Application of Integrated Verification Approach to FPGA-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*
[*]*Corresponding author: jcjung@kings.ac.kr*

1. Introduction

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 [1]. 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. The regulations and standards demand that sufficient V&V should be performed to demonstrate the safety level of the systems [2]. Generally in FPGA design verification, the designers make use of verification techniques by writing the test benches 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 to achieve a satisfied desire 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 applied 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.

2. Methods and Results

In this section the approach we used to achieve an integrated verification of the FPGA-based I&C system in NPP is presented. We took, as a 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, with emphases on increasing/rising trip. Section 2.1 discussed the Very high speed integrated circuit Hardware Description Language (VHDL) codes developed for bistable fixed setpoint trip algorithm, while section 2.2 presented the integrated verification models.

2.1 VHDL Code Development

In order to develop the VHDL code for fixed setpoint algorithm, finite state machine with data path (FSMD) is used so as to simplify the design and to make the design requirements easily traceable during verification. FSMD here also served as the modeling for requirement specifications. Producing appropriate requirements specifications is a key issue for all highly critical systems [3], as any error will most likely be propagated into the design and implementation of the actual system.

Figure 1 shows the FSMD design architecture for fixed setpoint trip algorithm with the interfacing inputs and outputs of the algorithm. The VHDL codes are then developed from FSMD. This involves writing synthesizable RTL that will be implemented on FPGA using any of the hardware description languages (HDLs). The widely use HDL languages are VHDL and Verilog. Although there is not significant advantages in times of the end product as to which language to be used, in this work, VHDL is chosen and used because of its flexibility and unique features. Among its unique feature is design reusability [4] which allows procedures and functions to be placed in a package so that they are available to any design unit that uses them. This is impossible in Verilog because there is no concept of packages in Verilog. VHDL also has some features such as *configuration*, *generate* and *package* statements, together with the generic clause, that help the designer to manage large designs; whereas in Verilog, there are no such statements. The Active-HDL software developed by Aldec is used for writing VHDL codes.

2.2 Integrated Verification Model

In this section, the MATLAB/Simulink HDL Co-simulation that is used to build the integrated verification model is described. The verification and testing of the FPGA-based trip logic (for example, the case of fixed setpoint logic) involves checking and observing the following RTL/gate-level code structures:

- ✓ The comparator logics are correctly implemented – the hysteresis is applied to the setpoint when the system process is in the expected level.

- ✓ The trip and pretrip logics are properly and correctly implemented – the logics respectively generate trip and pretrip signals when the process input exceeds the predefined limits.
- ✓ The behavior of the trip algorithm at every point is correct – that is, each logic performs the task it is designed for and does not compromise the performance of the other logics.
- ✓ The FPGA-based safety-critical I&C system satisfies the requirements of the fixed setpoint algorithm while it is in operation.

The integrated verification model is shown in Fig. 2. The model is built for four channels reactor protection system (RPS) with coincidence logic to mimic the real situation of four redundant channels RPS in NPP. Each channel is FPGA-based design modules of bistable fixed setpoint trip algorithm, and each module contains VHDL design entities/units. The integrated verification approach used in this work introduces and shows the opportunity to test multiple units and modules simultaneously without writing rigorous test benches. Instead, the test cases and test scenarios are developed using MATLAB/Simulink models, and the simulation results and system behavior are simultaneously observed on both Simulink scopes and Active-HDL simulator environment. This presents parallelism into the RTL/gate-level testing process and compares the function of a unit to some interface specifications. In this case, the design modules can be collectively tested. The collectivity and integrated testing reduces the testing and verification time, and therefore speed-up the verification process. As shown in Fig. 2, two-out-of-four coincidence logic receives independent trip signals from each of the four channels and issues the trip when at least two among the four channels provide a trip signal.

