OVERVIEW AND DESIGN STATUS OF THE FAST BEAM INTERLOCK SYSTEM AT ESS

A. Monera Martinez, R. Andersson, A. Nordt, M. Zaera-Sanz, ESS, Lund, Sweden
C Hilbes, ZHAW, Winterthur, Switzerland.

Abstract

The ESS, consisting of a pulsed proton linear accelerator, a rotating spallation target designed for an average beam power of up to 5 MW, and a suite of neutron instruments, requires a large variety of instrumentation, both for controlling as well as protecting the different hardware systems and the beam. The ESS beam power is unprecedented and an uncontrolled release could lead to serious damage of equipment installed along the tunnel and target station within only a few microseconds. Major failures of certain equipment will result in long repair times, because it is delicate and difficult to access and sometimes located in high radiation areas. To optimize the operational efficiency of the facility, accidents should be avoided and interruptions should be rare and limited to a short time. Hence, a sophisticated machine protection system is required. In order to stop efficiently the proton beam production in case of failures, a Fast Beam Interlock (FBI) system with a targeted reaction time of less than 5 microseconds and very high dependability is being designed. The design approach for this FPGA-based interlock system will be presented as well as the status on prototyping.

INTRODUCTION

The team in charge of ESS Machine Protection is facing a great challenge: design, deploy and operate a Beam Interlock System (BIS) needed to protect the machine from beam-induced damage. The unprecedented beam power of 5MW at ESS can lead to severe damage within 10-20 microseconds only and thus beam operation has to be stopped reliably in an even shorter time upon the detection of non-nominal beam conditions. Such non-nominal beam conditions will be detected by several beam instrumentation systems such as the Beam Current Monitoring System, the Beam Loss Monitoring System and the Beam Position Monitoring System. The BIS shall fulfil demanding requirements regarding the hardware failure rate and beam availability as well as the requirements for the very short response time of a few microseconds. There are only four years to develop, test, produce and install the whole system. First commissioning of the ESS linac is planned for the beginning of 2018, and a first version of the BIS has to be ready by then. First protons on target are expected in mid 2019.

In a first step, the possible failure modes of the accelerator systems have been analysed. This analysis has been used to define around 170 different protection functions needed to protect the linac from beam induced damage, directly or indirectly. For each of these protection functions, an execution time has been defined as well as the required rate of dangerous failures. The highest rate for a function found is of 10^{-6} to 10^{-7} failures per hour with a response time of 5 microseconds (including the detection, processing and execution time) [1].

SYSTEM SPECIFICATIONS

In order to design a Beam Interlock System it is important to understand the system requirements and specifications. The design of the BIS is following the IEC61508 [2] and the IEC61511 [3] standards where applicable. However, since the BIS is a mission critical system and not a safety critical system, it is not needed to be compliant with those standards. Still, the team felt, that it is good to follow the guidelines provided by these standards in order to achieve a good level of protection thanks to the solid framework that the standards offer.

The following selected specifications allow to have a clear picture of what is expected:

Remote Monitoring: The BIS should be able to inform about its status and in case problems occur, operators shall be notified or an alarm shall be raised. For that it is required that the BIS will be connected to the main control system (EPICS) for monitoring and parameterization purposes.

Fast response time: the fast reaction time of the BIS is resulting from a time allocation which is done for a full protection function. A protection function includes time to detect a non-nominal condition of the machine, to process this information, to propagate and inform the BIS, process the information on BIS level and initiate a stop of beam operation. The fastest reaction time found for a protection function is 4-5 microseconds implying a reaction time of the BIS below 2-3 microseconds. This time differs for different beam energies along the linac and is only valid for the low energy part of the linac and can be relaxed for higher beam energies. Hence the Beam Interlock System will be called the Fast Beam Interlock (FBI) System. In order to achieve this reaction time the development of an FPGA-based system is required.

High availability: The FBI System should not interrupt the beam operation unnecessarily. One of the main requirements for the ESS facility is to deliver beam with very high availability. Thus, it is needed to keep downtime and false beam stops due to failures in the FBI System at a minimum. Hence the FBI System should be highly reliable as well as highly available.

