ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-TUPHA107

TECHNICAL AND ORGANISATIONAL COMPLEXITIES WITH A DISTRIBUTED MP STRATEGY AT ESS

E. Bargalló†, R. Andersson, S. Kövecses, A. Nordt, M. Zaera-Sanz, European Spallation Source ERIC, Lund, Sweden

Abstract

The reliable protection of the ESS equipment is important for the success of the project. This requires multiple systems and subsystems to perform the required protection functions that prevent undesired hazardous events. The complexity of the machine, the different technical challenges and the intrinsic organisational difficulties for an in-kind project such as ESS impose serious challenges to the distributed machine protection strategy. In this contribution, the difficulties and adopted solutions are described to exemplify the technical challenges encountered in the process.

THE EUROPEAN SPALLATION SOURCE

The European Spallation Source (ESS) is a European project with the aim of designing, constructing and operating an Accelerator-driven neutron source in Lund, Sweden. The purpose of this installation is to enhance neutron science by replacing the use of reactor-based neutron sources and to be an important center of science in Europe. The first spallation neutrons are expected in 2020 and ESS is planned to operate for 40 years before decommissioning.

ESS is a greenfield facility where a very high percentage of the components are designed and fabricated in different European countries in the form of in-kind, rather than cash. This makes it more complex to manage and to identify clear responsibilities and interfaces. For the distributed machine protection (MP) system of systems, the characteristics of this project present important organizational challenges.

MACHINE PROTECTION AT ESS

Machine protection is embedded in all systems, from power supplies to the large target system and neutron instruments. The main goal of MP is to stop the escalation of any misbehaviour of the machine, bringing it back into a stable and protected state.

In the case of a power supply, any internal problem, for example a broken fan, will be detected by a rise in temperature. The power supply will be stopped to avoid worse consequences, such as damage of connected components, fire, etc.

In the case of larger systems such as ESS, MP mainly avoids the escalation of events that could lead to beam induced damage. This means that if any critical misbehaviour of one the systems involved in generating, focusing, accelerating, steering, bunching, or chopping the beam is detected, these systems have to inform the so-called Beam Interlock System (BIS) to stop beam operation, bringing the machine to a protected state. Another key part of the protection is done through the beam monitoring systems, which directly detect and observe the different beam properties (e.g. position, current, pulse length, profile, position). In case these systems detect the beam parameters to be outside pre-defined boundaries, they will trigger an interlock and inform the BIS. There are other important functions in the MP systems, such as the correlation of the different beam modes that limit certain beam parameters to a maximum allowed beam power, the beam destinations (e.g. target, tuning beam dump) and the different elements that interact with the beam. As an example, if an insertable beam instrument can withstand only a low-power beam without being damaged, the BIS will not allow its insertion unless the correct beam mode for that device has been selected.

System of Systems

Machine Protection is done in a distributed way, where single protection functions are performed by different parts of the machine. These are managed by different divisions or groups and designed and built by different laboratories around Europe. This requires a new way of organizing the responsibilities, which can be achieved by applying the System of Systems (SoS) approach. This work was presented in [1] and it is currently followed at ESS.

The systems that belong to the MP SoS can be seen in Figure 1. All of these systems play a role in the operation and the protection of the machine. These systems belong to different groups and divisions. The protection-related systems are mainly related to the correct operation of the different ESS systems. The Proton Beam Monitoring systems detect if the beam is in its expected state or if there is some unexpected behavior. The Beam Stop Actuation systems stop the beam operation in a reliable way (upon request by the BIS). Other systems, such as safety or controls also have a connection to the BIS. Finally, other systems are required to ensure everything is synchronized, and these have been grouped (in this context) to be the MP management systems.

†enric.bargallo@esss.se
szandra.kovecses@esss.se
riccard.andersson@esss.se
annika.nordt@esss.se

