ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-THCPR01

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], D. G. C. Di Giulio[1], B. Buonomo[1], L. G. Foggetta [1], M. Belli[1], P. Valente[2], A. Variola[2]
[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-mechanical 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 possible the risk of an accidental exposition of workers to ionizating 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].

* stefano.pioli@lnf.infn.it

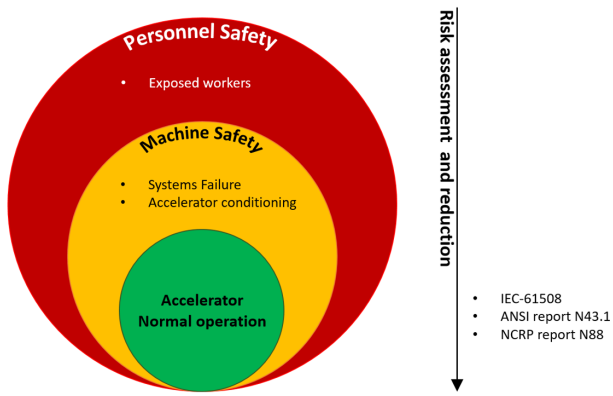

Figure 1: Risk assessment priority for particle accelerator facility.

At the National Laboratories of Frascati of the INFN, we developed a method to design and commissioning 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 requirements, Fig. 1, of the hosting particle accelerator facility.

Up to this moment several commercial solutions are available to suite with PSS and MPS requirements. PLCs can easily achieve required performances in terms of response time nevertheless introducing the compliancy with functional safety standards only few product can be involved for PSS purposes, due to a latency in response time of ~100 ms, and anyway with compliancy only from the hardware point-of-view. For these reasons we chose to develop hardware and software of a new kind of high reliability FPGA-based device according with IEC-61508 standard, NCRP report 88 and ANSI report 43.1 to match all requirements of PSS and MPS. 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 feasibility of our method to realize safety system suitable for new and old accelerator facility of the INFN with modern and mature technologies like FPGA and dismiss old and expensive relay crates.

The minimal features of such device will include:

- Response time able to perform real-time intervention (for accelerators with repetition rate of at least 1 kHz);

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-THCPR01

- Dual Modular Redundancy to maximize system reliability and availability;
- Modular and distributed design to scale the system through a multi-node network with optical links to fit with the architecture of large facilities;
- Fail-safe and fool-proof design to maintain the safety of the facility even in case of equipment malfunction;
- Scalable design to acquire/produce digital signals where needed from the infrastructure;
- Compliance with the IEC-61508 standard on "Functional Safety", NCRP reports 88 on "Radiation Alarms and Access Control Systems" and ANSI reports 43.1 on "Radiation Safety for the Design and Operation of Particle Accelerator" integrated in both hardware and software design.

This versatile device can be scaled to meet accelerator demands, the application on accelerator infrastructures will guarantee so high level of reliability such that a case-study for the integration also as Personnel Safety System, against workers exposure risks from prompt ionizing radiation, will be demonstrated.

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.

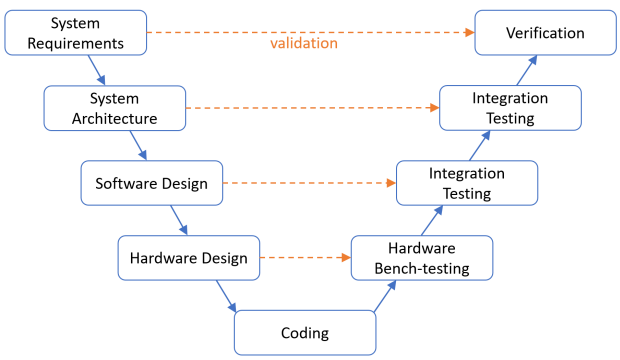

Figure 2: V-shaped safety-life-cycle developed to produce safety systems.

