ISBN: 978-3-95450-168-7 doi:10.18429/JACoW-IPAC2015-MOPTY048

MACHINE PROTECTION STRATEGY FOR THE ESS

A. Nordt, T. Korhonen, T. Friedrich, C. Hilbes*, European Spallation Source ESS, Lund, Sweden
*ZHAW, Zurich University of Applied Sciences, Winterthur, Switzerland

Abstract

The ESS proton beam power of 125MW per pulse (5MW average) will be unprecedented and its uncontrolled release could lead to serious damage of equipment within a few microseconds only. To optimize the operational efficiency of the ESS facility allowing for very high beam availability with high reliability towards the end-users, accidents should be avoided and interruptions of beam operation have to be rare and limited to a short time.

Finding the right balance between efficient protection of equipment from damage and high beam availability is the key idea on which the ESS Machine Protection Strategy is being based on. Implementing and realizing the measures needed to provide the correct level of machine protection in case of a complex facility like the ESS, requires a systematic approach, which will be discussed in this paper. A method of how to derive machine protection relevant requirements and how to assure completeness of these will be outlined as well.

THE ROLE OF MACHINE PROTECTION AT THE ESS

ESS is facing high beam availability requirements and is largely relying on custom made, specialized, and expensive equipment for its operation. Damage to this equipment could cause long shutdown periods, inducing high financial losses and, as a main point, interfering with international scientific research programs relying on ESS operation and related beam production. Implementing a fit-for-purpose machine protection concept is one of the key challenges in order to mitigate these risks.

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. Availability is interpreted as the average proportion of beam production time achieved during scheduled ESS research infrastructure operation time. In general, the availability characteristics of a system are determined by its reliability, maintainability and inspect-ability. The expected operational time between two consecutive corrective or preventive maintenance actions is defined as *mean time between maintenance* (MTBM). The time for diagnostics, corrective and preventive maintenance, logistics, cool down and restart times is defined as *mean down time* (MDT). Then, the operational availability can be described as:

$$\frac{MTBM}{MTBM + MDT}$$

High operational availability is thus achieved by increasing the mean time between maintenance while avoiding large mean down times. A detailed discussion in regard to varying user experiments is presented in [1].

The Machine or the Equipment Under Control (EUC)

In the context of ESS Machine Protection, 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. Figure 1 shows a simplified architectural view of the equipment under control (EUC) and the beam states.

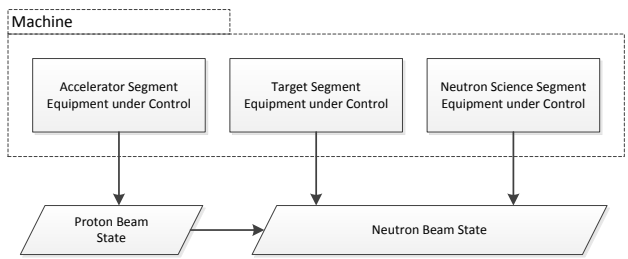

Figure 1: Simplified representation of the "machine". Equipment under control from the accelerator segment controls the proton beam state. The neutron beam state is controlled by the Target and Neutron Science Segment EUC and is influenced by the proton beam.

Machine Protection Goals

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 machine protection are defined as follows:

1. Machine protection 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.
2. Machine protection shall protect the machine from unnecessary beam-induced activation having a potential to cause long-term damage to the machine or increase maintenance times, in accordance with beam and facility related availability requirements.

Machine protection is concerned with operational goals of the ESS, that means, enabling neutron science

ISBN: 978-3-95450-168-7 doi:10.18429/JACoW-IPAC2015-MOPTY048

and investment protection. It is not concerned with safety aspects of the ESS that are regulated by legal authorities, such as personnel safety or public safety.

MEANS TO ACHIEVE MACHINE PROTECTION

The high operational availability goals can be achieved by four major means:

- Designing the equipment under control (EUC) with high inherent reliability and overall low damage potential,
- Minimization of the necessity for corrective maintenance and of the mean down time (MDT) of EUC by introducing dedicated technical systems preventing and mitigating damage,
- Minimization of the MDT of EUC systems by introducing dedicated operational and preventive maintenance procedures reducing the probability for (unscheduled) corrective maintenance.
- Introducing support systems dedicated to reduce MDT (analysis, management and recovery tools addressing operational activities related to machine protection, e.g. for post-mortem analysis).

The strategy to achieve the availability goals will involve a mix of those measures.

Machine Protection and EUC Design

Machine Protection can be achieved by designing EUC systems with an inherent high availability. This reduces the probability of mishaps per-se, which increases the MTBM, and also decreases the time to fix EUC systems in case of failure, decreasing the overall MDT. In an optimal case, potential sources of damage risks can be completely avoided or effectively mitigated by means of EUC design, for example, by EUC system shielding and positioning.

Machine Protection and Dedicated Technical Systems

Dedicated technical systems are needed for machine protection in order to prevent and mitigate production losses and equipment damage. These fall into four major categories being: EUC local protection and beam permit systems (LPS), proton beam monitoring systems (like the Beam Loss Monitoring system), the beam interlock system (BIS) and finally actuating systems needed to switch off the proton beam.

The EUC local protection and beam permit systems are interfacing the BIS, indicating whether the EUC is ready for beam operation or not. They also indicate whether a potentially damaging situation has been detected which requires stopping beam operation.

The BIS is deriving a global “beam permit” based on the input signals from the LPSs. On the other hand side the BIS can trigger a stop of beam operation by for example disabling the proton source or setting the LEBT chopper to deflect the beam onto a beam dump.

Scopes, boundaries and requirements for these different systems are still in the specification phase and need approval by the machine protection committee.

