ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-TUPHA101

APPLYING THE FUNCTIONAL SYSTEM INTERACTION PROCESS AT ESS

S. Kövecses de Carvalho†, R. Andersson‡, A. Nordt§, E. Bargalló¶,
European Spallation Source ERIC, Lund, Sweden
M. Rejzek‖, Zurich University of Applied Sciences, Winterthur, Switzerland

Abstract

The European Spallation Source ERIC is being built in Lund, Sweden to complement the existing neutron sources in Europe and worldwide. ESS will be the brightest neutron source ever built upon completion and aims to have an availability of 95% during steady state operations.

The purpose of Machine Protection at ESS is to protect the equipment in order to support the high availability. Due to the distributed nature of Machine Protection numerous design teams are involved to implement Protection Functions. The Machine Protection development at ESS follows the Functional Protection lifecycle for System-of-Systems developed at the facility. This paper focuses on the application of the Functional System Interaction Process part of the Functional Protection method.

To obtain the system interaction model, behavioural requirements and allocate Protection Functions, System Interaction Use Case workshops are held. The feasibility of different system architectures and protection function implementations are discussed and simulated by going through foreseen operational sequences, use cases. The different architectures and use cases are documented using Enterprise Architect.

INTRODUCTION

ESS

In 2014 the construction of the European Spallation Source (ESS) ERIC started in Lund, Sweden. ESS will be a user facility and 2000-3000 users a year are expected to visit in order to conduct neutron experiments. An important factor to make ESS attractive to users is the number of experiments that can be performed. The brightness of the source is vital for conducting experiments, as increased brightness shortens the experiment time. This in turn enables an increased amount of experiments to be conducted during the same time period. To achieve the high brightness a 5 MW proton beam will be sent to a four tonne tungsten target where neutrons will be created by spallation. An increased availability also increases the number of experiments that can be performed. ESS aims to have an availability of 95% during steady state operation [1].

The role of Machine Protection at ESS is to protect the machine against damage and unnecessary activation. Damage of equipment could lead to unplanned downtime, longer maintenance periods and increased cost. Activation of equipment could lead to premature failure and additional radiation cool down before maintenance. Machine Protection therefore supports the availability goals by protecting the machine [2].

ESS Machine Protection

The term "machine", in the context of ESS Machine Protection, includes all elements in the Accelerator, Target Station and Neutron Science Systems necessary for neutron production and neutron science experiments [3].

The Machine Protection objectives can only be achieved if a large number of systems, developed by different groups and divisions, interact in a well-orchestrated way. A systematic approach taking into account the independence of the systems, yet focusing on the emergent properties, is crucial for a successful Machine Protection implementation. This is why a System-of-Systems engineering approach has been selected [4].

Machine Protection at ESS can be divided into two main categories: local protection and global protection. A local protection function is a Protection Function where the sensor, logic and actuator chain is contained within the same system. A global protection function is a Protection Function where the sensor, logic and actuator chain is distributed over multiple systems. Global Protection Functions at ESS are often related to beam induced damage and beam loss [5].

The local protection is the responsibility of the system designer while the global protection is in the scope of the Machine Protection Group. Global Protection Functions tend to cut across different ESS divisions and systems. The Beam Interlock System (BIS) monitors the state of the machine and contains the main part of the global protection function logic. If a local protection system or BIS detects a state that might influence the proton beam in a way that causes a damage or activation risk to equipment, the proton beam generation is switched off in a controlled way to minimize damage and activation potential. The BIS is the only system at ESS that is purely dedicated to Machine Protection. All other systems have other primary purposes and implement Protection Functions in addition to their main functions.

FUNCTIONAL PROTECTION

What is Functional Protection?

Functional Protection is a technical risk management method suitable to apply on a System-of-Systems or other complex systems. The method was developed at ESS and can be integrated into the design and early commissioning phases of accelerator facilities to enhance their reliability

† szandra.kovecses@esss.se
‡ riccard.andersson@esss.se
§ annika.nordt@esss.se
¶ enric.bargallo@esss.se
‖ rejz@zhaw.ch

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-TUPHA101

and availability [6]. The method is compatible with IEC 61508 and 61511, the ISO standards 31000 and 16085 and originates from Functional Safety. As the name indicates it is applied to Protection rather than safety [7]. The Machine Protection design at ESS follows the Functional Protection lifecycle.

