ALS FPGA-BASED EXTRACTION TRIGGER INHIBIT INTERLOCK SYSTEM FOR TOP-OFF MODE*

J. Weber#, K. Baptiste, R. Mueller, LBL, Berkeley, CA 94720, U.S.A.

Abstract

The Advanced Light Source is a third generation synchrotron light source that has been operating since 1993 at Berkeley Lab. Recently, the ALS was upgraded to achieve Top-Off Mode, which allows injection of 1.9GeV electron beam into the Storage Ring approximately every 30 seconds. The ALS Top-Off Mode Beam Current Interlock System was installed to prevent the potential hazard of injected electrons propagating down user beam lines. One of the requirements of this interlock system is a fast response time from detected event to injection trigger inhibit. Therefore, solid-state devices, not electro-mechanical relays typically used in accelerator safety systems, must be used to implement the trigger inhibit logic. An FPGA-based solution was selected for this function. Since commercial FPGAs are not rated for high reliability or fail-safe operation, some of the logic resources were used to perform system self-checking to reduce the time to detect system failures and increase reliability. The implementation and self-checking functions of the Extraction Trigger Inhibit Interlock System will be discussed.

INTRODUCTION

The Advanced Light Source (ALS) currently operates for users in Top-Off Mode, in which electrons are injected into the Storage Ring (SR) with the Personnel Safety Shutters (PSS) open. Without additional controls, studies indicate that under certain conditions it is possible to steer electrons down a user beamline, potentially creating a radiation hazard on the experimental floor [1]. To mitigate such hazards, the ALS Top-Off Interlock System was implemented [2].

The Top-Off Interlock System consists of four interlock sub-systems: Stored Beam Interlocks (SBI), Energy Match Interlocks (EMI), Lattice Match Interlocks (LMI) and Beamline Radiation Interlocks. Interlock signals from the SBI, EMI, and LMI systems, along with mode control signals, are sent to the Extraction Trigger Inhibit Interlock System (ETI). Each of these sub-systems consists of two parallel redundant interlock chains (labeled chains A and B). The exception to this parallel architecture is that the trigger signals pass through the two ETI modules serially.

The ETI is responsible for inhibiting triggers to two pulsed magnets used for booster extraction, the Booster Thin Septum and Booster Thick Septum, to prevent injection into the SR in response to an interlock trip, system fault, or change in operating mode. The extraction triggers are intercepted at the output of the ALS Timing System, as shown in Figure 1.

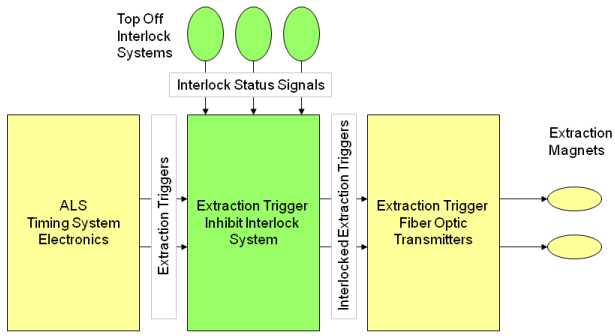

Figure 1: Extraction trigger and interlock control signal flow.

The overall system response time to any interlock trip is required to be less than 1 ms [1]. This time includes delays attributed to the transducer output, low pass filter, comparator and latch circuit, interlock current loop chain, ETI trigger inhibit, signal transmission, and the extraction magnet SCR trigger circuit. Therefore only a fraction of the timing budget is available to the ETI to inhibit the extraction triggers, precluding the use of electro-mechanical relays, which have switch times typically greater than 5 ms. Instead, solid-state devices were selected to perform the trigger inhibit function. However, the Top-Off Interlock System design, including the ETI system, also must conform to U.S. Department of Energy (DOE) design principles as well as best practices in personnel safety system design. The following section will describe these design principles, and how they are met with a system built using solid-state devices.

DESIGN PRINCIPLES

In general, best practices for designing a personnel safety system prescribe that the system be fail-safe, redundant, testable, visible, self-checking, and reliable. Many of these principles are spelled out in more detail in the DOE document governing safety system designs [3]. A fail-safe device or system is typically defined as one in which the likely failure scenarios prevent unsafe operation. In the case of an electro-mechanical relay, the device is considered fail-safe because the most likely failure scenario is a relay failing open, which can be easily implemented in a system to prevent unsafe conditions. The Top-Off Interlock System as a whole, and the ETI system in particular, were designed to meet all of these design principles wherever possible. However, due to the response time requirements, commercial-grade solid-state devices, which are not specified for fail-safe or

* Supported by the U.S. Department of Energy under Contract No. DE-AC02-05CH11231
#jmweber@lbl.gov

high-reliability applications, were required to implement the trigger inhibit circuit.

