Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P6420-cd

Hardware integrity assessment of the distributed Fast Beam Interlock System (FBIS) at the European Spallation Source (ESS)

Joanna Weng, Martin Rejzek, Silvan Fluri and Christian Sommer

Zurich University of Applied Sciences (ZHAW), Switzerland.
E-mail: wenj@zhaw.ch, rejz@zhaw.ch, flun@zhaw.ch, some@zhaw.ch

Johannes Gustafsson

European Spallation Source (ESS), Sweden.
E-mail: johannes.gustafsson@ess.eu

The European Spallation Source (ESS), a cutting-edge research facility under construction in Lund, Sweden, is designed to be the world's brightest neutron source. The Fast Beam Interlock System (FBIS) is a critical component for ensuring the integrity and protection of the ESS facility. Designed and built by the Safety-Critical Systems (SKS) group at the Zurich University of Applied Sciences (ZHAW), in collaboration with the Machine Protection System (MPS) team at ESS, the FBIS is mainly responsible for stopping the beam when technical problems with the ESS machine or beam anomalies are detected. The FBIS thus plays an essential role in ESS machine protection and is the logic solver element of most protection functions. To ensure the high reliability of the FBIS, a comprehensive analysis was conducted in accordance with the IEC 61508 functional safety standard to assess its hardware integrity. This reliability analysis played an important role in ensuring proper and uninterrupted operation of ESS. This paper presents the analysis methodology developed and outlines the steps necessary to verify the hardware integrity of this complex, distributed system. This includes the calculation of the Probability of dangerous Failure per Hour (PFH) and the evaluation of the architectural constraints by calculating the Safe Failure Fraction (SFF) and Hardware Fault Tolerance (HFT) of the system. These calculations are based on failure rate predictions using the Siemens SN 29500 standard. In addition, a detailed Failure Modes, Effects and Diagnostic Analysis (FMEDA) was performed. The analysis demonstrates that the FBIS meets the corresponding hardware integrity requirements. The developed methodology has been successfully applied to several hundred protection functions at ESS. An example reliability analysis of a complete protection function containing a sensor system and actuators is also shown.

Keywords: Beam interlock, Reliability Prediction, FMEDA, RBD, IEC 61508, Functional Safety, Hardware Integrity Assessment

1. Introduction

The European Spallation Source (ESS), under construction in Lund, Sweden, is designed to be the brightest neutron source worldwide. Ensuring the safety and reliability of such a large facility is paramount due to its complexity and operational demands. The Fast Beam Interlock System (FBIS) is a central component of the facility's Machine Protection System (MPS), which is responsible for stopping the beam of the proton accelerator in case of machine anomalies or technical issues. Developed collaboratively by the Safety-Critical Systems (SKS) group at ZHAW and the Machine Protection System team at ESS and built at ZHAW, the FBIS serves as the logic solver for various protection functions. This paper describes the reliability analysis methodology developed together by the SKS and ESS group and used to verify the MPS hardware integrity in compliance with the IEC 61508 functional safety standard, focusing on the FBIS reliability analysis.

2. Machine Protection at ESS

The aim of Machine Protection (MP) at ESS is to monitor the state of the machine and stop beam operation if a state that can cause damage is detected. Due to the physical distribution, the

complexity and diversity of the systems involved in the machine protection, the system of systems (SoS) approach has been selected for developing and implementing Machine Protection at ESS. The ESS Machine Protection System of Systems (MPSoS) consists of around 35 (sub)systems. The sensors used detect the state of the machine and the logic interpreting them are distributed across multiple components of the MP. The central component of the machine protection is the beam interlock system (BIS). The BIS collects the sensor inputs from the protection-relevant systems and the ESS timing system, and triggers a beam stop if required. The FBIS is part of the BIS and stops the beam by directly interfacing the beam-stop actuators. Due to the complexity of the various systems within the MPSoS and the ongoing construction and upgrades of ESS, this analysis has been underway for five years and contributed to the safe commissioning of the machine sections already completed.

