Review of the Regulatory Positions and Guidance on Addressing Potential Common Cause Failures in Digital Instrumentation and Control Systems

Seung Ki Shin* and Yong Suk Suh
Division of Research Reactor System Design, Korea Atomic Energy Research Institute
Daedeok-daero 989Beon-gil, Yuseong-gu, Daejeon 34057, Republic of Korea
*Corresponding author: skshin@kaeri.re.kr

1. Introduction

Digital instrumentation and control (I&C) systems can be vulnerable to a common cause failure (CCF) caused by software errors or software developed logic, which could defeat the redundancy achieved by the hardware architecture [1]. According to IEEE Std 603 [2] which establishes minimum functional and design criteria for safety I&C systems, an engineering evaluation for software CCFs of digital safety systems should be performed including use of manual action and non-safety systems, or components (or both) to provide means to accomplish the function that would otherwise be defeated by the CCF.

To evaluate I&C design against potential software CCFs of safety systems, the diversity and defense-in-depth (D3) analysis should be performed. This paper reviews the current USNRC's positions and guidance on addressing potential CCFs and D3 analysis for digital I&C systems, including the plan to update the current regulatory positions.

2. USNRC Regulatory Positions on CCFs in Digital I&C Systems

As digital technologies were introduced to safety I&C systems in nuclear facilities, the software CCFs in digital systems have emerged as a major concern for regulatory bodies. The USNRC documented its four positions with respect to CCF in digital systems and D3 as Item 18, II.Q, in SECY-93-087, which was subsequently modified in the associated staff requirements memorandum (SRM) [3]. In accordance with the SRM on SECY-93-087, the USNRC published the branch technical position (BTP) 7-19 of NUREG-0800 [1] to provide guidance for a D3 assessment of digital I&C systems and confirm the vulnerabilities to CCF. The BTP 7-19 requires that the followings be verified through a D3 assessment.

1) Adequate diversity has been provided.
2) Adequate defense-in-depth has been provided.
3) Displays and manual controls for critical safety functions initiated by operator action are diverse from digital systems used in the automatic portion of the protection systems.

The BTP 7-19 provides various acceptance criteria and requires a D3 analysis to ensure conformance with the regulatory positions on D3 for digital I&C systems.

The relevant regulatory requirements and guidance can be summarized as Fig. 1. The following sections reviews guidance on how to perform a D3 analysis and credit manual operator actions for safety critical functions.

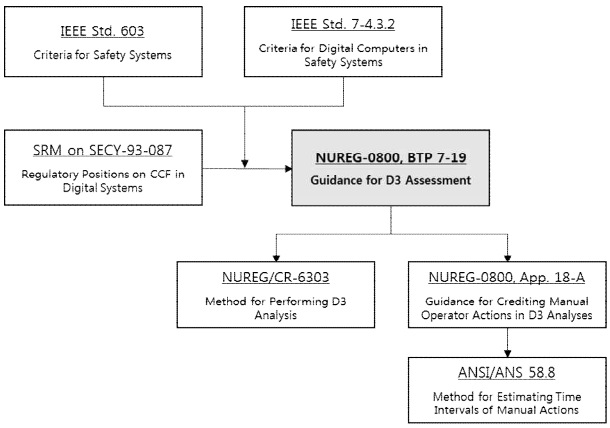

Fig. 1. USNRC regulatory positions and guidance on CCFs in digital I&C systems.

3. Method for Performing D3 Analysis

NUREG/CR-6303 [5] provides detailed D3 analysis methods for digital I&C systems to discover design vulnerabilities to CCFs. It describes fourteen specific guidelines for a D3 analysis.

The first step for D3 analysis is partitioning components or divisions of I&C systems into 'blocks'. A block is defined as the smallest portion of the system under analysis for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment. And then the degree of diversity between each block should be determined considering six attributes: design diversity, equipment diversity, functional diversity, human diversity, signal diversity, and software diversity.

According to the guidelines in NUREG/CR-6303, I&C systems are categorized into four echelons of defense as follows.

1) Control echelon
2) Reactor trip echelon
3) Engineered safety features (ESF) actuation echelon
4) Monitoring and indicator echelon

It should be verified that sufficient diversity among the echelons of defense exists so that any design basis

events (DBE) in conjunction with a software CCF of reactor protection system can be mitigated by the echelon of defense that is not impaired by the postulated CCF. For each anticipated operational occurrence and postulated accident in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic assumptions should not exceed allowable safety criteria.

