MACHINE PROTECTION RISK MANAGEMENT OF THE ESS TARGET SYSTEM

R. Andersson[1,†], E. Bargalló, L. Emås, J. Harborn, A. Lundgren, U. Odén, J. Ringnér, K. Sjögreen
European Spallation Source ERIC, Lund, Sweden
[1] also at University of Oslo, Norway

Abstract

The European Spallation Source target system is, together with the proton linac, the main component in the spallation process. ESS will use a 4-ton, helium-cooled, rotating tungsten target for this purpose, and its protection and availability is paramount to the success of ESS. High demands are placed on all of the target equipment, including cooling, movement, rotation, and timing, in order to reach the facility-wide 95% availability goal for neutron production. Machine protection has defined a set of protection functions that are to be implemented for the target system. This paper describes the development of these protection functions through the use of classic HAZOPs combined with modern safety standard lifecycle management. The implementation of these functions is carried out through close collaboration between the target system owners and the machine protection group at ESS.

INTRODUCTION

The European Spallation Source (ESS) is to be ready for the first proton beam on target at the end of 2019. This initial operation requires the proton linear accelerator (linac) to be ready to accelerate and direct a 590 MeV beam to the 4-ton, helium-cooled tungsten target wheel. When fully operational, the proton beam will be delivered in 2.86 ms long pulses at 14 Hz repetition rate, and the energy is to reach 1.3 GeV. The target wheel is divided into 36 sections and will rotate so that a new section is hit for each beam pulse. The rotating speed is thus 14/36, or 0.39 Hz.

This initial phase will have an average proton beam power of 3 MW, which will create spallation and thermal neutrons to be moderated to the right energies and reflected towards the 15 experimental stations. In the process, a large amount of heat load will need to be handled by the target cooling system. The exact rotational speed is important for successful experiments and to keep the ESS operation successful. In order to deliver an unprecedented facility experimental availability, a tailor-made risk management process has been developed to cope with the many risks of running such a state of the art research facility, in order to balance equipment protection and system availability. This paper briefly describes this risk management method and its use within machine protection, and describes its application on the ESS target system.

_____
† riccard.andersson@esss.se

MACHINE PROTECTION RISK MANAGEMENT AT ESS

Machine protection (MP) systems have held a key role in the success of modern accelerator facilities, such as the LHC, SNS, and J-PARC [1–3]. Their continuous development allows for increasingly fit for purpose solutions and MP plays a key role in avoiding lengthy facility downtimes due to damaged or activated equipment. Building on the success of MP for other facilities, ESS has developed a holistic approach to equipment protection that recognizes the interplay of many systems that are involved in fulfilling the protection goals. MP at ESS is viewed as a system of systems (SoS) and therefore applies some of these features [4].

Risk Management Process

The risk management process for MP at ESS is compliant with the ISO 31000 [5] and ISO 16085 [6] risk management standards as well as the key concepts from the IEC 61508 standard for functional safety [7]. This allows for the same approach, coordinated centrally by the MP personnel, to be taken towards all of the systems and equipment present at ESS, including the target system. The process focuses on managing *damage risk*, defined as a function of the *probability of occurrence* for a certain unwanted damage event, and its *consequence*. Further, the *consequence* has two parameters: the associated *cost* and *downtime*.

By identifying and analyzing each damage event and addressing each *hazard* that could lead to this damage event, through so-called *overall protection functions* (OPF), a *generic* set of objectives is first compiled and associated with each system. The OPFs are then subjected to audit by the associated MP personnel and system experts to derive technology-specific *protection functions* (PF), each containing one or more *sensors* that monitor the hazard, a *logic* element that takes the decision on whether action is required, and one or more *actuators* to carry out this action. In addition, the PFs include a *timing* requirement for how quickly the PF needs to be carried out, and a *protection integrity level* (PIL) that gives requirements on the quality of the PF [8].

All of the information and risk management process steps are required to be traceable and readily available for all interested parties. For these purposes, the collaborative Atlassian JIRA add-on Insight [9] is chosen as the official risk register during the analysis and design process. This allows for a continuous online work flow where all associated parts can follow and contribute to the analysis process. Once a set of PFs has finished its internal

iterations and suitability checks, it is documented and uploaded to the official ESS document management system for approval by the ESS machine protection committee (MPC).

Target System Architectural Setup

The target system is designed and delivered by different in-house and in-kind institutions, each one responsible for supplying the necessary equipment and instrumentation to operate according to specification. All of the constituent systems and their sensors are then integrated into the facility-wide control system framework EPICS 7 [10], whose interface is the designated target controls PLCs. Where relevant, as per the analysis presented in this paper, the sensor signals are split and also sent to the target protection system safety PLC. This PLC performs the initial data analysis and further distributes the signal to the ESS beam interlock system (BIS) when a beam stop is required, to prevent or mitigate a damage event. While all of the sensors are initially selected by the respective system designers, the ones involved in a PF are also checked for their suitability for protection purposes by the system designers and the MP personnel, after the first analysis iteration of PFs has been carried out.

