Study on CCF Detection Methods for Digital I&C

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

1. Introduction

The potential for common cause failure (CCF) in Nuclear power Plants (NPPs) has become an important issue. Digital Instrumentation and Control (DI&C) systems has been increased and applied consistently in NPPs due to the design change of old-age facility and technical development. 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. APR1400 I&C system features an advanced control room and digital control systems. This I&C system architecture of APR1400 consists of independent and diverse platforms such as Distributes Control System (DCS) platform, Qualified Programmable Logic Controller (PLC) platform. This diversity is important to address the CCF concern of DI&C systems. However, it is difficult for operators to quickly recognize the situation of CCF in DI&C systems. This paper presents methods for the operator to detect the situation of CCF occurrence in APR1400 DI&C systems.

2. Diverse Designs against CCF

In this section introduces the design concepts of used diversity and detection to defense against the CCFs induced from using a common platform for the ARR1400 DI&C systems.

2.1 Application of Diversity Principle

Diversity principle is applied to APR1400 DI&C systems to accomplish safety functions in the event of CCFs in safety systems. Diversity shall be used to achieve the reliability requirements and to fulfill the Defense in Depth concept. The APR1400 DI&C systems consist of two major platforms.

The qualified PLC platform is applied to the most important safety systems. The qualified PLC platform is composed of a set of commercial-grade hardware and previously developed software for use in NPPs as following systems.

- Plant Protection system(PPS)
- Core Protection Calculator System(CPCS)
- Engineered Safety Feature-Component Control System(ESF-CCS)

Distributed Control System (DCS) platform supports operator interface (MMI) functions for NSSS, BOP, and other miscellaneous monitoring and control systems. The DCS supports non-safety control and data processing functions that are used for plant normal operation. Following systems are implemented by DCS platform.

- Process-Component Control system(P-CCS)
- NSSS Process Control System(NPCS)
- Information Processing System(IPS)

DCS operator consoles also provide computerized procedures, which are implemented as a part of DCS, to support the MCR operator in performing emergency operating procedures and the normal operating procedures.

For defense against the CCF induced from using qualified safety platform, following diverse design features are in incorporated into APR 1400 DI&C systems.

Table I: Diversity I&C systems of APR1400

Systems	Platform	Main Function
DPS	DCS	Backup of reactor protection (Automatic)
DIS	DCS	Backup of accident management functions
DMA Switch	Analog Circuit	Backup of reactor protection (Manual)

2.2 Equipment diversity

The equipment diversity is provided between the Protection systems and diverse systems. The PPS is a digital based system using qualified PLCs. To achieve the safety function in case of unintentional PPS malfunction is provided hard-wired reactor trip switches. These switches are connected directly to the reactor trip switchgears that do not involve any digital communications or processing.

The ESF-CCS is using PLCs and hardwired diverse ESF manual actuation switches are provided in the MCR. These switches also connected to the Component Interface Module (CIM) directly and bypass all multiplexing and all computer processors with large software application.

The Diverse Protection System (DPS) is a diversity system form of protection systems. This system is available as a mean to cope with postulated failures that disable the PPS and ESF-CCS.

2.3 Plant Monitoring

Signals of plant condition may be transmitted from the reactor trip and the ESF-CCS to other display systems for plant monitoring purposes provided. The postulated CCF and its effects don't affect any related aspect of the manual action, providing information displayed that is necessary for operator action. The APR1400 control systems consist of non-safety equipment that is used in the normal operation. Some signals are transmitted from the safety system to non-safety system. Electrical and logical isolation ensures that failure of a monitoring or display system will not affect the safety functions. The data communication systems are composed of qualified PLC communication network and DCS communication network. The qualified PLC communication network is independent and diverse from the DCS network. The qualified PLC communication network of intra-channel provides the data communication path among the qualified PLCs, Control Panel Multiplexers (CPM), and gateways within a single safety channel. The inter-channel safety related communication network provides data communications among the safety channels and Qualified Indication & Alarm System – N (QIAS-N) displays. In case of failure of safety related system with CCF, it can be monitored through self-diagnosis function as shown in Fig.1.

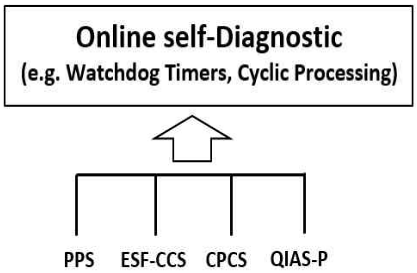

Fig. 1. CCF Detection Methods of Safety Systems.

3. Conclusions

Generally, diversity I&C systems can provide effective protection against CCF for digital protection system. Diversity in redundant I&C divisions may help prevent CCFs, and diverse backup system can be used to mitigate a failure or CCF after it occurs. Diversity is not the only means of protection against digital CCF. It is even more important for the operator to recognize and respond to this situation. Therefore, it is necessary to improve the design to recognize the CCF situations by using the online self-diagnostic function of the digital system.

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: Polity, 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.