Regulatory Issues on Using Programmable Logic Device in Nuclear Power Plants

G.Y. Park, Y.J. Yu, H. T. Kim, Y.I. Kwon, H.S. Park, and C. H. Jeong
Korea Institute of Nuclear Safety, 19 Kusong-dong, Yuseong, Daejeon, Korea.
{k703pgy, k644yyj, k719kht,yongil.kwon, k394phs,chjeong}@kins.re.kr

1. Introduction

For replacing obsolete analog equipment in nuclear power plant, the Programmable Logic Devices (PLDs) using Hardware Description Language (HDL) have been widely adopted in digitalized Instrumentation & Control (I&C) systems because of its flexibility. For safety reviews on Nuclear Power Plants (NPPs,) qualifying digitalized safety I&C system using PLDs is an important issue. As an effort to provide regulatory position on using PLDs in safety I&C system, there is a research project to provide the regulatory positions against emerging issues involved with digitalization of I&C system including using PLDs. Therefore, this paper addresses the important considerations for using PLDs in safety I&C systems such as diversity, independence and qualification, etc. In this point, this study focuses on technical reports for Field Programmable Gate Array (FPGA) from EPRI,. U.S. NRC, and relevant technical standards.

2. Summary on Relevant Documents

For the study, some technical reports and domestic regulatory experiences were carefully examined. The technical reports under review are EPRI 1019181 [1], NUREG/CR-7006 [2], RTCA/DO-254 [3], and IEC 62566 [4].

EPRI report describes that FPGA design is quite similar to that of software design in the point of use of software-based design tools and programming language. Therefore, it provides the V-shaped lifecycle for FPGA including 1) Component Requirement Specification, 2) Preliminary Design, 3) Design, 4) Implementation, 5) Verification, 6) System Integration and 7) System Validation. Additionally, this report provides the specific FPGA design guidelines and the worldwide experiences of use of FPGA including Wolf Creek NPP of U.S., Radiy FPGA-based safety system of Ukraine and Bulgaria, etc. The conclusion of the report describes the risk of using FPGA with embedded microprocessor Intellectual Properties (IPs) Core.

The objective of NUREG/CR-7006 is to provide the technical basis of safety review guideline for FPGAs similarly to NUREG/CR-6463 - Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems. This report insists that FPGA design includes both hardware and software characteristics, therefore, a specific design and review guideline are required. Therefore, it provides the specific hardware design issues and the FPGA design methodologies. As shown in Figure 1, this document provides the lifecycle similar to the waterfall model. It also provides the survey results of FPGA design guides and experiences relevant to NPP application.

RTCA/DO-254 is a design assurance guideline for avionics. This document is prepared by RTCA, which is a private, not-for-profit Corporation for an aircraft industry, and approved by U.S. Federal Aviation Administration (FAA). According to RTCA/DO 254, the hardware designs are classified as a simple or complex and the hardware design assurance levels are defined from level A to level E corresponding to the classification of failure-conditions : catastrophic, hazardous, major, minor and no effect. In this standard, as shown in Figure 2, hardware design lifecycle is including Planning, Hardware Design Processes, and Supporting Processes, which could be tailored

