VERIFICATION AND VALIDATION OF THE ESS MACHINE PROTECTION SYSTEM OF SYSTEMS (MP-SoS)

A. Nordt, M. Carroll, J. Gustafsson, G. Ljungquist, S. Gabourin, S. Pavinato,
S. Kövecses de Carvalho, A. Petrushenko, European Spallation Source, ERIC, Lund, Sweden

Abstract

The European Spallation Source, ERIC (ESS) is a source of spallation neutrons used for neutron scattering experiments, complementary to synchrotron light sources. ESS has very ambitious goals and experimentation with neutrons at ESS should be one or two orders of magnitude more performing compared to other sources. Each proton beam pulse generated by the linear accelerator will have a peak power of 125 MW. The machine's equipment must be protected from damage due to beam losses, as such losses could lead to melting of e.g., the beam pipe within less than 5 µs. System-of-Systems engineering has been applied to deploy systematic and robust protection of the ESS machine. The ESS Machine Protection System of Systems (MP-SoS) consists of large-scale distributed systems, of which components themselves are complex systems. Testing, verification and validation of the MP-SoS is rather challenging as each constituent system of the MP-SoS has its own management, functionality that is not necessarily designed for protection, and also the different system owners follow their own verification strategies. In this paper, we will present our experience gained through the first 3 beam commissioning phases, ESS has gone through so far. We will describe how we managed to declare MP-SoS to being ready for beam operation without complexifying the task, and we will present the challenges, issues, and lessons learned faced during the verification and validation campaigns.

SYSTEM OF SYSTEMS ENGINEERING APPROACH FOR ESS MACHINE PROTECTION

Modern particle accelerator facilities, realised by complex constellations of interacting systems, serve a variety of users as research enablers. While the constituent systems exhibit a significant degree of technical and operational independence and distinct life cycles, the performance required to conduct research still needs to emerge from their integration into one overall system, the research facility. This renders a Systems of Systems oriented approach to engineering useful. Furthermore, accelerator-based research facilities face increasing availability expectations. Achieving those expectations can be supported through a tailored application of functional safety standards as engineering methodology guideline on an SoS level, as explained in [1]. An SoS-Engineering approach utilising functional safety standards (IEC 61511, IEC 61508) in this way is concretised in the Machine Protection Systems of Systems at ESS.

ORGANISATION AND RESPONSIBILITIES

The ESS Machine Protection team is responsible to:

- Coordinate Machine Protection across ESS.
- Define global protection functions.
- Develop, operate, and maintain the Beam Interlock System (BIS).
- Ensure working interfaces with BIS.
- Foster awareness that things can break.
- Foster awareness that thorough testing leads to success.

The ESS System Owners are responsible to:

- Develop reliable systems.
- Implement local protection functions.
- Implement Machine Protection requirements in their system.
- Provide sensors needed for global protection.

PROTECTION FUNCTIONS

The requirements for the different protection functions (PF) are derived from analysis of the different systems that contribute to Machine Protection at ESS. Once the tolerable risk has been set and the necessary risk reduction estimated, the protection integrity requirements for the PF can be allocated in terms of Probability of Failure on demand (PFD) or Probability of Failure per Hour (PFH). The PFD and PFH correspond to one of the Protection Integrity Levels (PIL) specified in Table 1. Table 2 and 3 include the required Safe Failure Fraction (SFF) and the Hardware Fault Tolerance (HFT) that is required for each PIL.

Table 1: PIL Specified PFD and PFH

PIL	PFH (h^{-1})	PFD	MTBO (kh)
0	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-1}$ to $\leq 0,5$	10-100
1	$\geq 10^{-6}$ to $<10^{-5}$	$\geq 10^{-2}$ to $<10^{-1}$	100-1000
2	$\geq 10^{-7}$ to $<10^{-6}$	$\geq 10^{-3}$ to $<10^{-2}$	10^{3}-10^{4}
3	$\geq 10^{-8}$ to $<10^{-7}$	$\geq 10^{-4}$ to $<10^{-3}$	10^{4}-10^{5}
4	$\geq 10^{-9}$ to $<10^{-8}$	$\geq 10^{-5}$ to $<10^{-4}$	10^{5}-10^{6}

Table 2: Maximum Allowable Protection Integrity Level for a Protection Function with Type A Components

