Internal Diversity Strategy in Digital I&C Systems for CCF Mitigation

Hangyu Kim [a*]
[a]*KHNP, Central Research Institute, 70, Yuseong-daero 1312beon-gil, Yuseong-gu, Daejeon, 34101, South Korea*
[*]*Corresponding author: hangyukim@khnp.co.kr*

Keywords : Common Cause Failure, Defense-in-Depth and Diversity, Risk-Informed Approach, Internal Diversity

1. Introduction

The development of Small Modular Reactor (SMR) is accelerating globally to provide solutions for carbon neutral and meet the growing demand for electric power. For Innovative SMR (i-SMR) currently under development, the design optimization of Instrumentation and Control (I&C) systems through simplification and compactness is highly important to ensure both safety and economic efficiency.

However, digital I&C systems are susceptible to the inherent risk of Common Cause Failure (CCF) due to potential software defects. Traditionally, addressing CCF for digital I&C systems has relied on the deterministic mandates of SRM-SECY-93-087 [1], which typically requires separate external diverse systems to mitigate CCF.

However, the U.S NRC's recent policy expansion, SRM-SECY-22-0076 [2] introduces a risk-informed approach to address CCF. This a new approach allows more flexible Defense-in-Depth and Diversity (D3) analyses based on the safety significance of the systems.

In accordance with the expanded policy on potential CCF, the latest revision of Branch Technical Position (BTP) 7-19 (Rev.9) [3] provides the acceptance criteria for use of diversity within the digital I&C system to eliminate potential CCF.

This paper presents the internal diversity strategy in digital I&C systems for CCF mitigation.

2. Regulatory Background

2.1 Expanded Policy to SECY-22-0076

SECY-93-087, Item II.Q has been the foundational guideline, mandating the deterministic D3 assessment. This an approach requires the same level of diversity for all safety functions to mitigate CCF, regardless of actual risk or safety significance. As a result, the deterministic approach causes excessive hardware complexity and high maintenance burdens for digital I&C systems.

SECY-22-0076 has expanded the policy to allow the use of a risk-informed approach in performing the D3 assessment and in determining the adequacy of design techniques, prevention and mitigation measures to address potential CCF. As a result, the expanded policy provides a more flexible approach that determines the level of D3 application based on safety significance.

2.2 BTP 7-19 (Rev.09)

BTP 7-19 provides regulatory guidance for evaluation of D3 to address CCF due to latent design defects in digital I&C systems. The latest revision of BTP 7-19 has been updated to incorporate the expanded policy in SRM-SECY-22-0076. It provides guidance for risk-informed D3 assessment, in addition to the existing guidance for assessment based on best-estimate methods.

BTP 7-19 addresses the four points in SRM-SECY-22-0076 as shown Figure 1.

(1) The D3 assessment must be commensurate with the risk significance of the proposed digital I&C system.
(2) In performing the D3 assessment, each postulated CCF must be analyzed using either best-estimate methods or risk-informed approach.
(3) The D3 assessment must demonstrate that a postulated CCF can be reasonably prevented or mitigated or is not risk significant.
(4) Main control room displays and controls that are independent and diverse from the proposed digital I&C system must be provided for manual, system-level actuation of risk-informed critical safety functions and monitoring of parameters that support the safety functions.

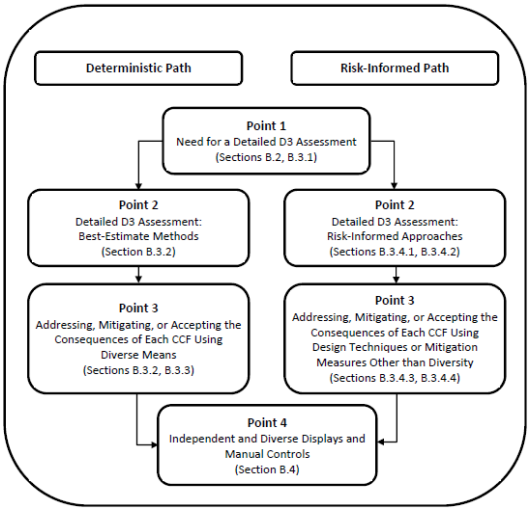

Fig. 1. Four points of SRM-SECY-22-0076

BTP 7-19 allows for diversity within digital I&C system to eliminate the potential CCF and provides specific acceptance criteria for its implementation.

