OVERVIEW ON THE DESIGN OF THE MACHINE PROTECTION SYSTEM FOR ESS

A. Nordt, ESS*, Lund, Sweden
A. Apollonio, R. Schmidt, CERN†, Geneva, Switzerland

Abstract

Scope of the Machine Protection System (MPS) for the European Spallation Source (ESS) is to protect equipment located in the accelerator, target station, neutron instruments and conventional facilities, from damage induced by beam losses or malfunctioning equipment. The MPS design function is to inhibit beam production within a few microseconds for the fastest failures at a safety integrity level of SIL2 according to the IEC61508 standard. These requirements result from a hazard and risk analysis being performed for the all systems at ESS. In a next step the architecture and topology of the distributed machine interlock system has been developed and will be presented. At the same time as MPS seeks to protect equipment it must protect the beam by avoiding triggering false stops of beam production, leading to unnecessary downtime of the ESS facility.

INTRODUCTION

The European Spallation Source (ESS), currently under construction, will be a multi-disciplinary research centre, being located in Lund/Sweden, enabling researchers from academia and industry to performing fundamental and applied research, using neutron beams. The ESS consists of a 600 m long linear mainly superconducting accelerator (LINAC), sending 2.86 ms long pulses of 2 GeV protons at a 14 Hz repetition rate to the rotating, helium cooled tungsten target, producing thermal and cold-moderated neutrons which are further guided to a large variety of state-of-the-art neutron instruments, supported by a suite of laboratories, as well as a supercomputing data management and development center. ESS will be a low-energetic neutron source of unprecedented high power and scientific performance; delivering the first spallation neutrons in 2019 and reaching its full design specifications in 2025, with a suite of 22 research instruments. The investment cost of the project is ca. 1800 million Euro [1].

One of the ESS' key tasks is to deliver neutrons with a 95% overall reliability and to be operational at high power with an average beam power of 5 MW per pulse for ~5000 h per year. In order to achieve these goals it is vital to perform reliability, availability, maintainability, inspect-ability as well as risk and hazard analyses throughout the whole lifecycle of ESS. One of the major systems impacting on beam availability and system reliability is the Machine Protection System.

MACHINE PROTECTION STRATEGY

To optimize the operational efficiency of the facility, accidents should be avoided and interruptions should be rare and limited to a short time. Objectives for MPS are:

- Protect the facility: MPS shall inhibit proton beam production upon detection of a critical condition leading to beam induced damage of equipment.
- Protect the beam: The MPS shall not generate interruptions of beam production if this is not strictly necessary.
- Provide the evidence: In case of terminating beam production, MPS shall support identifying the initial failure, also in case of multiple alarms (e.g. when one initial failure causes subsequent failures).
- Allow efficient operation of ESS: Beam operation should be possible if some parts of ESS are not ready for accepting beam. As an example, it should be possible to send beam to the beam dump via the tuning dump line if the target is not operational [2].

From these objectives the principles for the architecture follow. MPS consists of sensors provided by different systems such as the Beam Loss Monitoring System, vacuum system, RF system, etc., see Figure 1. These systems can detect a large variety of conditions leading to beam-induced damage by consistently and frequently comparing online-measurements with pre-defined damage thresholds. According to the result of this threshold comparison, a status signal OK equivalent to "signal < threshold" or NOK (not OK), equivalent to "signal ≥ threshold" can be derived and will be transmitted via hardwired links to the so-called Beam Interlock System (BIS). The BIS will then derive a BEAM PERMIT (0/1) signal according to pre-defined and hardcoded truth tables (see Table 1). No software processes shall be involved. Beam production shall be permitted if the BEAM PERMIT signal is valid (==1) and shall be inhibited otherwise, which means that a NOK signal is sent to redundant and fail-safe mitigation devices. All connections towards, within and from the BIS shall be implemented via hardwired links. Only one signal per system (or two for redundancy reasons) indicating a failure will be requested, not many (e.g. in case of the proton source it is not required to interlock the status of the cooling water, conductivity of the cooling water, the power supply status using single connections to the BIS; it is sufficient and preferred to aggregate such internal signals into one single proton source status signal simply

* http://europeanspallationsource.se/
† http://home.web.cern.ch/

indicating the readiness for beam production towards the BIS).

The ESS accelerator will be split into different sections, and the logics of the Beam Interlock System will take these sections into account. To limit the number of faulty triggers, the number of channels that may provoke an interruption of beam production will be minimised. This will establish a reasonable compromise between the requirement for protection and the requirement to avoid unnecessary downtime. The efficiency of the operation can be improved using a software interlock system (SIS). Beam stops triggered by this system can be disabled because there is always a second level of protection due to the hardwired interlocks of the BIS. To provide the evidence of a failure and assist the operator, the same design across different systems shall be used (for retrieval and analysis of post mortem data).