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	PIL1	PIL2	PIL3
60 % - <90 %	PIL2	PIL3	PIL4
90 % - <99 %	PIL3	PIL4	PIL4
≥ 99 %	PIL3	PIL4	PIL4

Table 3: Maximum Allowable Protection Integrity Level for a Protection Function with Type B Components

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	Not allowed	PIL1	PIL2
60 % - <90 %	PIL1	PIL2	PIL3
90 % - <99 %	PIL2	PIL3	PIL4
≥ 99 %	PIL3	PIL4	PIL4

When a partial analysis is made of a subsystem or element of a protection function, the preliminary requirements follow the Sensor-Logic-Actuator pattern typically adopted by functional safety standards. Based on industrial experience the following preliminary allocation of PFH/(PFD) is used:

- Sensor: 70% of overall PFH/PFD budget allocated for sensor systems.
- Logic: 10% of overall PFH/PFD budget allocated for logic systems.
- Actuator: 20% of overall PFH/PFD budget allocated for actuator systems.

Example of a Global Protection Function

Figure 1 shows an extract of the analysis done for vacuum sector gate valves that are distributed along the accelerator. A valve that is located upstream the selected beam destination can be damaged by beam if it is not fully open at the time of beam operation. In case the valve is located downstream the selected beam destination, it is not of relevance for Machine Protection whether it is fully open, or closed and its state is being ignored. Beam operation can start only if all relevant vacuum valves are detected to be in the open position and beam operation will be stopped immediately in case a valve is closing unexpectedly during beam operation. Table 4 summarises the requirements on the protection function including the requirement on how fast the function shall be executed (from detection to having stopped beam) and how reliable the function shall be (PIL). The requirements defined by a Protection Function are then handed over to relevant system owners who are responsible for implementing the Sensor/Detection part.

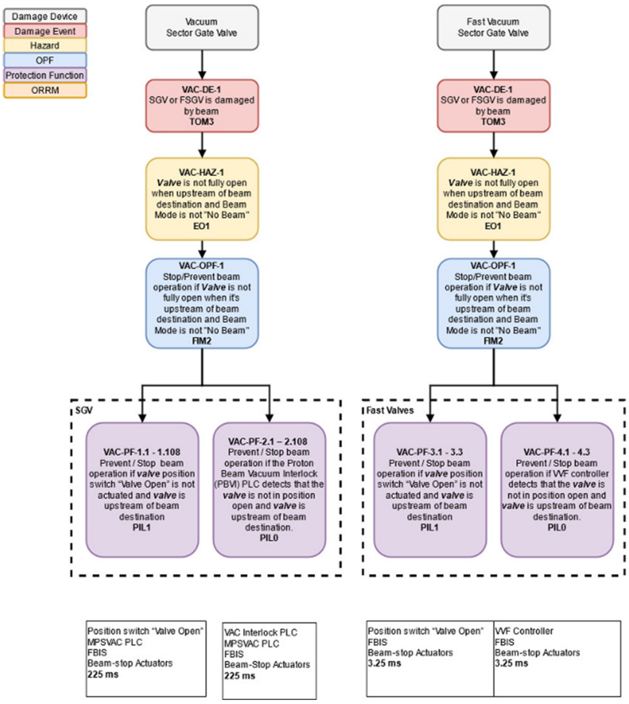
Damage Device
Damage Event
Hazard
OPF
Protection Function
ORRM
Vacuum Sector Gate Valve
VAC-DE-1 SGV or FSGV is damaged by beam TOM3
VAC-HAZ-1 Valve is not fully open when upstream of beam destination and Beam Mode is not "No Beam" EO1
VAC-OPF-1 Stop/Prevent beam operation if Valve is not fully open when it's upstream of beam destination and Beam Mode is not "No Beam" FIM2
SGV
VAC-PF-1.1 - 1.108 Prevent / Stop beam operation if valve position switch "Valve Open" is not actuated and valve is upstream of beam destination PIL1
VAC-PF-2.1 – 2.108 Prevent / Stop beam operation if the Proton Beam Vacuum Interlock (PBVI) PLC detects that the valve is not in position open and valve is upstream of beam destination. PIL0
Position switch "Valve Open" MPSVAC PLC FBIS Beam-stop Actuators 225 ms
VAC Interlock PLC MPSVAC PLC FBIS Beam-Stop Actuators 225 ms
Fast Vacuum Sector Gate Valve
VAC-DE-1 SGV or FSGV is damaged by beam TOM3
VAC-HAZ-1 Valve is not fully open when upstream of beam destination and Beam Mode is not "No Beam" EO1
VAC-OPF-1 Stop/Prevent beam operation if Valve is not fully open when it's upstream of beam destination and Beam Mode is not "No Beam" FIM2
Fast Valves
VAC-PF-3.1 - 3.3 Prevent / Stop beam operation if valve position switch "Valve Open" is not actuated and valve is upstream of beam destination PIL1
VAC-PF-4.1 - 4.3 Prevent / Stop beam operation if VVF controller detects that the valve is not in position open and valve is upstream of beam destination. PIL0
Position switch "Valve Open" FBIS Beam-stop Actuators 3.25 ms
VVF Controller FBIS Beam-stop Actuators 3.25 ms

