FAST MACHINE INTERLOCK PLATFORM FOR RELIABLE MACHINE PROTECTION SYSTEMS

R. Tavčar*, J. Dedič, K. Erjavec, R. Modic, Cosylab, Ljubljana, Slovenia
M. Liu, C. Yin, SINAP, Shanghai, China

Abstract

This article presents a machine interlock system (MIS), designed and developed in collaboration between SINAP and Cosylab. The design is based on the experience and requirements of different accelerator facilities around the world, with the goal of providing, out of the box, the flexibility, reliability, availability, determinism, response speed, etc., which facilities need for a Machine Protection System (MPS). The goal of the MIS platform is to provide a reliable tool, which covers all the common MIS behaviour, required by an MPS designer. The system is based on a proven hardware platform, uses radiation-tolerant FPGAs, has built-in redundancies for power supply, hardware components and logic and is configurable from EPICS. We present several design principles that were used and explain the features and principles of application. Furthermore, we present the system architecture, from hardware and firmware to software. The MIS system is currently being installed at the BNCT facility at the Ibaraki Neutron Medical Research Center in Japan and is planned in the treatment interlock system of APTRON, the Advanced Proton Therapy Facility in Shanghai, China.

INTRODUCTION: MIS VS. MPS

Large physics machines differ in many ways, including size, complexity and equipment cost. Depending on the severity of damage if something goes wrong during machine operation, different expectations are imposed on the system that protects the investment and personnel. When considering machine protection systems (MPS), they are often confused with a Machine Interlock System (MIS) hardware platform, but a Machine Protection System is more than just the hardware platform. The MIS may be just a small part of a purely technical aspect of the larger organizational, procedural and technical process that is a machine protection system. This article focuses on the MIS hardware and does not detail the other aspects of MPS.

DESIGN OF MIS HARDWARE

The machine interlock system is an autonomous system that collects signals from various devices and triggers the shutdown of the machine when any of the devices detects a failure. Our system design is based on powerful FPGAs, fiber optics etc. that are capable of monitoring hundreds of devices and triggering mitigation actions upon detecting a fault condition, with features like configurable responses, signal logging for post-mortem analysis, and input masking. Interlock systems need to have a very fast response, be able to handle a large number of devices and have a high level of reliability, and so pose unique design challenges.

Based on discussions with several accelerator facilities around the world, Cosylab engineers have gathered the most typical requirements for a machine interlock system:

- Response time ≤ 5 μs for failures in the crucial part of the accelerator.
- Design must include redundancy.
- Must provide the possibility to trace back to the origin of an event, which caused failure.
- Must support a large number of inputs.
- Must support input and output masking.
- System should timestamp all logged events.
- Must offer a simulation of input changes to verify the correctness of the configuration.
- Must provide binary input and output.
- Must be a distributed system.
- Must distinguish between critical and non-critical fault signals.
- Must support local and global responses.
- Different interlock responses for different machine modes.

Since some of the requirements cannot be met with commercial off-the-shelf equipment, we designed a flexible, reliable, distributed and fast system which we finalized together with SINAP, who also took over the design and production of hardware.

SYSTEM OVERVIEW

Figure 1 shows the MIS system overview and illustrates the relationship between its main components: Input card, Output card, Monitor card and Interlock card.

Input cards gather the binary not_OK/OK signals from the accelerator devices and pass the masked signals to the Interlock card and Monitor card. The Monitor and Interlock cards then generate their own response, using the inputs from Input cards via backplane and the global interlock from other MIS crates, propagated via optic fibre. Interlock cards are designed to generate identical responses, to provide redundancy. The Monitor card also implements this interlock logic, the result of which can be used to detect faulty behaviour of either Interlock card. The result of interlock logic is sent to the Output cards. The Output card can be configured to mask certain internal interlock signals, which allows the MIS system to implement different behaviour in different machine modes. All logic is implemented in FPGA firmware.

