CHEMICAL ENGINEERING TRANSACTIONS

VOL. 53, 2016

A publication of
AIDIC
The Italian Association
of Chemical Engineering
Online at www.aidic.it/cet

Guest Editors: Valerio Cozzani, Eddy De Rademaeker, Davide Manca
Copyright © 2016, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-44-0; **ISSN** 2283-9216

DOI: 10.3303/CET1653048

FPGA-Based I&C Systems in Nuclear Plants

Marcos S. Farias, Roque H. S. Martins, Pamela I. N. Teixeira, Paulo Victor R. Carvalho

Instituto de Engenharia Nuclear – 75 Hélio de Almeida str - Cidade Unversitária – Rio de Janeiro - Brazil
msantana@ien.gov.br

The FPGA (field programmable gate array) is a digital device widely used in various fields of industry. FPGAs can be used to perform functions that are safety critical and require high reliability, like in automobiles, aircraft control and assistance and mission-critical applications in the aerospace industry. With these merits, FPGAs are receiving increased attention worldwide for application in nuclear plant instrumentation and control (I&C) systems, mainly for Reactor Protection System (RPS).

Reasons for this include the fact that conventional analog electronics technologies are become obsolete. I&C systems of new Reactors have been designed to adopt the digital equipment such as PLC (Programmable Logic Controller) and DCS (Distributed Control System). But microprocessors-based systems may not be simply qualified because of its complex characteristics. For example, microprocessor cores execute one instruction at a time, and an operating system is needed to manage the execution of programs. As a result, nuclear power plant operators and I&C suppliers may consider other non-computer-based digital technologies, such as devices that may be configured using HDL (Hardware Description Language).

FPGAs, commonly referred to as HDL programmable devices (HPDs), can run without an operating system and the design architecture is inherently parallel. Despite the attractive features, the use of such programmable devices in safety critical systems for nuclear power plants is relatively new in many countries, and the regulatory approach to licensing such devices may not be clear.

In this paper we aim to assess advantages and the limitations on FPGA-based solutions, considering the design guidelines and regulations on the use of FPGAs in Nuclear Plant I&C Systems. We will also examine some circuit design techniques in FPGA to help mitigate failures and provide resilience. The objective is to show how FPGA-based systems can provide cost-effective options for I&C systems in modernization projects, ensuring safe and reliable operation, meeting licensing requirements, such as separation, redundancy and diversity.

1. Introduction

Instrumentation and control (I&C) functions, systems and components in nuclear plants may be classified into two categories: items important to safety and items not important to safety. Important to safety are functions, systems and components which contribute to safely shutting down the reactor and maintaining it in a safe shutdown condition while in accident conditions. Furthermore removing residual heat from the reactor core after shutdown, in all operational states and accident conditions (IAEA, 2015).

Conventional relay and analog electronics technologies used in original I&C systems of most nuclear plants are becoming obsolete. Utilities have been replacing these older systems with more modern microprocessor-based equipment. Also I&C systems of new nuclear reactors have been designed to adopt digital equipment such as PLC (Programmable Logic Controller) and DCS (Distributed Control System) and many microprocessor-based systems are in operation in plants worldwide.

As the nuclear power industry modernizes existing analogue instrumentation and control (I&C) systems in current nuclear power plants to incorporate digital I&C technology, as well as implementing new digital I&C systems in new plants, the industry is faced with significant challenges (IAEA NES, 2015), mainly in the form of uncertainty and inconsistency in developing and licensing digital I&C systems and equipment. There are difficulties with qualification and computer security that require substantial effort for evaluation and safety demonstration as part of the development, commissioning and licensing processes.

Please cite this article as: Farias M., Martins R.H.S., Teixeira P.I.N., Carvalho P.V., 2016, Fpga-based i&c systems in nuclear plants, Chemical Engineering Transactions, 53, 283-288 DOI: 10.3303/CET1653048

FPGAs offer the promise of greater simplicity and less burdensome regulatory approval. This is so because the end product can be designed such that it is purely hardware, similar to conventional analog electronics (EPRI, 2009).