Figure 1: Analysis overview for hazards related to vacuum valves.

Table 4: Example of a Protection Function for Vacuum Sector Gate Valves

PF ID	VAC-PF-1.1 to 1.111
PF Type	Global
Description	Prevent / Stop beam operation if ***Valve*** position switch "Valve Open" is not actuated and device is upstream of beam destination
Linked OPF	VAC-OPF-1 **Linked Hazard** VAC-HAZ-1
Sensor/Input	***Valve*** position switch" Valve Open"
Logic	MPSVac FBIS
Actuator	Beam stop actuator systems
PIL Requirement	PIL 1 **Timing Requirement** 225 ms
Comments	***Valve*** = Valve refers to any instance of the 111 VVS. The last number of the PF refers to a specific valve.

THE ESS BEAM INTERLOCK SYSTEM

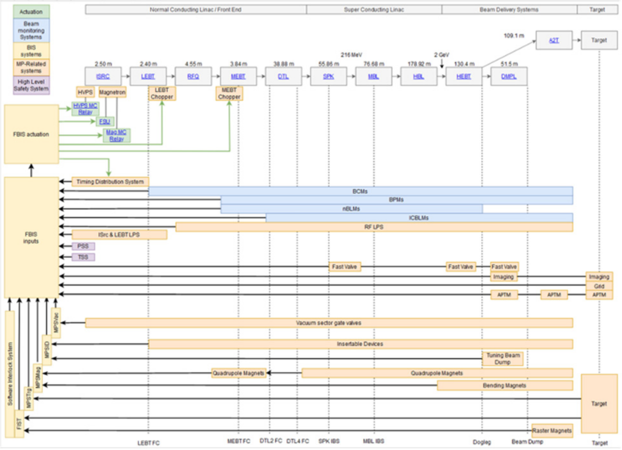

Figure 2: Overview on systems connected to the Beam Interlock System and their distribution.

Figure 2 shows an overview of systems in the ESS accelerator (and target) that are interfacing the Beam Interlock System and that are required to provide important protection functions. The ESS Beam Interlock System consists of the Machine Protection System for Magnets, Machine Protection System for Vacuum, Machine Protection System for Insertable Devices, Machine Protection System for Target, the Fast Beam Interlock System, the Fast Interlock System for Target, as well as the Software Interlock System. The Machine Protection Systems (4 in total) are based on PLC technology, requiring a reaction time of >10 ms and a Protection Integrity Level (PIL) 2. The Fast Interlock Systems (2 in total) are based on FPGA technology and require a reaction time in the order of a few ns to a few µs as well as a Protection Integrity Level (PIL) 2.

Figure 3 shows a more detailed overview on the distribution of the Fast Beam Interlock System (FBIS) across the facility.

The FBIS is the core system for Machine Protection at ESS and combines all input information into one global beam permit signal, that can be either OK or NOT OK (NOK). Depending on its state, the FBIS allows for beam operation or inhibits or stops beam operation.

It is the only system interfacing the different actuator systems used for Machine Protection that stop beam.

These actuator systems are the MEBT chopper, LEBT chopper, magnetron power supply, Fast Shutdown Unit, Timing System, and HV Power Supply of the Ion Source.

Whilst off the shelf equipment was used for the PLC based MP systems (safety PLCs), custom-made electronics had to be developed for the implementation of the FBIS.

Compliance with PIL 2 requirements for a custom-made system are a demanding, time consuming and resource consuming implementation but could be achieved for the ESS FBIS by now. The results have been thoroughly documented and the system is fully verified and validated against these requirements.

