Nuclear Engineering and Design 330 (2018) 325–331

Contents lists available at ScienceDirect

Nuclear Engineering and Design

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

Software verification process and methodology for the development of FPGA-based engineered safety features system

Restu Maerani, Joyce Kemunto Mayaka, Jae Cheon Jung*

Department of Nuclear Power Plant Engineering, KEPCO International Nuclear Graduate School, 1456-1, Shinam-ri, Seosaeng-myeon, Ulju-gun, Ulsan 689-882, Republic of Korea

ARTICLE INFO

Keywords:
FPGA
Verification
ESF-CCS
I&C

ABSTRACT

Verification process is very important for the new development or re-engineering process for Instrumentation and Control (I&C) in Nuclear Power Plant (NPP). Due to the fact that the Engineered Safety Feature-Component Control System (ESF-CCS) is safety critical system, it is necessary to specify a systematic approach to verify the performance of development design. For this verification process, a system engineering approach is used and refers to the software design life cycle to verify the VHDL code in the implementation of Field Programmable Gate Array (FPGA)-based ESF-CCS. Although FPGA does not use software, however, FPGA needs a Hardware Description Language (HDL) to describe digital and mixed-signal for an integrated system. Therefore, the VHDL code should be verified to make sure that this code level will not cause an error for the FPGA-based system, especially for ESF-CCS development. The verification method is started by looking at the requirements analysis, verification of the outputs of the design by develop software testing to verify the reliability of the code which is to support the FPGA-based ESF-CCS. White Box testing is used for software testing to demonstrate the responds from the VHDL code, whether the design is success or not, and the coverage test is at 100% coverage state. In addition, the Static Timing Analysis (STA) is applied to check the delay time. Once all verification steps have been performed, then the results of the design can be validated. In this paper, FPGA-based ESF-CCS using VHDL code is verified.

1. Introduction

Programmable Logic Controller (PLC) has been applied to Instrumentation and Control (I&C) system in NPP. However, due to microprocessor-based systems were found to have numerous shortcomings such as the susceptibility to software Common Cause Failure (CCF) (Wood et al., 2009), high maintenance costs, difficult and expensive verification, and has a quick obsolescence (Jung and Ahmed, 2016), it is necessary to update the I&C system using a new technology by measuring the effectiveness of the aspects of cost, the performance of the system and component, and how to reduce system complexity. This should be a priority by considering that the microprocessor-based system is a major component in the system design of NPP's I&C system. Currently, FPGA is being looked into as a replacement for the PLC-based system (Chen, 2011). FPGA-based system is expected to mitigate the potential for CCF vulnerabilities within the microprocessor-based system and can reduce the system complexity in term of ability to execute the independent functions in parallel which is not possible with PLC based systems (Wood et al., 2009).

According to the Standish Group's Chaos Report in 2015, the success rate of software projects was in small number (29%) and the failure rate was 19% (Standish Group 2015 Chaos Report – Q&A with Jennifer Lynch, 2015). Table 1, compare with the finding by Jung in (Jung et al., 2009) shows that the failure rate was significantly decreased from 49% in 2001 to 19% in 2015. On the other hand, in 2001, the success rate was 23% and then rose slightly to 29% in 2015. The data in Table 1 demonstrates why the software verification process is needed to avoid the occurrence of a failure, especially for I&C systems in NPP.

FPGA has abilities to capture the design requirements and to translate into FPGA logic, and commonly, VHDL are used because it is capable to make a documentation base for the review of this design step, and to trace back to the original design requirements (Bobrek et al., 2009a). FPGA also has ability to perform any arbitrary logic function after programming, and can be implemented in NPP for any logic function component such as trip logic units or ESF actuation decision logic. FPGA is simple enough to perform 100% testing for all functions of ESF-CCS. Therefore, FPGA-based ESF-CCS is developed to be a high-quality safety application. By developing the coverage test for this system to verify the design implementation, it will be shown how much system has been tested after developing the test case, and the

* Corresponding author.
E-mail addresses: maerani@email.kings.ac.kr (R. Maerani), jcjung@kings.ac.kr (J.C. Jung).

https://doi.org/10.1016/j.nucengdes.2018.02.009
Received 19 September 2017; Received in revised form 1 February 2018; Accepted 4 February 2018
0029-5493/ © 2018 Elsevier B.V. All rights reserved.

Table 1
Modern resolution for all projects from standish group chaos report 2015.

	2011	2012	2013	2014	2015
Successful	29%	27%	31%	28%	29%
Challenged	49%	56%	50%	55%	52%
Failed	22%	17%	19%	17%	19%

result will shows the undetected errors in development test scenarios (IEEE, 2012).

Since the existing regulatory documents have no specific standards for FPGA, we can follow the digital and software safety system issue for NPP to implement and verify the FPGA-based ESF system which is; IEC 62566 for development of HDL programmed (IEC, 2012), NUREG/ CR 7006 (Bobrek et al., 2009b), EPRI Std 1076-2008 (Fink et al., 2011), IEEE Standards 1012-2012 for system and software verification and validation (Bobrek et al., 2009a), and IAEA Nuclear Energy Series NP-T-3.17 (IAEA, 2016), as the guideline of the usage of FPGA in NPP. Considering that the software of the ESF-CCS cabinet is belong to the category of critical safety, FPGA based module shall be designed, tested, installed and maintained in accordance with the requirements defined in IEEE Std 828-1998 (IEEE, 1998). Therefore, verification process for the engineering tools within hardware and software in NPP is a very important phase in the development of safety related systems (Korsah et al., 2009). The purpose of the verification process is to ensure the performance of the developed systems and components (Wu et al., 2016). In this paper, the verification processes are presented by developing the coverage test using the Modified Condition/Decision Coverage (MC/DC), white box testing with Xilinx Vivado, and develop static timing analysis to analyze the time delay between signal input and output using Xilinx Vivado. All this methodology is developed to verify the design implementation of FPGA-based ESF-CCS.