Protection: The FBI System shall fulfil the requirement of a dangerous failure rate of 1.5×10^{-7} to 1.5

ISBN 978-3-95450-148-9

x 10^{-8} per hour. This requirement is based on a first risk analysis [1].

Number of Inputs: The number of inputs towards the FBI System will be in the order of a few hundred signals (~300), randomly distributed in a 600m long gallery (where the electronics is located). The final number of inputs is currently under investigation. However, it is not expected that this number will significantly increase.

The Environment

Initially underestimated by many, the environment in which the system is located plays an important role when defining the system's architecture and its distribution. All the electronics needed to operate the accelerator will be installed in the so called Klystron Gallery at ESS. This gallery is very close to the accelerator to keep the cable length at a minimum. Racks will grouped in two rows of 18 racks each and a group of 36 racks will be housed in an enclosure which is cooled, fulfilling the high temperature stability requirements for the RF system. There will be approximately 24 enclosures for ~800 racks in total. Due to the confinement of these enclosures and requirements for each of them, it could be difficult to distribute cables in and out. It is important to have this factor in mind when defining the location for the different electronics.

Additional non-physical factors like electromagnetic noise impact on the performance level of a system. The FBI System should be designed in a way that this noise doesn't damage the electronics and doesn't impact on the beam availability of the accelerator. Special attention will be given to the selection of cables and connectors, focusing on shielding and good noise immunity but not compromising price and installation cost significantly.

TRADITION VS TECHNOLOGY

Collaboration with many institutes has allowed us to get hold on already developed interlock systems, designed by experienced teams during many years and with proven functionality. The idea of developing a BIS in a short time reinforces the strength of such collaboration and offers the possibility of doing a fast development adapted to ESS needs. On the other hand, new technologies will allow tailor-made solutions for ESS at the cost of lack of reputation and longer time to develop and test.

PROTOTYPES UNDER DEVELOPMENT

Two main ideas are currently being developed, both based on the same principle: Interface modules will allow a wide variety of electronic devices to connect to the FBI System, concentrators will aggregate the signals to simplify and minimize the number of traces and a main master module that will decide if the beam operation has to be interrupted or not.

The FBI System will receive a boolean signal from the Local Protection Systems (LPS) and from Beam Instrumentation (BI) systems indicating if beam operation should be permitted or not. This boolean signal will be the "Beam Permit" signal. Upon removing this signal, beam operation will be stopped immediately by the FBI System.

Copper-based System

Following the approach that CERN took for their Beam Interlock Systems deployed at LHC [4], LINAC4 and other machines at CERN, ESS will build a similar system following the main design concepts of the CERN Beam Interlock System. This system is based on DC signals, a modular design and very reliable electronics.

Figure 1: CERN Interface Module (CIBU) (left), Beam Interlock Controller (right).

Designed for VME form factor, this system was designed not only to be very robust mechanically and electronically but also to be operated safely in radiation areas [5].

The ESS version of this system will have slight changes in the architecture in order to be accommodated to the ESS Klystron Gallery distribution and the size has been reduced to fit the restricted dimensions without compromising the mechanical strength.

The FBI System will be composed of the following:

The FBI Device Interface (FBI_DIF) will receive the first size reduction and higher integration count, aggregating into a 1U unit up to 8 interfaces without losing availability or protection integrity level. The electronic used will be very similar to the original CERN electronics keeping a wide input range (from 3.3V to 36V) allowing an easy connection, for PLC and FPGA based systems.

The FBI Master (FIB_M) and FBI Master of Masters (FBI_MoM) will undergo major re-design. The form factor will be changed from VME to MicroTCA (or Pizza box) and aggregation from 16 to 32 inputs into a single crate depending of the master location, is foreseen.

The FBI Actuator module (FBI_A) has been designed following ESS requirements. A redundant input and redundant signal path within the actuator are used to avoid dangerous failures. In addition, diagnostics have been implemented to supervise the behaviour together with redundant power supplies and a discrete critical path (no programmable devices on the permit path) ensuring high availability.