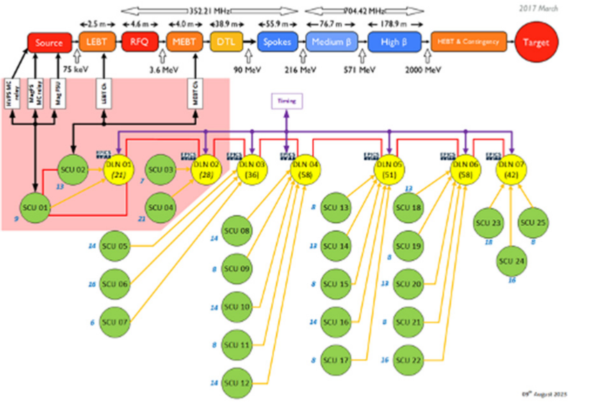

Figure 3: Overview on the distributed ESS Fast Beam Interlock System.

ESS BEAM INTERLOCK SYSTEM VERIFICATION

Functional Verification

After the System Requirement Specification (SRS) has been developed for a system, each of the individual system requirements are then broken down into a number of verifiable design specification items in a Detailed Design Specification (DDS) Document. The SRS and DDS items are linked through an SRS and DDS ID number for traceability. After all these design specification items are implemented in the system, they are verified in the various test reports which link from each test step back to the DDS item using the same ID number. This demonstrates that all detailed design specification items are implemented in the system, and that the system then fulfils all requirements. The requirements for which MPS are based on are the Machine Protection Capability Objectives (MP-G):

- 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 (MP-G-1).
- 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 (MP-G-2).

These two overall requirements are broken down into twelve Machine Protection General Requirements (MP-GR). The MP-GR are more specific than the MP-G. They describe in different ways how to fulfil MP-G-1 and MP-G-2. The MP-GRs together with PFs are translated into SRSs in the SRS document. They are specified in greater detail in order to determine how they shall be applied in the context of that system. The purpose of protection functions is to mitigate different hazards. The protection functions specify how a hazard can be detected and mitigated but not the exact details of how it shall be done. The detailed implementation and the equipment to be used for the implementation of the SRSs is specified in the DDS.

Electrical Hardware Verification

The electrical hardware is verified through the ESS engineering procedures and is reviewed in the process milestones Preliminary Design Review (PDR) and Critical Design Review (CDR).

The following hardware related document types are needed for the PDR:

- SRS - System Requirements Specification.
- Interface Control Documents - Documents with requirements and detailed information about interfaces to other systems.
- Interface Design Specifications - A summary of the MPS interfaces.
- Preliminary PIL Assessment - Either a written report or inspection of proposed solutions depending on complexity of PF, to provide input for choice of components, design architecture and/or functional requirements for the detailed design.
- Preliminary Hardware Design Documents - Cable database populated, component part lists, conceptual design

The following hardware related document types are needed for the CDR:

- SRS - System Requirements Specification.
- Interface Control Documents - Documents with requirements and detailed information about interfaces to other systems.
- Interface Design Specifications - A summary of the MPS interfaces.
- HRA - Hardware Reliability Assessment.
- Detailed Hardware Design Documents - Eplan Electrical design schematics, AVEVA E3D routing, 3D drawings, Power Phase balance, Cable & Conductor Calculations, 24V calculations, Fault loop impedance calculations, Power Dissipation. Additional type of schematics and calculations can be required depending on what needs to designed.

The following hardware related document types are needed for the Installation Readiness Review (IRR):

- FAT reports

The following hardware related document types are needed for the Test Readiness Review:

- SAT reports (Cable SAT, Rack SAT).

Validation

Beam operation of the facility, even with low power beam, is only possible if the minimum required MP-SoS protection functions are in place and validated. The constituent systems of the MP-SoS are developed and implemented according to the official ESS-schedule. The development and implementation follow the official ESS-schedule to make the different systems of ESS aligned and in sync with dependencies. The MP-SoS is assembled and commissioned continuously and iteratively as its constituent systems become available. The validation is performed step by step as well when the constituent systems or its prototypes are integrated into the MP-SoS. To validate and document that the MP-SoS meets the protection and operational requirements, a Final Integration Test (FIT) is made.

A demonstration of the system operating procedures is presented to all identified stakeholders in Operational Readiness Reviews (ORRs). The stakeholders then have access to all documentation, test specifications and test reports. The demonstration is carried out on the real system at the ESS site and covers the positive tests from the FIT.