2.1. *Fast Beam Interlock System (FBIS)*

The FBIS is a crucial part of MPSoS and acts as an observer. It only reacts when it detects a deviation of its inputs from the expected state or when it detects an FBIS internal inconsistency or failure. The majority of input signals to the FBIS are Beam-Permit and Ready signals reflecting the states OK and NOK. Depending on the physical type of interface, the FBIS may detect signalling errors (such as disconnected cables or short-circuits for example). Also, mode consistency is verified by ensuring that all systems are configured to the same operational mode, such as "beam on target." From a logical viewpoint, an erroneous signal is treated similarly to a signal having the state “NOK”, as both inputs should result in the protected state. The systems that request a beam switch-off using a Beam Permit or Ready signal are referred to in the following as “Sensor Systems”.

In case a deviation is detected, FBIS acts on the Beam Stop Actuator Systems (e.g., LEBT/MEBT chopper) by requesting a Beam Inhibit or Regular Beam Interlock. The FBIS checks whether the Beam Inhibit and the Regular Beam Interlock functions have been successfully carried out, i.e., whether the beam has been deflected and the beam production stopped. If a Beam Inhibit or Regular Beam Interlock fails, the FBIS escalates to an Emergency Beam Interlock. In this case the FBIS can act on additional actuation systems.

In the following, a brief overview of the FBIS architecture is given: The FBIS is subdivided into segments. The segmentation is motivated by the physical layout of the ESS facility and by the beam line sections. Each FBIS segment is composed of two principal system component types:

- Decision Logic Nodes (DLN), and
- Signal Conversion Units (SCU).

Each segment is composed of multiple of these system components. Typically, one DLN and several SCUs. The DLN and SCU system components consist of system modules (SMOD, for example, power supply). A simplified overview showing multiple segments, DLNs and SCUs, is shown in Figure 1.

2.2. *Protection function requirements*

The protection functions are an outcome of the machine protection analysis at ESS, a modified version of (Andersson et al. 2019). The analysis is based on a hazard and risk analysis of possible damage events related to a specific system. The damage events are then linked with their inherent hazards on a high level without going into specific failure scenario details if not necessary. Each hazard is allocated a corresponding overall protection function (OPF), which is carried out through a set of technology-specific protection functions (PF). The requirements for the different protection functions are derived from the analysis of the different MPS systems. 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

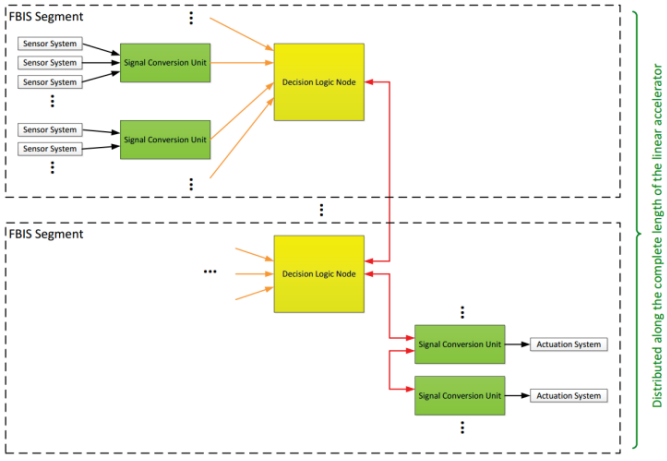

Figure 1: Graphical representation of FBIS signal chain.

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). The quantitative requirements on integrity against random hardware failures for Machine Protection are derived from the IEC 61508 (IEC 2010) standard, with slight adjustments, as shown in Table 1.

Table 1: Definition of PIL requirements on PFH and PFD.

PIL	PFH (1/h)	PFD
0	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-1}$ to < 0.5
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$

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 ESS uses the following preliminary allocation of PFH/(PFD):

- 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

Also, the architectural constraints, as defined in the IEC 61508 standard, are considered for the assessment of the protection functions.