Several solid-state components were used in the ETI design including Emitter-Coupled Logic (ECL) logic chips for compatibility with the extraction trigger signals, a field programmable gate array (FPGA) for interlock decision logic, and ECL to positive logic level shifters to interface between the FPGA and ECL circuits. These devices are not considered fail-safe because their transistor outputs can fail open circuit, shorted to ground, active, or inactive, and the most likely failure scenario is unknown. In addition, none of these solid-state devices are specified for high-reliability applications.

To increase the reliability of the system and address potentially unsafe failures of these solid-state devices, several self-checking functions were implemented in the FPGA logic. The self-checking functions include comparing redundant interlock signals for loss of redundancy, checking for potentially unsafe failures, and detecting glitches that would otherwise be interpreted as interlock trips. If the self-checking logic detects any of these conditions, it generates a system fault, which inhibits the extraction triggers and closes the PSS. System faults are administratively controlled such that the system cannot be restored to Top-Off Mode until the source of the fault is investigated by qualified personnel with the authority to determine if it is safe to continue to use the interlock system.

IMPLEMENTATION

The ETI system logic functions are shown in Figure 2. The extraction triggers are inhibited by ECL gates. The FPGA performs most of the logical functions in logic blocks, including trigger inhibit, test, monitor, and self-check.

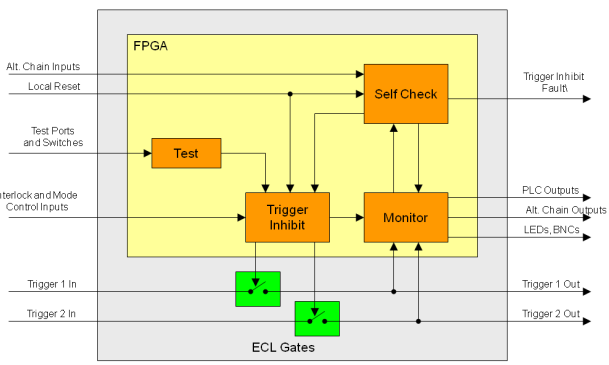

Figure 2: ETI logic block diagram.

The test block inputs include front panel pushbuttons and test ports that are used to generate test vector outputs to the trigger inhibit block. The trigger inhibit logic block inputs include interlock signals, mode signals, test signals, and reset, which are used to determine whether or not to inhibit the triggers. This block generates trigger enable output signals to the ECL gates in the trigger paths. It also outputs status of these inputs and outputs to the monitor logic block. The monitor block also looks at the output of the trigger enable gates and system faults generated by the self-check logic. It passes status information to front panel LEDs, a PLC I/O module for connection to the control system, the self- check logic, and the other ETI module in the redundant interlock chain. The self-check logic takes status information from the monitor block and inputs from the alternate chain ETI module, and outputs the status of the various fault conditions that it can detect.

Self-Checking Logic

The self-checking logic in the ETI FPGA is designed to quickly detect loss of interlock redundancy, glitches on interlock inputs, and other failures of the system. If any system fault is generated, the *Trigger Inhibit Fault* (sum of all system faults) is also generated, which inhibits the extraction triggers and closes the PSS. The quick detection of these failures allows them to be addressed and remedied before multiple failures lead to an unsafe condition. This added layer of protection minimizes operating time with single-point failures, and increases system reliability. An additional benefit of the self-checking is the early detection of fail-safe failures, so they can be addressed as they occur, rather than accumulating such that several problems need to be fixed during a scheduled test interval. A description of the various fault conditions detectable by the ETI system is shown in Table 1.

Table 1: Descriptions of System Faults Detected by ETI System

Fault Name	Detection
Trigger Enable Compare	Mismatch between interlock chain Trigger Enable signals
Trigger 1 Compare	Mismatch between interlock chain Trigger 1 signals
Trigger 2 Compare	Mismatch between interlock chain Trigger 1 signals
Trigger 1 Control	Trigger 1 output detected while Trigger Enable off
Trigger 2 Control	Trigger 2 output detected while Trigger Enable off
Trigger Enable Timeout	Trigger Enable pulse width exceeds timeout limit
Static Interlock Compare	Mismatch between interlock chain summed interlock input signals
Static Interlock Glitch	Mismatch between raw and latched interlock input signals
Injection Mode Compare	Mismatch between interlock chain Injection Mode input signals
Top Off Mode Compare	Mismatch between interlock chain Top-Off Mode input signals
Trigger Inhibit	Sum of all faults

Several of the faults monitor the status of dynamic signals. A *Trigger Enable Compare Fault* is generated when the Trigger Enable signal, which is a pulse ~2ms wide, from interlock chain A does not overlap in time with the chain B signal. A *Trigger 1/2 Compare Fault* is generated when a trigger is detected at the output of the ETI module in one chain, but not the other. A *Trigger 1/2 Control Fault* occurs when a trigger is detected at the ECL gate output, but the corresponding trigger enable

signal is not present. If a trigger enable signal lasts longer than the fixed timeout limit of 100ms, a *Trigger Enable Timeout Fault* is generated.

