A MODIFIED FUNCTIONAL SAFETY METHOD FOR PREDICTING FALSE BEAM TRIPS AND BLIND FAILURES IN THE DESIGN OF THE ESS BEAM INTERLOCK SYSTEM

R. Andersson*[1, 2], A. Monera Martinez[1], A. Nordt[1], E. Bargalló[1]
[1] European Spallation Source, Lund, Sweden
[2] University of Oslo, Oslo, Norway

Abstract

As accelerators are becoming increasingly powerful, the requirement of a reliable machine protection system is apparent to avoid beam-induced damage to the equipment. A missed detection of a hazard is undesirable as it could lead to equipment damage on very short time scales. In addition, the number of false beam trips, leading to unnecessary downtime, should be kept at a minimum to achieve user satisfaction. This paper describes a method for predicting and mitigating these faults, based on the architecture of the system. The method is greatly influenced by the IEC61508 standard for functional safety for the industry and implements a Failure Mode, Effects, and Diagnostics Analysis (FMEDA). It is suggested that this method is applied at an early stage in the design phase of a high-power accelerator, so that possible protection and mitigation can be suggested and implemented in the interlock system logic. The method described in this paper is currently applied at the European Spallation Source and the results follow from the analysis on the Beam Interlock System of this facility.

THE BEAM INTERLOCK SYSTEM

The Beam Interlock System (BIS) at the European Spallation Source (ESS) receives around 300 beam permit input signals and needs to stop beam operation in as short as 4-5 µs for some sections after detection of an error in the proton linear accelerator (linac) [1]. The requirement is based on possible damage from the high proton beam power on the surrounding sensitive equipment. The time scale requirement for the BIS is combined with a need to stop the beam in a reliable way, avoiding both false beam trips (stopping the beam without a hazard) and blind failures (missing to stop the beam when there is a hazard). By meeting these requirements, the BIS can help reaching the reliability goals for ESS and at the same time spare the equipment of any unnecessary damage.

There are four types of modules in the BIS at ESS. Together, they resemble a combined tree and star structure for a reliable transfer of the beam permit signal from the inputs to the actuators. Fig. 1 shows a conceptual flowchart of the BIS, disregarding the actual structure for simplicity. The BIS consists of close to 300 Fast Beam Interlock Driver (FBI_D) and Device Interface (FBI_DIF) Modules. For redundancy, each input signal goes to two FBI_DIFs. These modules interface with all input signals and transmit a beam permit signal to the BIS. Each signal into the BIS will be propagated through redundant links over the entire signal path. Table 1 displays nominal reaction times for the different modules in the BIS together with an example of the input signal from a Beam Current Monitor (BCM) and the LEBT chopper actuator. The table considers a worst-case scenario in terms of required reaction times. As is seen, if the modules perform as designed, the BIS achieves a total reaction time of less than 3 µs in the low energy part of the linac.

The rack configuration at ESS contains 24 enclosures with 36 racks each. All the signals from one rack enclosure are grouped into one pair of Master modules (FBI_M), making 48 FBI_M in total. The 48 FBI_Ms connect into two redundant Master of Master modules (MoM) located at the front end of the linac. These two MoMs then connect to three different Actuator Modules (FBI_A) – one for each actuator: Proton Source, LEBT chopper, and MEBT chopper. The FBI_As deliver the final trigger signal to the actuators to stop the beam, by deflecting beam to an absorber by the choppers, and inhibiting the creation of plasma in the proton source [2]. The BIS position in the Machine Protection (MP) conceptual level is seen in red in Fig. 2.

Figure 1: The BIS (red) transmits the input beam permit signals from the monitors and sensors to the actuators, which stop the beam in case of a hazard.

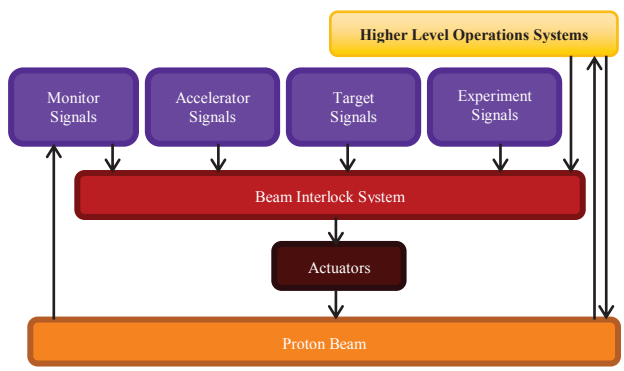

Figure 2: The BIS (red) role in the Machine Protection concept.

