ISBN: 978-3-95450-208-0 doi:10.18429/JACoW-IPAC2019-THPRB030

NOVEL FPGA-BASED INSTRUMENTATION FOR PERSONNEL SAFETY SYSTEMS IN PARTICLE ACCELERATOR FACILITY

S. Pioli[1]*, O. Frasciello[1], M. M. Beretta[1], P. Ciambrone[1], C. Di Giulio[1], B. Buonomo[1], M. Belli[1], P. Valente[2], A. Variola[1]
[1]INFN-LNF - Frascati National Laboratory, Rome, Italy
[2]INFN-Roma1 - Section of Rome, Italy

Abstract

Personnel Safety System for particle accelerator facility involves different devices to monitor gates, shielding doors, dosimetry stations, search and emergency buttons. In order to achieve the proper reliability, fail-safe and fail-proof capabilities, these systems are developed compliant with safety standards (like the IEC-61508 on "Functional Safety", ANSI N43.1 "Radiation Safety for the design and operation of Particle Accelerator" and NCRP report 88) involving stable technologies like electro-mechnaical relays and, recently, PLC. As part of the Singularity project at Frascati National Laboratories of INFN, this work will report benchmark of a new FPGA-based system from the design to the validation phase of the prototype currently operating as personnel safety system at the Beam Test Facility (BTF) of Dafne facility. This novel instrument is capable of: devices monitoring in real-time at 1 kHz, dual modular redundancy, fail-safe and fail-proof, multi-node distributed solution on optical link, radiation damage resistance and compliant with IEC-61508, ANSI N43.1 and NCRP report 88. The aim of this FPGA-based system is to illustrate the feasibility of FPGA technology in the field of personnel safety for particle accelerator in order to take advantage of a fully digital system integrated with facility control system, evaluate the related reliability and availability and realize a standard, scalable and flexible hardware solution also for other fields with similar requirements like machine protection systems.

INTRODUCTION

Particle accelerators require Personnel Safety Systems (PSSs) in order to reduce as much as possibible the risk of an accidental exposition of workers to ionazating radiation. These kind of systems must provide access control to any area involved with the accelerator facility (monitoring gates, shielding doors, dosimetry stations, search and emergency buttons) and produce an enabling signal to allow operation to radio-frequency systems.
In order to design properly a PSS, regulation and best practice guide lines and industrial standards are available, like IEC-61508 on "Functional Safety" [1], NCRP report 88 on "Radiation Alarms and Access Control Systems" [2] and ANSI report 43 on "Radiation Safety for the Design and Operation of Particle Accelerator" [3].

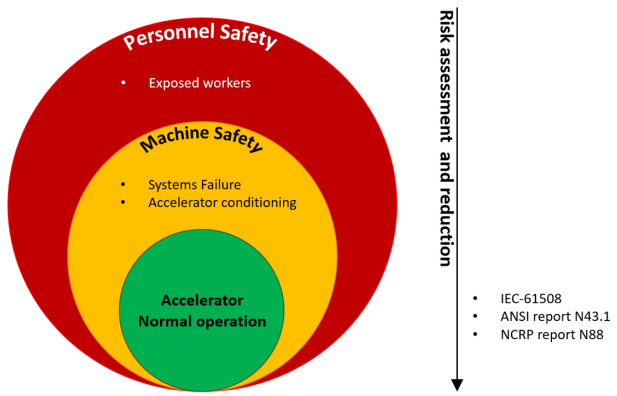

Figure 1: Risk assessment priority for particle accelerator facility.

At the National Laboratories of Frascati of the INFN, we developed a method to design and commisioning FPGA-based safety systems that could be involved for personnel and machine protection (MPS), compliant with the three standard listed in the previous paragraph. Such systems are designed, from both hardware and software point-of-view, to match with risk assessment and response time requirments, Fig. 1, of the hosting particle accelerator facility. According with our experience with IEC-61508 compliant safety systems [4], in this paper will be presented prototypes developed to operate as PSS (because it has higher constraints in terms of reliability compared to MPS) in order to investigate the faseability of our method to realize safety system suitable for new and old accelerator facility of the INFN with modern technologies like FPGA and dismiss old and expensive relay crates.

The project is split in two phases the development of this FPGA instrumentation:

1. A first prototype, based on FPGA on-the-shelf devices, have been used to test the method and especially the FPGA from both hardware and software point of view.

2. A second prototype, based on custom FPGA design, have been realized at INFN-LNF to test the method with a complete configuration of master and slave units.