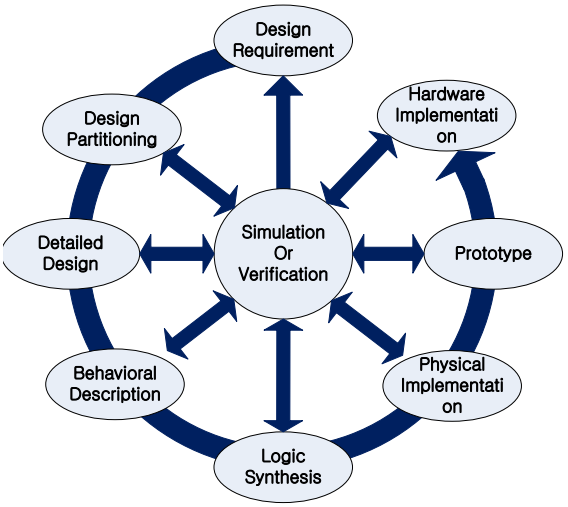

Figure 1. FGPA Design Flow of NUREG/CR-7006

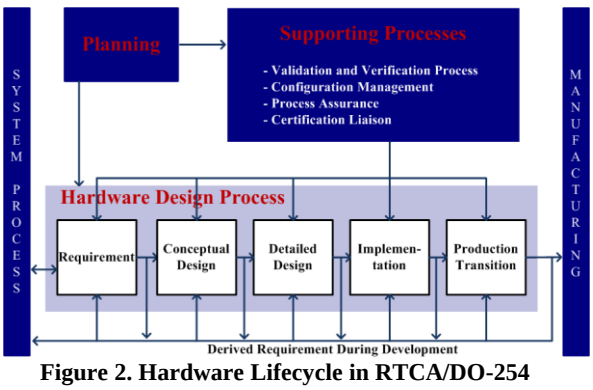

Figure 2. Hardware Lifecycle in RTCA/DO-254

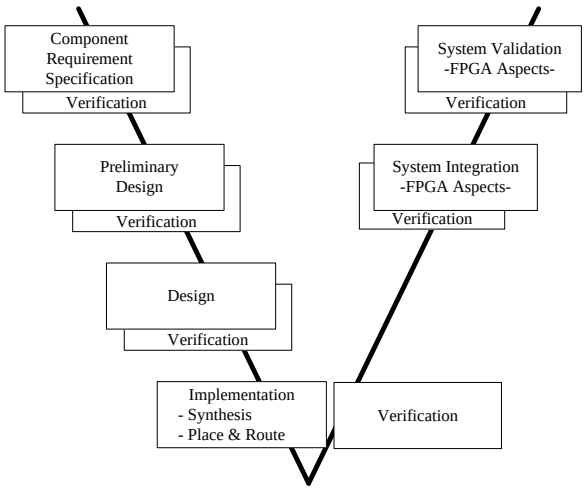

Figure 3. PLDs Design Processes

commensurate to its hardware design assurance level. The hardware design processes include Requirement Capture, Conceptual Design, Detailed Design, Implementation, and Production Transition. The supporting processes consist of Validation and Verification (V&V) Process, Configuration Management, Process Assurance, etc.

IEC 62566 is a technical standard for design of HDL-programmed Integrated Circuit (IC) for safety systems and officially published in January, 2012. This standard provides the V-shaped development lifecycle for HDL-Programmed Device including 1) HPD Requirements Specification, 2) HPD Design, 3) HPD Implementation, 4) HPD aspects of System Integration, and 5) HPD aspect of System Validation. It also provides the specific hardware-aspect requirements and lifecycle-based design products.

3. Regulatory Issues on Using PLDs

Through this study, we focus on the feasibility of applying criteria and technical standards related to software (i.e., IEEE Std 7-4.3.2, IEEE Std 1012, etc.) on PLDs design evaluation. According to the reviewed documents and domestic regulatory experiences, it is difficult to directly apply the software design criteria on the PLDs safety evaluation. The EPRI report describes that the standards for software design could be the basis for safety review on PLDs design because of the absence of standard for FPGAs. Additionally, the NUREG/CR report also describes that tailoring on V&V processes and design lifecycle are required to adapt for specific characteristics of FPGAs. Therefore, sufficient tailoring for software-based processes and standards would be required to apply on FPGAs design as shown in Figure 3.

The potential regulatory issues such as diversity, use of pre-developed item, and testing coverage are raised from the scrutiny on relevant documents. Because of the possibility of Common Cause Failure (CCF), the diversity design is required in the use of PLD design. According to EPRI report, the FPGA design for MSFIS (Main Stream and Feedwater Isolation System) of Wolf Creek NPP is implemented using diverse synthesis directives to implement the core logics. Furthermore, the diverse design included in MSFIS was verified by the independent V&V team. Additionally, the Ukrainian NPP's ESFAS based on Radiy FPGA platform was implemented using diverse ICs of different vendors to meet the Defense-in-Depth and Diversity requirement. Therefore, to mitigate the effect of CCF a sufficient diverse design is required for using PLDs.

Another issue for using PLDs is a use of pre-developed items such as software tools and IP cores. There are no sufficient methods or guidelines to assure the quality of these pre-developed items. It is also difficult to apply previous regulatory position for commercial item dedication on PLDs. For testing coverage, DI&C-ISG-04 of U.S. NRC requires 100% test coverage including the combination of all inputs, outputs, and internal states for PLDs, especially on the priority function. And, the simple digital device should be 100% tested [5]. However, generally 100% testing coverage is quite difficult to achieve. Therefore, providing sufficient methodologies or guidelines for these issues are important activities.

4. Conclusion and Future Work

Assuring the quality of PLDs design is an issue on the safety review on new NPP and Topical Reports. Therefore, the objectives of this study establish the design guideline for PLDs and the regulatory position for potential issues on use of PLDs such as diversity design, use of pre-developed item, and testing coverage. In this point, KINS prepares a Korean regulatory guideline for using PLDs in I&C systems.

5. Acknowledgement

This research is a part of the "Development of Safety Evaluation Techniques for Digital I&C System using Test Platform" and has been supported by the Nuclear Safety and Security Commission of Korea.

REFERENCES

[1] J. Naser, B. Fink, T. Nguyen, et al., Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems, EPRI Technical Report, 2009.
[2] M. Bobrek, D. Bouldin, et al., NUREG/CR-7006, Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems, U.S. NRC, 2010.
[3] RTCA/DO-254, Design Assurance Guidance for Airborne Electric Hardware, 2000.
[4] IEC 62566, Nuclear Power Plants–Instrumentation and control important to safety–Development of HDL-programmed integrated circuits for systems performing category A functions, 2012.
[5] Terry W. Jackson, Licensing of Simple Digital Devices, Proceedings of ICAPP08, pp 861 ~ 864, 2008.