The Diagnosis and Monitoring System of Common Cause Failure(CCF) for Digital I&C(DI&C) Systems

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

The problem of Common-Cause Failure(CCF) for Digital I&C(DI&C) systems in nuclear power plant is emerging as a continuous regulatory issue in the licensing of new power plants and the digital upgrade of existing power plants. CCF means that a potential defect in a digital system, including software, will fail simultaneously on more than one device or system. In general, safety-related DI&C in nuclear power plants require the CCF analysis evaluation and coping designs for the systems. To address potential problems with the fundamental CCF of safety related digital facilities, a design is adopted to ensure plant safety shutdowns as non-safety-related equipment and systems. In reality, there is no means of operators of main control rooms to monitor and recognize the occurrence of CCFs on safety-related digital equipment. This paper proposes a CCF diagnosis and monitoring system for DI&C systems.

2. The CCF Diagnosis and Monitoring System

In general, nuclear power plants are equipped with defense-in-depth design concepts that apply more than one line of defense to achieve safety functional goals. Inherent defects in digital systems can be activated at some point, causing equipment failures that can adversely affect the entire system when sharing incorrect information. The plant protection system(safety equipment) and diverse protection system(non-safety equipment) are designed and applied to ensure the safety shutdown for nuclear power plants. The diverse protection system is designed to safety shutdown a reactor when a plant safety-related facility becomes disabled by a common cause failure(CCF).

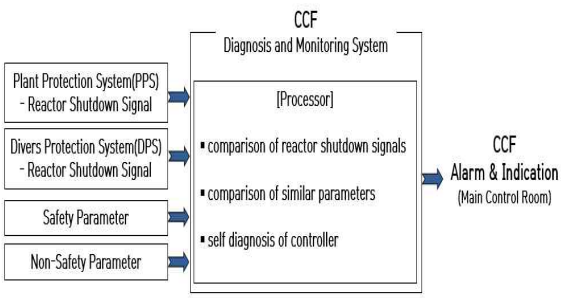

Fig. 1. The concept diagram for CCF diagnosis and monitoring system.

As shown in Figure 1. The CCF diagnosis and monitoring system determines whether a CCF has occurred by comparing the reactor shutdown signals from safety and non-safety equipment. In addition, it is possible to use the characteristic change of the indication when the safety and non-safety sensor signal of the same function is transmitted to another path and the controller's own self-diagnosis function.

2.1 The Comparison of Reactor Shutdown Signal

There are 14 field signals related to reactor shutdowns in nuclear power plants. The plant protection system generates a reactor shutdown signal if the safety-related parameters received from the field sensor exceed the set point. In order to ensure power plant safety, the diversity protection system receives the same signal and generates a reactor shutdown signal. Considering this, it can be concluded that a CCF has occurred when no reactor shutdown signal is generated in the plant protection system (safety equipment) and reactor shutdown in the diversity protection system (non-safety equipment) occurs. There are 14 signals related to reactor shutdown, including the high pressure of the reactor building, which are used as input variables for diagnosing CCF occurrence. Figure 2 shows the CCF diagnosis by comparing reactor shutdown signals transmitted from safety and non-safety systems.

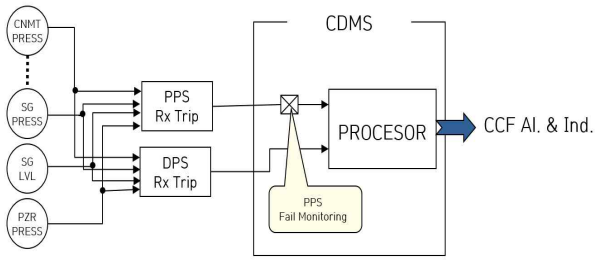

Fig. 2. The comparison of Rx Trip signal

2.2 Comparison of safety system variables with the same non-safety system variables

By monitoring the differences in process values for the same purpose of safety and non-safety equipment, CCF diagnostics and alarm signals of safety-related instrumentation and control equipment can be provided.

When CCF occurs in nuclear power safety system, the variable of safety system path is changed to abnormal state, signal stop or transient state. Nevertheless, the variables in the unsafe system path are healthy. Therefore, CCF diagnosis is possible when comparing each variable. For such variable state monitoring, it is advantageous to monitor the state of analog variables rather than digital variables. However, it is necessary to consider in advance that even the same variable signals have different response characteristics to the path.

2.3 Using the Self-Diagnosis Function of Control Equipment

Operator recognition for CCF (Safety System) can be diagnosed using the watch dog timer function of the controller itself. When failure occurs in more than two channel of the plant protection system at the same time, the reactor stop signal is automatically generated by the self-diagnosis function of the controller. In this situation, if no reactor automatic shutdown occurs, the operator of the main control room should preferentially perform a manual shutdown of the plant. In case of common cause of safety system failure, the priority of manual operation of the equipment of the field operator is the order of the field manual switch, the field interface module, and the breaker.

3. Conclusions

Most domestic NPPs have adopted Digital I&C technology because of its reliability, high-functionality and flexibility characteristics. In the CCF situation, it is difficult for the main control room operator to recognize immediately the CCF accident. Therefore, it is necessary to develop the cognitive system for MCR operators to quickly recognize the occurrence of CCF.

The CCF diagnosis and monitoring system is installed separately from the existing safety and non-safety facilities. For CCF diagnostics and monitoring, comparison of reactor shutdown signals in safety and non-safety facilities, comparison of similar safety and non-safety variables, and self-diagnosis information on the controller itself can be used. The CCF diagnostic monitoring facility is a non-safety facility and provides an alarm for the operator of the main control room to immediately recognize that a CCF has occurred. This system can secure the reliability of CCF diagnosis results by using signals from existing facilities.

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.