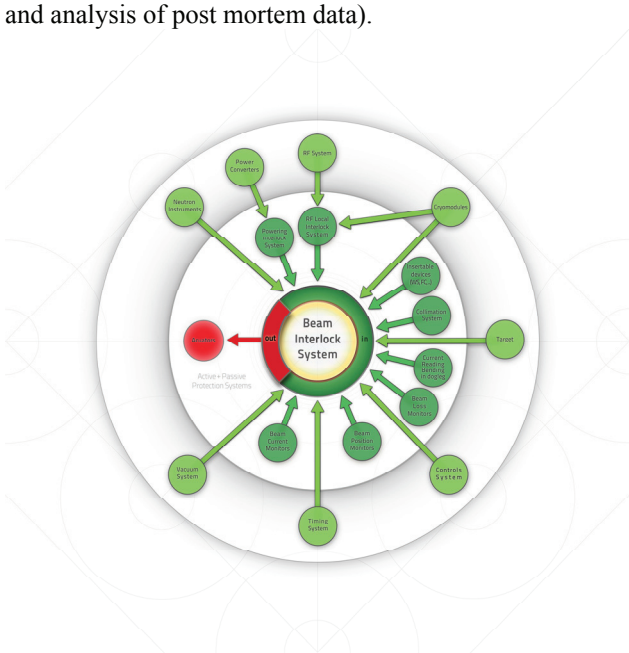

Figure 1: Overview on the machine protection framework: systems (in green), such as vacuum, RF or beam loss monitors send a status signal to the BIS indicating readiness for beam or not. In case one of them detects a critical situation, then the BIS triggers the actuators to terminate beam production within a few microseconds, depending on the location of detection (in red). Systems shown in the inner circle are active protection systems, and systems outside provide passive protection and/or status signals indicating their necessary availability and readiness for beam production.

For the diagnostic of beam losses, a beam loss monitoring (BLM) system is being designed. A second option to measure beam losses is using beam current monitors (BCMs): if the difference in beam current is too high between two BCMs within a LINAC section beam production can be inhibited. A few beam position monitors (BPMs) will be used to monitor the beam position and if the beam parameters are outside a tolerance window these monitors will also trigger a stop of beam production via the BIS. Other sensors monitor the parameters of hardware systems (RF, vacuum, cryogenics, magnets and power converters, etc.). Even when operating without beam, such sensors are used for the protection of equipment (e.g. sensors for measuring the magnet temperature, to detect arcs in HV systems etc.). When these sensors detect a failure, beam production is inhibited and the hardware protection is activated (e.g. switching off the magnet power supply or a modulator). Several beam absorbers are installed in the low energy part of the LINAC. To limit the beam losses in the LINAC, collimators will be installed in the MEBT. Reliable methods to stop active beam already in production are essential for protection from damage due to beam losses. It is proposed to use three different devices to stop and interrupt beam operation, with a possible fourth option:

1. The primary method of terminating beam production will be to switch off the proton source magnetron that terminates the generation of plasma. The system response however is relatively slow with around 100 µs.
2. Switching ON the high voltage to the LEBT chopper will deflect the beam into an absorber that is part of the LEBT structure. The response time of the LEBT chopper is about 300 ns. Using this chopper to stop the beam is tolerable for 2 - 3 nominal pulses only.
3. Switching ON the high voltage of the MEBT chopper. The response time is about 10 ns but the related absorber can only tolerate around 0.5 of beam before being damaged.
4. As fourth option, the RF supplying the RFQ could be switched off. This has the advantage that the power of the beam after the RFQ is reduced.

Table 1: Truth Table on Master Level for the Beam Interlock System

Ch	Signal Name	#1	#2	#3	#4	#5	#6
0	Software Interlock	1	1	1	1	1	1
1	Proton Source Status	1	1	1	1	1	1
2	Iris Status	1	1	1	1	1	1
3	Solenoid1+Steerer1	1	1	1	1	1	1
4	Solenoid2+steerer2	X	1	1	1	1	1
5	LEBT chopper OK	1	1	1	1	1	1
6	LEBT FC IN	1	0	0	0	0	0
7	LEBT FC OUT	0	1	1	1	1	1
8	EMU position	X	1	1	1	1	1
9	Control Room	1	1	1	1	1	1
10	PSS	1	1	1	1	1	1
11	LEBT vacuum	1	1	1	1	1	1
12	TSS	X	1	1	1	1	1