* riccard.andersson@esss.se

ISBN 978-3-95450-148-9

RELIABILITY ANALYSIS OF THE BIS

The reliability analysis of the BIS was made in two distinct parts. The first part consists of a Failure Mode, Effect, and Diagnostics Analysis (FMEDA) for each BIS module, described below. This part follows to a large extent the approach used for the Large Hadron Collider at CERN [3]. The FMEDA was done using a set of spreadsheets for module and component overview and easy backtracking. The second part uses Reliability Block Diagrams (RBD) on the system level using BlockSim from ReliaSoft [4] to obtain the overall BIS reliability figures.

Table 1: An Example of BIS Detection, Processing, and Reaction Times.

Module	Reaction Time	Accumulated Time
BCM	1 µs	1.0 µs
FBI_DIF	500 ns	1.5 µs
FBI_M	250 ns	1.75 µs
FBI_A	300 ns	2.05 µs
MEBT Chopper	300 ns	2.35 µs

FMEDA

The ESS BIS FMEDA involves (a) identifying the components of the four BIS modules, determine their (b) functionality, (c) failure rates, and (d) failure modes, (e) identify the components' impact on the module as a whole, and (f) find the diagnostic ability to detect the failures. The FMEDA process was launched in the mid 90s as an upgrade of the original Failure Mode and Effect Analysis (FMEA), developed in the 60s and 70s for the US Military Standards. It is a method that has grown increasingly popular in reliability engineering since its introduction.

The (a) components and (b) their functionality are extracted from the design of the circuit boards together with the designer. For the (c) failure rates and (d) modes, the US Department of Defense Military Handbooks 217F and 338B [5] were consulted, which provide failure rates per component and their failure mode allocation, respectively. In the cases where the component manufacturers provided failure rates from accelerated tests, these were used instead. The identification of (e) the components' impact on the module together with (f) the diagnostic abilities of the system is an iterative process together with the system designer in order to reach a satisfactory level of protection. An overview of the inputs and outputs of an FMEDA is seen in Fig. 3. It should be clarified that this process typically brings system flaws into light already at the first iterations and the system design itself is improved continuously throughout the FMEDA steps. Where applicable, the diagnostic coverage

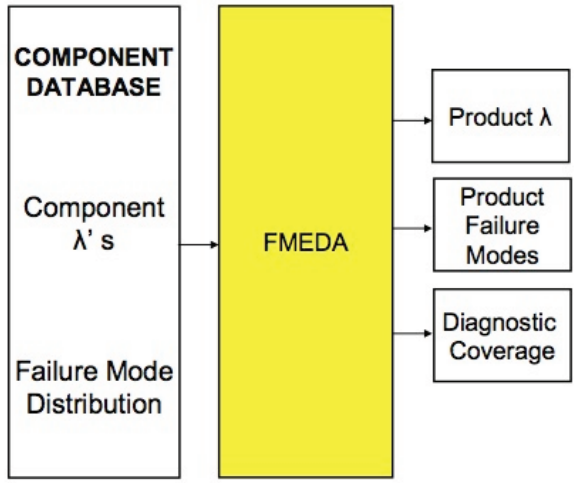

Figure 3: FMEDA inputs and outputs. Source: [6]

of the system can be enhanced in order to foresee and mitigate hazards before they cause the system to fail, as is seen in Fig. 3 where it is displayed as an output of the FMEDA.

From steps (a) through (f) above, the overall failure rates for the four different BIS modules are obtained, and these rates are then used in a system-level analysis using BlockSim. Four failure modes were identified as having impact on the system design and to be dealt with, being (in order of criticality) Blind, Trip, Maintenance, and Negligible. Blind means a blind failure where the system is unable to mitigate a hazard, Trip is a false trip where the beam permit is withdrawn erroneously, Maintenance means that the system can continue to operate under marginal protection but the component needs to be maintained "as quickly as possible", and Negligible means that the failure mode has no apparent effect on the system.

The diagnostic ability (f) was also divided into four different modes, being related to the failure modes and using the same color code. This way, one can easily get an overview of a failure mode's ability to be mitigated by the system's design and find possible flaws by quickly scrolling through the FMEDA spreadsheets. The diagnostic abilities are Test, Diagnostics, Inspection, and Hidden. Here, the Test is an internal test loop that checks the beam permit signal paths for faulty components, Diagnostics is the built-in diagnostic feature in the circuits able to detect anomalies in components, Inspection means that personnel has to go and inspect the component, and Hidden means that the error can not be seen without rigorous demounting and troubleshooting.

