ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-THCPR03

A SAFETY RATED FPGA FRAMEWORK FOR FAST SAFETY SYSTEMS

F. Tao†, B.M. Bennett, D.G. Brown, J. Jones, M. Stettler
SLAC National Accelerator Laboratory, Menlo Park, USA

Abstract

In the accelerator community, majority of credited safety systems are implemented with safety PLCs to reduce the enormous burden on functional safety compliance. However, for safety functions require fast response or complex signal processing, FPGA is often the only feasible solution, and the system design has to comply with the IEC 61508 standard. In this paper, we will introduce a generic safety-rated FPGA design template. FMEDA analysis, hardware reliability modelling, firmware development, verification and validation will be described in details to demonstrate the IEC 61508 compliant development process. In this dual redundant design, each chain consists a FPGA chip from different manufacturers to minimize the potential common cause failure. Cross checks between FPGAs and end-to-end testing are performed to increase the diagnostic coverage and improve the reliability. Based on this safety FPGA template, an Average Current Monitor (ACM) system is developed at SLAC with the addition of a safety PLC for diagnostics and a HMI for user interface. The overall system is deployed as part of Beam Containment System (BCS) to limit the beam current with the target Safety Integrity Level (SIL) 2.

DEVELOPMENT BACKGROUND

In SLAC, Radiation Safety Systems (RSS), which includes Personnel Protection System (PPS) and Beam Containment System (BCS), traditionally use simple analog/digital electronics and proven concepts to avoid complex failure modes. In the modernization of RSS, PPS uses safety PLCs to replace relay logic both at the system level, zone level and down to the chassis level. The adoption of safety PLC not only improves the safety and reliability performance but also makes the configuration control easier and more reliable. However, when it comes to BCS, PLC alone is not a feasible solution. As some BCS sensor signals require a fast and/or complex logic processing, such as beam loss monitors or average current monitors. Using safety PLC can't meet the response time requirements. For this reason, we have to find a new engineering solution for electronics design of safety critical applications.

Just cite the LCLS-II (Linac Coherent Light Source) BCS as an example. Since the maximal designed beam power is 1MW, the corresponding response time for the BCS is 200 micro-second, which is beyond the capability of any safety PLC on the market. Therefore, for all LCLS-II BCS control systems and subsystems, we have to split the system into fast portion and slow portion. A Siemens S7-1515F safety PLC will interlock to those slow sensors and customized electronics deal with the fast portion of the system.

Complex logic processing required in the BCS instruments easily rules out the potential of using traditional electronics. There are only two options left for safety-critical electronics system development. The first one is safety rated micro-controller (MCU). This type of IC has been widely used in automotive applications or has been used by automation vendors to build safety controllers such as PLC, motor drive etc. At the time of writing this paper, the fastest general purpose safety micro-controller from Texas Instrument (TI), a market leader on safety MCU, is TMS570 with 330MHz frequency. Considering that MCU requires multiple instruction execution periods to finish a task, which make it still impossible to meet the requirements for dealing with 20MHz sampling, which is a minimal requirement when deals with the beam related analogue signal processing.

The other option is FPGA (Field Programmable Gate Array). This is a type of IC widely used in the accelerator instrumentation and control. It can process inputs in parallel, which is advantage over the MCUs. As the quick technology development, it is much easier to find FPGA solutions for applications with even higher sampling frequency requirements. For this reason, we decided to adopt FPGA in the development for fast interlock systems.

SYSTEM'S FUNCTIONAL SAFETY

The functional safety standard IEC 61508 was published in 2000 and the second edition has been available since 2010. This functional safety standard is applicable to customized electronics development such as BCS. In addition, there is a guidance document from the US Department of Energy (DOE) on use IEC 61511, a second tier functional safety standard for process industry applications, to BCS design.

IEC 61508 is a performance based standard that uses Safety Integrity Level (SIL) as the measure for system's reliability performance on a particular safety function. To apply this standard, safety functions within the system have to be defined first; then for each safety function, assign a SIL based on the risk assessment.

