REVISED SUPPLEMENTAL 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:

Date of RAI Issue: **12/18/2015**

Question No. 07.08-6

Verify whether the statement made in Technical Report APR1400-Z-J-NR-14002-P, Rev.0, regarding the Component Interface Module (CIM) being fully tested, is true or not.

10 CFR Part 50, Appendix A, General Design Criteria (GDC) 22, requires design techniques such as functional diversity or diversity in component design and principles of operation. Item II.Q of the Staff Requirements Memorandum (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.”

Section 4.2.2, "Available I&C Functions," of Technical Report APR1400-Z-A-NR-14019-P, Rev.0, “CCF [common-cause failure] Coping Analysis,” states, “Command inputs ... are received from three sources to the CIM; two I&C subsystem (ESF-CCS and DPS) commands and DMA switches.” Earlier, the section states, “The CIM is a non-software-based qualified nuclear safety grade module. Therefore the CIM is not subjected to the same CCF with ESFCCS which is implemented by qualified PLC platform.”

Technical Report APR1400-Z-J-NR-14002-P, Rev.0, “Diversity and Defense in Depth,” Appendix A, "Conformance to BTP 7-19," Section 1.9, “Design Attributes to Eliminate Consideration of CCF,” states, “In addition, the sections of the CIM that are relied upon for both the safety systems and the diverse systems are fully tested.” Staff expected to see a similar statement in Technical Report APR1400-E-J-NR-14001-P, Rev. 0, "Component Interface Module," regarding fully testing or 100% testing of CIMs. However, since we did not, please verify whether the statement made in Technical Report APR1400-Z-J-NR-14002-P, Rev.0, regarding the CIM being fully tested is true or not.

Other areas in the application also refer to the CIM being fully tested, so the applicant is requested to ensure consistency throughout the application regarding CIM testing. In addition, if 100 percent testing will be performed on the CIM, describe how it will be 100 percent combinatorial testing as described in BTP 7-19.

Response – (Rev. 1)

The priority logic in the component interface module (CIM) is implemented by complementary metal-oxide-semiconductor (CMOS) (or transistor-transistor logic (TTL)) devices. The CIM is designed as Class 1E, and development is performed under a quality assurance program in accordance with 10 CFR Part 50 Appendix B.

ISG-04 addresses software common-cause failures of a priority module. In the APR1400 design, the priority module of the CIM does not have software and consists of simple TTL logic. Therefore, the requirement for 100% testing is not applicable to the priority module of CIM. The testing that was performed on the priority module of the CIM is described in Section 7 of the CIM technical report. The statement made in Technical Report APR1400-Z-J-NR-14002-NP, Rev. 0, “Diversity and Defense in Depth,” Appendix A, "Conformance to BTP 7-19," Section 1.9, regarding the CIM being fully tested will be deleted as indicated in the attachment. The term “fully tested” in Technical Report APR1400-E-J-NR-14001-NP, Rev. 0, "Component Interface Module," Section 2, third paragraph, will also be deleted as indicated in the attachment.

> The CIM consists of three sections: priority logic section, base section, and diagnosis section. The priority logic section and base section are implemented by hardware device and the design is tested. Therefore, there is no potential for a hardware or software design defect in these sections.

The test cases for the priority logic are considered for external output signals of the priority logic along with all input signal states. To clarify this point the following will be added to Section 5 of APR1400-E-J-NR-14001-NP:

> 5.4 Priority Logic Development Testing
>
> The priority logic section is tested to ensure there are no design defects in the priority logic configuration. The test cases confirm the logic generates the correct Energize/De-energize output states by encompassing all input signal state combinations, together with (1) all Input Select Switch and Mode Select Switch combinations, and (2) the logic states of any internal latches and time delays.
>
> To facilitate this testing all input and switch states are manually or automatically stimulated. The Energize/De-energize output states of the priority logic are manually or automatically compared to manually generated acceptance states. If an automated comparison method is employed, the automated test results are manually verified through sampling the test cases.

Supplemental Response

Deleted

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 2 and 5.4 of the Component Interface Module technical report, APR1400-E-J-NR-14001-NP, Rev. 0, and Section 1.9 of the Diversity and Defense in Depth technical report, APR1400-Z-J-NR-14002-NP, Rev. 0 will be revised, as indicated in the attachment associated with this response.

TS

RAI 342-8291 - Question 07.08-6

Table 5.3-1 Priority Mode Configurations

TS

TS

Figure 5.3-1 Priority Logic Configuration in the CIM for the APR1400

Insert following page

6. FAILURE MODE FEATURES

TS

6.1. Failure Modes and Effects Analysis

The FMEA of the CIM is shown in Table 6.1-1.

5.4 Priority Logic Development Testing

The priority logic section is ~~fully~~ tested to ensure there are no design defects in the priority logic configuration. The test cases confirm the logic generates the correct Energize/De-energize output states by encompassing all input signal state combinations, together with (1) all Input Select Switch and Mode Select Switch combinations, and (2) the logic states of any internal latches and time delays.

To facilitate this testing all input and switch states are manually or automatically stimulated. The Energize/De-energize output states of the priority logic are manually or automatically compared to manually generated acceptance states. If an automated comparison method is employed, the automated test results are manually verified through sampling the test cases.

RAI 342-8291 - Question 07.08-6_Rev.1

Section 1.9 Design Attributes to Eliminate Consideration of CCF

"Many system design and testing attributes, procedures, and practices can contribute to significantly reducing the probability of CCF. However, there are two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF:

Diversity or Testability

(1) Diversity – If sufficient diversity exists in the protection system, then the potential for CCF within channels can be considered to be appropriately addressed without further action.

(2) Testability – A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case ~~(100% tested)~~."

The response to Point 1 position of BTP 7-19 describes the features of the PPS, ESF-CCS and QIAS-P that minimize the potential for a CCF. Despite those features a defect that results in a CCF for all PPS, ESF-CCS and QIAS-P functions is assumed in the CCF coping analysis to address Point 2 position of BTP 7-19. The DPS, DIS and DMA switches provide diverse equipment to cope with the postulated CCF in the safety systems. The DPS and DIS are demonstrated to be diverse from the safety systems, through the diversity analysis provided to address Point 3 position of BTP 7-19.

The only safety components for which a design defect leading to a CCF is not assumed are the following:

a. Sensors
b. APC-S
c. CIM

These components are shared by both the safety systems and the diverse backup systems. To eliminate consideration of a CCF, these components use only conventional analog or binary logic technology (i.e., no software-based processing). In addition, the sections of the CIM that are relied upon for both the safety systems and the diverse systems are ~~fully~~ tested.