Functional Protection Lifecycle and Roles

Three teams are identified as vital for the Functional Protection Lifecycle progress; the Protection Analysis Team (PAT), the Integrated Protection Team (IPT) and the Implementation and Design Team (IDT), see Figure 1. The three groups have continuous interaction and follow ups during the lifecycle of the system. At ESS the PAT and IPT are fixed but the IDT varies depending on the analysed system.

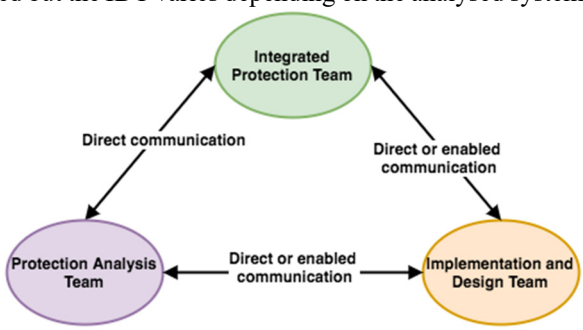

Figure 1: The three groups and their interactions as identified by the Functional Protection method [7].

The first step of the lifecycle is to have a clear concept and overall scope definition. Before any work starts it has to be clear what is in the scope of protection and to create boundaries for the analysis and integration.

The PAT is responsible for the Hazard and Risk Analysis, the Overall Protection Requirements and the Overall Protection Requirements Allocation. The analysis and integration work is mainly done in parallel, but it is beneficial to have access to a draft of the overall protection requirements and an idea of the architecture of the involved system (functional architecture) before starting the integration work.

The IPT defines System Interface Requirements, coordinates the System Interaction Use Case Analysis and defines System Interaction Protection and Behavioural Requirements. When the work of the two teams have reached a satisfying maturity, the IDT starts the implementation work.

The IDT plays an important role in the design and analysis phase by contributing with experience and judging the feasibility of different designs. The groups are involved in all lifecycle steps but are the main responsible for parts with the corresponding colour from Figure 1, as matched in Figure 2.

THE FUNCTIONAL SYSTEM INTERACTION PROCESS

System Interface Requirements

Before the work of the IPT starts, a representative for each protection relevant system has to be identified. The representative could be the designer, owner, or contact person for that system. The representatives are then gathered together with the IPT during a series of workshops.

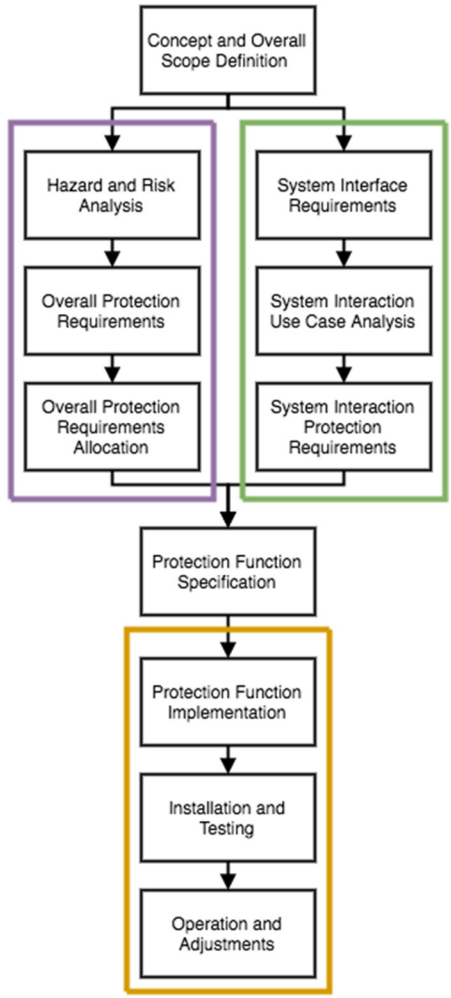

Figure 2: The Functional Protection lifecycle. All steps of the process are iterative and might need to be revisited multiple times.