Reliability Block Diagrams

BlockSim allows for RBD or Fault Tree Analysis (FTA) approaches to be used for complex systems, in order to analyze reliability measures through both analytical computation and simulation. The BIS was modeled with RBDs to resemble the system behavior. Each module type received its failure rates through the FMEDA described above. As each block in the software

ISBN 978-3-95450-148-9

can only represent one failure mode, one system setup was created for each of the four failure modes. By altering the connections and number of input signals per module, it was possible to analyze different designs for optimum performance of the system. The system was analyzed for no redundancy at all, redundant links (as is the current design choice) and for a 2-out-of-3 voting design throughout the system (not included in this paper).

THE ESS AVAILABILITY GOALS

ESS aims for unprecedented beam availability for neutron production, which places high demands on all systems involved. The BIS is the central system in avoiding major damage to the beam pipe and surrounding equipment, which causes long downtimes, and needs to avoid false beam trips, which cause short beam trips and unnecessary downtime. This demands an almost fault-free system that always premieres stopping the beam over a hazard of damaging equipment.

Protection Integrity Levels

The IEC61508 standard [7] includes so-called Safety Integrity Levels (SIL) that define the level of which a certain Safety Function (SF) reduces the probability of a safety hazard. These concepts are both applicable and manageable in the ESS MP work, but as MP only uses the standard to a fractural extent and is mission critical rather than safety critical, the concepts are modified to fit the needs and processes of the MP development work. As MP deals with protection, the Protection Integrity Levels (PIL) are introduced together with Protection Functions (PF) that play the same role as their safety counterparts in the analysis [8].

The PF for avoiding Blind failures at ESS needs to reduce the failure rate to 10^{-6} per hour, or the equivalent of once in 114 years. This failure rate has then been allocated to three different major systems: the sensors, the BIS, and the actuators. The sensors are expected to contribute with 35%, the BIS with 15% and the actuators with 50% to the overall PF. That leads to a Blind failure rate requirement for the BIS of $1.5 \cdot 10^{-7}$. The BIS then has to be designed to reach this hardware failure rate [1].

As stopping the proton beam does not introduce any potential for damage, the false Trip rate is related to the overall ESS reliability and availability requirements [9] and its determination lies outside the scope of this paper. In general, however, one can find that the Trip rate is increased as the Blind rate is decreased, as the two are opposites in the realm of MP.

ANALYSIS RESULTS

Analysis Assumptions

The analysis was carried out assuming only hardware failures with 12 input signals per rack enclosure and 24 rack enclosures, giving a total of 288 signals and the same number of FBI_D and FBI_DIF. Each enclosure also has one redundant FBI_M pair and there is one redundant pair of MoMs, adding up to a total of 50 FBI_M. Finally, there are 3 FBI_A, one for each actuator.

Further, it is assumed that all actuators must trigger a beam stop signal and are thus modeled in series. Two prototype designs were considered, named Prototype 0.1 and 0.2. There were two simulations run for each prototype, one without redundant links and one with redundancy.

The component environment is taken to be at 40°C and 45-60% humidity to avoid corrosion, condensation, and static electricity build-up. The components are considered to be mounted in a fixed rack configuration.

Results

Fig. 4 shows the analysis results for the four setups. The bars are explained in the caption of the figure. A non-redundant system does not reach the required failure rate and needs further redesign. In this analysis, a redundant system was considered, which does still not reach the requirement for the initial design, but does so for the second prototype design.

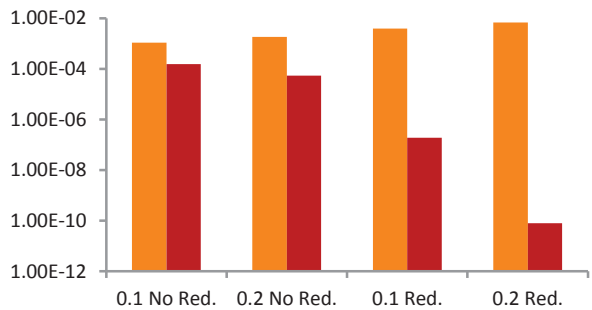

Figure 4: False trip (orange) and blind (red) failure rates for four different BIS designs. From left to right: Prototype 0.1 without redundancy, Prototype 0.2 without redundancy, Prototype 0.1 with redundancy, and Prototype 0.2 with redundancy.

BIS Design Features and Changes

While the current BIS design contains redundant links throughout the system, the option of a 2-out-of-3 voting system was analyzed. However, this also brings a cost issue into the design, as the component costs would increase by 50%. The FBI_Ms also have the ability to mask certain input signals, meaning that specific signals can be completely ignored for a predefined time. While this can increase system reliability in the case of certain components sending spurious signals to remove beam permit, there is also an associated risk with making certain inputs blind that has not yet been analyzed.