FPGAs also provide the capability to protect against obsolescence by circuit independent, i.e., portable circuit to different FPGA architectures. But even though the final product is a hardware component, the design and implementation of an FPGA-based system has strong similarities with software-based systems (Ranta, 2012). So, design issues on using FPGA-Based I&C systems in nuclear reactors have to consider a life cycle similar to software. This life cycle is consistent with the one suggested by IEC 62566 standard (IEC, 2012), the only nuclear-specific international standard published providing requirements or recommendations for Category A applications based on programmable complex electronic components, like FPGAs.

The rest of this paper is organized as follows: Section 2 contain information about FPGAs, advantages and limitations as compared to other technologies. Later, in Section 3 we discuss design issues on using FPGAs. Last, in Section 4, we draw some conclusions and point out some directions for future work.

2. FPGA - advantages and limitations

FPGA includes thousands or millions of logic gates aligned in an array. The interconnections between each gate are allowed to be programmed in the field. Figure 1 illustrates the types of electronic hardware technologies that can be applied in nuclear plant I&C systems.

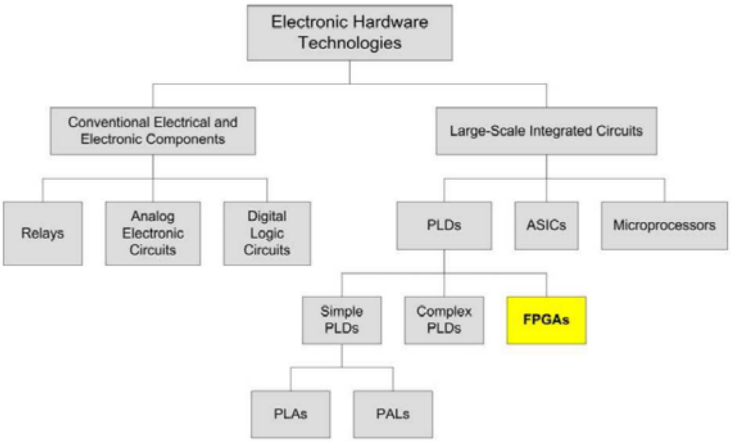

Electronic Hardware Technologies
Conventional Electrical and Electronic Components
Large-Scale Integrated Circuits
Relays
Analog Electronic Circuits
Digital Logic Circuits
PLDs
ASICs
Microprocessors
Simple PLDs
Complex PLDs
FPGAs
PLAs
PALs

Figure 1: Electronic Hardware Technologies Used in I&C Systems.

Conventional electrical and electronic components are rapidly becoming obsolete. Programmable logic devices (PLDs) fit into the overall landscape of electronic hardware technologies, including conventional technologies, ASICs and microprocessors. Application Specific Integrated Circuits (ASICs) are custom-designed and fabricated at the integrated circuit foundry. ASICs are cost-effective only when a much larger number of copies of the circuit will be deployed. FPGAs also can be considered PLDs, but they have a different internal architecture. A common basic architecture, illustrated in Figure 2, includes:

- A set of configurable logic blocks (CLBs). A CLB can be configured to implement any logic functions (AND, OR, XOR, NOT, etc.). Each CLB can be configured to implement an N-to-M Boolean function using simple logic gates, or may be configured to use a look-up table (LUT) to implement the logic function. Multiple CLBs can also be interconnected to generate more complex functions. The output of each CLB includes a flip-flop for synchronizing the data flow within the FPGA.
- A set of programmable Input/Output (I/O) blocks.
- An internal interconnection grid.
- Application data memory (RAM Block).

An FPGA is designed to be configured by a customer or a designer in the field, after being manufactured. Because, once programmed, an FPGA executes only that program repetitively and link only the functions needed for a given I&C application, they are substantially simpler than microprocessors, minimizing the risk posed by complexity (NRC, 2011).

