A Common Cause Failure Diagnostic Method for APR1400

Jaewoong Cho*, Hyeongsoon Yim, Hyunjeong Kim, Kihoon Jung
KEPCO E&C Company Inc., 989-111 Daedeokdaero, Yuseong-gu, Daejeon, 34057, Republic of Korea
**Corresponding author : jaewoong@kepco-enc.com*

1. Introduction

During Integrated System Validation (ISV) on APR1400, some cases were identified where it was difficult for operators to take manual action within an appropriate time during the Design Basis Event (DBE) concurrent with Common Cause Failure (CCF). To complement the situation, the CCF Diagnostic and Monitoring System (CDMS) design to provide the alarms for the operators is discussed and set off.[1]

In this article, a CCF diagnostic method of safety-related Instrumentation and Control (I&C) system using the CDMS is proposed for operators to take manual action within an appropriate time under the CCF situation.

2. The CCF Diagnostic Method using CDMS

In this chapter, the explanation of the alarms and logics to detect CCF of safety-related I&C system provided by the CDMS are described.

2.1. Trip Check Alarm

Trip Check Alarm is provided to operator in case that the reactor trip is not occurred by the Plant Protection System (PPS) when a situation should have occurred the reactor trip. To provide the alarm, CDMS uses the trip status information from Diverse Protection System (DPS) and PPS, and Virtual Reactor Trip (VRT) function performed by the CDMS.

The CDMS decides the VRT status of the following trip functions : Low Reactor Coolant Flow (LRCF), High Steam Generator Level (HSGL), Variable Overpower Trip (VOPT) and High Logarithmic Power (HLOGP).

To generate VRT signal, the process values are sent from APC-S to CDMS Controller CH.1 and CH.2, and CDMS Controller CH.1 and CH.2 generate VRT signal by using bistable logic and 2-out-of-2 (2oo2) coincidence logic. The generated VRT signals are sent to CDMS Server, and CDMS Server generates the Trip Check Alarm by using the VRT signals from the CDMS Controllers CH.1 and CH.2, 2oo2 coincidence logic, PPS trip status and DPS trip status. The generated Trip Check Alarm is sent to MTP through the CDMS internal network and to IPS through the DCN-I. The following table shows the conditions to generate the Trip Check Alarm by the reactor trip functions.

Table 1. The conditions to generate the Trip Check Alarm by the reactor trip functions.

Reactor Trip Function	Conditions
High Pressurizer Pressure	DPS trip + PPS non-trip
Low Pressurizer Pressure	DPS trip + PPS non-trip
Low Steam Generator Level	DPS trip + PPS non-trip
High Steam Generator Level	CDMS VRT(2/2) + PPS non-trip
Low Steam Generator Pressure	DPS trip + PPS non-trip
High Containment Pressure	DPS trip + PPS non-trip
Variable Overpower	CDMS VRT(2/2) + PPS non-trip
High Logarithm Power Level	CDMS VRT(2/2) + PPS non-trip
Low Reactor Coolant Flow	CDMS VRT(2/2) + PPS non-trip

2.2 Multichannel Trouble / As-is CCF Alarm

In the CDMS Server, Safety Platform Diagnosis (SPD) and Process Value Variation Monitoring (PVM) functions are used to detect Multichannel Trouble and As-is CCF.

The SPD function monitors the safety platform (PPS, ESF-CCS and RCOPS) diagnostic information from IPS, and generates SPD Multichannel Trouble Alarm when the SPD detected failure in two (2) or more channels in a single safety platform. When the SPD detected failure in three (3) or more channels in a single safety platform, the SPD As-is CCF Alarm is generated. When the SPD detect failure of the safety platform, the following examples can be used : PPS BP/CP CPU Error and BP SDL Error. The Figure 1 shows the example of SPD PPS BP CCF detection logic.

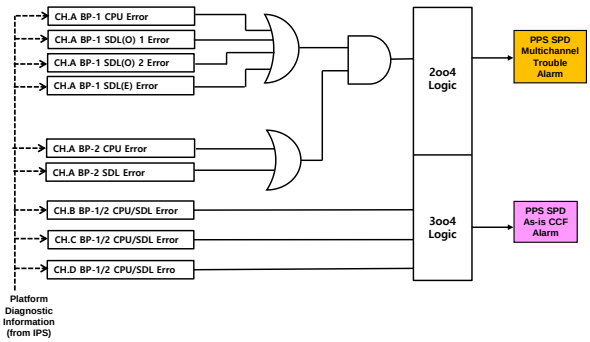

Figure 1. An example of SPD PPS BP CCF detection logic.

The PVM function monitors variability of the process variable values related PPS and RCOPS from IPS. Maximum, Average and Minimum values are calculated

from the acquired process value samples, and the PVM function decides the failure when the variability of the process variable value is smaller than the PVM setpoint. In case that the failures are found at two (2) or more channels, the PVM multichannel Trouble Alarm is occurred, and in case that the failure are found at three (3) or more channels, the PVM As-is CCF Alarm is occurred. Figure 2 shows a block diagram for PVM CCF diagnostic procedure.

