Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 25-26, 2012

Design Improvements of Diverse Protection System Regarding CCF and D3 Issues

Yang Gyun Oh [a], Jin Kwon Jeong [a], Hyeong Soon Yim [a], Sang Jeong Lee [b]
[a] KECO E&C, Inc., 1045 Daedeok-Daero,Yuseong-gu, Daejeon, 305-353, Korea, ygoh@kepco-enc.com
[b] Chungnam National University, 99 Daehak-ro, Yuseong-gu, Daejeon 305-764, Korea

1. Introduction

The Diverse Protection System (DPS) provides a diverse method to trip the reactor to satisfy the requirements related with Anticipated Transients Without Scram (ATWS) with a concurrence of the Common Cause Failures (CCF) in the safety I&C systems. All of the Optimized Power Reactor 1000 (OPR1000) and the APR1400 nuclear power plants have been designed with the DPS, which has the diverse reactor trip function and the initiation of diverse Auxiliary Feedwater Actuation Signals (AFAS) for the Engineered Safety Feature – Component Control System (ESF-CCS) components. For the mitigation of ATWS caused by the CCF within the PPS and ESF-CCS, and to overcome the diversity and defense-in-depth (D3) issues, various design changes have been made for new nuclear units to be built in Korea and abroad.

This paper briefly describes recent design improvements and possible design changes of the DPS regarding the CCF and D3 issues.

2. Design Improvements

2.1 Addition of Diverse SIAS Function

I&C system vulnerability to the CCF affecting the response to a Large-Break Loss-Of-Coolant-Accident (LBLOCA) had been accepted in the past. This acceptance is based upon the provision of primary and secondary coolant system leak detection, and pre-defined operating procedures that together enable operators to detect small leaks and then to take corrective actions before a large break occurs [1]. But the recent regulation regarding the response to the LBLOCA has been changed to exclude I&C system vulnerability to the CCF [2]. Furthermore, the wide applications of digital I&C systems in nuclear power plants have raised the concerns of various CCFs in the PPS and ESF-CCS. Therefore, an additional DPS function of Safety Injection Actuation Signal (SIAS) initiation has been introduced to new nuclear units (including APR^+ and SKN 5&6) to mitigate the CCF effects within the PPS and ESF-CCS during an LBLOCA event.

As the LBLOCA occurs, the RCS inventory flows out through the break. The discharge of RCS inventory rapidly reduces the RCS pressure. Because of the passive safety features, the RCS pressure drop triggers the coolant injection from the Safety Injection Tank (SIT) as depicted in Figure 1.

During the SIT coolant injection, the reactor core water inventory can be maintained without any fuel damage. Since the SIT inventory is limited, the SIT injection is soon terminated, and the RCS inventory decreases again, and fuel rods are also susceptible to being exposed. After the coolant depletion in the SIT, the reactor coolant leaks through the break, and the reactor water level is lowered. Therefore, the reactor fuel can be damaged after 5 minutes from the initiation of LBLOCA, because the fuel rod temperature rises as illustrated in Figure 2 if the plant has no other automatic function of coolant injection.

Per the regulatory position, the manual actuation within 30 minutes after an accident cannot be credited in the CCF evaluation. Therefore, the DPS - SIAS function needs to be implemented. With the DPS - SIAS actuation of safety injection within 5 minutes after the LBLOCA initiation, as illustrated in Figure 1 with red color, the reactor water level can be recovered, and the increase in fuel cladding temperature can be limited as illustrated in Figure 3 [4].

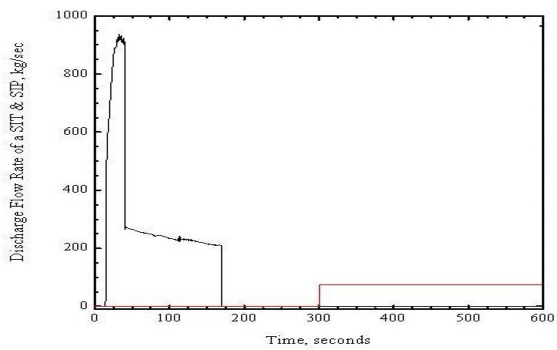

Fig. 1. SIT Discharge Flow after LBLOCA, and SI Flow by DPS-SIAS initiation after 5 minutes