Given this regulatory background, section 3 introduces internal diversity strategy in digital safety systems for CCF mitigation.

3. Internal Diversity Strategy

The Reactor Safety System (RSS) for i-SMR performs reactor trip and engineered safety features actuation functions. The RSS is composed of bistable logic, coincidence logic, and actuation logic, which are implemented as software to perform its safety function. Since these digital modules are susceptible to the potential CCF, a separate external diverse system is required to cope with CCF.

Unlike large scale nuclear power plants, the digital safety systems for i-SMR utilize heterogeneous FPGA platform instead of a separate external diverse system to cope with CCF. As shown in Figure 2, the RSS is implemented as heterogeneous FPGA platform: Type 1 is an SRAM-based FPGA, while Type 2 is a flash-based FPGA.

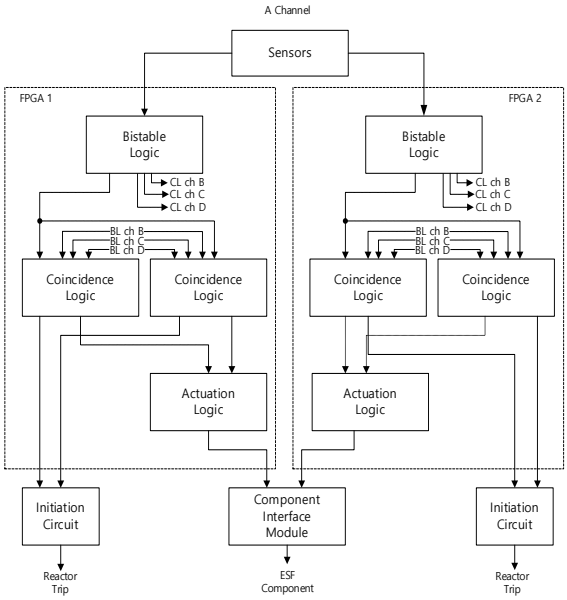

Fig. 2. Internal diversity of RSS for i-SMR

This combination provides a means of mitigating CCF by utilizing different hardware architecture. Also, two types operate completely independently and perform safety function without any mutual interference.

The technical justifications for internal diversity strategy are as follows:

(1) The RSS is designed with two types to perform safety function independently. A postulated CCF within one type cannot affect the safety function for RSS. That is, in the event of a postulated CCF in type 1, type 2 can normally perform reactor trip and engineered safety features actuation functions.

(2) Two types are completely physically separated and do not share any critical resources such as power supplies, memory, bus, or communication modules. The physical separation and functional independence ensure that failures generated in one type cannot propagate to the other type.

(3) Two types utilize different Hardware Description Languages (HDLs) and development tools by different FPGA vendors. As utilizing distinct logic synthesis and Place and Route (P&R) tools provided by different FPGA vendors, the risk of latent systematic errors originating from a single development environment is eliminated.
Also, Verification and Validation (V&V) activities are performed by independent organizations for each type. This ensures that a software bug in the development tool cannot affect both types simultaneously.

Therefore, the RSS ensures sufficient diversity within the system to mitigate potential CCF and maintain its safety function.

4. Conclusions

The proposed internal diversity strategy represents a significant advancement in the design of digital I&C systems. The FPGA-based internal diversity architecture is the advanced and optimized I&C design for i-SMR according to a risk-informed approach to eliminate CCF.

The FPGA-based internal diversity architecture successfully satisfies acceptance criteria for use of diversity within the digital I&C specified in BTP 7-19. Specifically, each diverse portion within the digital safety system performs its safety functions independently. Furthermore, each diverse portion is developed using diverse development tools, and do not share any critical resources.

Therefore, heterogeneous FPGA platform provides sufficient diversity within the system to mitigate potential CCF. Consequently, heterogeneous FPGA platform enables the elimination of separate external diverse systems and the design optimization of I&C systems through simplification and compactness.

Acknowledgement: 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 NRC, “Staff Requirements - SECY-93-087 - Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs”, July 1993

[2] U.S NRC, “Staff Requirements - SECY-22-0076 - Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems”, May 2023

[3] U.S NRC, NUREG-0800, BTP 7-19, Rev.9, “Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure due to Latent Design Defects in Digital Instrumentation and Control Systems”, May 2024