Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 29-30, 2026

A Study on Synchronization Design and Verification Scopes in FPGA based Safety System

Sunghyun Kim [a*], Heetaek Lim[a], Hyunki 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, nuclear, safety, CDC, Synchronization

1. Introduction

FPGA design applied to the safety systems of nuclear power plants requires strict deterministic operation and high reliability in accordance with relevant standards such as IEC 62566. Design and verification can be performed on an individual chip or card level depending on the project situation. In this environment, there is a possibility of overlooking the synchronization design with external interfaces, as only the synchronization of internal logic is considered. This paper points out the potential gaps that can occur when setting such design and verification scopes, and discusses the importance of inter-chip interface synchronization to enhance system reliability.

2. Characteristics and Gaps according to Design and Verification Scopes

In situations where verification is performed at the card or chip level, a single-clock scheme for internal flip-flops might be used to ensure timing consistency and deterministic operation inside the chip. Synchronous design, which configures a "clock domain" can achieve deterministic operation and provide design clarity. This approach fundamentally prevents Clock Domain Crossing (CDC) risks between signals in the internal logic and contributes to simplifying timing analysis.

However, if the verification scope remains within a specific card or chip level, the effects of asynchronous signals entering from interfaces between different chips or at the system level can be overlooked. When each chip or board uses an independent oscillator or different clock sources, if the synchronization of asynchronous signals at this boundary is not fully reviewed, it can lead to unexpected timing violations or metastability issues. In other words, there can be a gap where the completeness of individual chip or card level verification does not directly translate into the reliability of the entire system.

3. Inter-Chip Interface Synchronization

To guarantee the high level of reliability required for safety-grade systems in nuclear power plants, design principles that supplement these limitations of verification scopes should be accompanied.

Consideration of Inter-Chip Interfaces: In addition to resolving Clock Domain Crossing (CDC) issues using a single clock during internal chip or card design, considering external interfaces is essential. Especially in regions where the same clock synchronization cannot be applied, such as boundaries where chips or cards with independent clock domains meet, a clear synchronization design (e.g., multi-stage synchronizers, handshakes, etc.) must be implemented to resolve metastability issues

Expanded Verification Perspective: Rather than limiting verification to individual chip or card units, interface timing analysis under module-to-module connection environments and consistency verification for asynchronous conditions should be organically linked throughout the entire design process.

4. Conclusions

In FPGA designs for nuclear power plants, verification and synchronization design at individual chip or card levels can be considered as a way to fundamentally block asynchronous designs within specific internal domains. However, if asynchronous factors occurring at system boundaries or inter-chip interfaces are not fully considered, practical gaps can arise. Going beyond the scope of individual unit verification, implementing thorough synchronization designs at inter-chip interfaces and comprehensive verification will bring the design closer to the level of reliability targeted by the standards.

Finally, in addition to recognizing and resolving inter-chip interface synchronization issues, practical application of synchronizer-based FPGA systems to nuclear power plants requires quantitative MTBF analysis and evaluation criteria for synchronizer justification, as well as a CDC verification framework linked to the design lifecycle. These topics will be conducted as future research

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

REFERENCES

[1] KINS/RG-08.29, “Use of FPGA/CPLD in Safety Systems”, 2019.
[2] IEC 62566, “Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions”, 2012.
[3] IAEA Nuclear Energy Series No. NP-T-3.17, “Application of Field Programmed Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants”, 2016.