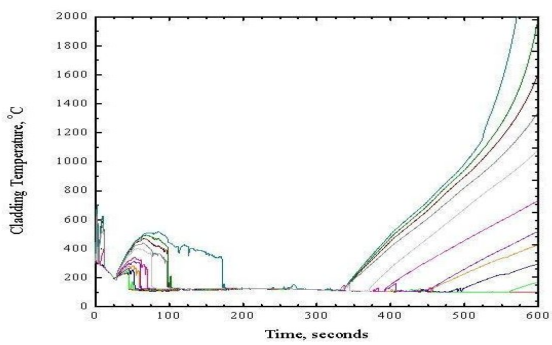

Fig. 2. Fuel Cladding Temperature after LBLOCA without the SIAS function of DPS

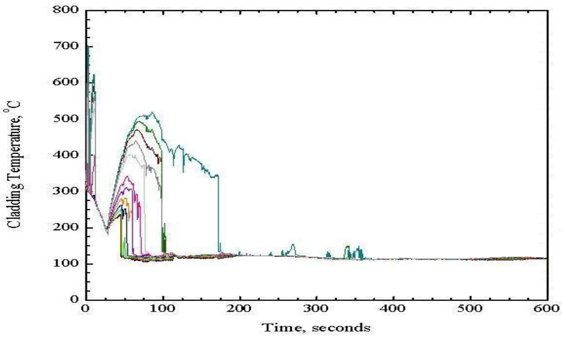

Fig. 3. Fuel Cladding Temperature after LBLOCA with the SIAS function of DPS

2.2 Application of Diverse Platform

Current DPS platform for APR1400 is the Distributed Control System (DCS) type, which is a diverse platform compared with the Programmable Logic Controller (PLC) type of safety I&C systems.

KEPCO Engineering & Construction Company, Inc. (KEPCO E&C) has developed an experimental prototype PPS [3] with a FPGA-based Logic Controllers (FLC). KEPCO E&C is now participating in a DPS improvement project for eight (8) operating nuclear power units in Korea for the purpose of DPS replacement using the FLC platforms by the end of March, 2015. In addition, recently developed APRs have Diverse Actuation Systems (DAS), which utilize the platform other than the DCS (i.e., conventional analog system for US-APWR, FLC for AP1000, non-microprocessor-based equipment for US-EPR).

Considering domestic DPS development and abroad DAS development situations, the DPS platform change from the DCS to the FLC is recommended regarding the Diversity and Defense-in-Depth (D3) issues.

2.3 DPS Data Communication and MMI

Current DPS data communication and MMI for APR1400 greatly depends on the Data Communication Network – Information (DCN-I) and the Operator Station of Information Processing System (IPS).

For the DPS for SUN 1&2, the DPS to the DCN-I communication methods are changed from two (2) way to one (1) way communication. Instead of using IPS engineer station, each DPS cabinet for SUN 1&2 has Maintenance and Test Panel (MTP). The DPS controllers communicate with the MTP in controlled two (2) way communication methods using an additional security device. The MTP can perform its various test and setpoint control functions only with the security device (i.e., a keylock), and it can only perform the monitoring function without the security device.

The DPS soft controls used in SKN 3&4 IPS operator stations has been replaced with the conventional switches for the DPS for SUN1&2.

For the minimization of CCF possibility, the DPS communication to other systems needs to be done through hard-wires or one-way type data links. Regarding the D3 issues, DPS Operator Module (DPS-OM) needs to be installed on the safety console for the MMI of the DPS.

2.4 DPS Channel Configuration

All OPR1000 and APR1400 units currently have the DPS with two (2) channels. Using the two-out-of-two (2/2) coincidence logic, the DPS can prevent any spurious reactor trip or spurious AFAS initiations. However, two channel DPS with a 2/2 coincidence logic can’t be fault tolerant, because it does not have any redundant channels. Current DPS for OPR1000 and APR1400 can’t perform its functions during the bypass of one channel for self-test or maintenances.

Considering domestic DPS situations and abroad DAS developments (i.e., four channel DAS in US-APWR and US-EPR), the channel configuration of the DPS needs to be changed from two channels with 2/2 coincidence logic to four channels with 2/4 coincidence logic for fault tolerance and reliability enhancements.

2.5 Coping with the CCF Coupling

The DPS functions should be maintained during the CCF events of PPS and ESF-CCS. Furthermore, the DPS functions should not be damaged by the CCF coupling from the plant events of fire and flood events, and power-source failures. Therefore, each DPS channel equipment needs to be located in a separate I&C equipment room. Besides, at least two separate power sources should be supplied to the DPS such that power sources for at least two DPS channels can be maintained.

3. Conclusion

As discussed above, various design improvements needs to be considered for future DPS developments. This paper presents KEPCO E&C’s design approaches for the DPS development. KEPCO E&C believes that the DPS will become more reliable and fault-tolerant system with the design changes described in this paper.

REFERENCES

[1] USNRC, NUREG-0800, BTP HICB-19 (Rev. 4), “Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-based Instrumentation and Control Systems”, June 1997

[2] USNRC, NUREG-0800, BTP 7-19 (Rev. 5), “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-based Instrumentation and Control Systems”, March 2007.

[3] Yoon-Hee Lee, Jae-Hong Ha, and Hang-Bae Kim, “FPGA-Based Plant Protection System”, ICI2011, Daejeon, Korea, August 21~25, 2011.

[4] Yang Gyun Oh, at al., “Reliability Enhancement of APR^+ Diverse Protection System regarding Common Cause Failures”, ICAAP ‘12, Chicago, USA, June 24~28, 2012.