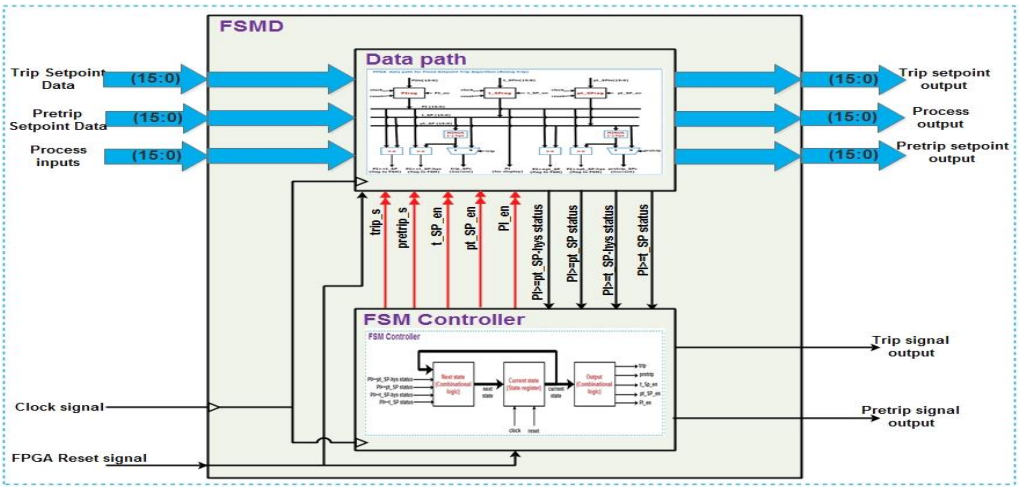

Fig. 1. FSMD design Architecture for fixed setpoint trip algorithm

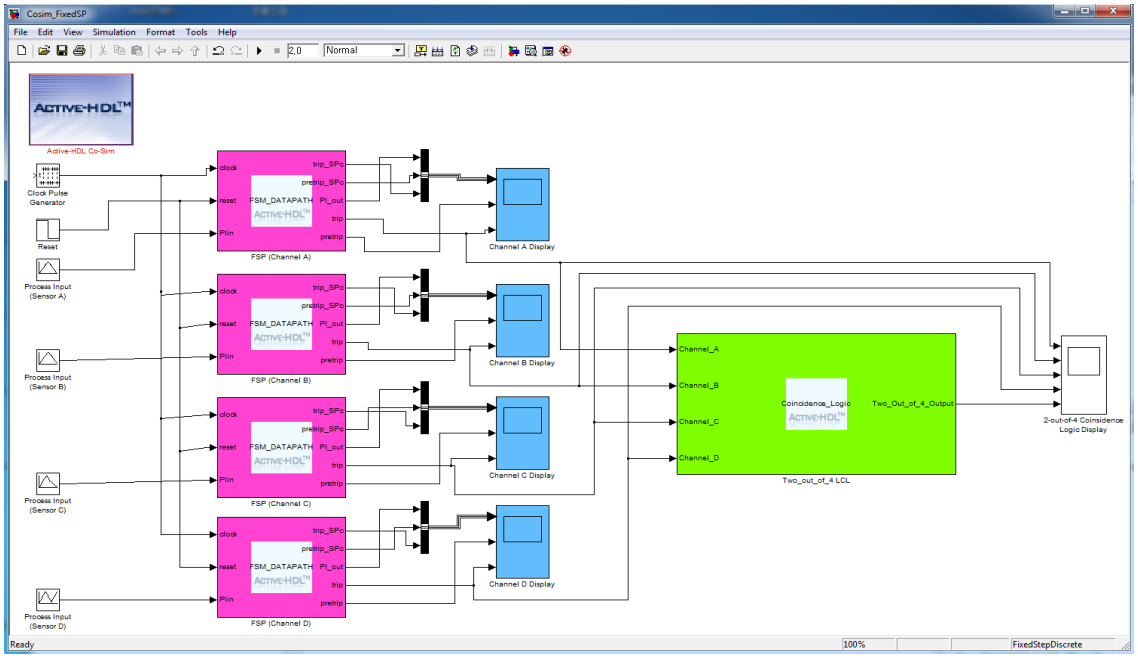

Fig. 2. Simulink model for integrated verification test (4 channels RPS with a coincidence logic)

