Nuclear Engineering and Technology xxx (2016) 1–14

Available online at ScienceDirect

Nuclear Engineering and Technology

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

Original Article

Field Programmable Gate Array Reliability Analysis Using the Dynamic Flowgraph Methodology

Phillip McNelles[*] *and Lixuan Lu*

Faculty of Energy Systems and Nuclear Science, University of Ontario Institute of Technology (UOIT), 2000 Simcoe Street North, Oshawa, Ontario, L1H 7K4, Canada

ARTICLE INFO

Article history:
Received 16 January 2016
Received in revised form
22 March 2016
Accepted 22 March 2016
Available online xxx

Keywords:
Dynamic Flowgraph Methodology
Field Programmable Gate Array
Instrumentation and Control
Nuclear Power Plant
Reliability

ABSTRACT

Field programmable gate array (FPGA)-based systems are thought to be a practical option to replace certain obsolete instrumentation and control systems in nuclear power plants. An FPGA is a type of integrated circuit, which is programmed after being manufactured. FPGAs have some advantages over other electronic technologies, such as analog circuits, microprocessors, and Programmable Logic Controllers (PLCs), for nuclear instrumentation and control, and safety system applications. However, safety-related issues for FPGA-based systems remain to be verified. Owing to this, modeling FPGA-based systems for safety assessment has now become an important point of research. One potential methodology is the dynamic flowgraph methodology (DFM). It has been used for modeling software/hardware interactions in modern control systems. In this paper, FPGA logic was analyzed using DFM. Four aspects of FPGAs are investigated: the "IEEE 1164 standard," registers (D flip-flops), configurable logic blocks, and an FPGA-based signal compensator. The ModelSim simulations confirmed that DFM was able to accurately model those four FPGA properties, proving that DFM has the potential to be used in the modeling of FPGA-based systems. Furthermore, advantages of DFM over traditional reliability analysis methods and FPGA simulators are presented, along with a discussion of potential issues with using DFM for FPGA-based system modeling.

1. Introduction

Field programmable gate arrays (FPGAs) are a type of programmable logic device. FPGAs can be utilized to construct digital logic circuits. These programmable logic devices are programmed by the end user to perform the necessary functions, and certain FPGAs are reprogrammable. FPGAs do not usually include software or operating systems, as the logic functions are programmed (synthesized) onto the chip itself. The programming itself is implemented using hardware description languages (HDLs) [1]. A well-known HDL, named VHDL (very-high-speed integrated circuit HDL), is used in this

* *Corresponding author.*
E-mail address: phillip.mcnelles@gmail.com (P. McNelles).

http://dx.doi.org/10.1016/j.net.2016.03.004

study. FPGAs can perform many of the control functions performed by other electronic logics, such as analog circuits, application-specific integrated circuits, microprocessors, and PLCs. FPGAs can be used in different nuclear instrumentation and control (I&C) systems, provided that they can be proved to satisfy the safety requirements [2,3].

In the nuclear field, many I&C systems that are currently in use in existing nuclear power plants (NPPs) are becoming obsolete. FPGAs are being considered as replacements to those systems. Compared with application-specific integrated circuits (ASIC) and analog circuits, FPGAs can be reprogrammed if needed. Compared with PLCs and microprocessors, FPGAs have been shown to have superior response time and faster processing speed [4,5]. FPGA implementations have taken place in Europe and Asia [6–8], and recently there is increasing interest in these systems in Canada and the USA [9–11].

Very strict safety and quality requirements have been put in place to ensure that the control systems in NPPs function safely. This means that any FPGA-based systems would have to undergo a thorough reliability analysis. To be used in an NPP, an I&C system will have to meet certain qualitative and quantitative reliability requirements; however, these requirements will vary among different regulators. In the case of digital I&C systems, the use of software in the system must also be verified. While FPGAs themselves do not run software, the HDL code is used in configuring the FPGA, which can introduce logic errors into the system. Therefore, both the hardware and HDL logic components of FPGA-based systems must be verified for FPGAs to be used in NPP I&C systems. In this paper, the focus is on the HDL logic, including the Institute of Electrical and Electronics Engineers (IEEE) logic standards, important logical components of the FPGA, and a small test system itself. Regulators may not set specific requirements for FPGA-based systems; however, there is a standard from the International Electrotechnical Commission [12], and guides in the form of International Atomic Energy Agency (IAEA) [13] and Nuclear Regulatory Commission (NUREG) [14] documents that provide guidance on the design and review of FPGA-based systems.