Next sections of the paper will focus on main aspects of the safety-life-cycle developed according V-shaped model as in Fig. 2.

SYSTEM REQUIREMENTS

In this phase an analysis of the generic requirements of the particle accelerator and/or the specific ones of each subsystem is performed. We determine goals that the protection system will have to perform. For each accelerator sub-system is used to highlight possible critical scenarios and limits of use that can lead to a malfunction.

In particular for PSS, the case study will highlight any risk or scenario in which workers may be accidentally exposed. For MPS, we highlight problems that could cause damage to the equipment of the particle accelerator affecting the operation of the machine both from the point of view of malfunctioning sub-systems, both from the point of view of possible damage caused to the equipment from accidental dispersion of the accelerated particle beam.

SYSTEM ARCHITECTURE

In this phase we classify functions of the system according to the critical aspects highlighted in the risk analysis through a functional division of the problems according to key criteria such as:

- Response time;
- Reliability;
- Criticality in case of failure.

Each group of case studies are thus divided into ''functions" so that for each one of them can provide to quantify the necessary level of failure rate, reliability and availability. At this point, a functional architecture scheme is developed equipped, for each function, with the hardware technology (FPGA in this case) and the appropriate redundancy strategies that guarantee the above criteria. This phase ends with the elaboration of a ''logical matrix" that indicates the correlations between the possible failures verifiable and the relative solutions.

SYSTEM DESIGN

Devices developed for this test have been installed at the Beam Test Facility (BTF) [5–7], 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 $< 10^{-6}$.

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.

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

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-THCPR01

- 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.

Hardware Design

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.

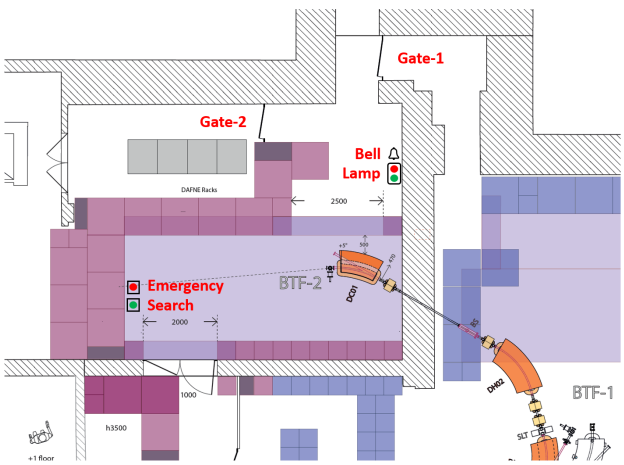

Figure 3: Topology of the BTF-2 hall with terminal user transfer line of Dafne facility at Frascati. Detailed with red labels the personnel safety devices monitored: 2 gates, 1 red/green lamp, 1 bell, 1 search and 1 emergency button.

In both cases, the hardware configuration is made of:

- **Prototype-1** - Two National Instruments cRIO-9039 with one Xilinx Kintex-7 325T each 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 outputs and one additional Zynq card with a FMC-XM105 module to operate as slave units through chained optical link.

Software Design

In this phase of the project, for every function of the architecture, an hardware design is elaborated according to satisfies the guidelines of the previous phase and a software design based on two modules: a finite-state- machine and an application. The state machine, as reported in Fig. 4, is based on a loop of states:

1. Identify - All input informations are pre-processed and/or combined to match the data format and additional informations on inputs.
2. Solve - Data from the previous state is processed by the "application", developed according to the logic matrix, to identify the action to perform in response to detected issues. For the PSS, a series of modules monitors the status of emergency buttons, gates and search buttons in order to drive lamps, bells and enabling signals to RF systems.
3. Execute - At this point the data processed in the previous state are converted into outputs to be applied to the accelerator sub-systems.
4. Sleep - This is a fail-safe status that replaces the "identify" state, when a failure of the system is detected, in order to send in safe state any module of the safety system and any connected sub-systems of the accelerator.