ISBN 978-3-95450-132-8

13	BCM2+LEBT chopper	X	1	1	1	1	1
14	MEBT OK	X	1	1	1	1	1
15	MEBT chopper OK	X	1	1	1	1	1
16	MEBT FC IN	X	1	0	0	0	0
17	MEBT FC OUT	X	0	1	1	1	1
18	DTL OK	X	X	1	1	1	1
19	DTL FC IN	X	X	1	0	0	0
20	DTL FC OUT	X	X	0	1	1	1
21	Spokes + MBeta1 OK	X	X	X	1	1	1
22	MBeta1 FC IN	X	X	X	1	0	0
23	MBeta1 FC OUT	X	X	X	0	1	1
24	MBeta2 + HBeta OK	X	X	X	X	1	1
25	Current Target OK	X	X	X	X	0	1
26	Target Line OK	X	X	X	X	X	1
27	Current DUMP OK	X	X	X	X	1	0
28	Dump Line OK	X	X	X	X	1	X
	Beam Permit	1	1	1	1	1	1

ESS MPS DESIGN APPROACH

The design of MPS will follow the IEC61508 standard [3], however since MPS is not a safety critical but mission critical system, it's not required to be compliant with that standard. The typical design approach for such systems should include the fail-safe principle: single point of failures must initiate a safe shutdown of the system. If the system itself contains a source of hazard, it should be possible to remove this hazard from the system so that its failure modes are no longer catastrophic. The safety integrity level (SIL) as defined within the IEC61508 standard, is realized through improved system reliability and safety, but also through management, systematic techniques, verification and validation. A probabilistic risk assessment, in which component reliability (in terms of component failure rates), and event probability are used in quantitative safety assessment methods, has been applied already during the early design phase for the ESS MPS. The losses considered for the ESS MPS risk analysis are:

- Production losses: characterized by not delivering beam to the end users/downtime;
- Property losses: characterized by damage to machine equipment.

The beam availability of ESS is used to characterize the average production loss during a certain time period. It represents the average proportion of the planned neutron production time. Availability characteristics are determined by reliability and maintainability. If Mean Time To Failure (MTTF) is the expected operational time between two consecutive failures and Mean Time To Restore (MTTR) is the repair time, inclusive diagnostics, logistics, cool down and restart times, then the availability is given by MTTF/(MTTF+MTTR).

Based on the findings from the preliminary risk analysis, a failure catalogue has been developed, providing information on the event leading to equipment damage or downtime, the initiating causes of the event and the time scale during which the event develops, the consequences and their severity as well as likelihood being ranked using a 4 x 4 matrix. The events found are ranked once without any mitigation measures (e.g. preventive maintenance, etc. are not taken into account) and once ranked with foreseeable mitigation techniques to understand by how much the risk is reduced adding the local protection measures. An MPS function is required only in case the risk is still too high when taking into account local protection measures. The SIL for each MPS function depends on the necessary risk reduction factor that the function has to provide. The highest SIL was found to be SIL3 for a few MPS functions, however it is foreseen to rather add higher local protection techniques to the systems affected than implementing a high SIL MPS function. Thus the requirement for the MPS SIL has been set to be at a SIL2 maximum.

An example for a SIL3 MPS function is related to the power supply (PS) of the bending magnets, one of the most critical devices. Depending on the settings of the PS, beam is sent to the dump line OR to the target station. Sending the "wrong" beam to either destination could lead to:

- Damage of the beam dump by sending beam with an average power of more than 10 kW.
- Damage of the target station, which can be due to a failed raster magnet system leading to critically deflected or focused beam, failures within the target station that do not allow acceptance of beam whilst beam is sent, etc.

Careful monitoring of this PS has been recommended and several layers of diverse redundancy will be implemented ensuring a high level of protection. Furthermore the Personnel Safety System as well as the Target Safety System will monitor this PS due to its safety-criticality.

CONCLUSIONS

The strategy to design the MPS for ESS has been presented in this paper. The results of a preliminary risk and hazard analysis, focusing on production and property losses were used to define protection functions and related risk reduction factors, helping to define and manage the signals connected to the BIS as well as required response times for sensors. A first draft of architecture could be derived and is presented.

REFERENCES

[1] Technical Design Report ESS 2013-001: http://europeanspallationsource.se/scientific-technological-documentation

[2] R. Schmidt et al., "Protection of the CERN Large Hadron Collider", New Journal of Physics 8 (2006) 290, http://www.njp.org, doi: 10.1088/1367-2630/8/11/290

[3] IEC International Electrotechnical Comission. "Functional safety of electrical/electronic/programmable electronic safety-related systems – part 1: General requirements", IEC61508-1: First edition 1998.

ISBN 978-3-95450-132-8