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.:	**348-8279**
SRP Section:	**07.09 - Data Communication Systems**
Application Section:	**07.09**
Date of RAI Issue:	**12/24/2015**

Question No. 07.09-17

Discuss if there are operational limits for message transfer.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. Clause 5.5 of IEEE Std. 603-1991 requires safety systems be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. In addition, Clause 4.10 of IEEE Std. 603-1991 requires, as a part of the design basis, identification of the critical points in time or the plant conditions, after the onset of a design basis event. To meet IEEE Std. 603-1991, Clause 5.5 and Clause 4.10, data communications systems in support of the protection system should demonstrate real-time performance in accordance with SRP Branch Technical Position (BTP) 7-21, "Guidance on Digital Computer Real-Time Performance."

Section 4.6.1.3 of Technical Report APR1400-Z-J-NR-14001-P discusses real-time, deterministic behavior of the SDL and SDN data communication networks and states message transfer is non-deterministic. Since message transfer is not performed cyclically, but only when one or more of the attached communication interfaces have data to send, the staff requests the applicant to discuss if there are operational limits for message transfer and how message transfer would not impact any safety functions.

Response

Subsection 4.6.1.3 of technical report APR1400-Z-J-NR-14001-P states that there are two modes of SDN data transmission. One mode is the process data transfer mode, which is deterministic, and the other is the message transfer mode, which is non-deterministic. Because of the non-deterministic nature of the message transfer mode of the SDN, the message transfer mode of the SDN will not be used in the APR1400 safety systems. This feature will be blocked in the implementation phase of the safety software.

To provide clarity, the statement in Section 4.6.1.3 of Safety I&C System technical report, APR1400-Z-J-NR-14001-P, will be modified to state the message transfer mode of the SDN will not be used in the APR1400 safety systems, as indicated in the attachment associated with this response.

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

The Safety I&C System technical report, APR1400-Z-J-NR-14001, will be revised, as indicated in the attachment associated with this response.

There is no difference in data transfer rate, data bandwidth, data accuracy and error performance during normal and abnormal operations (i.e., whether the nuclear power plant is in a steady state or undergoing a transient or accident condition).

The SDN has a deterministic network protocol that is used for non-node communication within a division. The controllers of PPS and ESF-CCS and FPDs will be nodes on the SDN.

There are two modes of data transmission of the SDN:

- Process data transfer - deterministic
- Message transfer - non-deterministic

Process data transfer is the mode of communications between the nodes in the same division. It is also the mode in which the FPDs receive data from the SDN network.

Message transfer is ~~received for on-demand data that is initiated from the FPDs.~~ not used in the safety systems.

Details for deterministic communication are described in Reference 12.

4.6.1.4 Reliability

Error checking techniques for data integrity such as CRC are incorporated into the communication protocol to assure the integrity of the transmitted data.

Upon detection of the communication loss within a safety system, the system is designed such that communication failures shall not prevent safety systems from performing their intended safety function as analyzed in Appendix C.

Refer to Appendix C and Section 5.6 of Reference 12 for a detailed description on the SDL compliance to the criteria in DI&C-ISG-04 Section 1.

4.6.1.5 Control of Access

Security provisions are provided for the data communication system associated with the system to which it is connected such as key locked door and protection against unauthorized software alteration.

4.6.1.6 Single Failure Criterion

The configuration of the data communication system is designed so that the requirements of the SFC are satisfied. The FMEA shows that no single failure will defeat more than one of the four redundant safety I&C system divisions as applicable.

The FMEA for the safety I&C system in the DCD Chapter 7 describes and provides a detailed evaluation; including network cable and equipment failures, failure to transmit and receive data or transmission of erroneous data. The data communication system is designed with redundancy and multiple data paths, if necessary.

4.6.1.7 Independence

The data communication system is designed to maintain the independence between the safety divisions (A, B, C, D), and the independence between the safety and non-safety systems.

Communication between safety I&C systems is performed via SDL fiber optic cables only.

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.:	**348-8279**
SRP Section:	**07.09 - Data Communication Systems**
Application Section:	**07.09**
Date of RAI Issue:	**12/24/2015**

Question No. 07.09-18

Discuss how the CPP and CEAC/CPP interdivisional communications support or enhance the performance of the safety functions.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, "Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function," and Clause 5.6.3, states, in part, "The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." DI&C-ISG-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

DI&C ISG-04, Section 1, Position 3, states, in part, "A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function." It is not clear to the staff how the CPP and CEAC/CPP interdivisional communication as described in Section C.5.1.3 of Technical Report, APR1400-Z-J-NR-14001-P, meets DI&C ISG-04, Section 1, Position 3. Specifically, how do the described CPCS interdivisional communications support or enhance the performance of the safety functions? The staff requests the applicant to address this portion of DI&C ISG-04 and update the FSAR and/or technical reports accordingly.

Response

To meet the requirements of IEEE Std. 603, Clause 5.6.1, ideally there would be four reed switch position transmitters (RSPTs) measuring each control element assembly (CEA) position independently for each core protection calculator system (CPCS) channel. This would allow each CPCS channel to independently calculate penalty factors (PFs) based on its own unique sensor data. However, due to physical space limitations on the CEA itself and in the reactor head area, including the necessary space for channel physical independence, there are only two RSPTs for each CEA. These are designated as RSPT1 and RSPT2.

Nevertheless, as described in Section C.5.1.3 of technical report, APR1400-Z-J-NR-14001-P, the departure from nucleate boiling ratio (DNBR) and local power density (LPD) calculations are compensated to account for any deviations between the positions of the four CEAs within each subgroup. To detect CEA position deviations within each subgroup, and thereby generate PFs, it is essential that each CPCS channel monitor the positions of all CEAs through interdivisional communication.

