Development of an Innovative Reactor-Safety System for Multi-module Small Modular Reactors (SMRs)

Hee-Taek Lim
SMR Development Laboratory, Central Research Institute,70 Yusenong-dearo, Daejeon, Korea, 34101
Heetak.lim@khnp.co.kr

***Keywords : SMR, Safety System, FPGA, self-diagnosis, Surveillance testing.**

1. Introduction

Reactor protection and Engineered safety feature actuation systems have become fully digital. The digital approach increases flexibility, but a considerable amount of time and cost is still required for verification and validation (V&V). Moreover, uncertainties arising from the inherent complexity of safety-critical software continue to constitute a paramount concern in the development, licensing, and assurance of nuclear power plant systems. [1-3].

To mitigate software common-cause failures and Anticipated Transient Without Scram (ATWS) events, diverse-protection schemes such as diverse protection systems, diverse manual switches and diverse indication system have been introduced. Although these measures enhance fault tolerance, they inevitably increase overall system architecture complexity and impose a higher operational workload on plant personnel. In the context of Small Modular Reactors (SMRs), the multiplicity of independent modules dictates that each module be equipped with a dedicated Reactor Protection System and a dedicated Engineered Safety Feature Actuation System. Consequently, the I&C capital and life-cycle costs are substantially higher than those of conventional large-scale reactors.

Therefore, a safety system that is simplified, robust against software-induced failures, and hardened against cyber-security threats is essential. This paper proposes a safety-system architecture that is specifically adapted to the multi-module SMR configuration, and it integrates self-diagnostic and automated periodic surveillance test functions so that surveillance interval can be extended.

2. Reactor Safety System for Multi-module SMRs

2.1 Simplifed Architecture for the Reactor Safety System

The reactor safety system presented herein is deliberately software-free during normal plant operation. In the innovative SMR concept the safety system is designed as a passive safety architecture, so that the actuation of engineered safety feature component is inherently deterministic and therefore greatly simplified. In contrast to traditional large-scale reactors, the engineered safety feature actuation does not rely on a loop-control function; it is performed on a de-energized actuation basis. Because these functions contain no complex arithmetic or branching logic, they can be implemented with field-programmable gate arrays (FPGAs) or micro-electromechanical-system (MEMS) technologies, thereby eliminating software-induced complexity and realizing a highly simplified architecture. Nevertheless, FPGA development relies on hardware-description-language (HDL) code, and a rigorous verification-and-validation (V&V) regime remains mandatory. Moreover, the use of heterogeneous FPGAs mixing SRAM-based and FLASH-based devices adds a layer of diversity that mitigates common-cause software failures. Consequently, the reactor protection system and the engineered safety feature actuation system are consolidated into a single, unified safety architecture based on these heterogeneous FPGAs. The conceptual layout of the proposed Reactor safety system is illustrated in Figure 1.

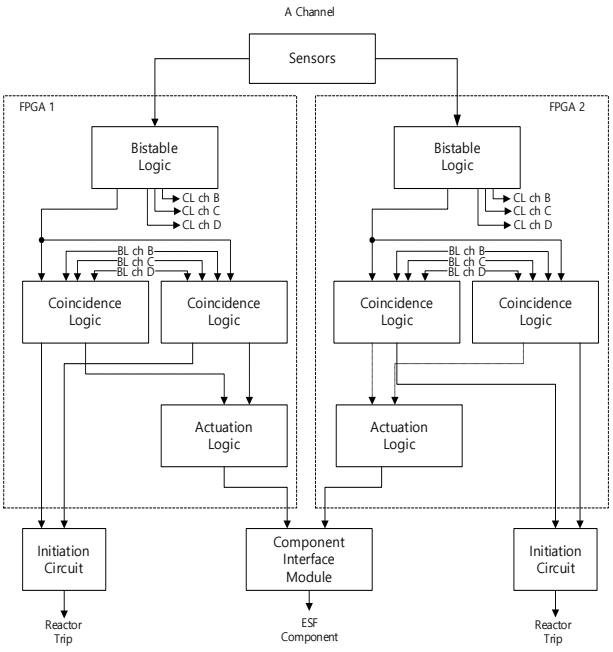

Fig. 1 Conceptual Layout of RSS

2.2 Automation of periodic testing

The second critical challenge for multi-module SMRs is the automation of periodic surveillance testing. For conventional reactors, surveillance tests are performed on a monthly or quarterly basis, depending on national regulations and the design of the safety system. In a

multi-module SMR each module possesses its own protection and engineered safety feature system, which inevitably enlarges the testing workload.