In a SLAC's typical BCS, there are two functions have the most criticality. One is the beam loss detection, and the other is the beam energy limit. The first is vital to protect the safety devices such as safety collimators, stoppers etc., while the second function is used to establish the basis for ray trace study, a method used by radiation protection physicists on risk assessment. During the risk assessment, we determine that the SIL rating is 2. For this reason, we will target the FPGA design for SIL2 applications.

† fengtao@slac.stanford.edu

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-THCPR03

Radiation Protection physicists at SLAC use an assumption that there would be 10 BCS faults each year, and use this assumption in the radiation hazard assessment. Aligning with this assumption, BCS instruments will work in the high demand mode, and the PFH (Probability of Dangerous Failure per Hour) should be used for the safety integrity performance, e.g.,

PFH Range for SIL 2: $10^{-6} – 10^{-7}$

As the PFH is for the complete safety function from end to end, usually the logic solve portion should only take up 10% ~ 15% of the overall PFH value.

System architecture is the most critical decision to make in a new safety system design. In SLAC, all RSS are dual redundant, e.g., system has identical Chain A and Chain B, the trip of either chain will trip off the system. Using the terminology from functional safety standard, this configuration is 1oo2 (1 out of 2) with Hardware Fault Tolerance 1 (HFT=1). According to Table 2 and Table 3 in Part 2 of IEC 61508 [1]:

Table 1: Max Allowable SIL for Type A Subsystem

SFF	Hardware Fault Tolerance		
	0	1	2
<60%	SIL 1	SIL 2	SIL 3
60% - 90%	SIL 2	SIL 3	SIL 4
90% - 99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Table 2: Max Allowable SIL for Type B Subsystem

SFF	Hardware Fault Tolerance		
	0	1	2
<60%	Not Allowed	SIL 1	SIL 2
60% - 90%	SIL 1	SIL 2	SIL 3
90% - 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Both tables are used in a typical electronic development. Once the overall electronics is divided by a simple part containing conventional analog/digital electronics, and a complex part which contains high density IC chips such as memory and FPGA etc. For the former, Table 1 is applicable while for the latter, Table 2 has to be referred. For example, from Table 2, it is clear that the subsystem containing FPGA must has a safe failure fraction (SFF) greater than 60%, other subsystems without using complex IC chips do not have restriction on SFF. However, a higher SFF will undoubtedly improve the overall system safety performance.

SAFETY RATED FPGA DESIGN

Hardware

One concern in the safety system development is the systematic failures and common cause failures. With the increasingly complex software packages needed for the hardware development, software errors are systematic problems shouldn't be underestimated. If two chains use the same hardware platform, then potential issues come from software will affect both chains and defeat the efforts on using redundancy.

For this reason, we decided to use FPGAs from different vendors for each chain. So each chain will be developed using different software tools. In addition, the firmware development of each chain will be carried out by different engineers to further reduce the potential common cause failures.

In Chain A, the FPGA chip chosen is the Xilinx Artix-7, and Chain B uses Lattice MACHX02. The configuration of FPGA in dual chain setup is shown in Fig. 1.

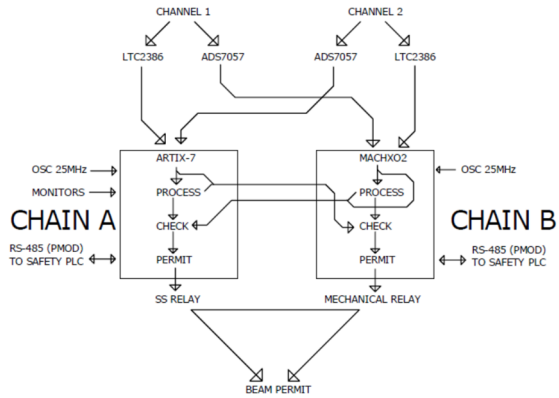

Figure 1: Chain A/B layout.

As shown in the board layout, the output of each chain will be serially connected to provide a dry-contact switch to other parts of BCS.

Mechanical enclosure used to contain the circuit board is the Stanford Research Systems (SRS) SIM 900 Mainframe, as shown in Fig. 2. Each module will be contained in the single wide SIM module that goes in the crate.

Figure 2: SIM 900 crate: front and back.

