A Study on the DI&C CCF Cognitive Methods in NPPs

Songhae Ye[*], Chanho Sung
KHNP CRI, 70, 1312eon-gil, Yuseong-daero, Yuseong-gu, Daejeon, 34101, Korea
[*]Corresponding author: songhae.ye@khnp.co.kr

1. Introduction

Recently, as the role of software of digital I&C (DI&C) in nuclear power plants(NPPs) has increased, the potential of a common cause failure(CCF) is an important subject of interest. The evaluation of CCF of DI&C system in NPP assumes a situation where the reactor protection system does not operate normally due to the occurrence of a software failure of the reactor protection system in conjunction with the design basis accident. Diverse Protection System (DPS), Diverse Indication System (DIS), Divers Manual Actuation (DMA) were introduced as a CCF alternative facility for the nuclear safety system and APR1400 model was applied. However, it is difficult for operators to recognize the CCF situation in DI&C systems immediately. Therefore, this paper presents cognitive methods for the operator to recognize the CCF occurrence in APR1400 DI&C systems.

2. Cognitive Methods of the DI&C CCF

In this section some of the cognitive methods used to recognize the DI&C CCF are described. The cognitive method includes the regulatory trends, evaluation of DI &C against the CCF, CCF cognitive methods.

2.1 The regulatory trends against CCF

NRC considers software CCF to be beyond a design basis accident that must be considered in the safety systems in DI&C. The DI&C systems are to be protected against the effects of anticipated operational occurrences (AOOs) and postulated accidents with a concurrent CCF. CCF vulnerabilities can arise from undetected systematic faults residing shared software or software-designed features among equipment with Embedded Digital Devices (EDDs). In the case of adopting digital devices using software, it is necessary to apply defense in-depth and diversity design techniques, including manual functions, in order to perform required protection functions even if a common cause failure occurs. Therefore, the reactor facility shall be equipped with a separate diversity protection system with reactor shutdown, emergency aux feed water supply operation and turbine shutdown functions in preparation for the possibility of a transient condition not to be stopped even though the reactor must be shut down.

Staff Requirements Memorandum for SECY 93-087 gives a Four-point position for assessing and mitigating CCF vulnerability. In particular, Point 4 is described as follows. A set of displays and controls, independent of the affected systems, must be provided in the main control room for manual, system-level actuation of criteria safety functions and monitoring of parameters that support the safety function.

2.2 Evaluation of DI&C against the CCF

The CCF assessment assumes that the reactor does not shut down normally due to a software failure of the reactor protection system occurring simultaneously under the design basis accidents. In the event of a plant protection system (PPS) failure, automatic reactor shutdown can be occurred by the automatic detection system (Watch Dog Timer). If CCF occurs in the power plant safety systems, it can affect two or more control and alarm systems as shown in following the figure 1.

When a CCF occurs in plant safety systems, it can not generate a pre-trip or trip alarm, which is a reactor shutdown signal generated by a reactor protection system (PPS) or an engineering safety facility system (ESF-CCS). However, it is possible to monitor the status of the power plant after a power plant accident using the variables of the diversity indication system (DIS), where all signals are linked by real wiring.

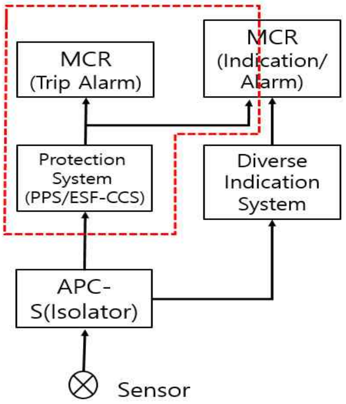

Fig. 1. Functional loss range in DI&C safety systems when CCF occurs

In the CCF situation, it is difficult for the main control room operator to immediately recognize the CCF accident by mixing erroneous information (pre-fault information, out-of-failure information, etc.) displayed on a large information display panel with ordinary information.

In general, emergency operation procedures are performed to safely shut down the reactor in the event of a design basis accident (DBA) or Beyond DBA with CCF. Following the Figure 2 shows the concept that the operator associates an emergency procedure with an abnormal procedure when a CCF occurs.

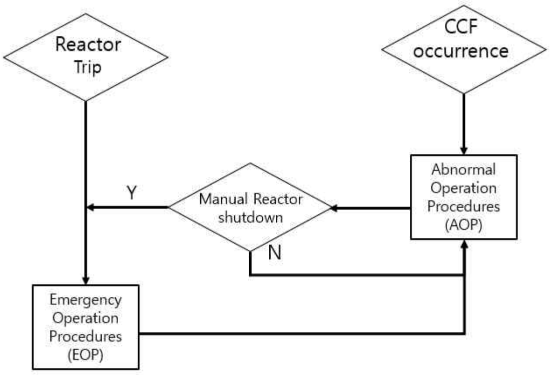
Reactor Trip
CCF occurrence
Abnormal Operation Procedures (AOP)
Manual Reactor shutdown
Y
N
Emergency Operation Procedures (EOP)

Fig. 2. CCF Abnormal Operation Procedures (AOP) Linkage Concept

The entry criteria for Emergency Operation Guidance (EOG) / Emergency Operation Procedure (EOP) during power plant operation is when reactor shutdown has occurred or is required. Therefore, AOP and EOP should not to be performed concurrently for rapid follow-up action of operators in CCF emergency situations.

2.3 CCF Cognitive method

As mentioned above, the rapid recognition and follow-up action of the operator in the CCF situation are the most important factor for maintaining the safety status of the plant. In this chapter, it will present some design improvements for MCR operators to quickly recognize the occurrence of CCF.

- The definition of CCF is required based on the network and FMEA analysis of the digital control platform applied.
- It is necessary to provide detailed classification and alarm for CCF faults such as safety network failure, safety control card failure, and safety operation screen failure.
- It is necessary to design an alarm using the self-diagnosis function of the safety grade control platform (Network fail, Watch Dog, self-diagnosis function).

3. Conclusions

Most domestic NPPs have adopted Digital I&C technology because of its reliability, high –functionality and flexibility characteristics. The potential for common cause failure (CCF) in digital safety systems should be considered importantly whether the systems are to be used in new plants or for upgrades in existing plants. In the CCF situation, it is difficult for the main control room operator to immediately recognize the CCF accident. The rapid recognition and follow-up action of the operator in the CCF situation are the most important factor for maintaining the safety status of the plant. Therefore, it is necessary to design improvements for MCR operators to quickly recognize the occurrence of CCF.

REFERENCES

[1] NRC, BTP-7-19, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer based Instrumentation and Control Systems., 2010.

[2] NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection System.

[3] EPRI TR 3002002990, Digital Common-Cause Failure Susceptibility, 2014.

[4] Reg. 1.97, Criteria for accident monitoring instrumentation for nuclear power plants.

[5] Safety Requirements Memorandum, "SECY-93-087: Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs, July 1993

[6] IEEE 603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations, 2009