During the workshops, the architecture, functionality and possible interfaces of each system are discussed. Based on the concept and overall scope definition, certain Protection Functions have to be performed. Depending on the level of progress of the development, the design and interfaces are more or less constrained. Typically, a more developed system is less flexible. This could cause difficulties if certain functions or hardware have not already been foreseen. When everybody has a clear view of the involved systems architecture, the allocation of Protection Functions is discussed. Questions such as, “Which sensors are available?”, “Where should the logic be implemented?”, “How is the information transmitted?” are asked and answered. A certain architecture and interface set is suggested and fixed for the coming System Interaction Use Cases.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-TUPHA101

System Interaction Use Case Analysis

The purpose of the Use Cases is to examine and document the intended interaction between the involved systems from a Machine Protection perspective. The goal is to derive appropriate and robust solutions for the signal types and interfaces. The Use Cases are one way to specify interfaces and requirements (especially with respect to Protection Functions), however they are not the unique source. The parallel work of PAT also results in a set of Protection Functions and requirements [8].

The Use Cases are set up to follow scenarios which will appear during regular machine operation such as a change of beam destination or a rearm after an interlock. Besides the "normal flow", which documents the operational scenarios as they are expected to happen, so called "alternative flows" are examined. Alternative flows document how the systems react if the scenario deviates from the normal flow. Typically, this is due to a fault or failure of a system or component. One or more use cases are selected and played through with the selected architecture.

During the use case studies, it may be identified that systems perform well as standalone systems but that the signal exchange with other systems is flawed or causes a different action than expected. This analysis may also derive additional interfaces that are then added to the system interface requirements.

During each of the lifecycle phases previously defined properties might need to be adjusted. This involves the architecture, the allocation of Protection Functions, system behaviour and interaction.

Normal Flow The first step is to make sure that it is possible to handle the case were everything goes as expected, the normal flow. Some systems might be able to perform their tasks very well on their own but encounter difficulties when they have to interact with other systems. The normal flow shows if all the necessary interfaces and functions are in place. The starting conditions and the end conditions of the use case are defined beforehand but the sequence of actions leading there is developed during the use case. It is important to check that all the necessary information is available to each system and that no deadlocks are created. The system representatives have an important role to provide input on how their system behaves. The actions, states and the information exchanges are mapped in a use case diagram.

Alternative Flow When the normal flow has been covered in a satisfying way, the alternative flows are studied. By studying the alternative flows, one can gain insight into the robustness of the system and about the vulnerable steps. The use case diagrams are a useful tool to gain understanding of the consequences of different failures. The system representatives have a vital role in this since they should have the best understanding of how their system reacts to unforeseen events.

Each action or information exchange failure would cause a different sequence of events. It is not feasible to go through every single alternative flow due to time constraints. Instead, a set of alternative flows are selected based on the events that are most likely to fail or events that seem to have the largest damage potential. The selection of alternative flows is done by estimations by the involved experts.

If unacceptable behaviour of the systems is observed due to a failure in the normal flow, it has to be adjusted. The normal flow should be adjusted to increase the robustness and decrease the vulnerability by changing the normal operational sequence.

System Interaction Protection Requirements

The system interaction protection requirements will, similar to the functional protection analysis technique, propose a set of Protection Functions. The requirements derived by the IPT are behavioural requirements. They are defined on the system level and based on the interfaces and interactions between protection-related and other systems. This analysis path completes the picture of the protection requirements in a way that is not possible through the damage-based analysis alone.

CASE STUDY OF A SYSTEM INTERACTION PROCESS

System Models

Due to the complexity of the equipment and systems used to operate ESS, the Machine Protection scope has to be separated into sub scopes. The sub scopes are selected to cover a certain type of devices or functions, i.e. Machine Protection System for Magnets or Beam Monitoring Systems. This is done to limit the number of people and functions to a manageable number. Each sub scope goes through the lifecycle of analysis, integration and implementation.

As mentioned previously, the first step is to discuss the architecture, functionality and possible interfaces of each system. A model containing a nonexclusive list of the state variables, functions and interfaces is made for each system to keep track of the properties.

