Approaches against CCFs for Low Safety Significance Digital I&C Systems

Y. M. Kim* and S. B. Park
Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon, Korea, 305-338
*Corresponding author: ymkim@kins.re.kr

1. Introduction

In general, the availability and potential of digital technology are expected to increase the use of digital technology for new and running power plants. In addition, however, concerns are increased over the possibility that the use of software-based components and systems in safety systems will result in failure of the systems due to design flaws in software or digital systems. So, the licensee shall be able to identify and assess events that have not been analyzed for malfunctions in various structures, systems and components(SSC). In addition, licensee should provide the results of sensitivity analysis to potential digital system failures, including common cause failures (CCFs), and to unintended behavior that may lead to plant malfunctions.

Despite the many advantages of digital facilities, nuclear power operators are burdened with appropriate application of the review criteria for the "simple system" associated with 100% testing of BTP 7-19, as well as demonstrating the adequacy of the digital I&C system development procedures. To improve the safety and reduce the burden on nuclear operators' licensing, it is necessary to develop regulatory technologies to cope with CCF of digital I&C systems to eliminate uncertainty, ambiguity, and redundancy of requirements and to ensure regulatory consistency.

So far, the regulatory position of the CCF for low safety significance digital I&C systems such as safety grade auxiliary supporting systems and non-safety systems is not clearly presented.

In this paper, we propose a graded approaches against digital CCF which can be used for digital based I&C systems for auxiliary supporting features and non-safety features.

2. Background

U.S. NRC provides regulatory positions for CCFs in digital I&C systems through SRM-SECY-93-087, II.Q1[1]. SRM-SECY-93-087 provides specific acceptance criteria for evaluating CCF and SRP BTP 7-19 provides guidance for evaluation. SRM-SECY-93-087 does not provide criteria that can preclude consideration of potential software flaws in defence-in-depth and diversity(DID&D) analysis. However, SRP BTP 7-19[2] sets out two criteria to exclude further evaluation of potential software CCFs. The first is to demonstrate that adequate internal diversity exists, and the second is to test all possible logic to ensure that the fault no longer exists.

In 2016, the U.S. NRC Commission approved the Integrated Action Plan(IAP)[3] of NRC staff through SECY 16-0070. The IAP consists of four modernization plans(MPs), and MP1 is related to the evaluation of digital I&C CCF. MP1 is developing guidelines for qualitative assessment of the probability of a defect for evaluation of CCF. MP1 consists of four purposes.

MP1A produces durable guidance for evaluating and documenting the proposed use of design attributes, quality of the design processes, and operating history to address CCF when replacing or modifying lower risk-significance safety system such as auxiliary supporting digital I&C systems, in the form of a supplement to RIS 2002-22[4]. MP1B evaluates NEI's proposed guidance in NEI 16-16 for address CCF in digital I&C systems, based on the application of design measures for preventing, limiting, or mitigating CCF. MP1C evaluates NRC's current position on protection of digital I&C systems and components against CCF. This objective was completed and the positions of NRC were described in SECY-18-0090[5]. MP1D revises BTP 7-19 to provide guidance to NRC staff on evaluating potential CCFs and associated diversity and defense-in-depth analysis.

3. Approaches to Address Software based Digital CCFs

Fig.1 shows examples of features belonging to the safety and non-safety I&C systems of the NPP. Since Hanul Unit 5&6, digital platforms have been applied to RTS(Reactor Trip System) and ESFs(Engineered Safety Features). Recently, safety grade smart transmitters classified as ESF's process sensors and safety grade digital undervoltage relays classified as auxiliary supporting features, have been applied to NPPs.

In KINS, as in SRP BTP 7-19, Safety Review Guide(SRG) App. 7.0-1 and App. 7-16 present two conditions that can eliminate further consideration of CCF: sufficient design diversity within the digital I&C system, or 100% testability based on simple structure. However, for typical digital systems/components, it is not easy to show sufficient design diversity and 100% testability. Also, it is inefficient to apply current regulatory requirements equally to all digital I&C systems.

For digital RTS and ESF, current regulatory positions are applied. In this study, we propose the graded

approach for the CCF evaluation only when digital technology is applied to the auxiliary supporting features, other auxiliary features and non-safety features.

3.1 Determining the Scope and Targets of CCF DID&D Analysis

KINS SRG Appendix 7.0-1 for Light Water Nuclear Power Plant, "Review Procedure for Digital I&C System" and Appendix 7-16 "Defense-in-depth and Diversity Assessment Guidance for Digital Computer Based I&C Systems," require DID&D analysis for digital reactor protection systems and engineering safety equipment operating systems.

From SRP BTP 7-19. rev.6 (2012) in the U.S., it is proposed that the assessment of CCF in digital I&C should be carried out by including digital-based auxiliary supporting features and other auxiliary features as well as RTS and ESF.

In case of domestic nuclear power plants, safety grade smart transmitters were used for construction plants after Shin-Gori NPP Unit 3&4, and they were required to perform DID&D analysis against software CCF for those devices. Also, for Shin-Hanul NPP Unit 1&2, non-safety control systems were evaluated for postulated software CCF of control systems[6].

