RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

Korea Electric Power Corporation / Korea Hydro & Nuclear Power Co., LTD

Docket No. 52-046

RAI No.:	**342-8291**
SRP Section:	**07.08 – Diverse Instrumentation and Control Systems**
Application Section:	**07.08**
Date of RAI Issue:	**12/18/2015**

Question No. 07.08-7

Clarify how the applicant knows when a software CCF has occurred within the safety system, including the Plant Protection System (PPS) and Engineered Safety Features – Component Control System (ESF-CCS).

10 CFR Part 50, Appendix A, GDC 22, “Protection system independence,” states, “The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.”

Item II.Q of the SRM to SECY-93-087, Position 3, states, “If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.”

NRC NUREG-800, Section 7.8, “Review Procedures,” states in part, “Information should be available in the control room to indicate the operation of the diverse I&C systems. This aspect of the review may involve considerations included in emergency operating procedures.”

Response

There are no CCF-specific alarms or indications. If a postulated software CCF occurs concurrently with a DBE, the DPS is automatically actuated and the trip alarms and indications

are displayed on the DPS operator module (DPS-OM) mounted on the MCR safety console, enabling the operator to be aware of the safety system CCF.

Operators in the MCR can acknowledge the occurrence of a postulated software CCF based on the occurrence of any combination of the following DPS reactor trip, auxiliary feedwater actuation signal (AFAS), and Safety Injection Actuation Signal (SIAS) trip alarm(s):

- DPS Pressurizer High Pressure Reactor Trip
- DPS Containment High Pressure Reactor Trip
- DPS Steam Generator No. 1 Low Level AFAS Trip
- DPS Steam Generator No. 2 Low Level AFAS Trip
- DPS Pressurizer Low Pressure SIAS Trip

One of the DPS design purposes is to mitigate the consequences of a DBE concurrent with a postulated software CCF of the safety I&C systems, including the PPS and ESF-CCS. The trip setpoints of the DPS are deliberately determined with more severe values compared with those of the PPS. During a postulated software CCF event, the PPS does not provide any expected protective actuations (i.e., a trip initiation of RPS or ESFAS function). In this case, the DPS provides the protective actuation (i.e., diverse reactor trip, AFAS or SIAS initiation) when required, because the DPS has system diversity compared with the safety I&C systems.

Section 4.2.3 of APR1400-Z-J-NR-14002-P, “Diversity and Defense in Depth”, will be revised to include the following:

“If a postulated software CCF occurs concurrently with a DBE, the DPS is automatically actuated and the trip alarms and indications are displayed on the DPS operator module (DPS-OM) mounted on the MCR safety console, enabling the operator to be aware of the safety system CCF.”

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

Section 4.2.3 of D3 TeR, APR1400-Z-J-NR-14002, will be revised as indicated in the attachment associated with this response.

4.2.3 Diverse Actuation System

The DAS performs diverse automatic protection functions, diverse manual ESF actuations, and diverse indication functions. The DAS is designed to meet the following regulatory requirements:

a. ATWS mitigation according to 10 CFR 50.62

b. Points 3 and 4 of the NRC position on D3 in BTP 7-19

The DPS includes diverse automatic trip and actuation functions that are (a) required for ATWS mitigation and (b) for mitigation of DBEs concurrent with a postulated CCF in the safety I&C systems.

The DMA switches are provided to permit the operator to actuate ESF systems from the MCR after a postulated CCF in the safety I&C systems. To achieve the ESF actuation independently and diversely from the ESF-CCS, the DMA switches are hardwired to the CIM through the isolators for remote manual actuation of the ESF systems.

The DMA switches bypass all PPS digital platform software including CPMs, gateways and the ESF-CCS controllers in order to perform the ESF actuation logic. The DMA switches are connected to fan-out devices in the MCR safety console to distribute the ESF actuation signals to individual component controls.

Two types of manual reactor trip controls are provided. Manual reactor trip switches are hardwired to the RTSS as required by IEEE Std 603-1991. In addition, manual reactor trip controls are also provided through the DPS operator module (DPS-OM) with soft controls.

The DIS displays the information required for operators to place and maintain the plant in a safe shutdown condition following a DBE concurrent with a postulated CCF in the safety I&C systems. The DIS receives field input signals through signal splitters/isolators before they are hardwired to the applicable processors of safety I&C systems. The DIS satisfies the diverse indication guidance provided in the Point 4 position of BTP 7-19. It consists of one channel of non-safety-related equipment. The DIS display device is located on the MCR safety console.

In addition, all process variables input to the safety I&C systems are not affected by the software CCF, and the information derived from those variables are available from the IPS.

If a postulated software CCF occurs concurrently with a DBE, the DPS is automatically actuated and the trip alarms and indications are displayed on the DPS operator module (DPS-OM) mounted on the MCR safety console, enabling the operator to be aware of the safety system CCF.