While the application program represents the coded version of the logic matrix, the finite-state-machine and the hardware are designed to ensure fail-safe and the fool-prof of the system. The fail-safe it is achieved through:

- Normally open switches to sub-systems that, in the absence of the power supply of the safety system, return independently to a safe status of the hardwired system.
- Continuous verification systems ("watchdog" and "heartbeat") that verify the correct operation of the state machine in the master unit and, if present, in secondary slave units and therefore also the integrity of the communications between them.
- Continuous verification of reaction times of the state machine which, even if system is working properly, it must be comply with the design criteria.
- Monitoring of nominal voltages of safety system power supplies.

About the fool-proof of the system, this protection against tampering is achieved through:

- Allow the main unit of the system and any secondary units to operate on isolated data network.
- By protecting the software with passwords that prevent modification.
- Isolate the security system and the terminal blocks in closed racks.
- In the case of PSS, an integrity check is performed to re-acquire the status of the enabling signal sent to the sub-systems. In case there is a discrepancy between

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-THCPR01

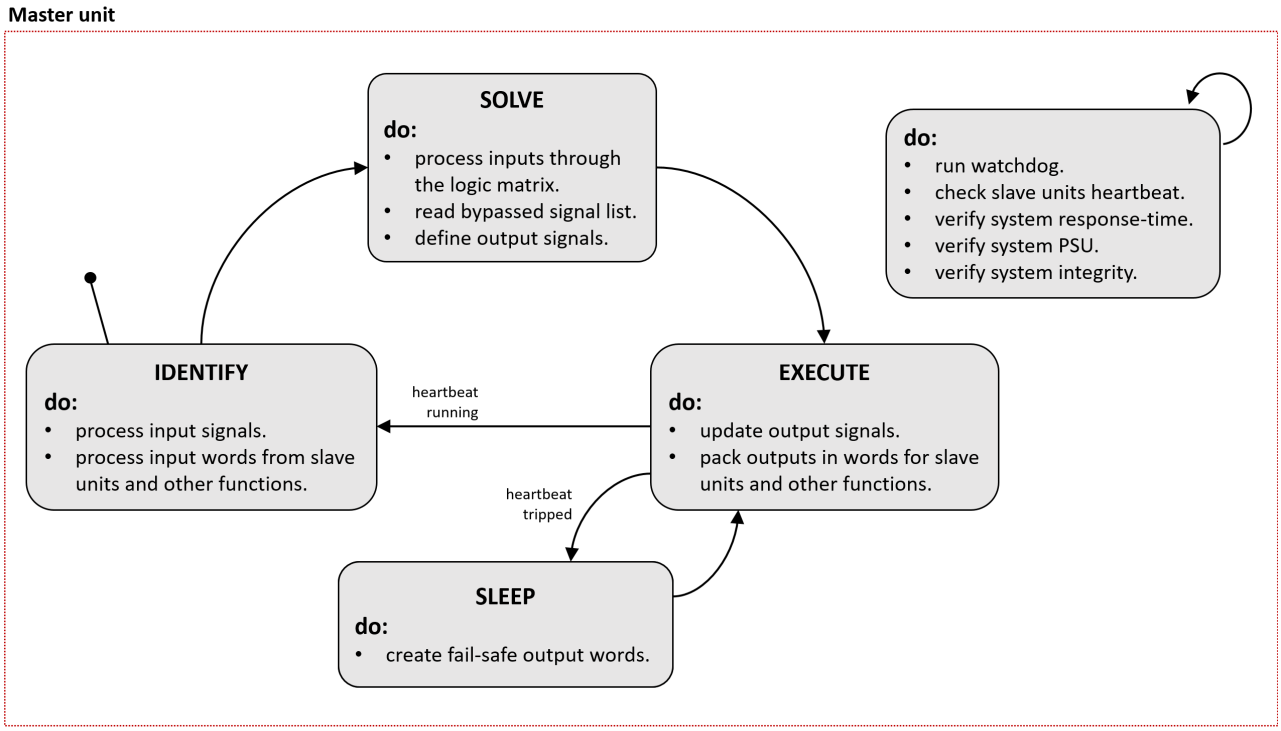

Figure 4: Master unit finite-state-machine. The identify-solve-execute loop acquire data, run the logic matrix and execute over the interface of the system. If the dedicated fail-safe and fool-proof loop detect a fault in the integrity of the system, the sleep mode is engaged streaming a fail-safe word through the system interface.