According to IEEE 7-4.3.2-2016, Regulatory Guide 1.152 (RG 1.152), and IEC 60671, in-service surveillance testing may be substituted by self-diagnostic functions—provided that the relevant failure modes are adequately detectable—or by automated-test functions. Consequently, the surveillance interval can be extended to a preventive-maintenance interval. The introduction of an automatic test function, however, obliges a rigorous safety-function impact assessment to demonstrate that any residual effect on safety-related performance is negligible.

Recent safety system platforms such as NuScale HIPS, Westinghouse ALS, and Westinghouse Common-Q for Vogtle 3,4 have already obtained U.S. NRC design certifications that authorize exemption from selected in-service tests by means of self-diagnosis or automated test capabilities.

Exempting periodic surveillance tests reduces the probability of human error induced scrams, lowers channel bypass related unavailability, and is consistent with the emerging industry trend of extending urveillance test intervals for digital safety systems. The architecture proposed in this paper incorporates both self-diagnostic and automated periodic-test functions, thereby supporting the extension or exemption of traditional in-service surveillance testing while remaining fully compliant with the aforementioned standards.

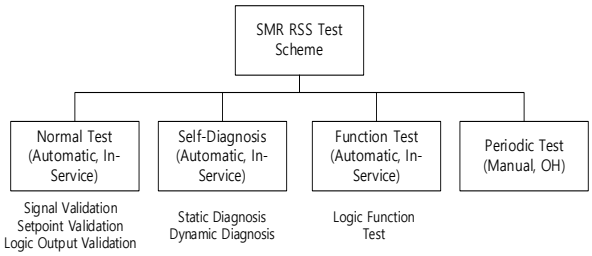

Fig. 2 RSS Test Scheme

3. Conclusions

A reactor safety system concept for multi-module SMRs is presented that mitigates software-induced unexpected behaviour by employing de-energized actuation realized with FPGA technologies and heterogeneous-FPGA architectures. This combination provides high reliability while greatly simplifying the overall system architecture. In addition, the incorporation of self-diagnostic and automated surveillance test functions permits the extension of surveillance testing interval, thereby reducing operator workload and enhancing system availability. Future work will concentrate on (1) the development of a prototype platform based on the proposed architecture, (2) verification and validation of the self-diagnostic algorithms, self-testing functaion and (3) qualification of the heterogeneous-FPGA implementation in accordance with IEC 61513, IEEE 7-4.3.2-2016, and NRC RG 1.152 requirements. The expected outcomes are a significant improvement in the economic competitiveness of SMR designs and a robust safety assurance that supports licensing of innovative small-modular reactors.

Acknowledgment

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

REFERENCES

[1] U.S. Nuclear Regulatory Commission, Research Information Letter (RIL) 1001 – Software-Related Uncertainties in the Assurance of Digital Safety Systems, NRC, 2011.

[2] U.S. Nuclear Regulatory Commission, Research Information Letter (RIL) 1002 – Identification and Analysis of Failure Modes in Digital Instrumentation and Congrol(DI&C) Safety Systems, NRC, 2014.

[3] U.S. Nuclear Regulatory Commission, Research Information Letter (RIL) 1101 – Technical Basis to Review Hazard Analysis of Digital Safety Systems, NRC, 2015.

[4] IEEE Std 7-4.3.2-2016, IEEE Standard for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE, 2016.

[5] U.S. Nuclear Regulatory Commission, Regulatory Guide 1.152 – Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants, Rev. 4, 2023.

[6] IEC 60671:2007, Nuclear Power Plants – Instrumentation and Control Systems important to safety - Suveillance testing, 2007.