The aim of the reliability analysis was to show that the protection functions defined for machine protection meet the defined PIL targets.

3. Machine Protection Hardware Reliability Assessment Methodology

In the following the workflow, methodology, standards, chosen tools and data sources used for hardware reliability assessment are described. The Isograph software (Isograph Inc 2019) is used for the reliability assessment. It combines several state-of-the-art analysis techniques and tools into one consistent workflow that is applied to all components of the complex ESS machine.

3.1. *General assumptions*

The following points summarise the general assumptions used in the analysis.

- If a failure occurs, it is assumed that on average it will occur at the mid-point of

the test interval. In other words, the fault will remain undetected for 50% of the test period.
- The analysis assumes constant failure rates and therefore the effects of early failures are expected to be removed by appropriate processes.
- Components are not operated beyond their useful life thus ensuring that failures due to wear-out mechanisms do not occur.
- It is assumed that the requirements stated in equipment safety manuals (if applicable) have been adhered to.
- When a diagnostic coverage is assigned to the dangerous failures, it must be ensured that the diagnostic coverage is properly analysed, so that the failure is detected and hazard mitigated within acceptable time period. Where this is not possible it should be assumed that there is 0% diagnostic coverage.

3.2. *Data sources*

To determine the failure rate of each subsystem and its elements, different data sources may need to be chosen depending on the type of component and the information available. Depending on the data source, the failure rates and failure mode ratios may be very different. The challenge is here that ESS is built collaboratively by in-kind partners in different countries and reliability data is often not available. To ensure that calculations made by ESS and its in-kind partners are based on the same values for the same type of components, a selected list of common data sources with the following prioritization should be used:

- Priority: Manufacturer data
- Priority: SN29500 (Siemens 2010)

3.3. *Reliability prediction methods*

The following methods are typically used for reliability prediction:

- **Part-Count:** A conservative approach by assuming part stress levels in their failure rate models that are significantly higher than most accepted de-rating policies / practices.
- **Partial Part-Stress:** An analysis that assumes average stress levels based on company design policies.
- **Full Part-Stress:** A technique that requires knowledge of the stress levels on each part to determine their failure rates. Depending on the type of component different stress factors are considered.

Starting from the Bill of Material (BOM), the Part-Count and the Partial Part-Stress technique is used to determine the failure rate. During the full-part stress determination, the different operating conditions are broken down into stress level dependence factors that will affect the failure rate. The failure rate for assemblies under operating conditions is calculated as follows:

$$\lambda = \sum_{i=1}^{n}(\lambda)_i = \sum_{i=1}^{n}(\lambda_{ref} * \pi_U * \pi_I * \pi_T * \pi_E * \pi_S * \pi_{ES} * \pi_Q * \pi_{PS})_i \quad (1)$$

Where:

- λ - Failure rate at operating conditions
- λ_{ref} - Reference failure rate
- π_{U}- Voltage stress level dependence factor
- π_{I} - Current stress level dependence factor
- π_{T} -Temperature stress level dependence factor
- π_{E} - Environmental stress level dependence factor
- π_{S} - Switching rate stress level dependence factor
- π_{ES} -Electrical stress level dependence factor
- π_{Q} - Quality dependence factor
- π_{PS} - Power stress level dependence factor

The stress level factors listed here are typical stress level factors used for MP. The Part-Count technique assumes average stress levels. Since no specification has been made for the ambient temperature of the accelerator tunnel, the π_T is set

to a temperature of 60° C. For the other areas, the local ambient temperatures are used.

Ideally, the Part-Count technique is applied early in the design phase to determine that the predicted reliability is in the "ballpark" with reliability requirements. As more detailed design information becomes available, such as detailed circuit schematics, the predictions are refined where necessary to reflect applied component stress levels. In some cases, the manufacturers of a component provide pre-calculated data. In those cases, the prediction calculation is skipped. This is mainly the case for the safety certified components such as a safety PLC. Where possible we use the Isograph Reliability workbench SN 29500 module for the calculation. The module implements all sections (1 through 16) of the Siemens SN 29500 standard. The module includes the failure rates and all formulas needed to do a full part-stress calculation for all the included component types.