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-THCPR03

Firmware

The firmware is implemented in accordance with IEC 61566-2 standard [2] for a class B safety system, in addition to the existing SLAC design process. It has been agreed on:

- There will be no pre-configured IP in the design
- The FPGA hardware for the two chains are different device families sourced from different silicon vendors. They do not share common software tools or design synthesis flow. This redundancy provides sufficient disparity to provide overall confidence in the synthesis of the two firmware logic implementation.
- The HDL language utilized in the firmware implementation will be VHDL (IEEE 1076) and/or Verilog
- The final firmware will be reviewed by outside experts.

AVERAGE CURRENT MONITOR

Average Current Monitor (ACM) is one of the most important beamline instrument for BCS, as the excessive beam current may cause the damage to the downstream devices, given the same beam energy. Radiation Protection physicists also rely on ACM to make sure the beam energy is within the specified range, and use this energy as the basis in ray trace study.

The design objective is to use the toroids as the sensor, FPGA as the core logic processor, and safety PLC to provide proper configuration control and user interface. The system block diagram is shown in Fig. 3.

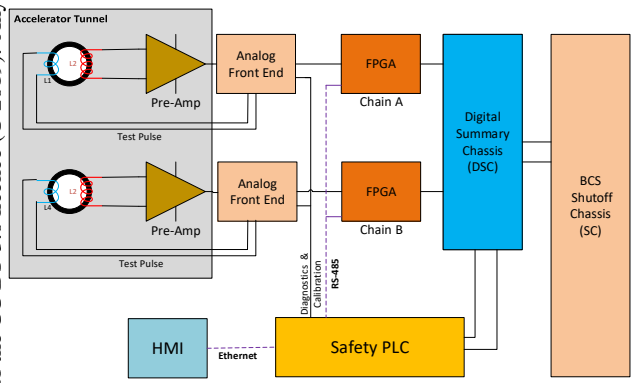

Figure 3: ACM system block diagram.

In the system block diagram, Digital Summary Chassis (DSC) and BCS Shutoff Chassis are existing designs. Safety PLC and Human Machine Interface (HMI) are COTS products require only configuration and programming.

Toroids are refurbished from previous projects and have been re-tested on the test bench. They have signal and calibration windings with a ratio 16:1. A picture of the toroid to be installed is shown in Fig. 4.

Figure 4: Toroid with two windings.

The Pre-amp and Analog Front End (AFE) module have been designed and shown in Fig. 5. In the figure, the Pre-amp module is on the top of the SIM crate and the AFE module is the first one from the left in the crate.

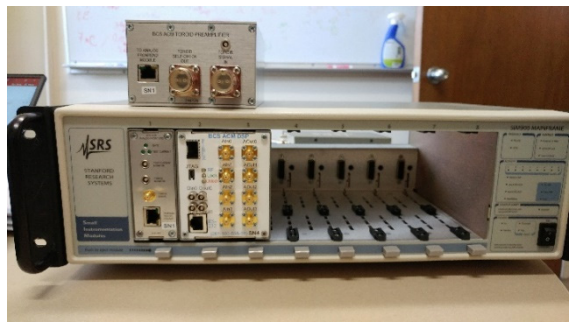

Figure 5: Pre-amp and AFE module.

The picture of the FPGA module is shown in Fig. 6.

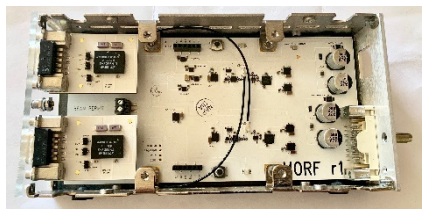

Figure 6: FPGA module.

FAILURE MODES EFFECTS AND DIAGNOSTIC ANALYSIS (FMEDA)

One critical difference between safety and non-safety design is that in a safety critical system development, the hardware design has to go through the FMEDA to make sure both the architectural constraints listed in Table 1 and Table 2 are met; and the dangerous undetected PFH number calculated from the FEMDA analysis is within the desired range.