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-TUPHA107

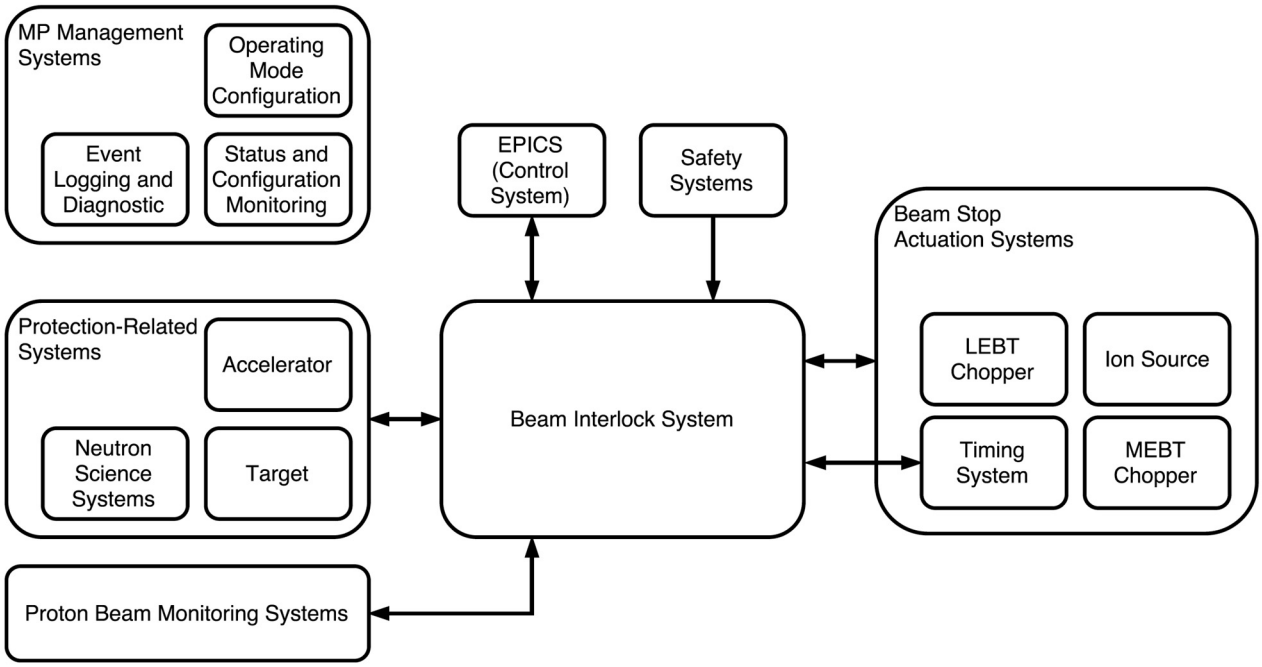

Figure 1: Machine protection System of Systems and the relation between the different entities [2].

MP CHALLENGES DURING THE DESIGN PHASE

The ESS MP team has faced many challenges during the past years with such a complex and distributed system. In this paper, a grouping of major issues encountered and the solutions implemented are described.

MP as a Convergence of Disciplines

MP in particle accelerators requires that different fields and disciplines converge into the single purpose of protecting the equipment, but still support high operational flexibility and increase availability of the function to be performed – in the context of global machine goals. This, in practice, means that various groups and people with different background and experience have to be involved in order to succeed in this very important goal. Some examples are beam physics, beam instrumentation, risk management, reliability engineering and PLC and FPGA experts among others.

This means that in addition to designing and deploying a very complex, fast and reliable system to protect the machine, the requirements and operational behaviour of the systems have to be identified and properly documented to be able to advance. However, in a project such as ESS, where parts of the accelerator design is performed in different laboratories in Europe and changes in scope, schedule and value-engineering exercises are performed continuously, the requirements have to be adapted on the fly [3].

Another important issue for MP is that the design of the machine is usually done from the requirements and needs coming from beam physicists, where the most important aspect during the design phase is to reach the desired beam power. On the contrary, other issues such as how to operate the machine, which systems that are required to operate it, or how the systems will interact are typically left for a later stage. This implies that the design of the MP systems has to be done in parallel with the understanding of the operation of the machine.

This problem has been solved in a pragmatic way, where some of the requirements that define our systems have been considered to be as good as reasonably possible. Other issues such as operability are still unknown; however, continuous discussions with the responsible people are done when help is needed to guide the design towards the likely required solution. In addition, at any new step of the design, the assumptions taken as well as the design options are discussed with the different experts. This is done to evaluate if design modifications are reasonable or if certain parts have to be re-designed.

Another tool used to identify missing information and to visualize how the systems interact with each other, are the Use Case Workshops [4]. In these workshops, examples of typical operational scenarios are simulated and analysed together with the system owners and the relevant experts. In the use cases, the signal sharing and the role of each system is checked in order to see the correct behaviour of them and optimise it towards high efficiency.

Local Versus Global Protection

As explained in the previous chapter, the protection of the machine occurs at different levels. At ESS, three main levels are considered:

- The first is at component level, where the manufacturer or the group building it takes care of it. Some

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-TUPHA107

examples are electronic boards, power supplies, or any stand-alone piece of equipment. This is quite straightforward to distinguish and will not be further discussed in this paper.

- The second is protection in between elements. This protection generally involves direct relationships between components in the form of services and connections. Some examples are water-cooling, controls, power supply, etc. In these cases, the elements usually belong to the same system and therefore they are the responsibility of the system owner. The protection functions involved in this category are called Local Protection Functions. The example in Figure 2 shows the local protection for a magnet system where the power supply performs the protection of the magnet. The power supply has to stop delivering power if overheating in the magnet coils is detected.
- The third level is focusing on protection functions that are located in-between systems. These functions usually cover beam damage events and require stopping the beam operation to bring the machine to a protected state. In Figure 2, a protection function to stop beam operation in case the magnet is not powered (hence beam is deflected in an unwanted and potentially critical way), is performed trough the magnet system, the BIS and the different Actuator systems. These functions are called Global Protection Functions and the ESS MP team is in charge of analysing them, retrieving the correct information about the systems that are part of the function, taking the correct decision on the level of the BIS and then triggering the actuators to stop beam operation.

At ESS, the responsibilities have been easily clarified in this way; however, a lot of interaction is required to ensure all protection functions are well identified. This interaction is also needed to define that the integrity levels of the protecting systems are in the same order as well as avoiding any gaps or undesired behaviours of the systems.

