ESS Availability and Reliability Approach", MOPTY045, IPAC'15, Richmond, USA (2015).

[3] E. Bargalló et al., "ESS reliability and availability requirements", ESS Report No 0008886, 2015.

[4] IEC61508 Edition 2.0

[5] IEC61511 Edition 1.0

[6] A. Nordt et al., "ESS Machine Protection Concept", ESS Report No 0035197 and No 0035388, 2015.

[7] Kwiatkowski, Maciej, "Methods for the Application of Programmable Logic Devices in Electronic Protection Systems for High Energy Particle Accelerators", PhD thesis, Warsaw University of Technology, Warsaw, Poland, CERN-THESIS-2013-216 (2013).

[8] A. Nordt et al., "Preliminary Risk and Hazard Analysis of the ESS Machine Protection System with Emphasis on Production and Property Losses in the ESS-LINAC ", ESS Report No 0003796, 2013.

[9] R. Andersson et al., "A modified functional safety method for predicting false beam trips and blind failures in the design of the ESS Beam Interlock System", *these proceedings*, MOPGF126, ICALEPCS 2015, Melbourne, Australia (2015).

[10] A. Monera Martinez et al., "Overview and Design Status of the Fast Beam Interlock System at ESS", *these proceedings*, MOPGF138, ICALEPCS 2015, Melbourne, Australia (2015).

[11] A. Nordt et al., "Machine Protection Strategy for the ESS", MOPTY048, IPAC'15, Richmond, USA (2015).

ISBN 978-3-95450-148-9