Testing Activities

To fulfil the requirements for testing, work is done according to the standard described in SS-EN-62381:2012 – Automation system in the process industry – Factory Acceptance Test (FAT), Site Acceptance Test (SAT), and Site Integration Test (SIT) and ESS procedures for FAT and SAT.

In Fig. 4, a structure of the tests is shown. The figure shows in what order the tests are done and in which phase they are done in.

A test report is done through filling in a test specification. The test specification is made based on a template.

There is a specific template for each kind of equipment, as for example one for Signal Conditioning Units (SCUs) and one for Racks.

To verify hardware, software, and system the following tests are performed.

The hardware FAT is performed at the vendor site or at ESS, to verify that the vendor component meets the hardware requirements. The test is conducted on for example the different crates, as the FATs or the SCU crates.

The purpose of the software review is to reveal potential software design defects and avoid systematic failures.

The firmware test is to verify that the input and output logic is correct for firmware.

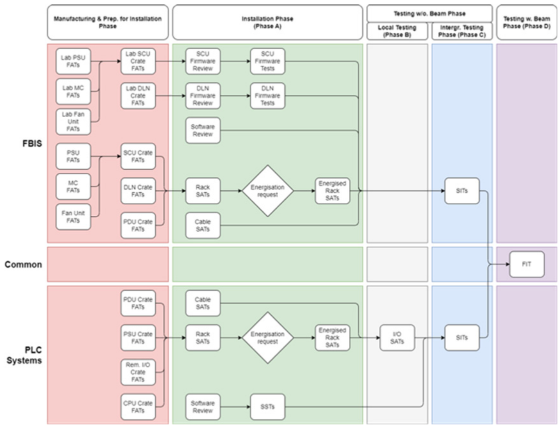

Figure 4: Structure of Tests.

The hardware SAT is performed at the ESS site, to verify that the equipment installed works as specified in its operational environment, that it meets the hardware requirements and has not got damaged during delivery to the site.

Note that this only verifies the MPS equipment itself and not the whole system which it shall protect.

Where it is reasonable, MPS does partial verification on the equipment one step up. The test is conducted on for example the MPS racks.

During the Software Simulation Test (SST), the software developer verifies the code in a simulation environment. The main verification objectives during SST are to verify compliance with the system requirements before going to the site integration testing. The verification is documented in a software simulation test report. Note that the software is not fully verified until the SIT.

The SIT is performed to verify that MPS meets the protection requirements and needs of stakeholders. During this test both the hardware and software are verified together.

The SIT covers the following:

- Normal operation for all proton beam destinations and proton beam modes.
- Abnormal operation situations. For example, operation with disabled redundancies, operation under heavy data traffic, etc.
- Interfaces to higher level control and other systems. For example, access over EPICS for configuration and debugging purposes.
- The FIT covers the following:
- Full chain testing for MP-SoS.
- Worst case timing situations. For example, switch-off requests with long signal paths from Sensor to Actuator systems.
- Machine protection tests with beam.

Non-Compliances

To track errors in tests, non-compliances are used. If there is a non-compliance item documented in the punch list in a test report and the error cannot be resolved directly, a fault description in the form of a Non-compliance report is made. The Non-compliance report is logged in the ESS documentation tool (CHESS). For tests not approved in the first test report a second test report is made in the already existing document in CHESS.

Test Overview Status

The tests that have been performed are tracked in an overview. The overview includes the status of the test specifications, test reports and information about the tested equipment (such as asset numbers).

Periodic Re-validation

System revalidation should be completed after major interventions or extended periods of shutdown to detect unintended changes or system degradation caused by intervention activities. Where possible automated test sequences will be developed to improve efficiency and repeatability of revalidation activities.

Proof Tests

Proof tests are periodic tests performed to detect dangerous hidden failures in the MPS systems so, if necessary, a repair can restore the system to a “good as new” condition or as close as practical possible.

The proof tests are a part of the HRA, which also determines the proof test intervals for the different components. The test procedures are determined by either:

- Manufacturer instructions.
- Tests based on the defined hidden failures in FMEDA analysis.
- Replacement of component.

Replacement Validation

When a component has broken down and is replaced or repaired, that component is re-validated. The re-validation of the component contains the same test points as during the commissioning; however, any software or firmware is not re-validated as there is no need to; but it is verified that the correct software or firmware revision has been deployed.