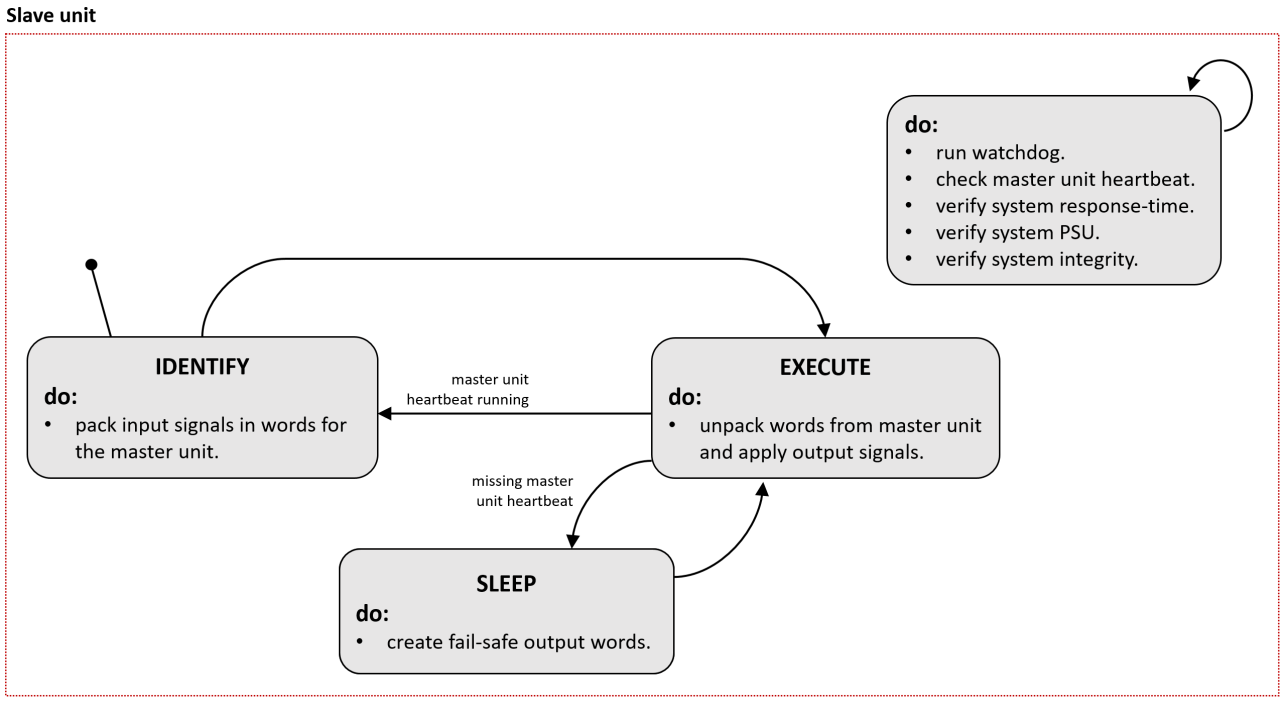

Figure 5: Slave units finite-state-machine. In these nodes of the system data are streamed in/out from the master unit that is always in charge to process the logic matrix. If the dedicated fail-safe and fool-proof loop detect a fault in the integrity due to missing communication with the master or due to fault detected from the master (maybe due to the failure of another slave unit), the sleep mode is engaged streaming a fail-safe word through the system interface.