The design and implementation of an FPGA-based system has strong similarities with software-based systems. Despite the similarities with software design, aspects of hardware design must be understood by the designer.

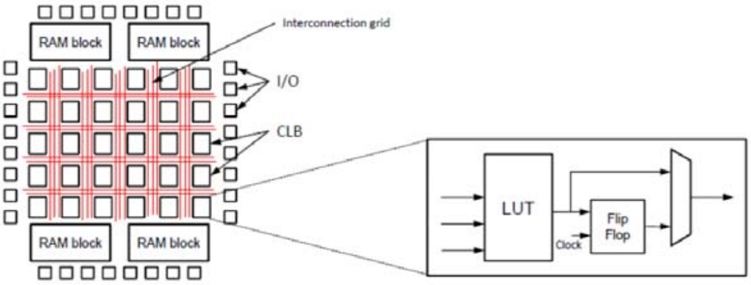


Figure 2: Typical FPGA architecture.

The levels of abstraction that a software-based system offers are not present in FPGA design. There is no system level or an operating system behind which the hardware issues are hidden. On the other hand, the complexity caused by the shared computing environment and interaction with other programs is absent (Ranta, 2012).

For applications with strict reliability and safety requirements, a design life cycle similar to software should be used. A safety-critical system is a system whose failure or malfunction may result in serious injury to people, loss or serious damage of equipment or environmental harm (Bernardeschi et al., 2015). A safety-critical system requires care in their specification and design in order to avoid errors that should result in unexpected system's behavior.

The FPGA programming process is usually composed of four main phases, along with the associated verification and validation activities, a life cycle consistent with the one suggested by IEC 62566 standard (IEC, 2012), as illustrated in Figure 3. The four phases are:

- Component requirements specification. These requirements usually result from I&C system architectural design.
- Preliminary design. Decide on the major design choices: balance between combinatorial logic and sequential design, decomposition into modules, the implementation of defensive design practices, and the identification of the circuit or circuit family to be used.
- Design. In this phase we develop a detailed description of the logic processing to be performed by the FPGA component. The design is usually expressed using a Hardware Description Language (HDL). A number of languages are available such as Verilog and Very-High-Speed Integrated Circuit (VHSIC) Hardware Description Language (VHDL).
- Implementation. Implementation is usually divided into two main steps: synthesis and place&route. The synthesis tool translates the circuit-independent (RTL) into an equivalent description that is expressed in terms of the resources provided by the selected FPGA circuit. The place&route tool calculates the best physical positions and mapping for the FPGA resources that are used. Lastly a bitstream is generated. The bitstream is the digital data that is sent to the FPGA circuit to program it.

In the FPGA design process (Figure 3), only the final steps (synthesis plus place&route) are dependent on the particular FPGA device circuit chosen. Thus, provided that the initial I&C system design incorporates appropriate provisions for this, when the circuit becomes obsolete it can be replaced by another one using the currently-available technology and the same RTL level representation of the design (EPRI, 2009).

FPGAs also has adequate capabilities for a wide range of applications because can process independent functions in a parallel hardware implementation and with high clock speeds. When specifically designed to support safety applications and to comply with nuclear industry standards, FPGAs are simpler, more reliability than microprocessor-based systems. Also, concerned to cyber-security, FPGA-based solutions have characteristics that tend to increase the level of difficulty that would be faced by a would-be attacker as compared to conventional microprocessor-based systems (EPRI, 2009). Malicious functions must be introduced as complete designs, using technology-specific engineering tools, raising the level of difficulty.

Though not an advantage of the technology as such, simply by being different from microprocessors, FPGAs provide an opportunity for a diverse implementation (Ranta, 2012).

Limitations on the use of FPGA results mainly from the need for specialized expertise on design team. The design team needs to have HDL coding expertise and an understanding of software-like development and V\&V processes to ensure that the design meets the application requirements (EPRI, 2009). The HDL description is not software code that will be translated into computer instructions to be run on a machine, but rather is a description of the behaviour of a circuit.