For component types that are not covered by the SN 29500 standard, or where the quality of the component is very different of what is defined in SN 29500, assumptions and manual calculations are made where possible.

3.4. *Failure Modes, Effects, and Diagnostic Analysis (FMEDA)*

A Failure Modes, Effects, and Diagnostic Analysis (FMEDA) is a structured qualitative method used to systematically identify, document, and prioritize potential functional failure modes within selected modules and components. The analysis begins with quantitative failure data for each part, organized hierarchically into subsystems or functional blocks. Each part's failure modes are mapped to the next higher level, culminating in system failures at the top level. Dangerous failure modes leading to the loss of required functions are identified, and their failure rates are estimated. Subsequently, the probability of detecting internal failures through automatic on-line diagnostics (diagnostic coverage) is determined, which is vital for maintaining reliability, especially in complex or standby systems. To ensure that calculations made by ESS and its in-kind partners are based on the same values for the same type of components, a selected list of common data sources with the following prioritization is used (Table 2).

Table 2: Priority list for failure mode data sources, including EN 61709 (IEC 2017), FMD (Quanterion 2016) and IEC 62061 (IEC 2005).

Priority	Failure modes data source
1	Manufacturer data
2	EN 61709:2017
3	FMD-2016
4	IEC 62061:2005

3.5. *Reliability Block Diagram (RBD) modelling*

ESS has decided to use the modelling form of reliability block diagram (RBD) and use Isograph – Reliability workbench for the modelling. A RBD is a diagrammatic form to model the set of events that must take place and conditions which must be fulfilled for a successful operation of a system or a task. The target of the analysis is represented as a success path consisting of blocks, lines and logical junctions. A success path starts from one side of the diagram and continues via the blocks and junctions to the other side of the diagram.

A RBD is a structural representation of the modelled system, similar to an electrical circuit. When the current finds a path from the input to the output, the modelled system is working properly, when the circuit is cut the modelled system is failed. This leads to the concept of minimal cut sets which represent the combinations of failures (i.e., places where the RBD is "cut") leading to the failure of the modelled system. The RBD can be transformed to an equivalent fault tree with the same minimal cut sets. Each block in the model represents a component of the system with a failure rate or a component/system function with the corresponding failure rate. The blocks are

modelled either in series or parallel paths or a combination of both with junctions at specific points. Parallel paths are redundant, meaning that all the parallel paths must fail for the parallel network to fail. A network with several parallel paths can have different voting schemes, the junction after the parallel paths decides the voting scheme of the network and decides how many of the paths need to fail before the network fails.

4. Reliability Analysis of the FBIS

A reliability prediction is performed for all FBIS modules, while a detailed FMEDA is performed only for selected modules. The failure modes that lead to a failure of a function are identified and a distinction is made between dangerous and safe failures. Whenever a detection of the failure mode considered is implemented, this is credited. Credit is given for automatic on-line diagnostics performed by the FBIS itself as well as automatic tests performed outside of the FBIS. The latter need to be properly implemented by the system integrator.

If there are multiple failure modes for the same component (for example a resistor), all modes are considered together with the percentage each failure mode contributes. The data sources are for the apportionment of failure modes are determined following Table 2.