ANALYZED TARGET SYSTEMS

The target system consists of several subsystems and support systems that fulfill specific tasks. The tungsten target itself needs to be adjusted to the correct position in three dimensions (a) as well as rotating with the correct speed during operation (b). The helium cooling system (c) needs to provide the correct cooling capacity to the tungsten target, while two primary water cooling systems (PWCS) provide cooling for the water moderators (d) and reflector structures (e). There is also a liquid hydrogen cryogenic moderator system (f) and a tuning dump system (g) that require attention from MP. These seven systems have been analyzed through individual hazard and operability analyses (HAZOP) by the target system experts, as well as through the ESS MP risk management method in collaboration between MP personnel and target system experts. Thus, the results presented in this paper are aimed at the following target systems:

a) Target wheel XYZ movement
b) Target wheel rotation system
c) Target wheel helium cooling system
d) Primary water cooling system – Moderators
e) Primary water cooling system – Reflectors
f) Cryogenic (LH$_2$) moderator system (CMS)
g) Tuning beam dump

The analyses are grouped so that the target wheel (a, b, c) is analyzed as one entity, the PWCS (d, e) as one, while the cryogenic moderator system and tuning beam dump are analyzed individually.

RISK MANAGEMENT ANALYSIS AND PROTECTION FUNCTION DEFINITION

The risk management process identifies and analyzes the damage events that are to be prevented or mitigated. Thus, the support systems, such as the water and helium cooling systems, are rather providers of operationally profitable settings than systems to be analyzed in detail for damage events. It is the responsibility of the system owners to design robust and reliable systems in line with the ESS requirements. The devices that are vulnerable to damage events are thus the target wheel, moderators (water and LH$_2$), reflectors, and tuning dump. These systems are individually discussed in this section, and a table outlines the associated PFs for each system.

As these systems are already controlled by the control system framework and contain certain protection barriers of their own, categorized as other risk reduction measures (ORRM) in the MP risk management framework, in accordance with the IEC 61508 standard, the remainder of the protection functionality to be carried out by MP-specific PFs during operation are associated with stopping the proton beam in case of overheating equipment or too high system pressure levels. For the sake of brevity, the tabulated PFs in the following subsections do not contain the description and role of the logic elements (the target protection safety PLC and the BIS) and the actuators (timing system/ion source, LEBT chopper, MEBT chopper) as these are the same for all target system-related PFs [11].

Target Wheel

Table 1: Protection Functions for the Target Wheel

Protection Function	Sensor	Timing	PIL
Stop beam if the differential pressure measurements in the helium outflow from the target wheel is too high or too low	Pressure	1 sec	0
Stop beam if the helium mass flow out of the target wheel is too low	Flow	5 sec	0
Stop beam if the helium temperature is too high in the outflow from the target wheel	Temperature	2 sec	0
Stop beam if the target wheel monitoring plug infrared monitor shows too high temperature	IR monitor	1 sec	1
Stop beam if the rotational speed of the target wheel is below minimum or exceeds maximum	Inductive rotational encoder	100 ms	1
Stop beam if the target wheel rotation phase is erroneous	Optical phase monitor	2.5 sec	1

The target wheel associated damage events are overheating from lack of cooling, overheating from the proton beam hitting the wrong position, and mechanical damage [12–14]. While the mechanical damage can be handled to an acceptable level by ORRMs that lock the wheel position before operation, appropriate limit switches, and mechanical structures, the overheating events need to be handled by machine protection PFs. These PFs are seen in Table 1. The estimated values for timing, as well as the usage of sensors, are based on [15].

Water Moderators and Reflectors

The water moderators and reflectors contain similar PWCS water loops and are analyzed identically [16]. As they are designed for full beam power as a nominal setting, their overheating due to receiving too much proton beam is excluded. Their MP-related PFs are thus associated with water cooling of the equipment, listed in Table 2.

Table 2: Protection Functions for the Water Moderators and Reflectors

Protection Function	Sensor	Timing	PIL
Stop beam if the cooling water flow in the moderator or reflector inlet is too low	Flow	1 sec	1
Stop beam if the cooling water flow in the moderator or reflector outlet is too low	Flow	1 sec	1
Stop beam if the cooling water temperature in the moderator or reflector outlet is too high	Temperature	10 sec	1
Stop beam if the cooling water pressure in the moderator or reflector inlet is too high	Pressure	1 sec	1

Cryogenic Moderator System

The CMS contains rigorous internal controls and feedback and has the role to both supply the moderating medium (LH_2) and provide cooling. As the system is cryogenic with an operating temperature between 17 and 20.5 K, it requires vacuum shielding and is analyzed for pressure increases (due to lost vacuum) and lack of cooling for the moderators [17]. The PFs are listed in Table 3.

