Annals of Nuclear Energy 108 (2017) 198–228

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Failure mode taxonomy for assessing the reliability of Field Programmable Gate Array based Instrumentation and Control systems

Phillip McNelles [a,b,*], Zhao Chang Zeng [a], Guna Renganathan [a], Marius Chirila [a], Lixuan Lu [b]

[a] Canadian Nuclear Safety Commission, 280 Slater Street, Ottawa, Ontario K1P 5S9, Canada
[b] University of Ontario Institute of Technology, 2000 Simcoe Street, Oshawa Ontario L1H 7K4, Canada

ARTICLE INFO

Article history:
Received 14 January 2017
Received in revised form 20 April 2017
Accepted 22 April 2017

Keywords:
FPGA
Failure modes
Taxonomy
Nuclear Power Plant
Digital I&C

ABSTRACT

Field Programmable Gate Arrays (FPGAs) are a form of programmable digital hardware configured to perform digital logic functions. This configuration (programming) is performed using Hardware Description Language (HDL), making FPGAs a form of HDL Programmed Device (HPD). In the nuclear field, FPGAs have seen use in upgrades and replacements of obsolete Instrumentation and Control (I&C) systems. This paper expands upon previous work that resulted in extensive FPGA failure mode data, to allow for the application of the OECD-NEA failure modes taxonomy. The OECD-NEA taxonomy presented a method to model digital (software-based) I&C systems, based on the hardware and software failure modes, failure uncovering effects and levels of abstraction, using a Reactor Trip System/Engineering Safety Feature Actuation System (RTS/ESFAS) as an example system. To create the FPGA taxonomy, this paper presents an additional "sub-component" level of abstraction, to demonstrate the effect of the FPGA failure modes and failure categories on an FPGA-based system. The proposed FPGA taxonomy is based on the FPGA failure modes, failure categories, failure effects and uncovering situations. The FPGA taxonomy is applied to the RTS/ESFAS test system, to demonstrate the effects of the anticipated FPGA failure modes on a digital I&C system, and to provide a modelling example for this proposed taxonomy.

1. Introduction

A Field Programmable Gate Array (FPGA) belongs to a group of digital technologies known as Hardware Description Language (HDL) Programmed Devices (HPD). These are large scale integrated circuits that are programmed (configured) by the end user after they are built, in order to perform certain digital logic functions (IAEA, 2016). These logic functions are performed using the FPGA hardware, as there is no software or operating system present on the FPGA chip itself. The blank FPGAs are configured using HDLs, of which VHDL and Verilog are the most popular, and both of those languages possess their own IEEE standards. The HDLs textually describe the architecture of the logic functions and connections that will occur inside the FPGA chip, and then the design is synthesized onto the FPGA chip using software tools, creating the physical routing and logic functions.

FPGAs have been the focus of research projects and implementation projects for safety-related and non-safety related Nuclear Power Plant (NPP) systems in several countries across North and South America, Europe and Asia (McNelles and Lu, 2013; Electric Power Research Institute, 2009; EPRI, 2011; Menon and Guerra, 2015). Often, the FPGA-based systems are installed to replace the existing analog or digital systems, which are becoming obsolete. FPGAs possess certain potential advantages over other Instrumentation and Control (I&C) technologies, such as reduced complexity, faster response times, the ability to partition safety and non-safety functions on the FPGA chip, and the inclusion of FPGAs could help meet diversity requirements (IAEA, 2016; Valtion Teknillinen Tutkimuskeskus, 2011). FPGAs are not without drawbacks though, and certain limitations of FPGA-based systems include a lack of experience in the nuclear field, a limited number of platforms/-tools, and less access to the internal signals of an FPGA, when compared to a microprocessor (IAEA, 2016; Valtion Teknillinen Tutkimuskeskus, 2011). The effect of FPGAs and other HDL technologies has been listed as one of the seventeen "important issues" facing digital I&C systems in Nuclear Power Plants (NPPs), according to the IAEA (IAEA, 2015). Nevertheless, FPGA implementations are continuing to take place in the nuclear field, with many examples seen in the technical literature (IAEA, 2016; McNelles and Lu, 2013; Electric Power Research Institute, 2009; EPRI, 2011; Menon and Guerra, 2015; Valtion Teknillinen Tutkimuskeskus, 2011).

* Corresponding author at: Canadian Nuclear Safety Commission, 280 Slater Street, Ottawa, Ontario K1P 5S9, Canada.
E-mail address: phillip.mcnelles@canada.ca (P. McNelles).

http://dx.doi.org/10.1016/j.anucene.2017.04.033
0306-4549/

In order to be able to analyze the reliability of FPGAs and FPGA-based systems, the potential failure modes of FPGAs, including both the hardware and HDL components, must be established. Previously, available technical literature on the topic of FPGAs has been reviewed and Failure Mode and Effects Analysis (FMEA) for FPGA-based systems has been compiled (McNelles et al., 2015), according to the International Electrotechnical Commission (IEC) FMEA standard International Electrotechnical Commission, 2006. This work is expanded on significantly in this paper, to create a taxonomy of FPGA failure modes that can be used in the modelling of FPGA-based systems, based on the taxonomy created for software-based systems.