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-THCPR01

outgoing and re-acquired enabling signals (indicating that the security system has been bypassed) the safety system goes in safe state.

The main unit of each function can acquire input signals from sub-systems accelerator, its slave units and other functions of the safety system. Signals produced as output are distributed by the main unit directly to the to the accelerator equipment either directly or via slave units.

The number of slave units varies according to the architecture of the facility. Slave units operate as extensions of the state machine of the master unit, as reported in Fig. 5, by through simplified coding of fail-safe and fool-proof criteria and input/output communications through master unit that is always in charge to run the "application" in the state-machine. Communications through different sub-units of a function of the system, or between the different functions of the system, take place via coded words.

BENCH-TEST

At this time the Prototype-1, Figs. 6 and 7, have been coded, tested and installed at BTF 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 investigated 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 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 ±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.

All these tests have been completed successfully and now this prototype, installed at the BTF in parallel with the oprating relay-based personnel safety system, is properly running and statistics acquired.

CONCLUSION

Both prototypes will run at BTF for 12 months in order to allow the evaluation of the safety system performances.

The overall reliability, of each prototype, is computed through Weibull distribution of two parallel devices. Assuming the Mean Time Between Failure (MTBF), provided by

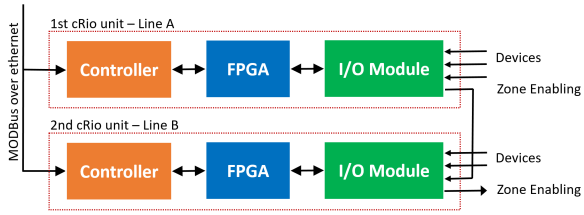

Figure 6: Functional block diagram of the cRio-based Prototype. Devices (gates, buttons, etc...) are acquired through digital I/O modules (in green). The FPGAs (blue) process the logic matrix for the PSS. Controllers (in orange) acquire FPGA data to stream to the accelerator control system with ModBUS protocol. The two unit operate in dual modular redundancy, then they are totally independent 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 7: The two National Instruments cRIO-9039 running the same FPGA code in dual modular redundancy mode.

Xilinx [8], of about 1×10^{10} h we estimated a PFH of $9,5^{-7}$ related to a SIL-2 classification that match with the requirements 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.

In future development we will involve up to 16 FPGA devices as upgrade of PSS and CAMAC systems of the BTF and LINAC of the Dafne facility. Taking in account previous fault of the PSS, these extensive setup will allow within 3 years to obtain enough statistics for a complete characterization of the reliability of such devices.

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-THCPR01

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] L. Scott Walker and J. Liu, "ANSI N 431 Radiological Safety in the Design and Operation of Particle Accelerators", 11. International Congress of the International Radiation Protection Association, Madrid, Spain, May 2004.

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

[5] P. Valente, B. Buonomo, D. G. C. Di Giulio, and L. G. Foggetta, "Frascati Beam-Test Facility (BTF) High Resolution Beam Spot Diagnostics", in *Proc. IBIC'16*, Barcelona, Spain, Sep. 2016, pp. 221–224. doi:10.18429/JACoW-IBIC2016-MOPG65

[6] B. Buonomo, D. G. C. Di Giulio, L. G. Foggetta, and P. Valente, "The Frascati LINAC Beam-Test Facility (BTF) Performance and Upgrades", in *Proc. IBIC'16*, Barcelona, Spain, Sep. 2016, pp. 396–399. doi:10.18429/JACoW-IBIC2016-TUPG29

[7] B. Buonomo, D.G.C. Di Giulio, L.G. Foggetta, and P. Valente, "A Hardware and Software Overview on the New BTF Transverse Profile Monitor", in *Proc. IBIC'16*, Barcelona, Spain, Sep. 2016, pp. 819–822. doi:10.18429/JACoW-IBIC2016-WEPG73

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