For the SCU Mezzanine Cards (MC), which are the interface to the Sensor and Actuation systems, the SCU and the DLN, the failure rate is determined using a detailed FMEDA. Each block analysed with the FMEDA provides the total failure rate as well as the amount of dangerous (detected/undetected) failures. Based on these results, a RBD model of the FBIS is implemented. The RBD structure reflects the physical FBIS architecture. Each function needed for the FBIS operation is modelled by one RBD block. The obtained failure rate from the reliability prediction or FMEDA is then allocated to the considered function, thus the corresponding RBD block. Redundancies are modelled by parallel paths. In the final step the minimal cut sets, the importance and the total PFH for the FBIS are calculated

Where no detailed FMEDA was performed, a division of failures into 50% safe and 50% dangerous is assumed. This procedure is recommended as generally acceptable for complex components by IEC 61508. As default a MTTR of 8 hours, a proof test coverage of 100% and a generic overhaul interval of 1 year (8760 hours) is chosen for the calculations. A specific overhaul interval is not specified for each component in Isograph. The general recommendation is here to replace each component at latest a few years before its MTBF or the period of “useful life” compared to the general industrial norm (up to 30 years). For the test Interval one year is assumed. IEC 61508 requires considering Common Cause Failures (CCFs) when evaluating the reliability of a subsystem in a redundant setup. A CCF analysis with Isograph was performed, leading to a β factor of 2% that is applied for all modules in the redundant channels A and B.

The FBIS RBD including all results from reliability prediction and FMEDA is quantified and the PFH for the switch-off function of the FBIS is determined. The FBIS is compatible with the ESS requirement for a PIL2 logic system of 10^{-7}/h (10% of 10^{-6}/h), with a PFH of $9 \cdot 10^{-8}$/h.

5. Reliability Analysis of complete MP Protection Functions

The MP-SoS connects to a large number of different systems, some with several hundred devices that need monitoring to ensure safe operation of the facility. The facility has a wide range of different types of function, from monitoring of water flow in cooling systems, where standard safety components can be used, to custom made systems that monitor the proton beam parameters and behaviour. Each system, for example a sensor system or an actuator system, is analysed separately, where the highest requirement determines how detailed the analysis needs to be for the different elements.

Where possible, a set of standard safety components is used. For example, one of the protection functions that is used to ensure that one of the systems is sufficiently cooled is using SIL rated transmitters, a signal conditioner and PLC equipment. In this case, a RBD is created for the sensor sub-system with the data provided by the manufacturers, see Figure 2.

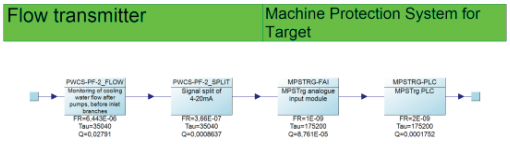

Figure 2: RBD example for a flow monitoring sub-system.

Many systems use custom made electronics, sensors etc, in these cases, a failure rate prediction using the SN29500 standard is made.

Where needed, a detailed FMEDA is performed to determine the SFF. When all elements and sub-systems have been analysed, a "full-system" RBD is done for each protection function, where all the different sub-systems are combined.

6. Analysis Example of ESS Protection Function

In this example of a full machine protection function, the Beam Current Monitors (BCM) are used to measure the proton beam current, pulse length, and repetition rate. The proton beam is switched off if any of the configured proton beam parameters are exceeded. The full protection function consists of the BCM sensor sub-system, the FBIS logic sub-system and the LEBT chopper sub-system as actuator. Each of the sub-systems were analysed separately and the PFH and SFF of all individual elements were analysed according to the developed methodology.

6.1. *Sensor sub-system*

The BCM sensor system comprises multiple modules, all of which must be included in the analysis. The sensors consist of two AC Current Transformers (ACCTs) with integrated front-end electronics. Designed specifically for charged particle beam measurements, the ACCTs can detect macro pulse currents as low as 1 mA AC. The ACCTs provide a ±10V analogue signal to the ACCT Interface Module (AIM), where the signal is split and distributed to two mTCA-based systems. In these systems, the Rear Transmission Module (RTM) serves as the input module, while the Advanced Mezzanine Card (AMC) functions as the logic module, also handling output signals. These output signals are the processed and converted to the RS485 format, before further transmission to the FBIS.

