Evaluation Procedures of Measures to Eliminate Further Consideration of 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 general, the application of digital technology can provide advantages that can improve reliability and safety. In particular, digital technology enables plant operators to continuously receive diagnostic and availability information related to plant integrity. In addition, the number of cases of improvement and replacement of existing systems and devices by applying digital technology is increasing due to the aging of operating nuclear power plant facilities, difficulty in procuring replacement parts, and increased maintenance costs. However, digital I&C technology can create potential risks such as software common cause failures (CCFs) that have been introduced as a result of the same software platform, use of software modules and interconnection between systems.

The domestic and overseas nuclear industries are demanding clear guidance to eliminate uncertainty and ambiguity, as the current regulatory standards for coping with CCF are too complex and inefficient compared to the rapid technological development of digital technology. Improving the safety of digital I&C systems and reducing the licensing burden of nuclear operators requires providing clear guidance on the means that can be used to exclude additional CCFs and adopting an efficient approach using a graded approach based on safety significance[1,2].

2. Classification and Assessment of Safety Importance for Graded Approach

In this study, the methods proposed in NSTAR-19NS42-107[3] are used to present classification using graded approach for the digital I&C systems and devices according to safety significance.

2.1 Safety Classification for Graded Approach

For graded approach, digital I&C systems are classified into three categories according to safety significance such as H, M, and L system.

- H: Safety-related digital I&C systems and devices
  - It contributes to the initiation and completion of control actions essential for maintaining plant parameters within the acceptable limits established for design basis events.
  - If the failure of the H system or device is not mitigated by the other H system, the accident condition directly causes unacceptable consequences.

- M: Safety-related digital I&C systems and devices and non-safety digital I&C systems and devices
  - As the safety digital I&C systems, auxiliary or indirect functions should be provided to secure and maintain safety of the plant with safety-related systems and devices, or keep the plant in a safe shutdown state after the plant reaches the initial safe shutdown state.
  - Non-safety systems, which directly affect the reactivity or output of the plant, or affect the integrity of the safety barriers (fuel cladding, reactor vessel, reactor building). Alternatively, multiple control functions may be incorporated into a single system, resulting in unacceptable consequences for plant safety.

- L: Non-safety digital I&C systems and devices
  - The system does not directly affect the reactivity or power level of the reactor.
  - Failure of the systems may not affect the safety of the plant or it can be detected and mitigated with significant safety margin.

Contributions to plant safety may be considered not only deterministic but also other methods, such as assessing using risk information. However, the licensee shall document and present the technical justification for the methods and results adopted for classification.

2.2 Graded CCF Assessment for Digital Facility

Fig 1 shows the graded CCF technical evaluation procedure according to the safety significance of digital facilities (systems and devices). In case of H systems with high safety significance of digital facilities, the D3 assessment shall be performed.

The D3 assessment shall be performed to protect H system with high safety significance from hazards to cause CCFs. The D3 assessment is performed as a procedure for assessing the means to eliminate CCFs, evaluating defensive measures against CCFs, performing analysis using realistic or conservative assumptions, and redesigning with added design

characteristics and defensive measures. First, consider a review of internal diversity, testability and defensive measures to exclude potential CCFs from further consideration. If one of three methods can show that the CCF has been sufficiently removed, it can be excluded from further consideration.

For the M systems with low safety significance, a more flexible positions are applied compared to the existing regulatory position, and qualitative assessment results are trusted. The L systems with low safety significance determines whether a qualitative assessment is carried out based on the presence of licensing concerns. If the L systems are likely to cause unanalyzed conditions due to integrated design functions, sharing of resources, and network connectivity with other systems and devices, or if there are licensing concerns, qualitative assessment is carried out. If a qualitative assessment is not performed, the justification for it should be documented.

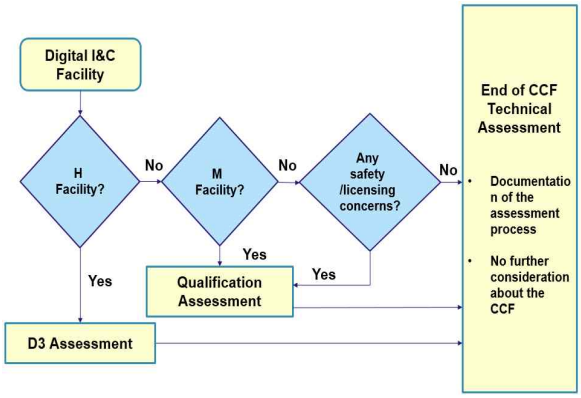

Fig 1. Graded CCF Technical Evaluation Process

3. Evaluation Procedures of Measures to Eliminate further consideration of Digital CCFs

3.1 Using sufficient internal diversity

The appropriateness of internal design diversity should be analyzed in order to utilize the internal diversity to eliminate further consideration of the CCFs. The evaluation procedures for this analysis are as follows:

a) Identification of safety functions and verification of design diversity

It should be verified that each safety function to be performed by the proposed design is achieved independently by diverse parts of the system. For this reason, the safety functions performed by the system are identified, and the satisfaction of the single failure criteria and the independence criteria is analyzed to ensure that the required safety functions can be performed even in the event of a single failure. It is also required to check whether each safety function is performed independently by diverse parts, and whether the final analysis result is documented.