The iterative FMEDA process highlighted the weakest links in the BIS layout, being the FBI_A. These modules were a main cause of system-level Blind failures and the redesign of the system lead to intra-module redundancy that removed the Blind failures. A similar approach was carried out for the FBI_M where the Blind failure rate

ISBN 978-3-95450-148-9

was drastically decreased. The schematics were also separated into different parts separating for example permit signals from test loops and diagnostics. This gave a better overview of the system as a whole and allowed for more efficient troubleshooting.

It should be clarified that the analysis in this paper only considers hardware failures in the BIS. How surrounding equipment, software and firmware, and configuration failures affect the system are not part of the analysis. The same goes for the potential for failures associated with masking. As testing and fault injection are still to be performed for the BIS, the results described here should be viewed as theoretical on the conceptual design level.

EXTENSION TO OTHER SYSTEMS

The analysis performed in this paper is developed in a generic way and is not system-specific. This way, the FMEDA can be extended to other systems at ESS and at other facilities. The intension is to widen the analysis to include all the systems that feed signals into the BIS (purple boxes in Fig. 1 and 2) and the actuators (brown box in Fig. 1 and 2). This way, one would be able to determine the overall reliability from a signal, e.g. a beam loss, to the action of stopping the beam. This plays a central role in fulfilling the ESS reliability and availability goals and pinpoints the weak links that need to be improved further in the signal chain.

CONCLUSIONS

The development and actualization of the FMEDA together with the system-level RBD analysis of the BIS at ESS described in this paper have allowed for important design improvements throughout the iterative process. These improvements are fundamental to reach the high reliability and availability goals of ESS. It is important to note that these studies should be done at an as early stage as possible in the design process of the system, to avoid expensive and cumbersome changes last minute or even during operation.

The results show how a hardware failure rate of $1.5 \cdot 10^{-7}$ for the BIS can be achieved for Blind failures on a system level, at the same time as reliability is kept at a manageable level. By introducing a BIS with redundant links for the entire signal chain, the hardware failure rate requirement is reached without the need to introduce more expensive system designs.

ACKNOWLEDGEMENTS

We would like to thank Christian Hilbes and the Safety Critical Systems Research Team at ZHAW in Zürich, Switzerland for their contribution in the concept design of the Machine Protection at ESS. The analysis in this paper is greatly influenced by the similar study done at CERN, and therefore we want to thank Benjamin Todd, William Viganò, and the Beam Instrumentation Group there. Lastly, the University of Oslo has been of great support academically and financially for the work described in this paper.

REFERENCES

[1] Nordt, Annika, et al., "Development and Realisation of the ESS Machine Protection Concept", TUC3O03, these proceedings, ICALEPCS 2015, Melbourne, Australia (2015).

[2] Monera Martinez, Angel, et al., "Overview and Design Status of the Fast Beam Interlock System at ESS", MOPGF138, these proceedings, ICALEPCS 2015, Melbourne, Australia (2015).

[3] Todd, Benjamin, *A Beam Interlock System for CERN High Energy Accelerators*, PhD thesis, School of Engineering and Design, Brunel University, West London, UK, CERN-THESIS-2007-019 (2007).

[4] ReliaSoft website, "BlockSim: System Reliability and Maintainability Analysis Software Tool"; http://www.reliasoft.com/BlockSim/ (Accessed: October 2015).

[5] U.S Department of Defense, "Guide for Achieving Reliability, Availability, and Maintainability: Systems Engineering for Mission Success" (2005); http://www.weibull.com/mil_std/RAM_Guide_080305.pdf

[6] Picture taken from: http://www.exida.com/Resources/Whitepapers/ FMEDA-Accurate-Product-Failure-Metrics. Accessed: 2015-10-01.

[7] International Electrotechnical Commission, "Functional safety of electrical/electronic/programmable electronic safety-related systems", IEC 61508:2010, CENELEC, Brussels, Belgium (2010).

[8] Kwiatkowski, Maciej, *Methods for the Application of Programmable Logic Devices in Electronic Protection Systems for High Energy Particle Accelerators*, PhD thesis, Warsaw University of Technology, Warsaw, Poland, CERN-THESIS-2013-216 (2013).

[9] Bargalló, Enric, et al., "ESS Reliability and Availability Approach", MOPTY45, IPAC2015, Richmond, Virginia, USA (2015).

ISBN 978-3-95450-148-9