System-of-Systems Models

When the step of creating system models is finished, a System-of-Systems model of the involved systems is created. This model includes interfaces and information flows between the systems, see Figure 3. The model is essential to create a mental overview and to take the step from standalone systems to a System-of-Systems. It is used as a template for the first System Interaction Use Cases. The first model is a draft and is typically revisited and updated multiple times.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-TUPHA101

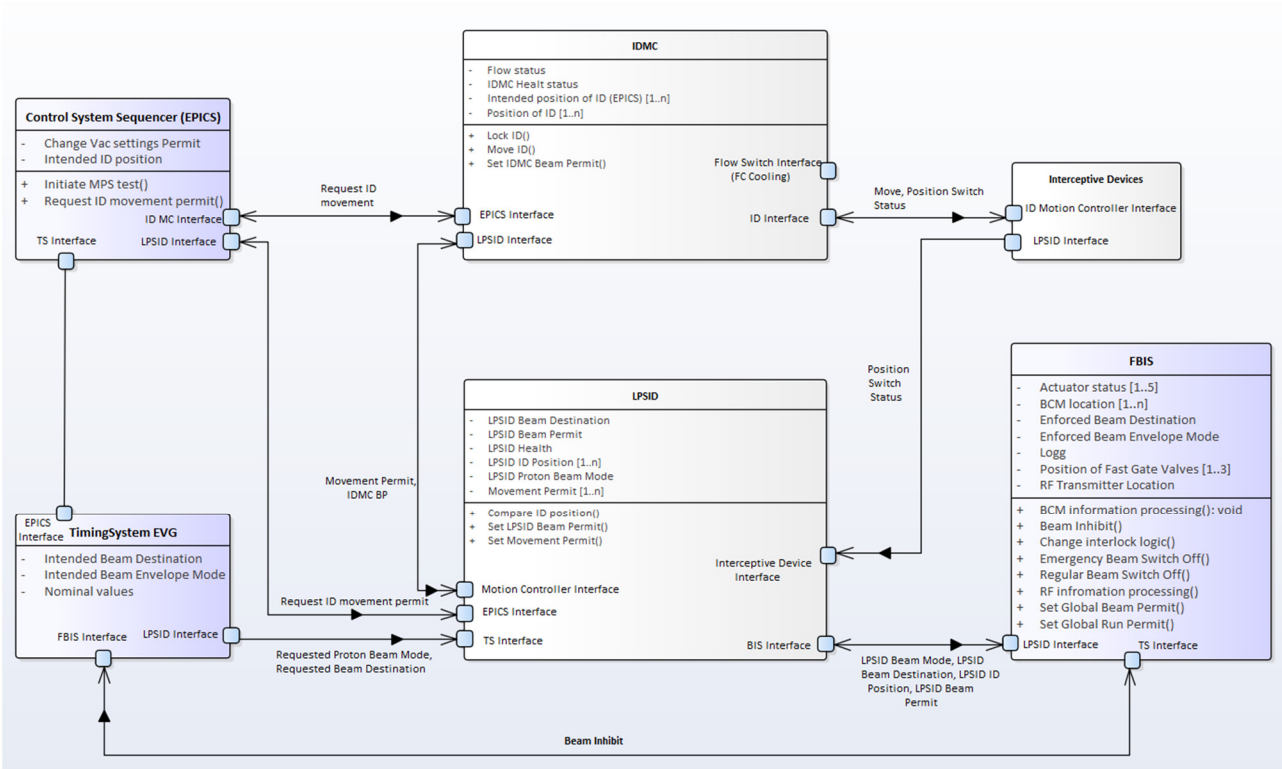

Figure 3: A model of the involved systems, their interfaces and the information flow.

System Interaction Use Cases

The use cases are represented in Enterprise Architect activity diagrams. The documentation of the Use Cases deviates from the typical models, which would be established when using UML/SysML. The decision to do so, is based on the specific circumstances at ESS. The diagrams are meant to be a tool used by a variety of people, many of whom are not familiar with these types of diagrams. In order to make the diagrams as intuitive as possible the formal usage has been traded for simplicity [9].