b) Verifying diversity properties

Assessment of the diversity of systems performing safety functions shall be carried out in accordance with the guidance described in NUREG/CR-6303[4] and NUREG/CR-7007[5]. Based on the diversity attributes presented in these guidelines, sufficient diversity is analyzed to ensure that it is adequately analyzed from the perspective of design diversity, device diversity, functional diversity, human diversity, signal diversity and software diversity.

c) Check common/shared resources

In order to verify that it has facilities or functions that can affect diverse parts, it is required to check the analysis details related to the power source, controller, memory, data network, and operator station, and to verify that it does not have common or shared resources that can affect each other. It is also confirmed that in terms of management, various parts of the system or accessories that are important to safety do not share engineering or management means that may affect both parts.

d) Check the operability of the required diversity function

It is required to verify the analysis results of diverse parts used for performing the required safety functions to ensure that plant conditions are reliably operated and continuously available as designed during the relevant design basis accident or anticipated operational occurrence.

e) Using periodic surveillance criteria and ensuring consistency with the technical specification

It is required to verify that the diverse designs are properly operated in accordance with the periodic surveillance criteria during the plant operation period in which the system is required. The verification includes checking the adequacy of the relevant monitoring standards in the technical specification, and also verifies that the analysis results are appropriate for the consistency between the proposed changes and the technical specification.

3.2 Using sufficient testing

In order to utilize sufficient testing to exclude further consideration of the CCF, it must be demonstrated that potential defects that may appear in the design and implementation of the system and device have been identified, reviewed and eliminated. The evaluation procedures are as follows:

a) Evaluation of simplicity

Ensure that the system or device to be tested is simple enough to prove that no potential defect exists through the testing.

b) Evaluation of operating environment

Ensure that the system and device to be tested can be tested in the same environmental conditions as the

actual operating environment.

c) Conducting mandatory test items

c-1) Verify the outputs for all input combinations

The test shall be performed for all possible input combinations of the system and device. It also verifies the accuracy of the output for the input combination.

c-2) I/O testing for all timing sequences

If the output value of the system or device depends on the input timing or changes in the internal state, the test shall be performed by creating a test case that includes all possible timing sequences.

c-3) Perform I/O tests on the status of previous data

If memory is included in the system or device, a test case is created and carried out considering the order (arrangement) of all previous states. If the test is difficult, the analysis should be performed to prove that the order of the all past condition does not affect the output of the system or device.

c-4) Processing of unused logic (circuit)

If the logic (circuit) contained in the system or device is not used in the actual considered operating environment, the test may be excluded. However, unused logic should prove that it does not interfere with the normal operation of the system or device even in the following circumstances:

- Malfunction or failure within the system or equipment
- When the external conditions (temperature, humidity, vibration, etc.) of the system or equipment change,
- Other logic or circuit operation included in the system or device

3.3 Using appropriate defensive measures

In order to eliminate further consideration of the CCF, its appropriateness and effectiveness of the defensive measures to be applied must be analyzed and demonstrated. The following order indicates the evaluation procedure for the utilization of the defensive measures and shall meet the conditions for each of these procedures. The associated CCF evaluation procedures are follows;

a) Identification of hazards

The vulnerabilities or risks of the corresponding digital systems and devices, considering the application of the defensive measures, shall be identified.

b) Selection and application of defensive measures

A description of the defensive measures that are implemented to address identified vulnerabilities or risks shall be given.

c) Understanding the operating principles of defensive measures

Explanation of how CCF is prevented and restricted through the proposed defensive measures should be given.

d) Verification and evaluation of defensive measures

Technical criteria should be given for the reasons why the defensive measures applied to prevent and limit the vulnerabilities or risks identified in the digital device are acceptable. It should also include an analysis of how the effects of the applied defensive measures can be verified.

e) Evaluating other risk factors

Assessments should be made for other potential hazards that could be caused by CCF.

4. Conclusion

In this paper, a proposal was presented to classify CCF evaluation for digital systems and devices into three categories: H, M and L according to safety significance. The D3 assessment should be performed for H systems and devices, and qualitative assessment could be performed for M and some L systems. In addition, the evaluation procedures of measures such as sufficient internal diversity, sufficient testability and the use of appropriate defensive measures which can be used for eliminating further consideration of the CCF for the H system were presented.

It is expected that proposed procedures could be utilized for safety review related to CCF when digital upgrading of operational nuclear power plants and adopting digital systems and devices for new nuclear power plants.

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] 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. NRC.

[2] NRC RIS 2002-22, Supplement 1, “Clarification on endorsement of nuclear energy institute guidance in designing digital upgrades in instrumentation and control systems”

[3] NSTAR-19NS42-107, “Analysis Report for Graded Approach for Digital CCF”, 2019

[4] KINS/RR-2044, “Software Validation and Test against Digital CCFs”, 2020.6

[5] NUREG/CR-6303. “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,”, December 1994.

[6] NUREG/CR-7007, “Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems”, December 2008.