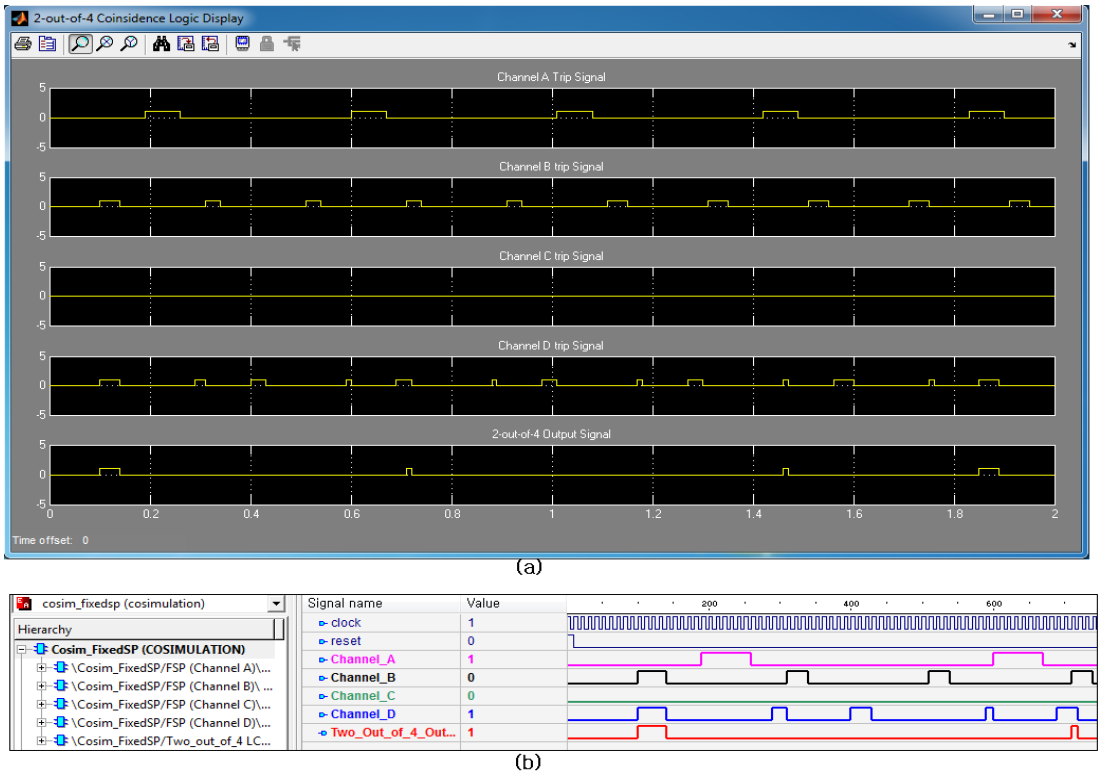

Fig. 3. Integrated verification results of four channels FPGA-based PPS – (a) Simulink result (b) Co-sim from Active-HDL simulator

Figure 3 presents the four channel PPS results that are collectively tested on Simulink which are simultaneously shown on both Simulink scope (Fig.3(a)) and Active-HDL simulator (Fig.3(b)). At beginning of the simulation, the output of two-out-of-four coincidence model is at logic "0" ("2-out-of-4 output" = 0) at the point where none of the channels issue a trip signal. The output of two-out-of-four logic goes to logic "1" ('2-out-of-4 output" = 1) where *channel B* and *channel D* simultaneously issue a trip signal and remains at logic "1" for the period of *channel B* and *Channel D* trips. At the point where only one channel issued the trip signal, the output of two-out-of-four model remained at logic "0". This, in fact, confirmed the requirements of redundancy that, at least two channels among the four channels must be at logic "1" for a two-out-of-four coincidence model to provide a trip signal.

3. Conclusions

Verification is conceivably, the most difficult and complicated aspect of any design, and an FPGA design is not an exception. Therefore, in this work, we introduced and discussed how an application of integrated verification technique to the verification and testing of FPGA-based I&C system design in NPP can facilitate the verification processes, and verify the entire design modules of the system simultaneously using MATLAB/Simulink HDL co-simulation models.

In conclusion, the results showed that, the integrated verification approach through MATLAB/Simulink models, if applied to any design to be verified, could speed up the design verification and reduce the V&V tasks. This is because the entire FPGA-based system design modules to be verified are modelled collectively, and the test cases and test scenarios are from the Simulink models which are easy to develop compare to writing test benches using any of the HDL languages.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIP) (Grant Number: NRF-2011-0031773).

REFERENCES

[1] EPRI, Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems, EPRI, Palo Alto, CA, 1019181, 2009.
[2] International Atomic Energy Agency, Safety Assessment and Verification for Nuclear Power Plants, Safety Guide No. NS-G-1.2, Vienna, 2001.
[3] International Atomic Energy Agency, Application of Field Programmable Gate Arrays in Instrumentation and Control of Nuclear Power Plants, Nuclear Energy Series No. NP-T-3.17, Vienna, 2016.
[4] D.J. Smith, HDL Chip Design - A practical guide for designing, synthesizing and simulating ASICs and FPGAs using VHDL or Verilog, 1st ed., Doone Publications, Madison, Ali, USA, 1996.