6.2. *Logic sub-system*

The FBIS model needs to be adjusted to only include the relevant parts for the specific protection function. The first step is to determine the signal chain for the protection function (Figure 3):

1. BCM sends two redundant signals (purple arrow) to a RS485 MC in SCU01.
2. The SCU sends the summary of the signals through redundant S-Link (black arrow) to the DLN01.
3. The DLN evaluates the signals from all SCUs and sets the status of the OPL (orange arrows).
4. The SCU02 reads the incoming OPL status and sets the output OPL to the same status.
5. The choppers that are connected to SCU02 are activated and deflect the proton beam.

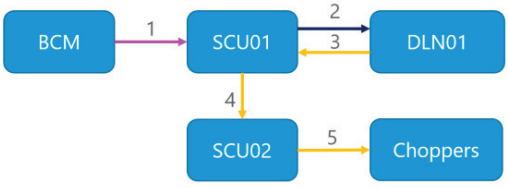

Figure 3: Representation of FBIS signal chain.

6.3. *Actuator sub-system*

The final element is the LEBT chopper, which when used as an actuator for the machine protection system, deflects the proton beam into a beam dump. The LEBT chopper consists of two redundant low voltage control modules each with a separate power supply and each of the modules sends signals to the high voltage supply which activates the chopper plates that creates the magnetic field that deflects the proton beam. The RBD of the LEBT chopper is shown in Figure 4.

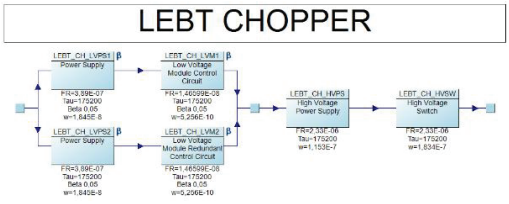

Figure 4: Example RBD of the LEBT Chopper.

6.4. *Full protection function*

Once all subsystems have been integrated into the final RBD, the overall PFH can be determined. Additionally, the architectural constraints, including SFF and HFT, are derived from the results of each subsystem. The analysis of this example protection function confirmed that both the PFH and architectural constraints comply with the PIL2 requirements. In total, approximately 1300 different protection functions, some with identical functionality but different components, must be analysed. This analysis is an ongoing process, continuously evolving to align with construction progress and accommodate design changes in the ESS facility.

7. Conclusion

The developed hardware reliability assessment methodology was applied successfully on the ESS machine protection, including the FBIS. The ESS machine protection is a complex system of systems with around 35 (sub)systems and around 1300 protection functions, some with the same functionality but different components, and is essential for ensuring safe beam operation at ESS. The assessment presented in this paper has been ongoing for over five years, following the construction of the accelerator at ESS and being continuously adjusted and improved. The assessment utilised failure rate predictions following the Siemens SN29500 standard, detailed Failure Modes, Effects, and Diagnostic Analysis where required, and detailed Reliability Block Diagram modelling. The methodology proved to work reliably, identifying cases where redesigns or additional functionality were required. The analysis confirmed that the FBIS meets the quantitative Performance Integrity Level requirements, while the ongoing assessment of protection functions has already validated compliance for hundreds of them. The results of this continuously evolving, extensive analysis contributed to the safe and reliable operation of the already completed, commissioned, and tested sections of the ESS machine.

References

Andersson, R., E. Bargalló, and A. Nordt (2019). A Functional Protection Method for Availability and Cost Risk Management of Complex Research Facilities. *ASME J. Risk Uncertainty Part B* 5(3), 031002.

International Electrotechnical Commission IEC (2010). IEC 61508: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems (Part 1 to 7).

Isograph Inc (2019). Isograph Reliability Workbench V14.0.

Siemens AG (2010). SN 29500: Failure Rates of Components. München: Siemens AG

International Electrotechnical Commission IEC (2017). IEC 61709: Electronic Components – Reliability – Reference Conditions for Failure Rates and Stress Models for Conversion.

Quanterion (2016). FMD-2016 Databook.

International Electrotechnical Commission IEC (2005). IEC 62061: Functional Safety of Safety Related Electrical, Electronic and Programmable Electronic Control Systems.