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.:	**37-7882**
SRP Section:	**07.03 - Engineered Safety Features Systems**
Application Section:	
Date of RAI Issue:	**06/18/2015**

Question No. 07.03-1

Demonstrate how software common cause failure (CCF) is addressed and the quality requirement is met for the component interface modules (CIM) used downstream of both the Engineered Safety Features - Component Control System (ESF-CCS) system and the Diverse Protection System (DPS).

10 CFR 50, Appendix A, General Design Criteria (GDC) 21 states, in part, that the protection system (or safety system) shall be designed for high functional reliability commensurate with the safety functions to be performed. 10 CFR 50.55a(h), “Protection and Safety Systems,” requires compliance with IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” and the correction sheet dated January 30, 1995. Clause 5.3 of IEEE Std. 603-1991 requires, in part, that safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Item II.Q, “Defense Against Common-Mode Failures in Digital Instrument and Control Systems,” of the Staff Requirements Memorandum (SRM) (ML003708056) on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs” contains the NRC regulatory guidance and position on the diversity and defense-in-depth (D3). It says, in part, that 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 as the safety system, shall be required to perform either the same function as the safety system function that is vulnerable to common mode failure or a different function that provides adequate protection. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary functions under the associated event conditions.

Technical Report (TeR) APR1400-E-J-NR-14001-P, Rev. 0, "Component Interface Module," states, in part, that the field programmable gate array (FPGA) portion of the CIM is safety-related for the diagnostic and surveillance features which are used in associated safety functions. As shown in Figure 4.2-1 of the above TeR, several outputs from the FPGA portion of the CIM are sent to the safety-related ESF-CCS Loop Controller. As described in Branch Technical Position 7-19, Rev. 6, the staff considers programmable technology (firmware) to be software. In addition, it appears the FPGA portion of the CIM is potentially involved in safety functions since it sends signals to the safety-related ESF-CCS Loop Controller. Describe how software common cause failure is addressed, and quality requirement met, for the entire CIM including the FPGA. If applicable information is in other portions of the application, provide the necessary references to those sections. Update the final safety analysis report (FSAR) and technical reports accordingly.

Response

TS

Section 4.2 of TeR APR1400-E-J-NR-14001-NP, Rev. 0, “Component Interface Module” will be updated to clarify the inputs and outputs of the diagnosis section.

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 of Technical Report APR1400-E-J-NR-14001-NP, Rev. 0, “Component Interface Module” will be revised as indicated in the attachment associated with this response.

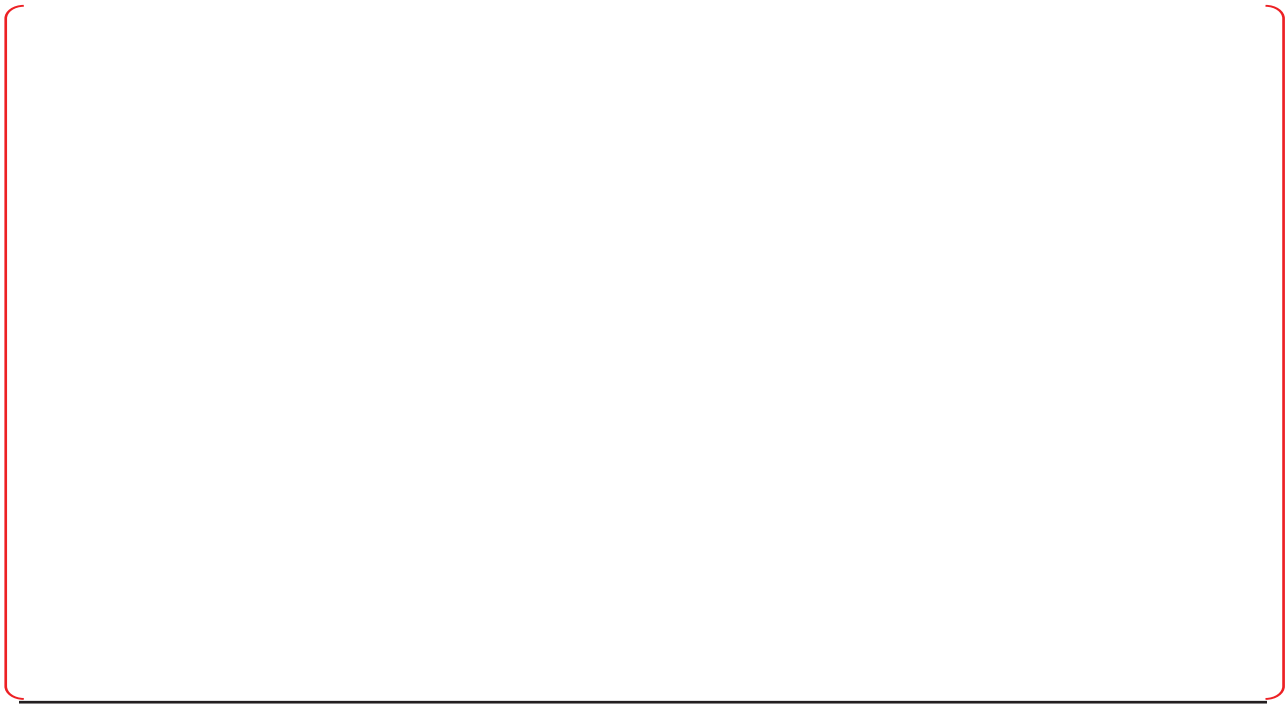
TS

Figure 4.1-1 Block Diagram of the CIM Interface

4.2. CIM Configuration

The overview diagram of the CIM is shown in Figure 4.2-1. As discussed earlier, the CIM consists of the priority logic section, base section, and diagnosis section. The purpose of each section is as follows:

TS



Intentionally blank

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.:	**37-7882**
SRP Section:	**07.03 - Engineered Safety Features Systems**
Application Section:	
Date of RAI Issue:	**06/18/2015**

Question No. 07.03-2

Clarify what functions the FPGA portion of the CIM performs.

Both 10 CFR 50.54(jj) and 10 CFR 50.55(i) require structures, systems, and components subject to the codes and standards in 10 CFR 50.55a to be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. As indicated in Figure 4.2-1 of TeR APR1400-E-J-NR-14001-P, Rev. 0, "Component Interface Module," the FPGA portion of the CIM sends outputs to the safety-related ESF-CCS Loop Controller. However, Section C.5.2.1 of Appendix C in TeR APR1400-Z-J-NR-14001-P, Rev. 0, "Safety I&C System Technical Report," states the diagnosis section only receives signals from the priority logic section and base section of the CIM. Clarify the inconsistent description of the functions of the CIM FPGA portion.

Response

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

Subsection C.5.2.1 of Appendix C in the “Safety I&C System” Technical Report (APR1400-Z-J-NR-14001-NP, Rev. 0), will be revised as indicated in the attachment associated with this response.