MP-SOS VERIFICATION OVERVIEW

Figure 5 shows the workflow that is being followed for the verification of systems that interface the Beam Interlock System and are part of MP-SoS.

In a first step it is required that the system owner of the interfacing system (e.g., Beam Current Monitors, vacuum system, magnet system) has locally verified the correct functioning of their implementation of the relevant protection function within their system. To ensure that this is done as smooth as reasonably possible, the MP team is reviewing the test specifications of the interfacing systems – with focus on verifying that related protection functions are appropriately covered in the test specifications. This approach of MP team checking test specifications has turned out to be highly beneficial for both teams: the team responsible of the system interfacing the BIS and the MP team.

In a second step the interfaces between a MP-SoS system and the BIS are verified. This is done through IO testing to ensure correct cabling and correct signal exchange between the systems (according to the interface control documentation).

In a third step the BIS systems are verified as described in the previous chapter (SIT). This is called MP-SoS SIT.

As a last step, a subset of the protection functions is tested in the Final Integration Test for full chain verification. This is done without beam and later on with beam.

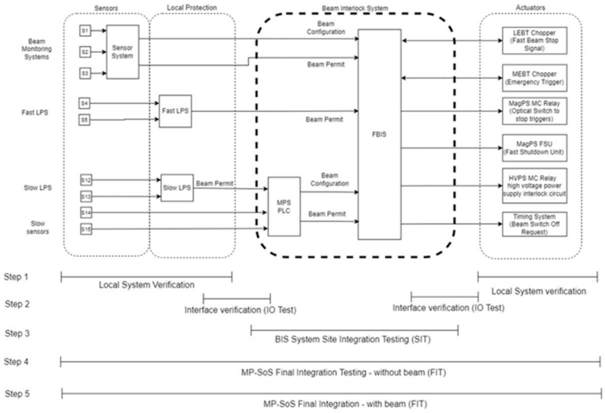
Sensors
Local Protection
Beam Interlock System
Actuators
Beam Monitoring Systems
S1
S2
S3
Sensor System
Beam Configuration
Beam Permit
Fast LPS
S4
S5
Fast LPS
Beam Permit
FBIS
Slow LPS
S12
S13
S14
S15
Slow sensors
Slow LPS
Beam Permit
MPS PLC
Beam Configuration
Beam Permit
LEBT Chopper (Fast Beam Stop Signal)
MEBT Chopper (Emergency Trigger)
MagPS MC Relay (Optical Switch to stop triggers)
MagPS FSU (Fast Shutdown Unit)
HVPS MC Relay high voltage power supply interlock circuit
Timing System (Beam Switch Off Request)
Step 1
Local System Verification
Local System verification
Step 2
Interface verification (IO Test)
Interface verification (IO Test)
Step 3
BIS System Site Integration Testing (SIT)
Step 4
MP-SoS Final Integration Testing - without beam (FIT)
Step 5
MP-SoS Final Integration - with beam (FIT)

Figure 5: Overview on MP-SoS Verification.

LESSONS LEARNED

Before the MP-SoS SIT is executed, a Test Readiness Review (MP-SoS TRR) is conducted. During this review, the following is being investigated and assessed:

- Are the test specifications from FBIS interfacing systems addressing correctly all tests needed to verify correct functioning of the protection functions that the system is supposed to implement?
- Have these tests been executed?
- Have all required test reports been created and filled correctly?
- Are all important punch list items resolved?
- Is the system ready for integrated testing?

Results from MP-SoS SITs during 3 Beam Commissioning Phases

So far, three different beam commissioning phases have been conducted, where Machine Protection was required.

These are:

- Beam to MEBT Faraday Cup (MEBT FC)
- Beam to DTL1 Faraday Cup (DTL1 FC)
- Beam to DTL4 Faraday Cup (DTL4 FC)

The results from the MP-SoS TRRs for these three phases in the sense of readiness of sensor, actuator and BIS systems, are the following:

- Phase 1 (MEBT FC) – 97% ready
- Phase 2 (DTL1 FC) – 80% ready
- Phase 3 (DTL4 FC) – 20% ready.

It is important to analyse why the percentage in readiness has dropped significantly over the course of these three phases, even though the scope and amount of newly interfacing systems had not significantly increased. The assessment and findings can be categorised and four major findings have been identified.

