Nuclear Engineering and Design 317 (2017) 232–241

Contents lists available at ScienceDirect

Nuclear Engineering and Design

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

Design verification enhancement of field programmable gate array-based safety-critical I&C system of nuclear power plant

Ibrahim Ahmed [a], Jaecheon Jung [b,*], Gyunyoung Heo [a]

[a] Department of Nuclear Engineering, Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104, Republic of Korea
[b] Department of Nuclear Power Plant Engineering, KEPCO International Nuclear Graduate School, 658-91 Haemaji-ro, Seosang-myeon, Ulju-gun, Ulsan 45014 Republic of Korea

HIGHLIGHTS

- An enhanced, systematic and integrated design verification approach is proposed for V&V of FPGA-based I&C system of NPP.
- RPS bistable fixed setpoint trip algorithm is designed, analyzed, verified and discussed using the proposed approaches.
- The application of integrated verification approach simultaneously verified the entire design modules.
- The applicability of the proposed V&V facilitated the design verification processes.

ARTICLE INFO

Article history:
Received 29 October 2016
Received in revised form 14 February 2017
Accepted 2 March 2017

Keywords:
Enhanced functional flow block diagram (EFFBD)
Field programmable gate array (FPGA)
Finite state machine with data path (FSMD)
Modified condition decision coverage (MC/DC)
Safety-critical system

ABSTRACT

Safety-critical instrumentation and control (I&C) system in nuclear power plant (NPP) implemented on programmable logic controllers (PLCs) plays a vital role in safe operation of the plant. The challenges such as fast obsolescence, the vulnerability to cyber-attack, and other related issues of software systems have currently led to the consideration of field programmable gate arrays (FPGAs) as an alternative to PLCs because of their advantages and hardware related benefits. However, safety analysis for FPGA-based I&C systems, and verification and validation (V&V) assessments still remain important issues to be resolved, which are now become a global research point of interests. In this work, we proposed a systematic design and verification strategies from start to ready-to-use in form of model-based approaches for FPGA-based reactor protection system (RPS) that can lead to the enhancement of the design verification and validation processes. The proposed methodology stages are requirement analysis, enhanced functional flow block diagram (EFFBD) models, finite state machine with data path (FSMD) models, hardware description language (HDL) code development, and design verifications. The design verification stage includes unit test – Very high speed integrated circuit Hardware Description Language (VHDL) test and modified condition decision coverage (MC/DC) test, module test – MATLAB/Simulink Co-simulation test, and integration test – FPGA hardware test beds. To prove the adequacy of the proposed approaches, the design architect that focused on the RPS bistable trip logics which are the safety-critical functions of RPS are designed, analyzed, verified and discussed, using bistable fixed setpoint trip logic algorithms as case study. The results showed that the proposed approaches can enhance the design verification processes alongside the reduction in rigorous V&V tasks of FPGA-based safety-critical I&C system for NPP.

1. Introduction

In general, the nuclear power plant (NPP) is design primarily to have a safe plant operation throughout the plant design life. This safe operation is assured by incorporating safety systems in NPP. One of these systems is instrumentation and control (I&C) system which monitor, control and protect the status of the plant condition. Reactor protection system (RPS), being the most safety-critical aspect of this I&C systems implemented on programmable logic controllers (PLCs), plays a vital role for achieving the safe operation of the plant. The primary objective of RPS is to provide a reliable and rapid reactor trip if monitored parameters approach the specified setpoint limit.

The challenges such as fast obsolescence, the vulnerability to cyber-attack, and other related issues of software systems have currently led to the consideration of field programmable gate arrays (FPGAs) (EPRI, 2009) as an alternative to PLCs because of

* Corresponding author.
E-mail address: jcjung@kings.ac.kr (J. Jung).

http://dx.doi.org/10.1016/j.nucengdes.2017.03.005
0029-5493/

their advantages and hardware related benefits. However, safety analysis for FPGA-based I&C systems, and verification and validation (V&V) assessments still remain important issues to be resolved, which are now become a global research point of interests (Lu et al., 2015; McNelles and Lu, 2016; Wu et al., 2016). The regulations and standards demand that sufficient V&V should be performed to demonstrate the safety level of the systems (IAEA, 2001). Generally in FPGA design verification, the designers make use of verification techniques by writing and developing the test benches (Bryant, 1991; Ding et al., 2011; Kim et al., 2011; Kim, 2013; Wu et al., 2016; You et al., 2008) which involved various stages of verification activities of register-transfer level (RTL), gate-level, and place and route. Writing the test benches is considerably time consuming and require a lot of efforts before achieving the expected results. Furthermore, performing the verification at each stage is a major bottleneck and demanded much activities and time. In addition, verification is conceivably, the most difficult and complicated aspect of any design.

