REVISED 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.:	**68-7892**
SRP Section:	**07.07 - Control Systems**
Application Section:	**Section 7.7**
Date of RAI Issue:	**07/10/2015**

Question No. 07.07-4

Provide information on fault detection capabilities of the non-safety I&C, as mentioned in Technical Report APR1400-Z-J-NR-14012-P, Rev.0 "Control System CCF Analysis."

IEEE Std. 603-1991, Clause 5.6.3 states, in part, that the safety system design shall be such that credible failures in, and consequential actions by other systems, as documented in the design basis per Clause 4.8, shall not prevent the safety systems from meeting the requirements of this standard. Section 4.4.2, "Redundacy," of Technical Report, APR1400-Z-J-NR-14012-P, Rev. 0, states, "A comprehensive set of diagnostics aids in fault detection, locating and repairing problems before they lead to more serious operational concerns. Failure of the primary controller would result in fail-over to the standby controller and an alarm. Failure of the standby controller would only result in an alarm as the primary controller is already controlling." This section goes on to further discuss the redundancy between the primary and standby controllers and the fail-over action. However, the section provides no other details to substantiate the claim of a comprehensive set of diagnostics exists or what these diagnostics are. Section 4.4.4.1, "Design Features to Prevent Spurious Control Commands," of APR1400-Z-J-NR-14012-P, Rev. 0, details some data communications error checking features of the DCS controllers but that would not appear to constitute a comprehensive set of fault detection measures in the non-safety I&C systems within the boundaries of this technical report.

1. Provide the full set of the automated fault detection features implemented in the non-safety I&C that are used to support the control system CCF analysis.

2. What types of faults would require a fail-over from primary to standby controllers? Describe the logic that implements the fail-over function between the controllers.

3. How does the design prevent a faulted controller from continuing to send signals onto data communication network-information (DCN-I) network or any other connected network?

4. For failures of either the primary or standby DCS controller, where does the alarm appear for these failures?

Response – (Rev. 1)

TS

TS

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

Subsections 4.4.2 and 4.4.3 of technical report APR1400-Z-J-NR-14012-NP, Rev. 0, “Control System CCF Analysis” will be revised as indicated in the attachment associated with this response.

Due to the continuous operation of most control systems, triggered failures are self-announcing because they cause component repositioning. Therefore, when the defect is announced, it can be corrected in all controllers, before it causes a CCF of multiple controllers.

The detailed requirements of segmentation are described in Section 4.5. Though the segmentation of control functions makes the concurrent failure of those multiple control functions highly unlikely, multiple concurrent failures of more than one control group due to a CCF is considered as a credible failure and is evaluated in Section 5.3 as a beyond design basis event.

4.4.2. Redundancy

The control system is provided with the following redundancies in the platform design:

- Digital processors
- Input/output modules
- Communication networks
- Power supply

This statement is moved into Subsection 4.4.3

Non-safety system cabinets include redundant power supplies with outputs auctioneered to power the digital processors, I/O modules, and other system peripherals. No loss of function occurs when either power supply is turned off or on, with the other supply being powered.

The non-safety system incorporates network communication configurations that have dual or redundant communication paths.

The non-safety system incorporates digital processors in configurations that have redundant processing. A failure that results in shutdown of the primary processor will automatically hand off system functionality to a backup processor. The non-safety system incorporates redundancy with selected inputs or outputs.

There are different approaches available to incorporate this redundancy. Depending on the approach taken, component and instrument segmentation are considered to that extent needed to preserve the desired fault tolerance for safety analysis.

~~A comprehensive set of diagnostics aids in fault detection, locating and repairing problems before they lead to more serious operational concerns. Failure of the primary controller would result in fail-over to the standby controller and an alarm. Failure of the standby controller would only result in an alarm as the primary controller is already controlling.~~

Redundancy enhances system availability due to many component failures. However, redundancy cannot prevent the adverse effects from a failure that results in erroneous or spurious signals.

Therefore, redundancy is not credited in the Failure Type 1, 2, 3 or 4 analyses.

Insert "B" on the next page.

Page intentionally blank

4.4.3. Diagnostic and Alarming Functions

For all applications the non-safety DCS controller is provided in a redundant-pair configuration to provide fault tolerance. The non-safety DCS controller is fully redundant with a backup controller designed to operate in a masterless scheme. Each controller in the redundant pair executes the same application with the primary controlling the outputs while the secondary tracks the primary. Fail-over detection and switching control to the backup process controller is done automatically and smoothly.

The non-safety DCS controller utilizes multiple control areas to support multitasking and preemptive task scheduling. The controller has high-capacity control capability. The functions executed within one controller are typically limited only by the amount of memory or flash disk available, to execute simple or complex modulating and sequential control and by the throughput performance required for the application.

Diagnostic and alarming functions are not credited in the Failure Type 1, 2, 3 or 4 analyses.

Insert "A" on the next page.

4.4.4. Design Features of the Information Flat Panel Display

TS

Page intentionally blank