Lesson 1- Don't Aim too High and Ensure the Scope is Clearly Understood Instead

Stakeholders tend to become rather defensive and underestimate the scope of work to be done if asked about status in a certain and too simplistic way. It is crucial to understand how to phrase questions around readiness. If asking a system owner or stakeholder if they can be "ready" for an integrated systems test, then almost inevitably the answer will be positive, ie the question is not really manageable nor is it sufficiently specific for the purpose.

Therefore, it is considered important to assess and manage the achievable scope differently. It is not sufficient to rely on answers to simple questions, like "are you ready". It is important to develop detailed and precise check lists that focus on critical and most important functionality. Further, it is deemed important to defer any "nice to have" functions or scope and focus on "most basic and important" functions only. This requires a more detailed set of questions around readiness.

Lesson 2 – Be Very Transparent about Issues and Challenges

Stakeholders shall not assume that declaring readiness is just a formality or that ticking off a milestone on paper is sufficient. It is much more important to be honest and transparent about issues encountered, e.g., during local testing of systems. Don't allow others push you to declaring readiness just to make planners and managers satisfied. Any issue that is not getting the appropriate attention at the time required, will become an even bigger issue if being deferred to later.

It is vital to admit to issues and problems. It is important to develop a mindset that allows understanding that it is not a weakness to admit that tests and verification of functions are not done correctly – it is rather to be considered a strength to do so and that this kind of mind set actually will lead to real success on the long term. In case of ESS beam commissioning during the third phase, the non-readiness of several systems at the time of MP-SoS TRR did lead to the need of fixing the systems during the planned beam commissioning time, which consequently led to reduced beam time; beam time that was intended to being used for machine commissioning.

Lesson 3 – Don't Underestimate the Importance of Thorough Verification

Separating functions that go across many systems into smaller portions and testing these portions one by one has been of great benefit for ESS MP-SoS Verification. To test each portion of protection functions as allocated to single systems, thoroughly in the lab or other test environments before installing the systems on site has been proven to be vital for fast and effective commissioning. Whenever such thorough local testing in the lab or other test environment was done, the integrated testing and commissioning on site, once the systems were installed on site in their final location was done at a very high level of success in a very short time. Debugging and fixing was done quickly and efficiently.

Following basic systems engineering approaches from the beginning is very beneficial and saves time in the long run. This includes having system requirements in place, as well as design documentation, test specifications that can be traced back to the requirements and detailed design specifications of the system, and also clear and unambiguous written test documentation. Though it takes time to develop thorough and clear documentation, it will save significant time on the long term.

Lesson 4 – Know and Understand Your Stake-Holders

Try continuously to understand your stakeholders and try to understand how they see the world. Make an effort in understanding their situation; what are the issues in their teams? Do they have sufficient and competent support to do the tasks you require them to do for your purpose? Is their management aware of these (extra) tasks and is it supportive? How can you communicate better what is needed to be successful? Instead of having status progress meetings with your stakeholders consider visiting and inspecting the installations in the lab and on site on a regular base. Be in close contact with the people in the field and try to understand what blockers there may be and help resolving these early on.

CONCLUSION

Implementing highly complex but delicate and important systems like Machine Protection for a machine with high damage potential like ESS, where a huge set of interfacing systems has to be managed and orchestrated towards one common goal (i.e., machine protection), requires not only strong systems engineering approaches, thorough testing plans and verification campaigns, but also a good amount of awareness on the behavioural and psychological aspects that appear throughout the instantiation.

Due to the nature of Machine Protection requirements for complex machines, and the fact that one has to rely on systems to providing protection that are not designed for protection as their main purpose and that are managed by different teams with very different set-ups (in management, in budgets, in manpower, competence, etc.), the aspect of sensitive, discreet, diligent, and close stakeholder management seems to be much more important than originally anticipated.

The most important and relevant lesson learned from ESS MP-SoS perspective at this point in time seems to be around listening carefully and in an open-minded manner to the many stakeholders' issues with strong focus on understanding their challenges in detail; trying to identify supporting measures and provide that support, rather than trying to change their ways of working or enforcing a specific systematic approach – even if this is deemed most straight forward from an MP perspective.

REFERENCES

[1] T. Friedrich, C. Hilbes, and A. Nordt, "Systems of systems engineering for particle accelerator based research facilities: A case study on engineering machine protection", *IEEE Int. Sys. Conf.*, Apr. 2017. doi:10.1109/SYSCON.2017.7934806