An example of the connector chosen and the mechanical redesign is shown in Fig. 2.

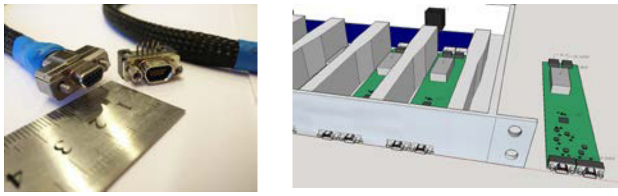

Figure 2: Micro D connector cable for the FBI System (left), 3D model for the FBI Interface module (right).

In order to fulfil the required dangerous failure rate, the FBI System will be installed in a redundant configuration. However, due to restrictions on budget and space limitation in the accelerator, the Input devices will not be redundant, only the FBI System will be, offering redundancy from the FBI_DIF up to the Master of Masters. The FBI_A will act as a final, simple but very robust concentrator that will use both permits to turn the actuators on and off when needed.

Furthermore, to avoid single points of failures at the inputs of the FBI System, the Local Protection Systems and Beam Instrumentation systems shall offer a redundant output independently connected from the CPU or FPGA that processes the main protection function.

A small diagram of the system's architecture can be seen in Fig. 3.

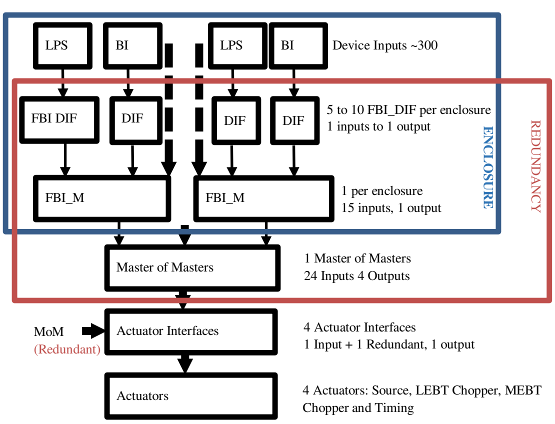

Figure 3: Schematic of the Fast Beam Interlock System based on copper connections.

A recent Failure Mode, Event and Diagnostics Analysis (FMEDA) [6] has been performed for the first engineering model of the FBI System. The results of this analysis show that the system with minimum firmware and redundant channels would offer 1 dangerous failure within 450 years while keeping the false beam trips to less than 3 per month and a reaction time of less than 2 microseconds excluding delays induced by cables.

In addition to the hardware and mechanical modifications made to the CERN System, an extra level of protection has been added to ensure full system functionality and reduce likelihood of blind failures even more.

Self-Testing Functionality

In order to ensure that the FBI System is ready to allow for beam operation, a self-test will be implemented and executed before each beam injection. This test will force the FBI System and input devices to prove their ability to transmit a non-permit command from the protection function to the FBI Master of Masters. Using this self-testing sequence, it would be possible to find dangerous failures on the FBI System itself but also at the input devices.

Due to time restrictions and to minimize the system blindness, this test should be only applied to the FBI System itself and to FPGA-based systems but not to the PLC based systems, which have a slower reaction time.

In addition, this test sequence will be realized on different time scales for each channel. That means, that at all times, only one out of two channels is in test mode.

Additional System Tests

Two additional tests will be used in order to ensure the full functionality of the whole FBI System.

Slow Test: This test will be initiated by the timing system when there is no beam in the machine. The test will virtually generate all the events that can trigger a protection function ensuring the correct behaviour of all elements that form part of every protection function. This test would be scheduled after each technical stop to warranty the protection integrity.

Actuator Test: This test will be executed after the Slow Test but with minimal beam power. During this test the Master of Masters will generate independent triggers that will test all the beam stopping mechanisms (one at the time).

Adding testing and diagnostics functions reduce the dangerous failure rate to below one failure in 1000 years [6].

Optical Fibre Gigabit System

During the analysis of the copper based FBI System it has been found that DC data paths can be easily corrupted due to potential electromagnetic interferences. Using DC signals for transmitting critical information may hide dangerous system failures. An alternative system design that will use gigabit optical links transmitting data packets instead of RS485 links with DC signals, is being evaluated currently.