* rok.tavcar@cosylab.com

ISBN 978-3-95450-147-2

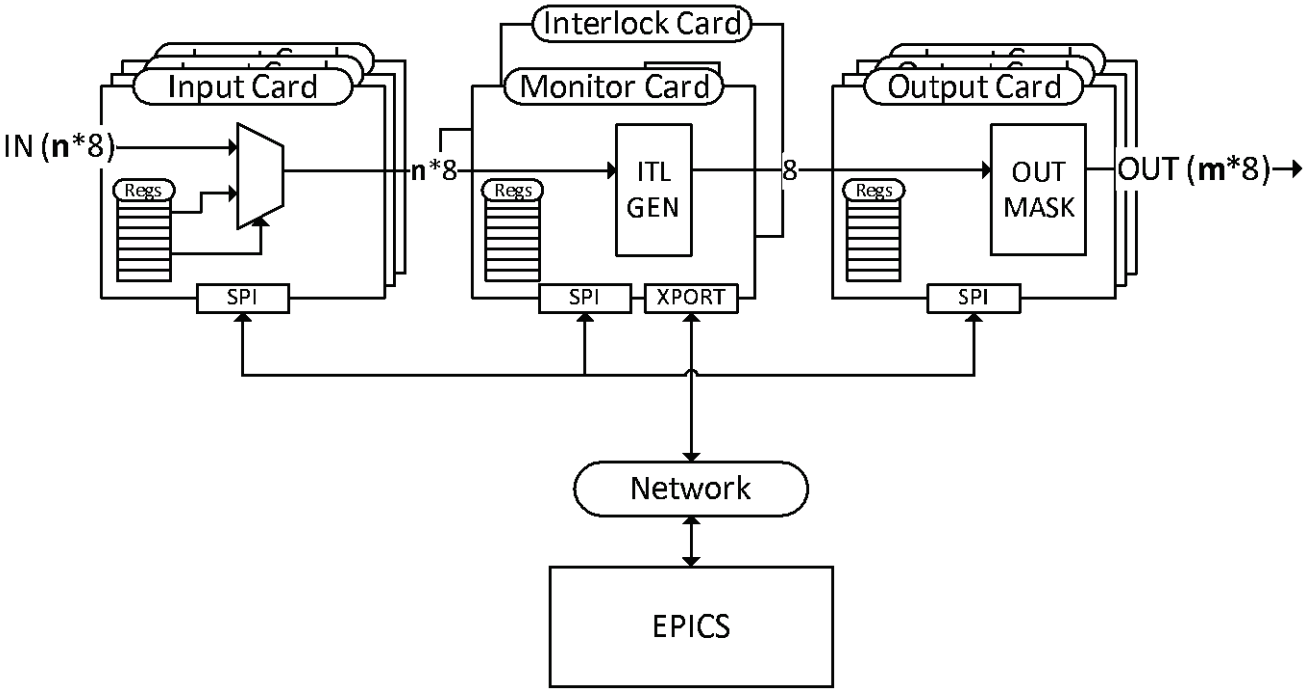

Figure 1: Machine interlock system overview: relationships between core functional components.

SOFTWARE SUPPORT

While the firmware is fixed, the interlock logic configuration can be changed via the EPICS [1] software that interfaces the Monitor card via Ethernet.

The EPICS software is built from several layers:

- Asynchronous Port Driver [2], which interfaces the EPICS database and hardware.
- EPICS [1] software database, which abstracts the hardware registers.
- Graphical interface – Control System Studio [3], which conveys feedback and control options available to the user.

DESIGNED FOR SAFETY, FLEXIBLITY, RELIABILTY AND SPEED

Increased system complexity can nonlinearly increase risks of failure and also increases complexity of risk analysis.

Figure 2: Machine interlock system hardware.

Therefore, one of the core design principles we used was to isolate the safety critical part, which handles interlock responses, from the safety non-critical part, which handles the configuration, managerial and monitoring parts of the system. To further minimize design risks, the backplane hardware is largely based on compactPCI, a proven backplane design, which we adapted for specific functionality of our MIS platform.

Safety-critical Functionality

To assure fast response times and determinism of signal paths, the logic is implemented in low-level FPGA logic in Interlock cards. Considering the environmental conditions of a particle accelerator, the MIS system uses radiation-tolerant FPGAs, based on non-volatile flash technology.

For mitigating failures of the MIS hardware itself, the system supports redundancy of interlock logic, by duplicating functionality in two separate Interlock cards. Similarly, MIS design also features redundant power supplies (Figure 2).

Safety non-critical Functionality

To separate it from the safety-critical part, the safety non-critical functionality is implemented in the Monitor card. The Monitor card is responsible for monitoring the behaviour of all other cards in the system, post-mortem logging, integration with timing system (for timestamping), interface to the control system etc.

Inputs and Outputs

The MIS design is able to support different IO standards, by using different Input and Output cards. So far,

TTL and HFBR IO cards have been implemented, but it is possible to include relay cards, analogue threshold, etc.

Scalable Redundant Optic Network

Depending on number and location of IOs involved in the interlock system, multiple MIS crates can be connected in a fully redundant optical network, using ring topology. Propagating redundant interlock signals in opposing directions (Figure 3) to reduntant Interlock cards, effectively splits the global interlock propagation time in half. Other MIS topologies could be achieved and require a dedicated switching mechanism. Because interlock logic is distributed, the MIS is seamlessly expandable when systems are added to the protected machine, which is especially useful during system-by-system commissioning.