Other faults monitor essentially static signals. The static interlock signal is the sum of all static interlock inputs: SR Energy Match, SR Lattice Match, and SR Beam Current. Each static signal is A *Static Interlock Compare Fault* indicates a mismatch between the chain A and B static interlock signals. The static interlock signal is then latched. A *Static Interlock Glitch Fault* indicates an active input is detected on a static interlock input when the input has already been latched inactive. The *Injection Mode Compare Fault* and the *Top-Off Mode Compare Fault* are generated when their chain A and B signals differ from each other. The mode signals are the only inputs to the system that are relay based, since they do not require fast response time. Due to variations in response time between the two interlock chains, a 500 ms grace period is given for a signal to match its counterpart in the other interlock chain before a fault is generated. The faults are not required to meet the 1 ms response time because they indicate a system failure resulting in a loss of redundancy, not a potentially dangerous machine condition.

Failure Analysis

An analysis of likely single-point failures was done to see what type of faults would be useful to detect. Some common single-point failures that must be addressed in any safety system design are loss of power, open circuits, and shorts to ground. Single-point failure analysis assumes the rest of the system is working properly. In the event of a loss of power to both ETI modules during Top-Off operation, the system is fail-safe because the trigger signals are active high, and cannot be propagated without power present. If only one module loses power, the other will generate several compare faults, indicating that the two ETI modules have outputs in different states.

If any of the critical interlock signals, including interlock status inputs, cross-connected interlock status outputs, trigger inputs, or trigger outputs, are disconnected or fail open circuit, the system will fail-safe because each signal is active high and pulled low when open circuit. If any part of the input or output logic connected to any of these signals fails open circuit, a compare fault will be generated by the working ETI module. If they fail shorted to ground, the system will fail-safe because the signals are active high. If any of the related logic fails shorted to ground, a compare fault will again be generated.

If there is a single-point failure in an ETI FPGA that causes an input or output to fail open circuit or shorted to ground, in most cases the other FPGA will detect a mismatch and generate a compare fault. In some cases, this failure may not be detected until the next time Top-Off operation is terminated, which occurs at least every two weeks, or until the next system test, which is currently performed every 6 months. In the meantime, the system as a whole is still safe, but no longer redundant. If one of the ECL gate inputs or outputs in the trigger path fails open circuit or shorted to ground, a *Trigger Compare Fault* will be generated on the next injection cycle.

Another scenario that must be considered likely for analysis purposes is a solid-state device failing active, which in isolation is considered not fail-safe. If a critical interlock signal (as defined above) fails active, a compare fault will be generated when Top-Off operation is terminated. If one of the ECL gate outputs fails active, a *Trigger Control Fault* or a *Trigger Enable Timeout Fault* will be generated immediately. If one of the ECL gate inputs fails active, one of these faults will be generated when Top-Off operation is terminated. In any case, this detection is usually much faster than waiting for the 6 month system test interval. Also note that if any of these failures occur while the ALS is not operating in Top-Off mode, a fault will be generated immediately or while transitioning back into Top-Off operation.

CONCLUSION

The selection of an FPGA-based design for the ETI system allowed inclusion of logic functions that increase the reliability of a system containing several solid-state devices. In addition to performing trigger inhibit decision logic, the FPGA also performs monitoring and self-checking functions that significantly decrease time to detection of many single-point failures and increase system reliability. These added measures provide the confidence to deploy a personnel safety system based on solid-state devices, despite their unknown likely failure modes.

The Top-Off Interlock System has been operational since February. Overall the system has been quite reliable since then; however, several faults have been detected and addressed over the same period. The sources of these faults are well understood and none of them occurred during Top-Off operation, meaning the system has not yet operated during Top-Off with a detectable failure. Operational experience with this system is discussed in greater detail here [2].

REFERENCES

[1] H. Nishimura, et al., “Advanced Light Source’s Approach to Ensure Conditions for Safe Top-off Operation”, submitted to Nuclear Instruments and Methods, 2009.

[2] K. Baptiste, et al., “ALS Top-Off Mode Beam Interlock System”, these proceedings.

[3] DOE G 420.2-1, “Accelerator Facility Safety Implementation Guide for DOE O 420.2B, Safety of Accelerator Facilities,” 2005.