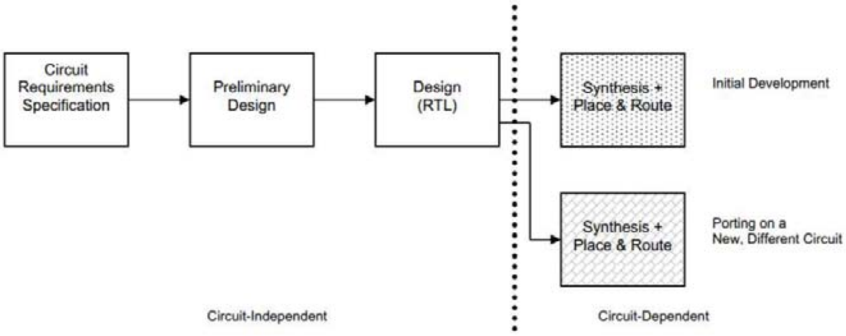

Circuit Requirements Specification
Preliminary Design
Design (RTL)
Synthesis + Place & Route
Initial Development
Synthesis + Place & Route
Porting on a New, Different Circuit
Circuit-Independent
Circuit-Dependent

Figure 3: Porting applications to a new or different FPGA circuit vendor

3. Design issues on using FPGA

There are three main technologies applied for storing the configuration of the interconnection grid and the configurations of the CLBs and I/O blocks in an FPGA:

- SRAM - static random access memory or SRAM is re-writable, which means that the implemented functionality can be modified without physically replacing the FPGA component. With SRAM the programming is not retained by the circuit on a loss of power.
- Flash and EPROM - erasable programmable read-only memory (EPROM) and flash technologies are re-writable and non-volatile.
- Antifuse - this technology is non-rewritable and non-volatile.

It is considered that the best choice for safety-critical systems, such as those in nuclear plants, is antifuse technology. The non-volatility and non re-programmability prevent accidental and malicious changes to functions. Antifuse also has the best resistance to radiation.

The majority of FPGA families are SRAM-based. This option is volatile. Thus, at power-up they must be reloaded from an external configuration system. Also, most SRAMs are susceptible to random, radiation-induced hardware alterations (so-called Single-Event Upsets, or SEUs).

SEU is a “soft” error that changes the state of a bistable element. A SEU affecting a combination part makes a transient error in logic gates. This can be propagated to the sequential part and make a bit-flip error. Figure 4 illustrates how an SEU makes a bit-flip error in a flip-flop (Asadi and Tahoori, 2005). This susceptibility should be addressed as required in the design, based on the expected environment and the risks associated with the impact of SEUs (EPRI, 2009).

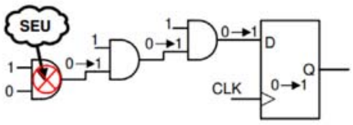


Figure 4: Bit-flip error caused by SEU

Among all SEU mitigation techniques, Triple Modular Redundancy (TMR) has become the most common practice because of its straightforward implementation and reliable results. The TMR mitigation scheme uses three identical logic circuits performing the same task in parallel with corresponding outputs being compared through majority voters (Carmichael, 2001). Figure 5 shows a representation of TMR with a single majority voter.

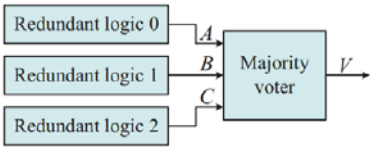


Figure 5: TMR with a single majority voter.

The function of the majority voter is to output the logic value (“1” or “0”) that corresponds to at least two of its inputs. For example, if two or more of the voter’s three inputs are “1”, then the output of the voter is “1”.