Therefore, in view of these, this work developed a systematic design and verification strategies and implementation procedures in form of model-based approaches for FPGA based RPS design and verification that can lead to the enhancement of the design verification and validation. In addition, this work demonstrated an integrated verification approach to the verification of FPGA-based I&C system in NPP that simultaneously verified the whole design modules using MATLAB/Simulink HDL Co-simulation models. After analyzing the requirements that need to be satisfied from which the design specifications for the final design output are derived, we develop a functional model using enhanced functional flow block diagram (EFFBD) using Vitech's CORE® Model Based Systems engineering tool that modelled the FPGA-based RPS bistable trip functions and verified the functional execution of the trip logics prior to the main design. The functional requirements and specifications are generated and documented from EFFBD which serves as the basis for requirement traceability during the entire design process. The reason for this is that, it is important to produce appropriate requirements specifications which is a key issue for all highly critical systems (IAEA, 2016), as any error will most likely be propagated into the design and implementation of the actual system. We then applied a modularity design pattern approach using finite state machine with data path (FSMD) that leads to the design simplification and speeds up the design procedures as well as enhanced the design verification that makes the final design easy to be verified and validated; hence reducing the rigorous V&V loads. To carry out V&V tasks, we applied four sequential step modes which are HDL test, modified condition decision coverage (MC/DC) test, MATLAB/SIMULINK HDL Co-simulations test, and integration test (using FPGA test beds). In order to prove and demonstrate the applicability of these approaches, we took, as case study, the bistable logic for fixed setpoint trip algorithm among the three types (fixed, variable manual reset, and variable automatic rate limiting setpoints) of safety-critical trip logics in nuclear power plant. The increasing/rising process of fixed setpoint algorithm is considered. This implies that the trip and pretrip setpoints have a fixed setpoints higher than the process input, and the model is expected to issue a pretrip or trip signal when the process input rises to or above the value of pretrip or trip setpoints. The application of these approaches successfully showed how FPGA-based I&C systems design verification can be enhanced by reducing the rigorous V&V tasks.

2. Background

In nuclear industry, I&C systems including RPS were analog-based systems at beginning. Although they performed their intended functions, there were some primary concerns with the analog-based systems, such as effects of aging that leads to mechanical failures and obsolescence. As result of these effects, the nuclear industries transited from analog-based to digital-based systems in the mid-1980s (IAEA, 2012). The main purpose for the transition was due to their significant benefits over analog systems. Such benefits include free of the drift and improvement on the system performance and computational capabilities (U.S. NRC, 1997). Subsequently, the implementation of the RPS functions was achieved by using programmable logic controllers (PLCs) (EPRI, 2002; Kwon and Lee, 2009), which are microprocessor-based software system. That is, PLC operates by using both operating system (OS) and application software.

There are several research works on the I&C systems of NPP and research reactors, especially on the reactor protections and how to improve the reliability and design of I&C system architectures (Khalil Ur et al., 2016, 2014; Khalil Ur and Heo, 2015; Shin et al., 2006) as well as simplification of software development and safety analysis for safety-critical I&C systems of NPP (Jung et al., 2009). However, in recent years, FPGA is considered as an alternative to PLCs or used in diverse applications with PLCs because of advantages and hardware related benefits of FPGAs. An FPGA is a digital semiconductor device in which its function is determined by the circuit embedded in the device. FPGAs have the capability of parallel processing of logic functions independently in a circuit, hence lower response time and higher processing speed compare to PLCs (She and Jiang, 2012). FPGAs are extensively gaining attention worldwide for application in NPP I&C systems, especially for safety-critical and safety-related systems. FPGA platforms for safety-critical and safety related systems are developed and being developed by various vendors for use in NPP (Bakhmach et al., 2009; Choi and Kim, 2016; Ranta, 2012; RPC Radiy, 2014; Westinghouse, 2013). Even though the end product of FPGA is hardware, its design processes involve the use of software tools. However, the FPGA needs to be designed and configured which involves the development and the verification and validation (V&V) of hardware description language (HDL) codes. This may be a challenging task and may introduce design and logic errors into the safety system if appropriate and more robust design procedures are not employed from the starting point of the design process.

3. Materials and methods

In order to implement the proposed design approaches, the methodology that will lead to the enhancement of the design verification for safety-critical I&C system must be simply and clearly defined. As such, several methodologies and relevant tools are used in this work. Fig. 1 shows the overall scheme of the proposed design and verification approach. The enhanced design flowchart is shown in Fig. 1(a), while the verification part of the flowchart is elaborated in details in Fig. 1(b) which indicated the activities to be performed at each stage of the verification test. The flowchart is an enhanced one because it systematically employed the simple steps that clearly involved the logic control flow of activities to be performed in form of model-based methodology. This indeed, will enhance the design verification and traceability.

The requirement analysis is presented in Section 3.1 where the relevant requirements and guidelines are discussed. Prior to the development of the FSMD that provides the structural design methodology in Section 3.3, Section 3.2 presented the enhanced functional flow block diagram (EFFBD) system engineering tool used to model the functional requirements of the safety-critical FPGA-based trip algorithms using Vitech's CORE® Model Based Sys-