		Sense and Command Features	Execute Features	Power Sources
Safety System	Reactor Trip System and Engineered Safety Features	• Process Sensors • Signal Conditioning • Decision Logic • Manual Switches • Process Control • Indicators for Operator Actions, etc	• RTS Trip Breakers • ESF Breakers • ESF Moters, Starters • ESF Pumps • ESF Motor Operated Valves, Solenoid Valves, etc	
	Auxiliary Supporting Features	• Room Temperature Sensor • Pressure Switches and Regulators • Undervoltage Relays, etc	• HVAC Fans, Filters • Lube Pumps • Component Cooling Pumps • Breakers, Starters, Moters, etc	• Air Compressors and Receivers • Batteries • Diesel Generators • Inverters • Transformers • Busworks, etc
	Other Auxiliary Features	• Built in Test Equip. and Circuitry • Bypass and Reset Circuitry • Electric Protective Relaying • Manual Switches, etc	• Safety System Isolation Devices • Breakers to Nonessential Loads	• Batter Chargers • Transformers • Buswork • Distribution Panels, etc
	Non-Safety Features	• Process Sensors • Signal Conditioning, etc..	• Pump, Valves, etc	• Transformers • Buswork • Distribution Panels, etc

Fig.1 Examples of equipment of safety and non-safety I&C systems

Given the revision of SRP BTP 7-19 and regulatory trends for domestic nuclear power plants, an impact assessment on software-induced potential CCFs is required for all digital-based I&C systems and components even non-safety I&C system.

3.2 Graded Approach against Digital I&C CCF

Figure 2 shows the basic three-step procedures for address digital I&C CCFs. The first step is to perform the dependability analysis of the digital I&C systems/components. The dependability analysis is a qualitative assessment, and the technical evaluation utilizes the following three factors presented in NEI 01-01[7].

- Design attributes
- Quality of design process
- Operating experience

The analysis can be completed if the qualitative analysis using above three factors determine that the adoption of new digital I&C or proposed digital I&C modifications are sufficiently low likelihood to fail.

The second step is to perform the propagation analysis. This is the case if the proposed digital systems/components have network connections or shared resources with other channels/divisions/systems. If the results of the CCF propagation analysis can show technical justification to demonstrate that the adverse effects on other systems are sufficiently low, the analysis is completed.

The third step is the DID&D analysis phase. The DID&D analysis performs a qualitative/quantitative analysis of each event in the safety analysis section of the SAR for the postulated CCF.

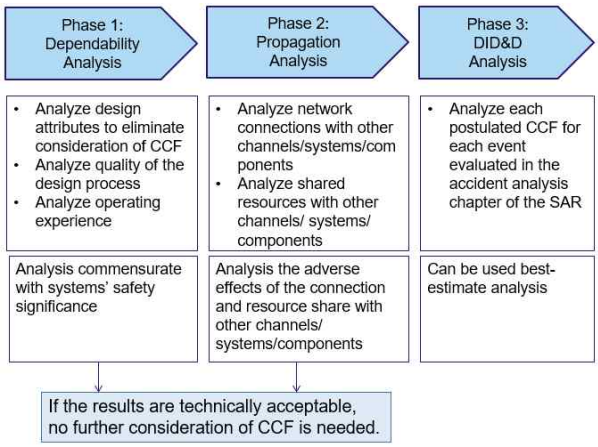

Fig.2 The CCF evaluation procedure for digital equipment for the auxiliary supporting features and non-safety features

3.3 Guideline of the assessment

The process and results of the dependency assessment should provide technical justification corresponding to the safety significance of the target digital I&C systems/components. If a qualitative assessment indicates that the likelihood of a postulated CCF or the adverse impact on the safety functions is sufficiently low, no further consideration of the CCF is required. If digital I&C systems and components have network connectivity or shared resources with other channels/divisions/systems, a more in-depth review is required. However, if the assessment results are not satisfactory, a DID&D analysis should be performed on each postulated CCF for the each event in Chapter 15 of the SAR to show that CCF does not adversely affect the performance of safety functions and the condition of the

plant.

4. Conclusion

In this paper, we proposed a graded approach that can be used to address CCFs of digital-based I&C systems for auxiliary supporting features, other supporting features, and non-safety features. Applying these graded approaches to digital I&C assessments requires detailed guidance and acceptance criteria for qualitative assessment. The future studies plan to develop regulatory guide for qualitative assessment for applying graduated approach and to present various applicable defensive measures which can be used for the dependability improvement.

Acknowledgements

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety (KOFONS), granted financial resource from the Nuclear Safety and Security Commission (NSSC), Republic of Korea (No. 1805006).

REFERENCES

[1] SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” U.S. Nuclear Regulatory Commission, Washington, D.C, 1993.
[2] Branch Technical Position (BTP) 7-19, “Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems,” revision 7, U.S. Nuclear Regulatory Commission, Washington, D.C., 2016.
[3] NRC, “Integrated Strategy to Modernizing NRC Digital I&C Regulatory Infrastructure”, Jan. 2019
[4] NRC RIS 2002-22, Supplement 1, “Clarification on endorsement of nuclear energy institute guidance in designing digital upgrades in instrumentation and control systems”
[5] SECY-18-0090, “Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Control,” U.S. Nuclear Regulatory Commission, Washington, D.C, 2018.
[6] Y. M. Kim and S. B. Park, “Regulatory Experience against Digital I&C CCFs of NPP”, Transaction of the Korean Nuclear Society Autumn Meeting, Yeosu, Korea, 2018
[7] NEI 01-01, “Guideline on Licensing Digital Upgrades”, EPRI TR-102348 Revision 1, Mar. 2002