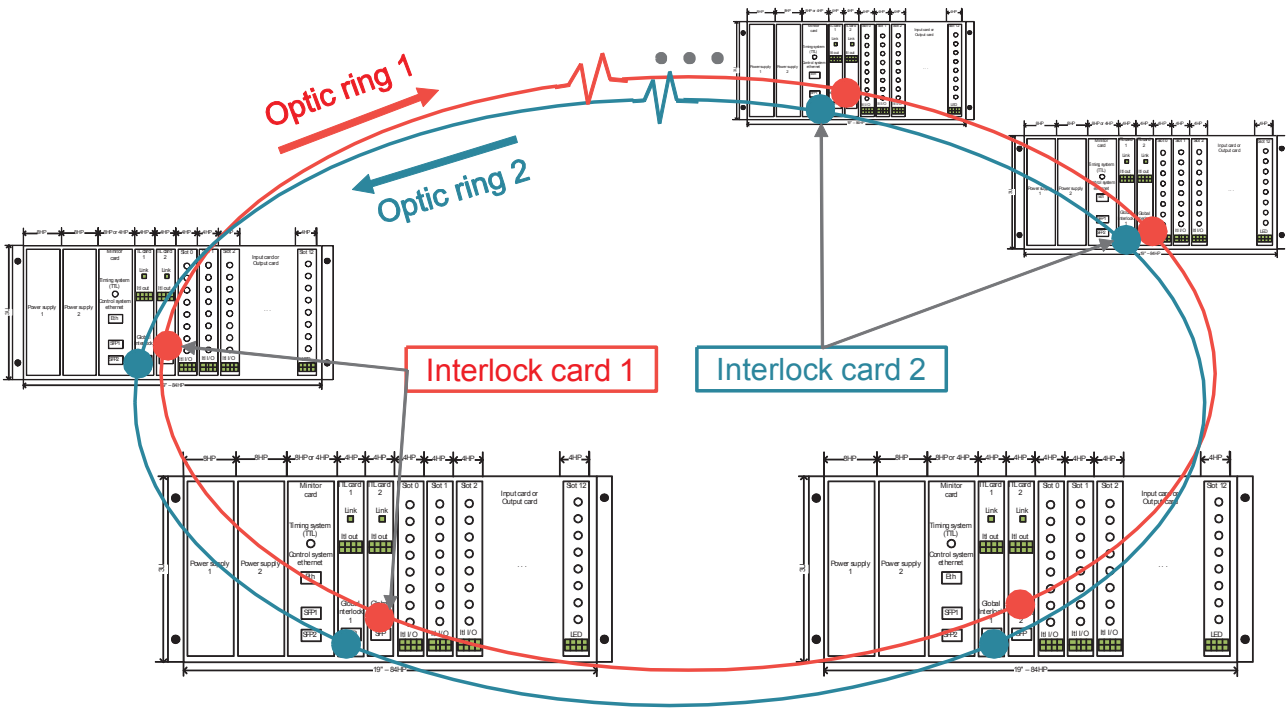

Figure 3: Scalable, fully redundant ring topology.

Balance between Reliability and Availability

Another important aspect of machine protection is the balance between reliability (safety) and availability of the protected machine. On one hand, this balance is affected already by the configuration of the fault detection devices, which provide input to the MIS, by carefully setting their thresholds. On the other hand, the MIS platform enables to affect this balance by e.g. supporting several interlock levels and different interlock behaviour for different machine modes.

CONCLUSION

Since large physics machines are expensive, it is important to have a machine protection system that prevents damage of accelerator devices in the event of failures. The machine interlock system is an important part of the technical aspect of a full machine protection system. The MIS, presented here, was designed to cater to the demanding requirements of machine interlock systems in terms of fast response time, signal path determinism, IO capability, scalability, integration with the control system, integration with the timing system and other functionality like post mortem logging, configuration verification, redundancy, etc. The MIS was developed to be flexible, allowing many configuration options and at the same time, streamlined for high system reliability. The MIS system is currently being installed at the BNCT facility at the Ibaraki Neutron Medical Research Center [4] in Japan and is planned in the treatment interlock system of APTRON, the Advanced Proton Therapy Facility [5] in Shanghai, China.

REFERENCES

[1] EPICS, http://www.aps.anl.gov/epics/

[2] Kraimer, Martin R., Mark Rivers, and Eric Norum, “EPICS: Asynchronous driver support”, ICALEPCS. Vol. 5. 2009.

[3] Clausen, Matthias, J. Hatje, and J. Penning., “The CSS Story”, Proceedings of PCaPAC2012, Kolkata, India (2012).

[4] Yoshioka, M., *et al.*, “Construction of Accelerator-based BNCT Facility at Ibaraki Neutron Medical Research Center”, Proceedings of UCANS-IV (2014).

[5] Xu, J., *et al.*, “Radiation Calculations for Advanced Proton Therapy Facility”, Extraction 70 (2013): 250MeV.

ISBN 978-3-95450-147-2