CPCS Design to meet Single Failure Criteria (SFC)

To comply with the SFC, the two RSPTs on a CEA are assigned to separate safety channels, and both signals are interfaced to their respective CPCS channels prior to distribution to all CPCS channels via cross-channel serial data link (SDL). Although there are only two RSPT channels per CEA, the 186 RSPTs (two each per 93 CEAs) are distributed among all four CPCS channels.

Within each CPCS channel there are two separate PF calculations, one based on CEA positions only from RSPT1, and the other based on CEA positions only from RSPT2. These PF calculations are performed by CEA Calculator 1 (CEAC1) and CEA Calculator 2 (CEAC2), respectively, within each CPCS channel. The PFs from each of the two CEACs are transmitted to the CPC within the same channel. Each CPC then uses the more conservative of the two PFs in its final DNBR and LPD calculations.

Enhancement of the safety functions

The DNBR and LPD reactor trip functions are credited for anticipated operational occurrences (AOO) and postulated accidents (PA) in the APR1400 safety analysis.

Because of their location around the periphery of the core, excore neutron detectors are most sensitive to the fuel assemblies at the periphery of the core which are typically not the limiting locations relative to protecting fuel safety limits. Radial flux distribution is a function of CEA position. Each CPCS channel corrects the output of its excore detectors for changes in power distribution due to CEA insertion. For example, deeply inserted CEAs in the center of the core force power to the peripheral fuel assemblies, while CEAs inserted at the core periphery have the opposite effect. Without direct CEA position monitoring, uncertainties and assumptions must be factored into the excore detector measurements to relate the indirect measurements to the calculated real conditions in fuel assemblies closer to the center of the core.

The CPCS has 23 CEA subgroups, each consisting of four CEAs symmetrically distributed to the four quadrants of the reactor core (A, B, C or D). The twenty-third subgroup consists of 4 CEAs distributed to the four quadrants of the reactor core and CEA number 1 which is located at the center of the core. All CEAs in each subgroup normally move concurrently to maintain an even radial power distribution. However, in reality CEAs occasionally experience stepping malfunctions that result in deviations between the positions of the CEAs within the same subgroup. These deviations are an important component of the DNBR and LPD calculations because differences in CEA positions within the same subgroup can skew the normally symmetrical power distribution within the core.

Therefore, CEA position monitoring is necessary to achieve accurate DNBR and LPD calculations.

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

There is no impact on any Technical, Topical, or Environmental Report.

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.:	**348-8279**
SRP Section:	**07.09 - Data Communication Systems**
Application Section:	**07.09**
Date of RAI Issue:	**12/24/2015**

Question No. 07.09-19

Discuss failures which have been identified through analysis but cannot be detected through equipment or diagnostics, and how those undetectable failures are addressed.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, "Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function," and Clause 5.6.3, states, in part, "The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." DI&C-ISG-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

Section C.5.1.3.7(2) of Technical Report, APR1400-Z-J-NR-14001-P states conformance to DI&C ISG-04, Section 1, Position 2, and discusses failures modes for Reed Switch Position Transmitter (RSPT) which are detectable by CPCS and through diagnostics. Staff requests applicant to discuss failures that have been identified through analysis but cannot be detected through equipment or diagnostics, and how those undetectable failures are addressed.

Response

Failure modes for reed switch position transmitters (RSPT) which are detectable by the core protection calculator system (CPCS) are described in Section C.5.1.3.7 (2) of the Safety I&C System technical report, APR1400-Z-J-NR-14001-P, and KHNP's response to RAI 50-7911, Question 07.02-8. As described in Section 8.0 of the Safety I&C System technical report, the platform has been dedicated and qualified for nuclear power plants and accepted by the NRC after reviewing "Common Qualified Platform Topical Report", WCAP-16097-P-A, Rev. 3, February, 2013. According to the Common Qualified Platform Topical Report, there are various types of diagnostics and self-testing to continuously monitor the integrity of the system as it performs its safety function. Using these diagnostics and self-testing, failures can be detected by the application software of safety systems. Nevertheless, there may be failures undetected by the diagnostics and self-testing of platform or application software.

Considering the undetectable single failure in one control element assembly calculator (CEAC) side including RSPTs, as described in the Safety I&C System technical report, the other CEACs in all four channels normally calculate the penalty factors (PFs) and send PFs to the core protection calculator (CPC) to generate the departure from nucleate boiling ratio (DNBR) and the local power density (LPD) trips. Finally, the plant protection system (PPS) still remains in 2-out-of-3 coincidence logic.

Furthermore, failures which cannot be detected by self-diagnostic features can be found by the surveillance testing of Surveillance Requirements 3.3.1.7 and 3.3.1.10 of the Technical Specifications. Identifiable by analysis, but undetectable failures that cannot be detected through periodic testing or revealed by alarm or anomalous indication shall be assumed to have occurred. The safety systems in the APR1400 include redundant components and channels to mitigate the effects of a failure, to improve system availability, or to provide the diverse protection system in the case of common mode failure of all safety systems.

To provide the clear analysis, item 2-14a, which was provided in response to RAI 50-7911, Question 07.02-8 will be added in the Table 7.2-7 for un-recognized hardware or software malfunction.

Impact on DCD

DCD, Tier 2, Table 7.2-7 will be revised, as indicated on the markup which was provided in the attachment to KHNP's response to RAI 50-7911, Question 07.02-8.

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

There is no impact on any Technical, Topical, or Environmental Report.