The systems or actors are represented as vertical swim lanes. Examples of actors are: The Control System Sequencer (EPICS), the Timing System Event Generator (EVG) and the Fast Beam Interlock System (FBIS). Activities are represented as rounded rectangles, where each activity is assigned to one and only one actor. As a consequence of that, activities are always in between a pair of swim lanes. The activities sequence is represented by arrows. The arrows sketch the flow of the use case, some of the arrows represent a physical signal while others may not. In certain cases, the flow splits into parallel activities and conversely parallel flows are joined to a single one. This is denoted with horizontal Fork and Join bars. Rectangles located at the top right of a swim lane are used to represent states and variables. The value of the Requested Proton Beam Mode for instance. Arrows to a state indicate a change of that state. Arrows from a state indicates that the state somehow affects the next action.

Similar facilities start by sending a low energy beam to an intermediate beam destination. As the tuning and the setting is done, the proton beam is sent to more and more distant beam destinations and finally to the target where neutrons are produced. One event selected for System Interaction Use Cases is the seemingly simple use case of changing the beam destination.

Inhibit Beam - Normal Flow

Before a Use case is started, the start and end conditions are defined. For the mentioned use case the starting conditions are: The machine is operating with Probe Beam sent to the Faraday Cup in Low Energy Beam Transport (LEBT-FC). The end conditions are: machine is operating with Probe Beam sent to the first Faraday Cup in Drift Tube Linac (DTL1-FC).

The use case consists of several larger steps; inhibiting the beam (preventing future beam pulses), reconfiguring the systems, reconfiguring the machine (hardware) and stop inhibiting the beam (enable beam pulses). Figure 4 shows the first part of the use case, the steps to inhibit beam.

When the operator requests to change beam destination, the Control System Sequencer starts a predefined sequence, where the first step is to “Request FBIS to inhibit Beam”. FBIS receives this request and updates the variable “FBIS Actuation State” and causes the Timing System to stop sending “Triggers”. The Timing System is transmitting the Requested Proton Beam Mode, Requested Proton Beam Destination as well as triggers. The triggers tell the receiving systems to act. Without triggers no beam is generated. FBIS is continuously checking if the Timing System is indeed “inhibiting”. When the Beam is inhibited the Control System Sequences initiate the next step.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-TUPHA101

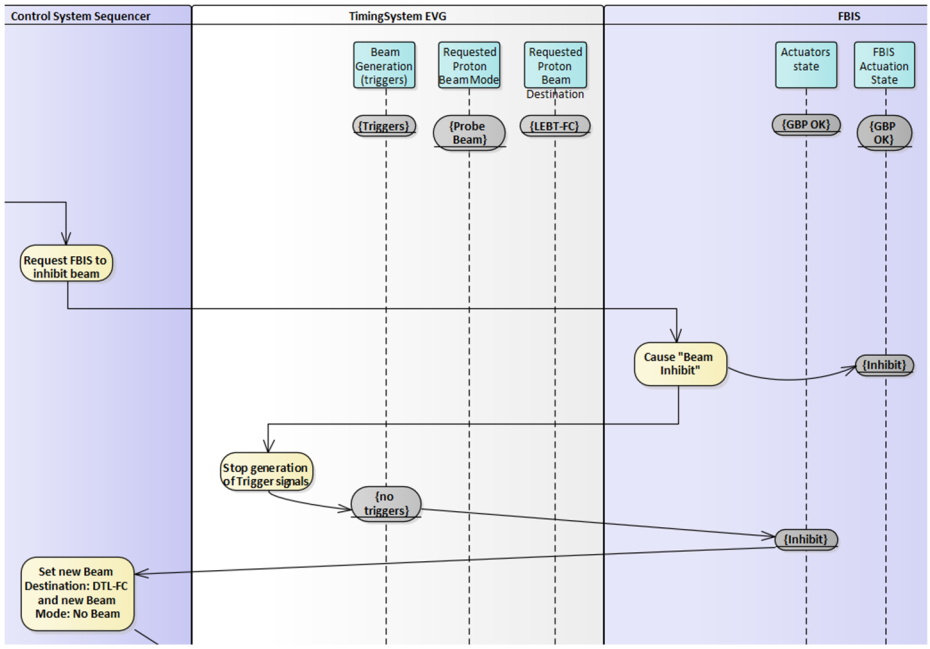

Figure 4: Inhibiting beam, the first steps of the use case "Changing beam destination".