To perform the analysis, we need to equip with reliability data of electronic components as well as the failure modes of each component. There are multiple sources of the reliability data, include RIAC 217+, EPRD (Electronic Parts Reliability Data), NPRD (Nonelectronic Parts Reliability Data), just name a few. For specialized IC chip like FPGA, the vendor also periodically publishes the reliability data on their quality report. However, the reliability data from vendors may not meet the requirements from the standard and make it not useful in the FEMDA. Then the designer has to use generic reliability data with the assumption of the number of transistors in the IC chip. A typical sources of reliability data for those complex ICs is the Siemens Norm SN 29500.

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-THCPR03

In addition to the failure rates, the other information necessary is the failure mode distribution. For conventional analog/discrete components, this type of information can be found in standards such as IEC 61709 [3]. A more comprehensive source is FMD (Failure Mode Distribution) compiled by RIAC.

In the system design, diagnostics is critical in improving the SFF. As the design is dual redundant with different component selection. The two chains will be crossed checked to detect any single point failures from sensor inputs all the way to logic processing output. In addition, we implements following modes to enhance the end-to-end diagnostics:

- Normal operational mode: cross check between dual redundant logic processing paths
- Test mode: the AFE module can generate 4 reference currents as the calibration signal sending to the calibration winding. Depending on the trip threshold, the operator can choose the corresponding level of the reference current that is high enough to trip off the system.
- Calibration mode: when the primary beam is off, the operator can manually initiate the system calibration to determine if the system can still maintain its accuracy.

Safety PLC used in the system plays an important role in the test and calibration modes. Safety PLC uses the safety discrete output (SDO) to bypass the channel under test from the DSC (shown in Fig. 7) it connects to, which make the end-to-end test feasible without trip off the beam operation. The communication configuration within the safety PLC, EPICS and the FPGA module is shown in Fig. 8.

Figure 7: Digital Summary Chassis (DSC).

CONCLUSION

In this paper, we discussed a FPGA based system design for fast interlock system. Important aspects of safety hardware design including architectural constraints, firmware development methodology and FMEDA are discussed. Based on this proposed scheme, we combine the customized hardware with Siemens safety PLC to implement an ACM system for BCS, which can reach the SIL 2 safety rating.

ACKNOWLEDGEMENTS

The authors would like to thank SLAC engineer Robert Ragle and Ryan Herbst on their contributions to the former MR-ACM project, which inspires us on this new FPGA development framework.

REFERENCES

[1] "Functional safety of electrical/electronic/programmable electronic safety-related systems," International Electrotechnical Commission, Number IEC 61508, 2010.

[2] "Nuclear power plants – instrumentation and control systems important to safety – Development of HDL-programmed integrated circuits – Part 2: HDL-programmed integrated circuits for systems performing category B or C functions," Draft, International Electrotechnical Commission, Number IEC 62566-2, 2017.

[3] "Electric components – Reliability – Reference conditions for failure rates and stress models for conversion," International Electrotechnical Commission, Number IEC 61709, 2017.

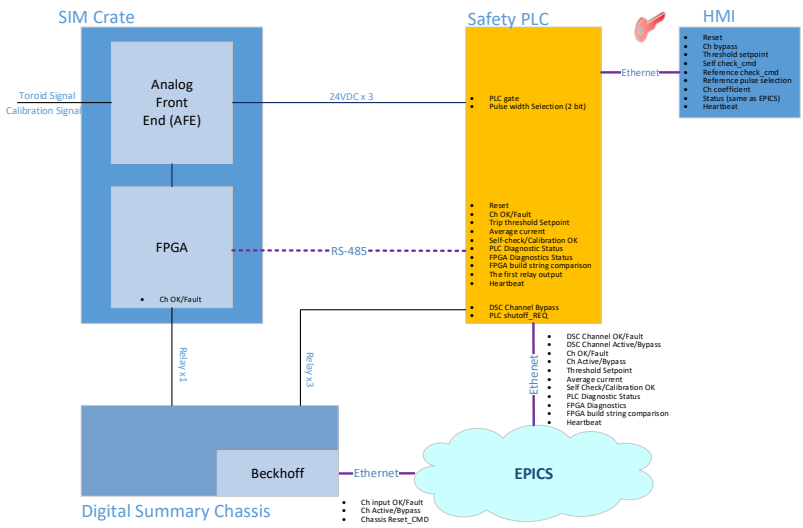

Figure 8: Inter-system communication diagram.