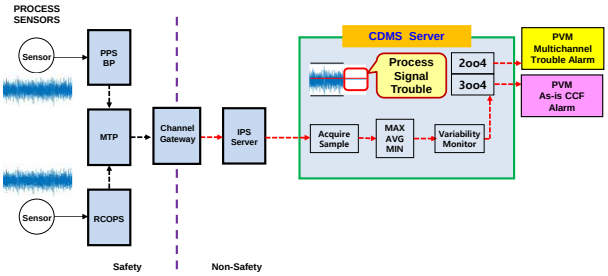

Figure 2. Block Diagram for PVM CCF Diagnostic Procedure

When the SPD Multichannel Alarm or PVM Multichannel Alarm are occurred, CDMS Server generates Multichannel Trouble Alarm, and sends the alarm to MTP through the CDMS internal network and to IPS through the DCN-I network. Also, when the SPD As-is CCF Alarm or PVM As-is CCF Alarm are occurred, CDMS Server generates As-is CCF Alarm, and sends the alarm to MTP through the CDMS internal network and to IPS through the DCN-I network.

2.3 CCF concurrent with DBE

The CDMS Server generates the CCF concurrent with DBE alarm when the Trip Check Alarm and As-is CCF Alarm are occurred at the same time. The generated CCF concurrent with DBE alarm is provided to MTP through the CDMS internal network and to IPS through the DCN-I network.

2.4 Identified DBE Category

When the DBE is occurred under CCF situation, the CDMS Server identifies the DBE, and provides to operator. The following DBE information that addressed in SAR 7A are identified and provided.

- Increase Feedwater Flow
- Loss of Feedwater
- Low Reactor Coolant Flow
- Control Element Assembly Ejection
- Steam Generator Tube Rupture
- Loss of Coolant Accident
- Steam Line Break (Inside)
- Steam Line Break (Outside)

The CDMS Server performs DBE category identification based on following signals from IPS.

- LRCF VRT status
- HSGL VRT status
- VOPT VRT status
- DPS HPP trip status
- DPS LPP trip status
- DPS LSGL trip status
- DPS LSGP trip status
- DPS HCP trip status

Identified DBE category is provided to MTP through the CDMS internal network and to IPS through the DCN-I network.

Figure 3 is a CDMS Block Diagram that shows the procedures to generates the CDMS Alarms that are mentioned in the section 2.1 through 2.4.

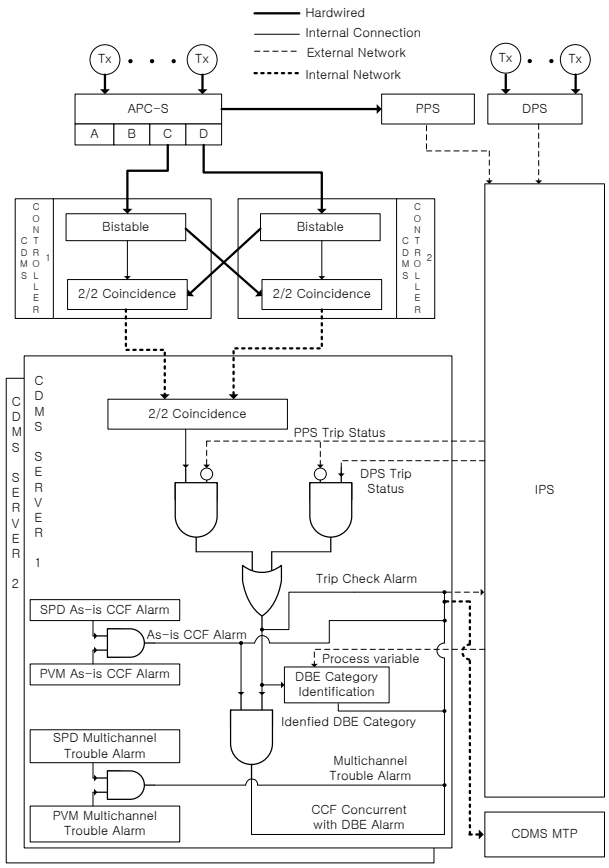

Figure 3. CDMS Block Diagram

3. CDMS Hardware Configuration and Safety Class

The hardware configuration and safety class of CDMS is described in this chapter.

3.1 Hardware Configuration

CDMS is consist of the following components.

- One (1) cabinet
- Two (2) CDMS Controller (CH.1 and CH.2)
- Two (2) redundant CDMS Server
- One (1) MTP (PC, FPD, Keyboard and Mouse)
- Two (2) redundant Power Supply

3.2 Safety Class

The safety class of CDMS is Non-Safety, and Quality Class is 'A'.

4. Conclusion

The method using CDMS for CCF detection of safety-related I&C system is proposed. At the situation of CCF, the CDMS provides the following alarms to operators for appropriate actions in time.

- Trip Check Alarm
- Multichannel Trouble Alarm / As-is CCF Alarm
- CCF concurrent DBE
- Identified DBE Category

REFERENCES

[1] Yim Hyeongsoon, Jung Kihoon, Lee Yoonhee, Hong Hyeongpyo and Yun Jaehee, Planned Design for Common Cause Failure Diagnostic and Monitoring (CDMS), The Symposium for NUPIC 2019, November 2019.