When the reactor protection system cannot perform automated protective functions due to a potential software CCF, the required protective functions should be accomplished through diverse means, either an automated system or manual operator actions performed from the main control room. The automated system is generally preferred for the diverse means. To use manual operator actions as a diverse means to perform protective functions, the manual operator actions should be credited using a suitable human factors engineering (HFE) analysis.

4. Guidance for Crediting Manual Operator Actions

NUREG-0800, Appendix 18-A [6], defines a methodology to credit manual operator actions as a diverse means of coping with design basis events that are concurrent with a software CCF of digital protection system through four phases as below.

1) Analysis of time available and time required for manual operator actions
2) Preliminary validation of time required to take manual operator actions
3) Integrated system validation of manual operator actions
4) Maintaining long-term integrity of credited manual operator actions

It should be demonstrated that the 'time available' to perform the required manual actions is greater than the 'time required' for the operator to perform the actions, so that the operator can perform the actions correctly and reliably within the time available.

The time available to perform the actions should be based on best estimate thermal-hydraulic analysis of the reactor response to the design basis events using realistic assumptions.

The time required for the manual operator action should be based on an HFE analysis of operator response time. The ANSI/ASN 58.8 [7] provides the methodology to estimate the time required for individual task components. The time required to be analyzed can be divided into several sub-intervals as shown in Fig. 2.

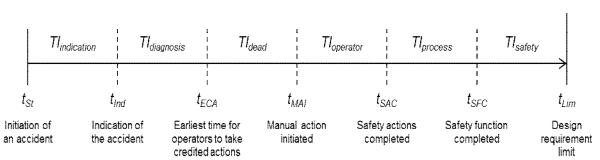

Fig. 2. Definition of time intervals for manual operator actions.

5. Plan to Update Regulatory Positions on D3

The USNRC's plan to clarify guidance associated with evaluating and addressing potential CCF of digital I&C systems is documented in SECY-18-0090 [8]. It clarifies that the existing policy was adequately flexible, but that USNRC's implementation of the policy had been overly restrictive for some types of modifications. It also identifies guiding five guiding principles for consistent application of the direction provided in SRM on SECY-93-087.

The USNRC has a plan to revise the BTP 7-19 incorporating the guiding principles identified in SECY 18-0090. The main focus for the revision will be to recognize that the approach for CCF is inherently meant to be graded. The graded approach refers to analyses performed for equipment of differing safety significance in which CCF concerns apply. In addition, the revision will complement the approach established in the RIS 2002-22, Supplement 1[9] which clarifies endorsement of nuclear energy institute guidance in designing digital upgrades in I&C systems.

6. Summary and Conclusions

As safety I&C systems adopted digital technologies, the software CCF has been one of the major issues for the safety of nuclear facilities and the concept of D3 should be introduced in I&C design to minimize detrimental effects of the CCF on safety.

This paper reviews the current USNRC's positions and guidance on addressing potential CCFs and D3 analysis for digital I&C systems, including the plan to update the current regulatory positions. This paper can be used as a guideline for applicants to design I&C systems and perform a D3 assessment.

Through a D3 analysis, potential vulnerabilities to a software CCF can be identified and required corrective actions can be taken considering the analysis results. If any design change is implemented in I&C systems, the D3 analysis should be carried out iteratively. The earlier a D3 analysis is performed with available design data, the less it would cost for design modifications.

REFERENCES

[1] USNRC, NUREG-0800, Branch Technical Position 7-19, Revision 6, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems, 2012.

[2] IEEE Power & Energy Society, IEEE Std. 603-2009, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, 2009.

[3] USNRC, Staff Requirements Memorandum on SECY-93-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs, 1993.

[4] IEEE Power & Energy Society, IEEE Std. 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2010.
[5] USNRC, NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, 1994.
[6] USNRC, NUREG-0800, Appendix 18-A, Crediting Manual Operator Actions in Diversity and Defense-in-Depth Analyses, 2014.
[7] ANSI, ANSI/ANS 58.8, Time Response Design Criteria for Safety-Related Operator Actions, 1994.
[8] USNRC, SECY-18-0090, Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls, 2018.
[9] USNRC, Regulatory Issue Summary 2002-22, Supplement 1, Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems, 2018.