The framework used to develop the FPGA taxonomy is based on the OECD-NEA Taxonomy for Digital I&C Systems (OECD-NEA, 2015). It considered a generic, software-based digital I&C system, such as one based on a microprocessor, so FPGAs and other HPDs were not in the scope of that framework. One of the recommendations in the OECD-NEA taxonomy stated that future work should involve *"Complementation of the failure modes taxonomy with issues that were left out of the scope, e.g., control systems, networks, PLD technology (FPGA/ASIC)"* OECD-NEA, 2015. This makes the extension of the OECD-NEA taxonomy to include FPGA-based systems, via the FPGA FMEA and resulting FPGA taxonomy a useful and logical endeavor. This taxonomy was further enhanced through the inclusion of high-level fault classifications as well as IEC fault classifications, to provide additional information on the failure modes and the mitigation measures. In order to extend the framework of the OECD-NEA taxonomy to incorporate FPGAs and other HPDs, and therefore creating the FPGA Taxonomy, the authors of this paper propose the creation of the "Logic Process" block. This block represents the all digital logic hardware and software/HDL code for any form of digital logic device, making it a suitable bridging point for HPDs such as FPGAs and the OECD-NEA taxonomy.

This paper is organized as follows: Section 2 discusses the OECD-NEA digital failure mode taxonomy that is used as the basis for this paper, and the extension of that taxonomy for the inclusion of FPGA-based systems, including the creation and implementation of the "Logic Process". Section 3 discusses failure mode categorization methodologies as well as the FPGA FMEA. Section 4 presents the FPGA taxonomy, in-line with the generic digital failure modes taxonomy. Section 5 showcases the demonstration of FPGA taxonomy. Conclusions from this research will be drawn in Section 6. A list of all failures used in this paper is provided in Appendix A.

2. Extended taxonomy

To fully implement the FPGA taxonomy within the framework of the OECD-NEA taxonomy, it must be extended to incorporate FPGA-based systems. As the OECD-NEA taxonomy did not explicitly consider HPDs such as FPGAs, the OECD-NEA taxonomy must be modified to incorporate FPGA-based systems. To do so, this paper proposes the introduction of a "logic process" block, which incorporates established implementations of digital hardware and software. Section 2.1 explains the importance and relevance of creating the FPGA taxonomy. Section 2.2 provides a detailed overview of the OECD-NEA failure mode taxonomy. Section 2.3 discusses the extension of the OECD-NEA taxonomy to include FPGA-based systems, through the use of the "logic process".

2.1. Importance and relevance of the FPGA taxonomy

The importance of constructing a failure modes taxonomy for FPGA-based systems is well-supported in the literature. This is seen in information published from international organizations (IAEA, IEEE and the OECD-NEA), as well as in a survey of the scientific/technical literature.

2.1.1. Information from international organizations

According to documents from the IAEA, "An increased number of FPGA based applications can be expected as nuclear operators and regulators become more familiar with the advantages of the technology" and that "…the technology is expected to be applicable to large scale replacement of I&C systems in modernization projects, as well as providing complete I&C systems (safety and non-safety) in new Nuclear Power Plant designs" (IAEA, 2016). Additionally, although FPGAs have seen increased implementations in NPP I&C functions, those are mainly recent implementations, so information regarding "lessons learned" and technical standards are not prevalent (IAEA, 2015). With the increased use of FPGA-based I&C systems in nuclear plants, this taxonomy will provide additional technical information for the purpose of hazard analysis.

The reason for performing hazard analysis is said to be to *"identify and control conditions that produce or contribute to a hazard"* (IEEE Power and Energy Society, 2016). This includes the identification, avoidance, evaluation and resolution of hazards in all phases of the system lifecycle. These hazards are caused by failure modes, which must be identified and evaluated. Therefore, the FPGA taxonomy presented in this paper provides a means of identifying, categorizing and modelling the failure modes for use in hazard analysis, during the design and review of FPGA-based I&C systems. This would provide a basis for the decisions on engineering and safety based on system review criteria (Mossman et al., 2013).

Regarding the OECD-NEA taxonomy, it was stated in that document that "An activity focused on the development of a common taxonomy of failure modes is seen as an important step towards standardised digital Instrumentation and Control (I&C) reliability assessment techniques" (OECD-NEA, 2009) and "The taxonomy will be the basis of future modelling and quantification efforts" (OECD-NEA, 2015). These statements from the OECD-NEA underscore the importance of having a failure modes taxonomy for the analysis and assessment of digital systems. As stated previously, the OECD-NEA taxonomy considered a software-based system, and stated that the development of an FPGA taxonomy would be a source of future work on this topic.

Furthermore, the OECD-NEA taxonomy document laid out certain criteria, which the taxonomy was intended to meet. The only criteria that was designated as "Not Met", was entitled "*Should capture defensive measures against fault* Propagation (detection, isolation and correction) and *other essential design features of digital I&C*", and was again left as a topic of future work (OECD-NEA, 2015). In this FPGA Taxonomy, potential mitigation methods were also included, for the example failure modes/failure categories. These mitigation methods considered both FPGA-specific mitigation methods (Wang et al., 2011; Kretzschmar et al., 2016; Habinc, 2002) as well as mitigation methods for generic I&C systems (Hwang et al., 2010; Salewski and Taylor, 2007). Therefore, this FPGA taxonomy fulfills two important areas of future work, as described by the OECD-NEA taxonomy (OECD-NEA, 2015).

2.1.2. Information from the technical literature and author's experience

It has been seen in the literature that there has been a great deal of work put into the design, verification and validation (V&V) and safety analysis of FPGA-based control systems in general (Brombacher and van Beurden, 1999; Monmasson and Cirstea, 2007), and specifically in the case of the nuclear industry (Lu et al., 2015a,b; Wu et al., 2016; Jung and Roh, 2017). The unique properties of FPGAs present certain challenges during the safety analysis process, which may be different challenges than with