Transactions of the Korean Nuclear Society Autumn Meeting
Goyang, Korea, October 24-25, 2019

A Study on improvement plan against potential digital CCFs of NPP

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 the case of operating nuclear power plants, it is necessary to modify existing systems and components due to the aging of facilities. But, there are suffering from difficulties in procuring replacement parts and increased maintenance costs. Digital technology is expected to be used for facility replacement of operating power plants, because it can generally provide advantages such as improved performance, reliability and availability. However, digital-based technologies pose a risk to software-induced common cause failures (CCFs). Thus, when digital technology is used, licensee must perform identification, analysis and evaluation of malfunctions of new systems or components. In particular, the use of embedded digital devices(EDDs), such as smart sensors and actuators, requires attention at the plant level as well as the quality of individual parts. For example, if the plant protection system (PPS), the diversity protection system (DPS) and the control system all use the same EDDs, there is a risk of the same error.

The main purpose of this study is to provide a common regulatory framework and understanding of dealing with digital CCFs when applying digital I&C and power facilities to nuclear power plants. This paper presents the basic improvement direction of the current CCFs coping regulatory guidance and the approaches for the CCFs that can be applied to safety system and non-safety system equipment except RPS and ESFAS.

2. Background

The application of digital technology to various systems, including emergency diesel generators, transmitters, relays, pumps and valves, has recently been expanded to new and operating power plants. But, the U.S. nuclear power industries have raised that the biggest obstacle to digital technology's application of nuclear power plants is to meet regulatory requirements for licensing digital CCFs.

In addition, the current regulatory acceptance criteria for digital CCFs are too complex and inefficient. And they have required clearer guidance that have been removed from uncertainty and ambiguity. In Korea, safety-grade digital devices other than the existing digital RPS and ESFAS have been installed in new and operating nuclear power plants. The domestic nuclear industry has suggested that clearer coverage should be set first for systems and components other than RPS and ESFAS to apply regulatory requirements for coping with CCFs [1].

U.S. NRC provides regulatory positions for CCFs in digital I&C systems through SRM-SECY-93-087[2]. 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[3] 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 issued SRM-SECY-15-0106, which directed the NRC staff to develop an integrated strategy to modernize the NRC's digital I&C regulatory infrastructure. In developing integrated action plan(IAP), the Commission directed the staff to consider the broader context of digital I&C regulatory challenges and updates to the policy on CCFs in SRM-SECY-93-087. The U.S. NRC approved the Integrated Action Plan(IAP)[4] 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 CCFs. In 2018, SECY-18-0090 informed the NRC staff's plan to update and clarify guidance associated with evaluating and addressing potential CCFs of digital I&C systems.

3. Basic Improvement Plan

The basic improvement directions for regulatory positions related to digital CCFs for NPP are as follows.

3.1 Expanding the CCFs Analysis Coverage

Until SRP BTP 7-19, rev. 5 (March 2007), digital reactor trip systems and engineering safety facilities were subject to CCFs analysis, but since SRP BTP 7-19, rev. 6 (July 2012), the target systems have been expanded to digital software-based auxiliary supporting features and other auxiliary features.

Since Shin-Kori Units 3 and 4, the use of software based smart sensors and digital relays have been used in nuclear power plants. It is understood that various sensors, switches, transducers, breakers, and protective

relays for the auxiliary supporting features are being digitalized in operating nuclear power plants [5]. It is necessary to clearly state the regulatory position on embedded digital devices (EDDs) that are expected to increase the use of them in auxiliary supporting features and other auxiliary features.

3.2 Using the qualitative assessments

In RIS 2002-22, Supplement 1 [6], NRC has clearly indicated how NEI 01-01 [7] is used to upgrade digital I&C systems by applying 10 CFR 50.59 Rule. RIS 2002-22, Supplement 1, suggests that a qualitative assessment can be used to conclude that the likelihood of failure due to digital I&C upgrades or modifications is "sufficiently low." However, the current regulatory position should be maintained for the RPS and the ESFAS, and the utilization of the qualitative assessment could be applicable to systems and devices with low safety significance. NEI 01-01 suggests that digital I&C systems can be used for qualitative assessment of the following three attributes:

- Design attributes
- Quality of design process
- Operating experience

3.3 Graded approach commensurate with safety significance

In 2018, SECY-18-0090 presented the basic principles for the revision of SRP BTP 7-19. The main modifications to BTP 7-19 are the D3 analyses commensurate with safety significance and the credit of the defensive measures. Existing SRP BTP 7-19 does not provide regulatory requirements commensurate with safety significance for safety-grade digital I&C systems. SECY-18-0090 accepted the opinions of the U.S. nuclear industry and set out the direction of the revision to perform the D3 analysis of digital I&C CCF commensurate with the safety significance of the system. In some cases, a D3 analysis may not required for systems with low safety importance.

The two defensive measures that are credited in the existing SRP BTP 7-19 are internal diversity and 100% testability. It suggests that the CCF of the digital system/component should no longer be considered if appropriate internal diversity or all possible logic tests to ensure that no more defects exist can be demonstrated. However, the U.S. nuclear industry has suggested that proving the internal diversity and 100% testability described above for various digital systems/components with IT technology is too complex, ambiguous and inefficient. NRC has suggested that any defensive measures credited need technical justification that demonstrates that an effective alternative to internal diversity and testability has been implemented. That is, NRC has proposed that the use of other defensive measures is acceptable if it can be demonstrated to be an effective alternative to internal diversity and testing.

3.4 Effects of Spurious Actuation Caused by CCF

The SRP BTP 7-19 (rev.6, rev.7) raised that the effects of spurious actuations due to software CCF expected from an automatic protection system may not be evaluated in the safety analysis of SAR's Chapter 15. In such cases, an analysis should be performed to determine whether such a postulated spurious actuation results in a plant response that falls outside the values or ranges of values chosen for controlling parameters as reference bounds for design. In addition, these analyses should identify whether there is an appropriate coping strategy for these postulated spurious actuation. If the existing coping strategy is not effective in responding to the expected postulated spurious actuation that results in plant conditions falling outside those established as bounding for plant design, the licensee should develop additional coping strategy.

4. Conclusion

To cope with CCFs of digital systems/components used in various forms, quality of purchase, development and operation of individual equipment should be ensured, and plant level safety should be considered. In particular, safety against digital CCFs should be ensured if the same EDDs are used for the different systems of the nuclear power plant. In this paper, it has been proposed to improvement plan for current regulatory requirements for digital I&C and electrical systems coping with CCFs. The improvement plan includes expanding of CCF analysis coverages, using the qualification assessments and graded approach commensurate with the safety significance, and consideration of effects of spurious actuation caused by CCF.

The future studies plan to develop regulatory guide for applying basic improvement plan and to present various applicable defensive measures which can be used for the qualitative assessment and regulatory decision.

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] KINS/RR-1875, Analysis of Common Cause Failure Technology for Digital I&C and Power System
[2] 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.

[3] 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.
[4] NRC, "Integrated Strategy to Modernizing NRC Digital I&C Regulatory Infrastructure", Jan. 2019
[5]KINS/GR-616, "Development of Proof Test Model and Safety Evaluation Techniques for the Regulation of Digital I&C Systems used in NPPs", 2018.04.
[6] NRC RIS 2002-22, Supplement 1, "Clarification on endorsement of nuclear energy institute guidance in designing digital upgrades in instrumentation and control systems"
[7] NEI 01-01, "Guideline on Licensing Digital Upgrades", EPRI TR-102348 Revision 1, Mar. 2002