Transactions of the Korean Nuclear Society Autumn Meeting
Yeosu, Korea, October 25-26, 2018

Implementation of Common-Cause Failure Malfunctions to APR1400 Simulator

J. B. Lee[*]
Central Research Institute, KHNP, 70, 1312 beon-gil, Yuseong-daero, Yuseong-gu, Daejeon
[*]Corresponding author: jbdoll01@khnp.co.kr

1. Introduction

Since the introduction of digital I&C systems to nuclear power plants, diverse means to cope with CCFs (Common Cause Failures) have been applied through intensive evaluation programs. Manual operation actions can be credited as one of coping means to AOOs and postulated accidents that are concurrent with a software CCF of the digital I&C protection system as mentioned in BTP 7-19 [1] after evaluating the operator action time based on ANSI/ANS 58.8 [2]. These operator action times are used as assumptions in safety analysis. In order to credit the operator action times assumed in safety analysis, they should be evaluated using full-scope simulator which has the function of inserting CCF-related malfunctions. Here, a brief description of the method of the function is presented.

2. Methods and Results

In this section some of the techniques used to model the CCF-related malfunctions are described. The model includes malfunctions of both safety systems and non-safety systems.

2.1 MMIS Architecture of APR1400

MMIS platform of APR1400 consists of safety systems such as PPS, ESF-CCS, CPCS, QIAS-P, and QIAS-N and non-safety systems. Figure 1 shows brief architecture of APR1400 MMIS. Digital protection systems are safety systems in the figure, and are marked as purple boxes.

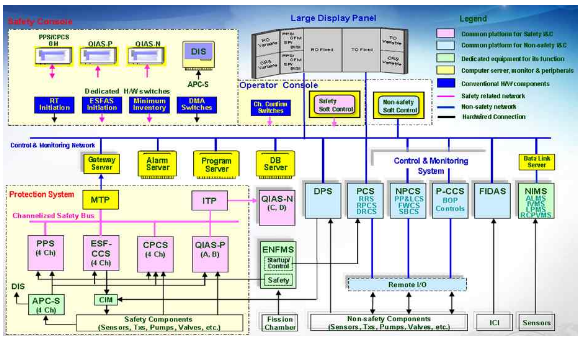

Fig. 1. A Brief Diagram of APR1400 MMIS which consists of safety systems and non-safety systems.

2.2 CCF in Digital Protection System of NPP

Digital I&C systems can be vulnerable to CCF caused by software errors or software developed logic, which could defeat the redundancy achieved by hardware architecture [1]. Thus, while CCF in digital systems are considered as BDB (Beyond Design Basis), nuclear plants should be protected against the effects of AOOs (Anticipated Operational Occurrences) and postulated accidents with a concurrent CCF in the digital protection system.

A diverse means is used to cope with CCF. The diverse means can include manual non-safety systems if the system is able to perform the necessary function under the associated event conditions within the required time [1]. The required time is used as an assumption in safety analysis of CCF under DBE condition. In order to credit the time, it should be estimated and validated. One of validation method is real-time validation on a suitable simulator [3] which has capability to simulate CCF conditions concurrent with DBE.

2.3 Malfunctions Modeling in the Simulator

The CCF-related malfunctions can be categorized as 7 types according to the path of information as ESF-CCS CCF, QIAS-N CCF, QIAS-P CCF, CPCS CCF, PPS CCF, transmitter CCF, and non-safety system CCF.

In order to keep the simulator model simple, one identifier or flag was introduced to logic diagrams and transmitters. The flag can represent each safety system and non-safety system. If the value of the flag is 0, the system works as normal. But if it has non-zero value, the system consider CCF has occurred and the information transition of its path freezes and its displayed physical value on IPS such as LDP and operator workstations does not change. In order to distinguish each CCF case, unique non-zero values are assigned to each system, and summarized as Table 1.

Table I: CCF Flags

Value of Flag	Status of the System
0	Normal
1	CCF of ESF-CCS
2	CCF of QIAS-N
4	CCF of QIAS-P
8	CCF of CPCS
16	CCF of PPS
32	CCF of Transmitter
128	CCF of Non-Safety System

By using bit numbering as an indicator for the flag, it can be possible to simulate diverse conditions at the same time. For example, when the flag has a value of 5, it represents CCF states of ESF-CCS and QIAS-P. So, its function freezes when inserting a CCF malfunction of ESF-CCS or QIAS-P.

3. Conclusions

Digital protection system can be vulnerable to CCF. Diverse means to cope with CCF are used in design and manual operator actions can be one of them. To credit the operator action times, it should be estimated and validated. Real-time validation using a suitable simulator is one of the validation methods. Here, a brief method of making a suitable simulator for CCF analysis is described. Using the suitable simulator adopting this method, diverse and defense-in-depth analysis for CCF of APR1400 have been successfully performed.

REFERENCES

[1] NUREG-0800, Standard Review Plan, BTP 7-19, “Guidance for Evaluation of Diversity and Defense-in-depth in Digital Computer-Based Instrumentation and Control Systems Review Responsibilities,” , Rev. 7,U.S. Nuclear Regulatory Commission, 2016.

[2] ANSI/ANS 58.8 1994, “Time Response Design Criteria for Safety Related Operator Actions,” American Nuclear Society, 1994.

[3] NUREG-0800, Standard Review Plan, 18.0, Attachment A, “Guidance for Evaluating Credited Manual Operator Actions,” Rev. 3,U.S. Nuclear Regulatory Commission, 2016.