Next sections of the paper will focus on main aspects of the safety-life-cycle developed in following to IEC-61508 standard, Fig. 2.

* stefano.pioli@lnf.infn.it

Content from this work may be used under the terms of the CC BY 3.0 licence (© 2019). Any distribution of this work must maintain attribution to the author(s), title of the work, publisher, and DOI

This is a preprint — the final version is published with IOP

ISBN: 978-3-95450-208-0 doi:10.18429/JACoW-IPAC2019-THPRB030

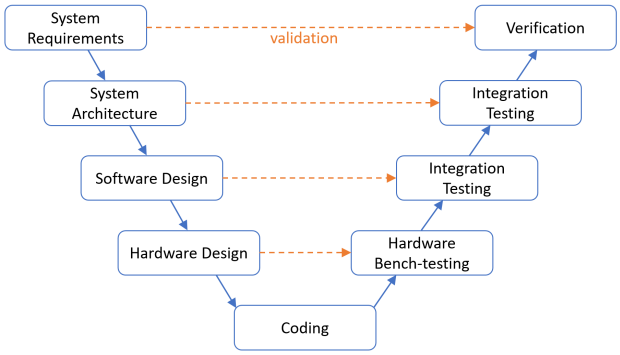

Figure 2: V-shaped safety-life-cycle developed to produce safety systems.

ARCHITECTURE AND DESIGN

Devices developed for this test have been installed at the Beam Test Facility (BTF), of the Dafne accelerator at INFN-LNF, to operate as dummy access control system in parallel with the operating PSS relay-based.
According with IEC standard, we identified the reliability required for the safety system, expressed as Safety Integrity Level (SIL), that for this kind of application should be at least SIL-2 or related to a Probability of Failure per Hour (PFH) $\geq 10^{-7}$ and $< 10^{-6}$.

For both FPGA devices a dual modular redundancy have been chosen in order to reach easily the overall reliability required for the system. Same strategy had been involved for the running PSS, then all the gates and buttons and so on are already equipped with double line dry contacts. For this test we replicated the safety of BTF-2 hall, as shown in Fig. 3, made of: 2 gates, 1 search and 1 emergency button, 1 red/green lamp and 1 bell. Dual line signals for every device have been collected, in parallel with the other system to doesn't affect it. In addiction with signals from devices, we collected the enabling signal from the running PSS in order to compare and log the reference enabling signal with our prototypes.

In both cases, the hardware configuration is made of:

- **Prototype-1** - Two National Instruments cRIO-9039 with one Xilinx Kintex-7 325T esch one equipped with one NI-9425 module for digital inputs and one NI-9485 relay module for digital outputs.

- **Prototype-2** - Two Xilinx Zynq FPGA master units each one equipped with a FMC-XM105 module to handle input and ouputs and one addictional Zynq card with a FMC-XM105 module to operate as slave unts through chained optical link.

In order to achieve all the requirements from ANSI and NCRP reports, we focus on several innovative strategies to achieve the proper fail-safe and fool-prof criteria.

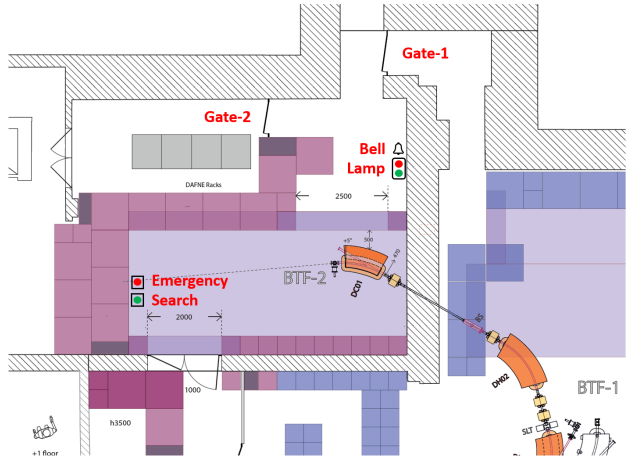

Figure 3: Topology of the BTF-2 hall with terminal user trasfer line of Dafne facility at Frascati. Detailed with red labels the personnel safety devices monitored: 2 gates, 1 red/green lamp, 1 bell, 1 search and 1 emergency button.

- All devices (gates, shielding door, ionizating chambers, etc...) and any output module on the safety system must be configured as normally open and interlock assumed active low. In this way, in case of power loss, the system will be intrinsecally safe.

- A continuos monitoring system based on watchdog and heartbeat, between either for FPGA and CPU either between master and slave units, allow to ensure deterministic communication.