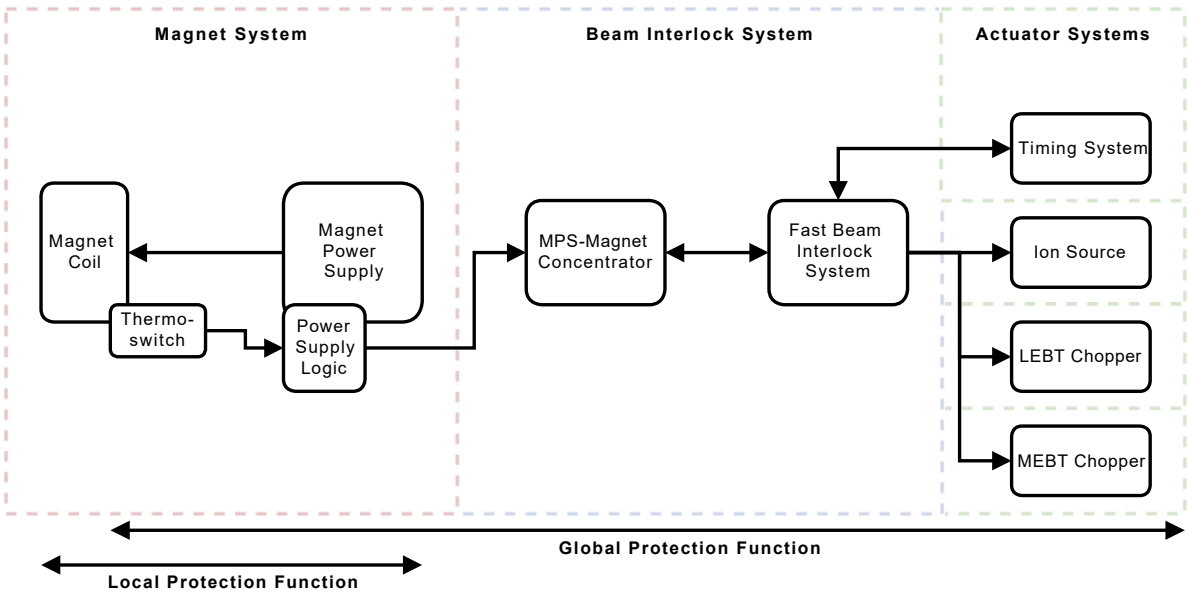

Figure 2: Example of a global and a local protection function at ESS.

Risk Management

Protecting a complex facility such as ESS requires a standard way of analysing and evaluating the hazards, the damaging events, their consequences and the protection functions needed to minimize the undesired consequences. A method capable of defining how important a protection function is and how reliable it has to be would be very beneficial in the moment of classifying critical systems and evaluating the elements that perform these functions.

MP itself has no relevant standard to use in a particle accelerator context for this purpose. This is why, at ESS, a new method was developed taking safety standards IEC 61508 and IEC 61511 together with risk management standards ISO 31000 and ISO 16085 into account and adapting them to MP [2]. This method permitted to guide the effort of MP into the most critical and most important functions, classifying the systems that required protection and defining the integrity levels required for their protection functions.

Interfaces Between MP-Related Systems

Another important issue is the interfaces with other systems. Due to the changing design and the fact that many of the systems are in-kind, it is not easy for the MP team to access detailed and relevant information. It was therefore decided to have a standardisation in FPGA processing boards with a standard interface to the BIS as well as standardised PLCs allowing for such a standardised interface. In addition, connectors and cables are also standardised. Furthermore, since there are some interfaces

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-TUPHA107

that are still to be defined, the fast part of the BIS has the possibility of replacing mezzanine cards in a signal conversion board to allow the connection of different types of signals and connectors.

The principal way to define such interfaces is with the so-called Interface Control Documents, where the different system owners agree on the signals and connectors in the interfaces they share. This has been proved to be a very good way of having the different teams on-board.

CONCLUSIONS AND NEXT STEPS

MP for a machine such as ESS requires special attention from many angles due to its distributed nature, its intrinsic complexity and its challenging organisational environment. In this contribution, the main problems faced and the solutions adopted have been presented. At the moment, many of these challenges are still be overcome; however, the current stage of the project and its way forward shows that the solutions adopted are contributing to its success.

REFERENCES

[1] T. Friedrich, *et al.*, "Systems of Systems Engineering for Particle Accelerator based Research Facilities", IEEE, 2017.

[2] R. Andersson, "A Machine Protection Risk Management Method for Complex Systems", Ph.D. thesis, Faculty of Mathematics and Natural Sciences University of Oslo, Oslo, Norway, 2017.

[3] R. Andersson, *et al.*, "Challenges in Technical Risk Management for High-Power Accelerators", ICANS XXII, Oxford, UK.

[4] S. Kövecses, *et al.*, "Strategy for Allocating Highly Distributed Protection Functions at ESS", ICALEPCS 2017, Barcelona, Spain, poster TUPHA101, this conference.