Another flexible fault mitigation method is triple device redundancy (TDR) in which a single FPGA design is replicated three times in redundant FPGA devices, as showed in Figure 6. These devices could be from different technologies (SRAM, Antifuse). TDR can filter multiple event upsets, multiple transient upsets, and any other functional interrupts including total device failure (Carmichael, 2001).

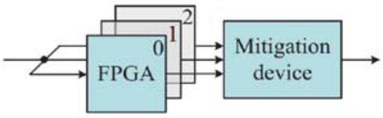


Figure 6: TMR implemented for the entire device.

3.1 Testing the TMR mitigation scheme

To test the TMR scheme, the logic of a reactor protection system was modeled in LabView environment, both in the original circuit as in redundancy with circuit triple and voter. Figure 7 shows a small part in the LabView (original circuit and triple redundancy morevoter).

In LabView, signals were generated that randomly alter the bit at the output of the logic circuit, from "0" to "1" and vice versa.

The use of triple redundancy and voter in the eight protection logic is shown in Figure 8. The protection logic circuits, whose outputs are represented on the left side of Figure 8, receive 34 logic signals from the plant. The result of false trips generated and unidentified trips proves the best expected performance of circuits with redundancy in the task of mitigating SEU errors.

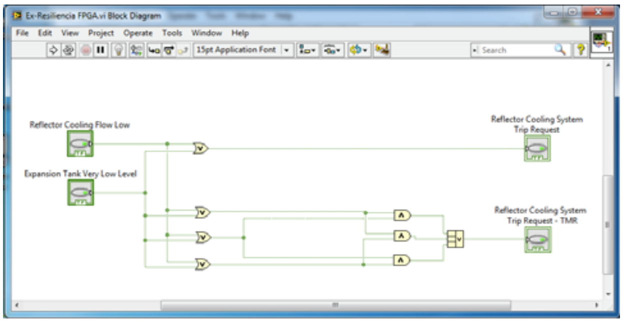
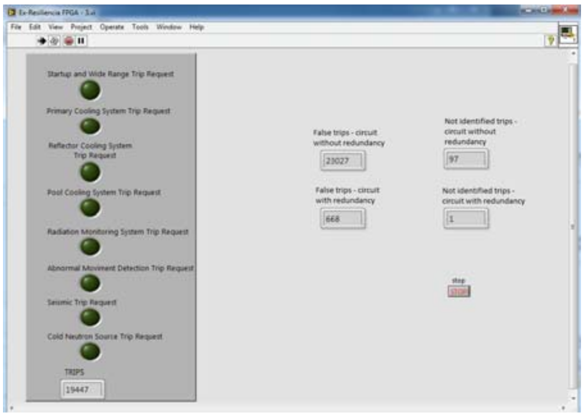

Ex-Resiliencia FPGA.vi Block Diagram
File
Edit
View
Project
Operate
Tools
Window
Help
15pt Application Font
Search
Reflector Cooling Flow Low
Expansion Tank Very Low Level
Reflector Cooling System Trip Request
Reflector Cooling System Trip Request - TMR

Figure 7: Small part of protection logic modeled in LabView.


Ex-Resiliencia FPGA - 3.vi
File
Edit
View
Project
Operate
Tools
Window
Help
Startup and Wide Range Trip Request
Primary Cooling System Trip Request
Reflector Cooling System Trip Request
Pool Cooling System Trip Request
Radiation Monitoring System Trip Request
Abnormal Moviment Detection Trip Request
Seismic Trip Request
Cold Neutron Source Trip Request
stop
STOP

TRIPS 19447

False trips - circuit without redundancy 23027

Not identified trips - circuit without redundancy 97

False trips - circuit with redundancy 668

Not identified trips - circuit with redundancy 1

Figure 8: Simulation results in LabView.

3.2 Diversity

FPGA-based equipment provides an attractive design option when Diverse Actuation Systems (DAS) are required according to current regulations to prevent common cause failures.