Machine Protection and Operational and Preventive Maintenance Procedures

Effective machine protection will finally not be achievable without defining plans and procedures that guide human interactions with the EUC. Those include:

- Procedures directly related to the operation of the EUC, like cool down and restart procedures, with a goal to minimize stress to the EUC,
- Preventive maintenance plans and general maintenance procedures for the EUC.

Machine Protection Support Systems

Machine Protection support systems enhance the effectiveness and efficiency by which ESS staff can execute Machine Protection related tasks. Machine Protection support systems can relate to post-mortem analysis which helps to identify the root cause of a failure that was leading to the stop of beam operation, early fault detection methods and tools, alarm analysis, root cause analysis, documentation of Machine Protection related events and their statistical evaluation.

THE MACHINE PROTECTION MANDATE AT THE ESS

ESS Machine Protection 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 machine protection concerns, the ESS Machine Protection Committee (MPC). The MPC coordinates Machine Protection related activities with the relevant ESS divisions, working groups, in-kind contributors and experts of the ESS equipment and operation teams. This includes to

- Coordinate the identification, assessment and documentation of relevant risks, hazards, failure scenarios of the EUC,
- Coordinate the coherent development (including design, integration, commissioning) of the EUC and its future changes or upgrades in regard to Machine Protection,
- Coordinate the operation of the ESS concerning machine protection in line with the ESS goals,
- Identify possible bottlenecks that would prevent neutron beam production according to ESS goals.

The MPC formally approves overall Machine Protection decisions. This includes to

- Approve overall machine protection requirements and machine protection functions,
- Approve the overall technical decisions,
- Approve the delegation of tasks (system development, commissioning, operation, etc.) to the divisions,

ISBN: 978-3-95450-168-7 doi:10.18429/JACoW-IPAC2015-MOPTY048

- Define boundary conditions for operation (proton beam power, repetition rate, etc.) and authorities/ procedures for short-term interventions (e.g. overnight relaxation of operational boundaries),
- Approve the overall development approaches for EUC local protection systems.

The MPC is composed of representatives of all ESS divisions who are stakeholders in Machine Protection, with decision-making authority for their division. Currently it includes representatives of the Accelerator division, the Target division, the 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 Machine Protection Panel (MPP), a discussion forum, that is meeting regularly in order to gather relevant Machine Protection information and communicate Machine Protection issues into the organization.

ENGINEERING APPROACH

Functional safety standards [2] and [3] are used as development guideline for addressing a limited number of high criticality protection functions. While Machine Protection is not subject to safety certification, the ESS protection group applies these standards for the purpose of investment protection and achieving high availability. In practice, this approach is applied primarily to beam related protection functions addressing high severity risks, (e.g. long downtimes). Typically these protection functions are addressed by dedicated hardwired, fast interlocks. This standard guided approach enables the ESS protection group to implement a development process that is based on the state of the art in engineering dependable systems as well as tailored to particular ESS system properties and ESS goals and organization [4].

Using Functional Safety Standards for Machine Protection Purposes

Prior to typical system development processes (common V-model approach [5]), the Machine Protection related systems are subject to a dedicated phase of analysis and protection function specification. This includes the iterative generation of a number of interrelated documents, which enable to trace machine protection concerns from *overall* considerations to detailed technical specifications. This document package includes

- Overall concept outline,
- Scope definitions of different systems,
- Risk and hazard analyses,
- Overall protection requirements specifications,
- Overall protection functions specifications,
- Protection systems requirements specifications.

Further, dedicated *planning* documentation is created regarding overall operation, maintenance, installation, integration and validation of the Machine Protection related systems. This package is used as a specification input for the actual development process of the Machine Protection related systems, which will follow the V-model approach. Overall commissioning, validation, operation and maintenance activities will be executed accordingly. The outlined document generation efforts prior to and accompanying the detailed technical planning, design and implementation phases enable to achieve a high degree of completeness and traceability of design decisions regarding machine protection concerns.

Challenges Encountered using Functional Safety Standards for ESS Machine Protection

The introduction of standard-based functional safety concepts into accelerator design faces various challenges. The typical unfamiliarity of the accelerator community with safety standards can result in uncertainty about their suitability for machine protection purposes. The estimation of potential extra efforts, staff competence needs and the added value can be difficult to anticipate. The standards' application in practical terms, i.e. the tailoring to the particular system and project, requires a balance between rigidity and other concerns, e.g. pressing schedules. Building the organisational support for this approach can constitute a significant communicative challenge.

DISCUSSION AND CONCLUSIONS

For the small but crucial set of beam related machine protection functions, the ESS Machine Protection group is elaborating and executing a novel engineering approach that builds on the state of the art in safety engineering, while equally tailoring the approach to the particularities of the ESS systems and goals. This approach is considered suitable for achieving the demanding goals of the ESS, and will be followed further during the ESS construction period. Generally, the adoption of this approach is considered to be beneficial for future accelerator facilities with high availability demands. However we see improvement potential concerning support of applying functional safety standards for Machine Protection in research facility environments, e.g. practical guidance in their application. We therefore suggest to the accelerator community the continuous elaboration of engineering approaches for machine protection based on safety standards, and promote case studies in future projects, to which we intend to contribute with our experiences.

REFERENCES

[1] E. Bargallo et al., "ESS Availability and Reliability Approach", *these proceedings,* MOPTY045, IPAC'15, Richmond, USA (2015).
[2] IEC61508 Edition 2.0.
[3] IEC61511 Edition 1.0.
[4] R. Schmidt et al., New J. Phys. **8,** 290 (2006).
[5] http://en.wikipedia.org/wiki/V-Model