Tuning Beam Dump

To run the proton beam to the tuning beam dump, the beam power needs to be below 12.5 kW. This means that the beam dump can only take four nominal pulses at full power [18]. To prevent the event of a powerful beam running to the dump, the two dipole magnets in the accelerator-to-target area need to confirm that they are activated before high-power beam is allowed, which would send the beam to the target wheel. However, there are two beam current monitors (BCM) in the beamline leading up to the beam dump, which are used for a PF as shown in Table 4.

Table 3: Protection Functions for the Cryogenic Moderator System

Protection Function	Sensor	Timing	PIL
Stop beam if LH_2 flow in the moderator inlet is too low	Flow	1 sec	1
Stop beam if LH_2 pressure is too high	Pressure (hydrogen)	1 sec	1
Stop beam if LH_2 temperature in the moderator inlet is too high	Temperature	5 sec	0
Stop beam if LH_2 temperature in the moderator outlet is too high	Temperature	5 sec	0
Stop beam if the CMS vacuum system pressure is too high	Pressure (vacuum)	5 sec	1

Table 4: Protection Functions for the Tuning Beam Dump

Protection Function	Sensor	Timing	PIL
Stop beam if the dump beamline BCMs detect a beam above 12.5 kW	BCM	280 ms	1
Stop beam if tuning dump temperature sensors notice too high dump temperature	Temperature	3 sec	0

CONCLUSIONS

To reach the high availability requirements of ESS, a holistic approach to machine protection is necessary. The method developed and presented in this paper is applicable to the target systems as well as the accelerator systems, and has derived a set of protection functions from the identified damage events related to operating the analyzed systems. The protection functions will be implemented in the design and commissioning of the ESS machine protection system of systems in the following years.

ACKNOWLEDGEMENTS

REFERENCES

[1] Andersson R., Nordt A., Adli E., Machine Protection Systems and Their Impact on Beam Availability and Accelerator Reliability, *IPAC2015*, Richmond, VA, USA, 2015.

[2] Wenninger J., Machine Protection and Operation for LHC. *CERN Yellow Report 2016:377–401*, doi:10.5170/CERN-2016-002.377, 2016.

[3] Schmidt R., Machine Protection. *CAS Update 2013:1881–3*, doi:10.1016/j.fusengdes.2013.05.065, 2013.

[4] Friedrich T., Hilbes C., Nordt A., Systems of Systems Engineering for Particle Accelerator based Research Facilities - A Case Study on Engineering Machine Protection, *SysCon 2017*, Montreal, Canada, 2017.

[5] ISO 31000: *Risk management - Principles and guidelines*, 2009.

[6] ISO 16085: *Systems and software engineering - Life cycle processes - Risk management*, 2006.

[7] IEC 61508: *Functional safety of electrical/ electronic/programmable electronic safety-related systems,* 2010.

[8] Andersson R., Bargalló E., Hilbes C., Nordt A., Machine Protection Risk Management Process, ESS Internal Document (ESS-0095000), 2017.

[9] Riada AB, Insight for JIRA, https://riada.se/insight, 2017.

[10] EPICS Community, http://www.aps.anl.gov/epics, 2017.

[11] Hilbes C., Nordt A., Machine Protection - Systems Requirements and Architectural Framework, ESS Internal Document (ESS-0057251), 2015.

[12] Emås L., HAZOP - Target Wheel X-Y-Z movement, ESS Internal Document (ESS-0084807), 2016.

[13] Harborn J., HAZOP - Target Wheel Helium Cooling, ESS Internal Document (ESS-0081405), 2016.

[14] Emås L., HAZOP - Target Wheel Rotational speed, ESS Internal Document (ESS-0081414), 2016.

[15] Sjögreen K., Target wheel, drive and shaft description of loads and operational limits, ESS Internal Document (ESS-0060625), 2017.

[16] Emås L., HAZOP - Water Moderators Primary Cooling System, ESS Internal Document (ESS-0043423), 2015.

[17] Emås L., HAZOP - Cryogenic Moderator System, ESS Internal Document (ESS-0092008), 2017.

[18] Lee Y., Olsson A., Eshraqi M., Miyamoto R., Möller M., Shea T., et al. Working Concept of 12.5 kW Tuning Dump at ESS. *IPAC2017,* Copenhagen, Denmark, 2017.