FPGA-based equipment can provide a more practical and cost-effective solution compared to providing a diverse microprocessor-based system, or when diversity requirements demand a non-microprocessor-based solution (EPRI, 2009). Applications allow the use of two additional kinds of the diversity (Yastrebenetsky, 2014):

- FPGA vs. MP (Microprocessor-based) - main system is developed using FPGAs, diverse system is developed using MPs.

- FPGA1 vs. FPGA2 - different manufacturers (Altera, Xilinx, Actel-Microsemi), technologies (SRAM, Flash, Antifuse) development techniques are used to develop main and diverse systems.

Also is possible the diversity between two logic cores in the FPGA (EPRI, 2009). This is achieved through use of different synthesis directives. Once the HDL is created, it is synthesized differently for the two different cores, resulting in a different hierarchical structure, finite state machine encoding, and state decoding for each core. A self-test circuit detects any mismatch between the outputs of the two parallel diverse logic cores.

4. Conclusions

In this paper the authors have presented issues on using FPGA-Based I&C Systems. FPGA is relatively new digital technology in the nuclear industry. A notable feature of FPGAs is its simplicity compared with microprocessor-based systems. FPGA-based systems do not need any operating system, and can implement application logic directly into the FPGA circuits. FPGA-based systems also can provide cost-effective options for I&C systems in nuclear reactors, ensuring safe and reliable operation.

For safety-related applications, it is of overriding importance to keep the design as simple as possible. This helps avoid problems in the final product and makes verification and validation easier. We presented some methods to keep the design simple while addressing regulation requirements such as diversity and redundancy.

Hardware design expertise when designing FPGA-based systems is necessary. But with the advent of HDL and tool suites that allow FPGAs to be programmed by people who may only have software expertise, the need for electrical engineering design expertise is often overlooked. The main point is that both aspects are important a good understanding of software development processes and V&V (Validation and Verification) to ensure that no errors are designed into the programming of the FPGA, and a good understanding of hardware design issues to ensure reliable operation of the device (EPRI, 2009).

The demands arising from new projects in Brazil, as I&C modernization projects and the RMB (Brazilian Multipurpose Reactor), will bring the need of new professionals with training in regulation and guidance regarding the use of FPGA technology in the nuclear industry.

Acknowledgments

The authors gratefully acknowledge the support of the National Council of Scientific and Technological Development (CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico), the support of the Rio de Janeiro Research Support Foundation (FAPERJ - Fundação de Amparo a Pesquisa do Rio de Janeiro), and also the support of National Nuclear Energy Commission (CNEN – Comissão Nacional de Energia Nuclear).

References

Asadi G. and Tahoori M. B., 2005, Soft error rate estimation and mitigation for SRAM-based FPGAs. In 13th international symposium on Field-programmable gate arrays.

Bernardeschi C., Cassano L. and Domenici A., 2015, SRAM-based FPGA systems for safety-critical applications: A survey on design standards and proposed methodologies. Journal of Computer Science and Technology

Carmichael C., 2001. Triple Module Redundancy Design Techniques for Virtex FPGAs. Xilinx Application Notes, XAPP197.

EPRI, 2009, Guidelines on the Use of Field Programmable Gate Arrays (FPGA) in Nuclear Power Plant I&C Systems. Palo Alto, USA.

IAEA, 2015, Instrumentation and Control Systems and Software Important to Safety for Research Reactors, Safety Standards No. SSG-37, Vienna, Austria.

IAEA NES (Nuclear Energy Series), 2015, Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants, Vienna, Austria.

IEC, 2012, Nuclear Power Plants Instrumentation and Control Important to Safety Development of HDL programmed Integrated Circuits for Systems Performing Category A. International Electrotechnical Commission 62566.

NRC, 2011, Digital Instrumentation and Controls. U.S. Nuclear Regulatory Commission

Ranta J., 2012, The current state of FPGA technology in the nuclear domain. Technical report, VTT Technology.

Yastrebenetsky, M., 2014 Nuclear Power Plant Instrumentation and Control Systems for Safety and Security. IGI Global.