- Real-time analysis of the response time of the system to verify the detection and execution time of the system.

- Integrity verification of system enabling to ensure the safety of the system and avoid tampering.

BENCH-TEST

At this time the Prototype-1, Figs. 4 - 5, have been coded and tested while Prototype-2 is under final development phase.
About the first device, both cRIO FPGAs have been programmed in order to replicate the logic to search the BTF. During bench-tests, reliability of the safety system has been invastigated through 3 main aspects: logic, response time and stability.

- Over 1000 times the search process have been tested with lamp, bell and a dummy search button. Same procedure has been repeated for the emergency button and for each one of fail-safe and fool-prof criteria.

- The response time measured from the FPGA itself shown a stable execution time of 15 μs. In order to measure the overall execution time of FPGA with IO modules, we involved an oscilloscope (LeCroy

This is a preprint — the final version is published with IOP
Content from this work may be used under the terms of the CC BY 3.0 licence (© 2019). Any distribution of this work must maintain attribution to the author(s), title of the work, publisher, and DOI

ISBN: 978-3-95450-208-0 doi:10.18429/JACoW-IPAC2019-THPRB030

HDO4000A) to measure the time required to trip the enabling signal in output when the emergency button signal trigger happens. From such test, repeated 100 times, results a stable overall execution time of about $0,5 \pm 0,012$ms due to relay switching latency.

- The stability of the device has been tested by searching the system and monitoring for 4 months its persistence of in this state.

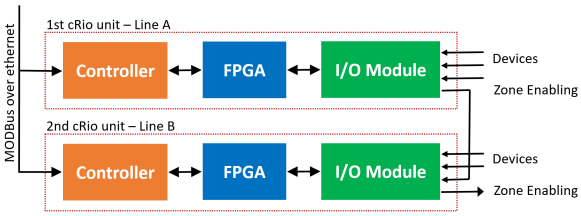

Figure 4: Functional block diagram of the cRio-based Prototype. Devices (gates, buttons, etc...) are acquired through digital I/O modules (in green). The FPGAs (blue) process the logic matrix for the PSS. Controllers (in orange) acquire FPGA data to stream to the accelerator control system with ModBUS protocol. The two unit operate in dual modular redundancy, then they are totally indipendent with same software on the FPGA. Each cRIO monitors the one of the two line of each device. Zone enabling signals, for RF systems, are daisy-chained in order to obtain a logic AND gate.

Figure 5: The two National Instruments cRIO-9039 running the same FPGA code in dual modular redundancy mode.

All these tests have been completed succesfully and now we are installing this prototype at the BTF in parallel with personnel safety system.

CONCLUSION

Both prototypes will run at BTF for 6 month to allow the evaluation of the safety system performances.
The overall reliability, of each protitype, is computed through Weibull distrubution of two parallel devices. Assuming the Mean Time Between Failure (MTBF), provided by Xilinx [5], of about 1×10^{10} h we estimated a PFH of 10^{-10} related to a SIL-4 classification that match with the requirments for any application of access control and machine protection.
If the final testing in BTF of both prototypes will be concluded successfully, as expected from bench-tests, we demonstrated the compliance with IEC, ANSI and NCRP standard then we could proceed with the update of safety systems taking advantage of a flexible and cheaper system, based on programmable electronics like the FPGA, able to process signals with a fast response time of 15 μs suitable for real-time monitoring of both personnel and machine safety systems.

REFERENCES

[1] *IEC-61508 - "Functional Safety"*, https://www.iec.ch/functionalsafety/

[2] *"Report No. 088 – Radiation Alarms and Access Control Systems"*, NCRP 1986. ISBN:0-913392-84-7

[3] Scott Walker et al, "ANSI N 431 Radiological Safety in the Design and Operation of Particle Accelerators", 2004.

[4] S. Pioli *et al.*, "The Machine Protection System for the ELI-NP Gamma Beam System", in *Proc. 8th Int. Particle Accelerator Conf. (IPAC'17)*, Copenhagen, Denmark, May 2017, pp. 1824–1826. doi:10.18429/JACoW-IPAC2017-TUPIK058

[5] *Xilinx, "Device Reliability Report"*, https://www.xilinx.com/support/documentation/user_guides/ug116.pdf

Content from this work may be used under the terms of the CC BY 3.0 licence (© 2019). Any distribution of this work must maintain attribution to the author(s), title of the work, publisher, and DOI

This is a preprint — the final version is published with IOP