2. Theory and methodology

2.1. ESF-CCS

ESF-CCS has actuation logic for Safety Injection Actuation Signal (SIAS) (Kepco International Nuclear Graduate School, xxxx). SIAS actuates the component to inject borated water into the reactor coolant system and actuates component for emergency cooling (Chapter 16, xxxx). I/E converter is to convert current to voltage. The sensor inputs a current signal to the Auxiliary Process Cabinet – Safety (APC-S) which converts it to voltage. APC-S functions include signal conditioning/ splitting for the safety field sensor signals shared by the Plant Protection System (PPS), core protection calculator system, and ESF-CCS loop controller (LC), or safety systems and non-safety systems, and provide isolation when signals are split to the non-safety system (KEPCO and KHNP, 2014a). Each ESF-CCS channel receives ESFAS initiation signals from Main Control Room (MCR), Remote Shutdown Room (RSR), Diverse Manual Actuation (DMA), Maintenance Test Cabinet (MTC), Minimum Inventory (MI) and all four channels of the PPS and performs automatic initiation of the affected ESF system(s) when the certain coincidence logic conditions are satisfied. ESF-CCS consists of two modules, the first module is Group Controllers (GC) which processes the signals coming from MTC, MI and PPS to decide 2-out-of-4-actuation signal. MCR, RSR, DMA commands are processed in the second module is LC which processes the signals coming from MCR, RSR, DMA, Fig. 1 demonstrates the operation of ESF-CCS.

The purpose of this design is to use the two FPGA Basys3 boards to implement the whole SIAS to actuate the pump for emergency cooling. SIAS will be automatically initiated by a low pressurizer pressure signal or a high containment pressure signal. In software design phase, software requirements are transformed into architecture and a detailed design for each software component. The design includes databases and system interfaces (e.g. hardware, operator/user, software components, and subsystems). The design of FPGA-based systems is expressed in Hardware Definition Language (HDL). In this paper, the use of VHDL are adopted from IEEE (2009) as a language reference manual.

The system was divided into several software modules:

- System Level Actuation Processing
- Component Actuation Processing
- Start and Stop Command Processing

2.2. Software design life cycle

According to Everett and McLeod (2007), software testing and software development have interconnected relation for the success of implementation. The processes of testing and development depend on other supporting management processes, especially, requirements management, which must be carried out before verification. The Digital I&C system are designed to be capable of sharing of code, data transmission, and process equipment, to a greater extent than traditional analog systems.

In order to ensure this, Branch Technical Position 7-14 (U.S. NRC, 2007), requires that reviewers of digital I&C systems:

- Confirm that acceptable plans were prepared to control software development activities,
- Obtain evidence that the plans were followed in an acceptable software development life cycle (SDLC), and
- Obtain evidence that the process produced acceptable design outputs.

SDLC processes must be clearly defined: the method of carrying out the processes, relevant standards, outputs, and associated verification process. FPGA has the reusability to make 100% testability if there is something need to be added, or to update the VHDL code for command, therefore, Y model is chosen. L. Capretz also said that Y model is chosen for a large software development (Capretz, 2005). Fig. 2 demonstrates the development of FPGA-based ESF system using Y Model.

The purpose of Y model for SLDC even though it does not have official standards such as V or another life cycle model, but Y model is known in the use of software development because the ability to support a system that can be used again in the future, and this will certainly support the re-engineering I&C with FPGA-based system in the future.

2.3. Requirements analysis

Since this development of FPGA-based I&C System is for APR1400 the Korean NPP, the International Standard that can be follow should recommended by Korea Institute of Nuclear Safety (KINS) as the regulatory body. The standards document related to I&C system of NPP and FPGA to be follows; 10 CFR 50, regulatory guides from US. nuclear regulatory commission, branch technical position and standards. IEC 62566 (IEC, 2012), IAEA, No. NP-T-3.17 (IAEA, 2016), NUREG/CR-7006 (Bobrek et al., 2009a), EPRI TR-1,019,181 (Fink et al., 2011), OEDC/NEA MDEP No DICWg-05 (MDEP, 2013), IEEE Std 1012-2012 “Standard for System and Software Verification and Validation” (IEEE, 2012), IAEA Technical Report Series No. 384 (IAEA, 1999) is the International standards which is related to I&C system for NPP, FPGA and verification process.

Measuring the effectiveness of the project is important, as the user needs to indicate the quality of the design and to discover the issues during analysis (Fisher, 1996). Since verification process are needed to check the inputs and outputs of each step of the development process which is usually undertaken from documentation (IAEA, 1999). This FPGA-based system is verified after one of the measures of effectiveness defined, was 100% of the code coverage testing (Hayhurst et al., 2001). This requirement is based on the reference of DO-178B for MC/DC

Download English Version:

https://daneshyari.com/en/article/6759206

Download Persian Version:

https://daneshyari.com/article/6759206

Daneshyari.com