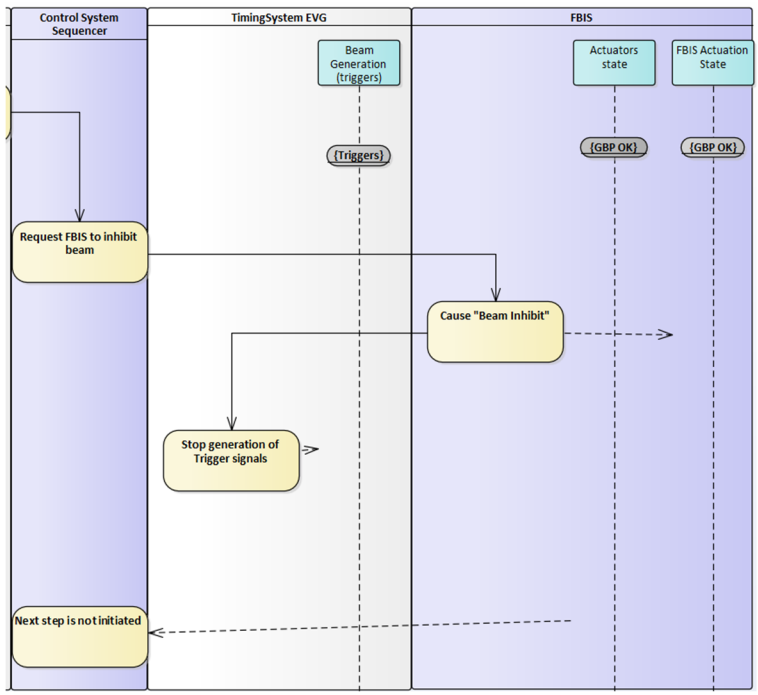

Figure 5: The alternative flow for the failure to inhibit from the normal flow shown in Figure 4.

Inhibit Beam - Alternative Flow

One of the Alternative flows selected for this use case is the event were FBIS fails to interpret the inhibit request correctly, Figure 5. The operator requests to change beam destination, the Control System Sequencer "Request FBIS to inhibit Beam". The FBIS does not update its internal "FBIS actuator state" and will as a consequence not cause the Timing System to stop the triggers. Since the Control System Sequencer is set up in such a way that the next step is not initiated unless the beam is properly inhibited the sequence of events stops here. This is the first level of protection, in case the Control System Sequencer fails as well and initiates the next step there are other levels of protection not shown here.

CONCLUSION

The Machine Protection Design at ESS is complicated by multiple factors. The distribution of protection among systems drives a System-of-Systems approach. The Functional Protection lifecycle is well suited as a method for this and the System Interaction Process provides tools to identify gaps in system interaction and to find behavioural requirements of the involved systems.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-TUPHA101

REFERENCES

[1] ESS Home Page, https://europeanspallationsource.se/about/, 2017.

[2] Riccard Andersson, Annika Nordt, and Erik Adli. Machine Protection Systems and Their Impact on Beam Availability and Accelerator Reliability, paper MOPTY044. *Proceedings of IPAC2015*, 2015.

[3] C. Hilbes, A. Nordt, T. Friedrich, ESS Machine Protection Concept (short version), *ESS Internal Document, ESS-0035197*, 2015.

[4] A. Nordt, C. Hilbes, T. Friedrich, Machine Protection - Systems Engineering Management Plan, *ESS Internal Document, ESS-0057245*, 2016.

[5] Szandra Kövecses, Machine Protection Glossary, *ESS Internal document, ESS-0124263*, 2017

[6] Riccard Andersson, A Machine Protection Risk Management Method for Complex Systems, Ph.D. thesis, Phys. Dept., University of Oslo, Oslo, 2017. (to be published).

[7] Riccard Andersson, Enric Bargalló, and Annika Nordt. A Functional Protection Method for Availability and Cost Risk Management of Complex Research Facilities. Submitted to *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering*, 2017.

[8] Riccard Andersson, Enric Bargalló, Szandra Kövecses, Annika Nordt, Christian Hilbes, and Martin Rejzek. Development and Status of Protection Functions for the Normal Conducting Linac at ESS, paper TUPIK079. *Proceedings of IPAC2017,* Copenhaguen, Denmark, 2017.

[9] Rejzek M., Machine Protection Benchmark Use Cases, *ESS Internal Document (to be published)*, 2017.