A failure mode and effect analysis (FMEA) at the component and system levels will determine the potential failure modes that can be used as top events in the analysis of FPGA logic. The FPGA logic in these cases will be analyzed to determine the top and initiating events that could lead to failures in FPGA logic subcomponents and in the logic of the system itself. Analysis of FPGA hardware components is beyond the scope of this paper.

There are many reliability analysis techniques in the literature and in industrial practice. The methodology used in this paper is the dynamic flowgraph methodology (DFM). DFM is a dynamic (time-dependent) methodology used to model and analyze digital control systems. In this paper, DFM is shown to be able to validate the logic of FPGA-based systems, including uncovering errors that occur in the logic, and the effect those errors could have on the system or system components. The use of ModelSim simulations adds evidence to the DFM results, to help confirm that DFM can accurately model FPGA system logic. This, in turn, helps validate the use of DFM in the analysis of FPGA-based systems, and allows for DFM to be applied to more in-depth qualitative and quantitative analyses in future research projects.

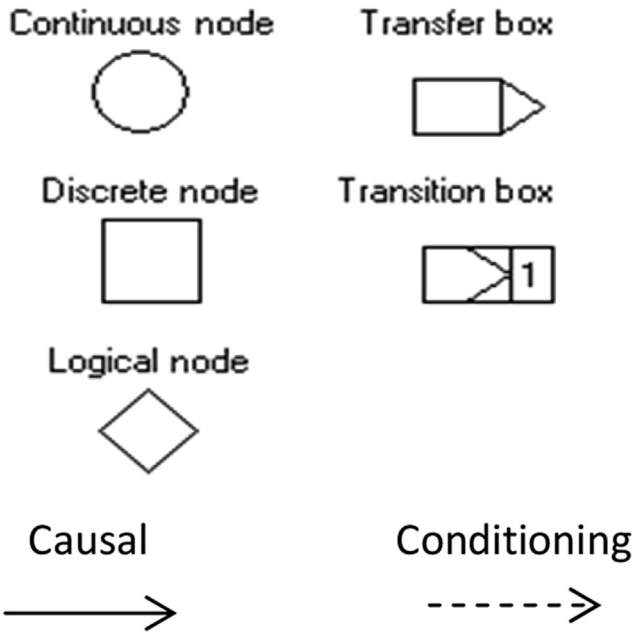

Fig. 1 – DFM nodes, transfer boxes, and connectors. DFM, dynamic flowgraph methodology.

A detailed description of DFM and its advantages over other reliability analysis techniques are presented in Section 2. Using this methodology, several important aspects of FPGA systems are modeled and analyzed. Section 3 discusses three important aspects of FPGA-based systems: the IEEE 1164 standard, registers, and configurable logic blocks (CLBs). Afterward, an FPGA-based dynamic signal compensator is presented, and a simplified sample FMEA is discussed. The results of the analyses based on the models created in Sections 3 are presented and discussed in Section 4. Finally, the advantages of DFM for FPGA modeling and potential issues are covered in Section 5.

2. Dynamic flowgraph methodology

This section describes the theory and application of DFM. Section 2.1 will provide an overview of DFM. Section 2.2 will discuss the actual DFM model, and Section 2.3 will discuss the main limitation regarding the use of DFM.

2.1. *DFM overview*

DFM represents the system being analyzed using a directed graph model. After the model is built, it can be analyzed by the inductive and deductive algorithms built into the methodology [15]. The DFM deductive analysis will return a list of "prime implicants" (PI), which are sets of occurrences that would cause the top event (failure event). They are understood to be the multivalued logic equivalent of minimal cut sets. The

Please cite this article in press as: P. McNelles, L. Lu, Field Programmable Gate Array Reliability Analysis Using the Dynamic Flowgraph Methodology, Nuclear Engineering and Technology (2016), http://dx.doi.org/10.1016/j.net.2016.03.004