The FBI System based on optical fibres will use high speed optical links between FPGAs through SFP optical transceivers, allowing for a noise free communication at very high speed. If compared to the copper based system, the gigabit links will always fail into a safe state due to the interruption of the data packs. 10 km transceivers will be chosen for the 600m long Klystron Gallery, allowing a long lifespan of the transceivers and withstand some optical fibre degradation before start failing. It is expected that thanks to the high speed devices, the system will be have a much shorter reaction time.

ISBN 978-3-95450-148-9

Furthermore FPGA internal serializers with speeds of up to 6gps, will reduce the number of components and the size of the different boards.

The Beam Permit signals will be transmitted together with the device serial number, supply status and other diagnostics features in data packets allowing not only to know if the beam permit is on or off but also knowing about the health of the interface connected.

While trying to analyse the system, it is clear that the FPGA will become the most critical element in this scheme and thus potentially a weak point due to the higher complexity of the device. At the same time the short lifespan of the fibres may increase the maintenance cost of the system. However, if it is proven that the dangerous failure rate and reliability improves, this increase in maintenance is affordable.

The conceptual idea has been drafted and the design of the first engineering model will start soon.

Optical Fibre System Layout

When designing a system, it is important to consider the integration of the system as well as the installation. In case of ESS, the rack enclosures will heavily impact on the maximum number of cables that can go in and out of each enclosure together with the time required for cable installation.

In order to allow for an easy integration, each enclosure will be equipped with an FBI_Master module combining all the signals from devices located within each rack enclosure into one single permit line. This line will be then connected to the main master or Master of Masters (MoM) located close to the actuators.

Following this strategy allows for the reservation of space for cables and racks within each enclosure ensuring the presence of an FBI_Master module in each enclosure and maintaining low cable installation cost.

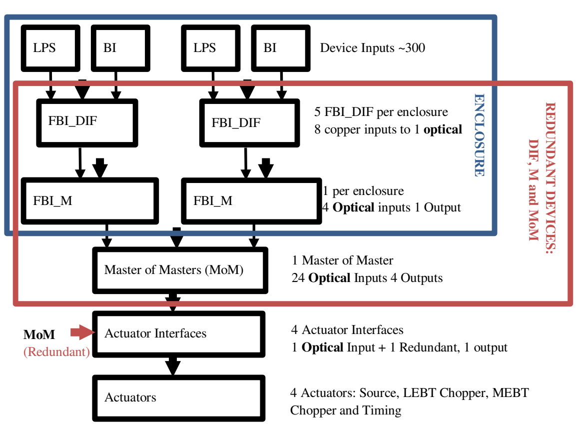

Figure 4: FBI System Optical Layout.

CONCLUSIONS

A first prototype based on the copper connections has been developed already but other design concepts are under investigation. Future iterations will take the ESS architecture more into account, trying to minimize the total installation cost.

An FMEDA analysis can improve the design significantly, such that weak points in the design can be easily detected. Further improvements will be done for the copper based FBI System, reducing the dangerous failure rate and improving the systems reliability.

REFERENCES

[1] A. Nordt et al., “Preliminary Risk and Hazard Analysis of the ESS Machine Protection System with Emphasis on Production and Property Losses in the ESS-LINAC”, ESS Report No 0003796 (2013).

[2] IEC61508 Edition 2.0

[3] IEC61511 Edition 1.0

[4] B. Todd, A Beam Interlock System for CERN High Energy Accelerators, Brunel University, London, United Kingdom (2006).

[5] B. Puccio et al, “Machine Interlock System in LHC Point 7”, CERN, Geneva, Switzerland (2008).

[6] R. Andersson et al, “A Modified Functional Safety Method for Predicting False Beam Trips and Blind Failures in the Design of an Accelerator Beam Interlock System”, MOPGF126, these proceeding, ICALEPCS’15, Melbourne, Australia., (2015).

ISBN 978-3-95450-148-9