Necessity of Verifiable Design in FPGA-based Safety-grade Signal Processing Systems for Nuclear Power Plants

Sunghyun Kim [a*]
[a]*Korea Hydro & Nuclear Power Co. (KHNP), Central Research Institute,*
1312 Beon-gil, Yuseong-daero, Yuseong-gu, Daejeon, 305-343, Republic of Korea
[*]*Corresponding author: saint.kim@khnp.co.kr*

Keywords : FPGA, I&C, nuclear, safety, verifiable design

1. Introduction

Instrumentation and control (I&C) systems in nuclear power plants are required to perform deterministic and predictable operations under all conditions. To achieve this, all software and hardware components must ensure traceability and verifiability, and the use of external black box elements is strictly limited by regulations. Historically, PLC(Programmable Logic Controller)-based platforms have been widely used, allowing complex operations such as logarithmic, trigonometric, and exponential calculations to be performed using standard C language library functions. These functions, categorized as Pre-Developed Software (PDS), were applied to safety-grade systems under the condition that vendor documentation and user-level verification were provided.

2. Background of FPGA Adoption and the Need for Verifiable Design

Recently, the performance limitations, obsolescence, and supply chain instability of PLC platforms have led to the adoption of FPGA (Field-Programmable Gate Array)-based platforms in safety-grade systems. FPGAs offer several advantages, including high performance through hardware parallelism, long-term component supply stability, and enhanced reliability from reduced system complexity. However, in addition to the regulatory standards applied to PLCs, more stringent requirements are being applied to HPDs (HDL Programmed Devices), including FPGAs, under IEC 62566. Furthermore, the IAEA report on the subject of FPGA application in the nuclear industry recommends minimizing the use of black box intellectual property rights (IP) in safety-related systems.

In addition to the view of compliance, a verifiable (self-developed) design is required to take advantage of the strength of the FPGA. Verifiable design mitigates vulnerabilities related to common cause failures (CCF). Since the introduction of software into nuclear safety systems, stricter regulations addressing CCF risks have been implemented. The inherent characteristics of FPGAs, such as the absence of operating systems and their full testability, make them a robust platform to reduce CCF vulnerabilities. Therefore, in safety-grade FPGA designs, it is essential to avoid external IP usage and implement all safety-related functionalities as verifiable modules.

3. Challenges of Direct Implementation

Developing every functions from elementary level imposes significant burdens on designers. For example, while a simple call to the log function from the standard library is sufficient in a PLC environment, FPGA implementations require the use of CORDIC algorithms, LUT-based approximations, or polynomial methods for designing logarithmic functions. Additionally, designers must conduct functional verification, formal verification, and timing analysis, substantially expanding the scope of Verification and Validation (V&V). Although direct implementation increases development costs and schedules, it is necessary process to ensure design transparency and regulatory compliance.

4. Conclusions

While eliminating external IP and developing all computational blocks internally increases short-term development burdens, it provides long-term advantages such as securing own internal IP asset, mitigation of CCF vulnerabilities, and strengthened regulatory compliance. Future work should focus on developing standardized, verifiable FPGA IP libraries for nuclear safety systems. In other words, a study is planned to directly implement core computing functions and compare and analyze performance and accuracy. Through this, the necessity presented in this paper will be applied to specific practice and connected.

Acknowledgment: This work was supported by the Innovative Small Modular Reactor Development Agency grant funded by the Korea Government (MOTIE) (No. RS-2024-00408005).

REFERENCES

[1] IEEE Std 7-4.3.2-2003: IEEE Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Stations.
[2] IEEE Std 1012-2012: IEEE Standard for System and Software Verification and Validation.
[3] IEC 62566-2012: Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions.
[4] IAEA Nuclear Energy Series No. NP-T-3.17-2016: Application of Field Programmed Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants.