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.:	**522-8633**
SRP Section:	**07.07 - Control Systems**
Application Section:	**7.7**
Date of RAI Issue:	**10/01/2016**

Question No. 07.07-18

10 CFR 50.55a(h)(3) requires compliance to IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, the safety system design shall be such that credible failure in, and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. In a response to RAI 356-7881, Question 07-08, the applicant provided technical information with regard to its analysis of postulated common cause failure (CCF) of components with embedded digital devices in Section 4.10 of the Control System CCF Analysis technical report, APR1400-Z-J-NR-14012. The information provided by the applicant was vital in the staff's understanding of the background information used to make analytical conclusions within the report as this information provided clear and concise technical basis for these conclusions. However, in order to make its safety finding, the NRC staff needs more detail added to the technical report than the applicant committed to provide.

The staff requests the following from the applicant:

1. Update Section 4.10 of the Control System CCF Analysis technical report to specifically state the embedded technology used in safety and non-safety applications are diverse from each other, as stated in part one of the applicant's response.

2. Add the table that lists the different types of embedded digital devices and their functions, provided in part one of the applicant's response, to Section 4.10 of the Control System CCF Analysis technical report.

3. Add the explanation regarding Class 1E devices with embedded technology in part 4 of the response to Question 07-08, to Section 4.10 of the Control System CCF Analysis technical report or another suitable area of the licensing documentation. This is essential as this explanation describes the existence of embedded technology in safety applications.

Response – (Rev. 2)

Section 4.10 of technical report APR1400-Z-J-NR-14012-P, Rev. 0, “Control System CCF Analysis” has been revised as indicated in the attachment to the Rev. 0 response to specifically state the embedded technology used in safety and non-safety applications are diverse from each other and to add the table that lists the different types of embedded digital devices and their functions.

The explanation regarding Class 1E devices with embedded technology that is included in part 4 of the response to RAI 356-7881 Question 07-08 will be moved into Section 6.2.5 of technical report APR1400-Z-J-NR-14002-P, Rev. 1, “Diversity and Defense-in-Depth” from Section 4.10 of technical report APR1400-Z-J-NR-14012-P, Rev.1, “Control System CCF Analysis” to provide an overall diversity analysis of APR1400 as indicated in the attachment 2 & 3 associated with this response.

In addition, the design commitment that embedded digital devices used in non-safety applications will be diverse from embedded digital devices used in safety applications will be added as an ITACC item in APR1400 DCD. APR1400 DCD Tier 1, Rev. 1, Subsection 2.5.5 will be revised as indicated in the attachment 1 associated with this response.

Impact on DCD

APR1400 DCD Tier 1, Rev. 1, Subsection 2.5.5 will be revised, as indicated in the attachment 1 associated with this response.

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

Technical report APR1400-Z-J-NR-14012-P/NP, Rev. 1, “Control System CCF Analysis,” Section 4.10 will be revised, as indicated in the attachment 2 associated with this response.

Technical report APR1400-Z-J-NR-14002-P/NP, Rev. 1, “Diversity and Defense-in-Depth,” Section 6.2.5 will be revised, as indicated in the attachment 3 associated with this response.

functions (i.e., the critical function success paths). The IFPDs are used for non-safety control, and safety related component selection in conjunction with control through the ESF-CCS soft control modules (ESCM).

While the IFPDs play an important role in the integrated HSI for APR1400, they are not credited for compliance to GDC 13 for anticipated operational occurrences and accident conditions. Compliance to GDC 13 is achieved through independent Class 1E HSI devices, which consist of the qualified indication and alarm system-P (QIAS-P), the Class 1E ESCMs, and minimum inventory switches. Since the IFPDs are not the credited HSI for abnormal plant conditions, but commensurate with their use as the primary operator interface, they are designed with the software grade designated as important to availability (ITA). Also the IFPDs are qualified to seismic Category II and the interface portion of IFPD for ESCM is qualified to same seismic criteria of the plant safety systems to prevent adverse impact to safety devices in the MCR.

4. The IFPDs display information for monitoring critical safety functions, and information and safety component selections for the plant systems/components used to control those functions.

5. The IFPDs are independent from Class 1E HSI devices.

6. The application software for the IFPD is implemented according to each life cycle phase in the software development process: concept phase, requirements phase, design phase, implementation phase, test phase, and installation and checkout phase. The outputs including documentation of each lifecycle phase in the software development process conform to the requirements of that phase.

7. The IFPDs do not adversely affect safety devices in the MCR during seismic conditions that would exist before, during, and following a design basis event.

2.5.5.2 Inspection, Test, Analyses, and Acceptance Criteria

The inspections, tests, analyses, and associated acceptance criteria for the PCS and P-CCS are specified in Table 2.5.5-2.

Some field equipment uses non-safety embedded digital devices. These non-safety embedded digital devices are diverse from the safety systems. In case of the ultrasonic level transmitters, these devices are used in both safety and non-safety applications. The design diversity for these devices is achieved by using different manufacturers'software and hardware designs.

8. The ultrasonic level transmitters for the non-safety system are diverse from the ultrasonic level transmitters for the safety system ~~by using different manufacturers' software and hardware designs~~.

Table 2.5.5-2 (3 of 3)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
6. (cont.)	6.d An inspection and analysis of the outputs including the documentation of the implementation phase will be performed.	6.d The implementation phase outputs including documentation exist and conclude that the implementation phase activities are performed and these activities conform to the requirements of the implementation phase.
	6.e An inspection and analysis of the outputs including the documentation of the test phase will be performed.	6.e The test phase outputs including documentation exist and conclude that the test phase activities are performed and these activities conform to the requirements of the test phase.
	6.f An inspection and analysis of the outputs including the documentation of the installation and checkout phase will be performed.	6.f The installation and checkout phase outputs including documentation exist and conclude that the installation and checkout phase activities are performed and these activities conform to the requirements of the installation and checkout phase.
7. The IFPDs do not adversely affect safety devices in the MCR during seismic conditions that would exist before, during, and following a design basis event.	7. Analysis of the as-built IFPDs will be performed.	7. A report exists and concludes that the IFPDs do not adversely affect safety devices in the MCR during seismic conditions that would exist before, during, and following a design basis event.
"Add" 8. The ultrasonic level transmitters for the non-safety system are diverse from the ultrasonic level transmitters for the safety system ~~by using different manufacturers' software and hardware designs~~.	8. Inspection of the design documentation will be performed to confirm that non-safety ultrasonic level transmitters are designed by using different manufacturers' software and hardware designs from safety ultrasonic level transmitters.	8. ~~The as-built non-safety ultrasonic level transmitters are designed by using different manufacturers' software and hardware designs from safety ultrasonic level transmitters.~~

the as-built

Inspection results confirm that the as-built non-safety ultrasonic level transmitters use different manufacturers' software and hardware designs from the safety related ultrasonic level transmitters.

4.10. CCF Analysis of Embedded Devices in Field Equipment

TS

TS

Table 4.10-1 Embedded Digital Device Type used in Non-safety System

TS

[redacted]

4.10.1. Evaluation for the CCF of Non-safety Field Instruments

TS

[redacted]

4.10.2. Evaluation for the CCF of Non-safety Field Actuators

TS

[redacted]

4.10.3. Evaluation for the Effect on Field Instruments due to Controller Failures

TS

[redacted]

RAI 522-8633 - Question 07.07-18_Rev.1

7. REFERENCES

1. NUREG-0800, USNRC Standard Review Plan, Revision 3, 15.0 Introduction - Transient and Accident Analyses, March 2007.

2. DI&C-ISG-04, “Highly Integrated Control Rooms – Communications Issues,” Rev. 1, 2009

3. IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”

4. APR1400-Z-J-NR-14013-P, “Response Time Analysis of Safety I&C System,” February 2017.

5. APR1400-Z-J-NR-14002-P, “Diversity and Defense-in-Depth,” February 2017.

RAI 522-8633 - Question 07.07-18_Rev.1

Signal diversity – The ESF actuation signals from DMA switches are diverse from the ESF signals from the PPS/ESF-CCS. The ESF signals from the DMA switches are directly connected to the CIM using hardwired cables without using common safety PLC platform like PPS/ESF-CCS. The signals from the DMA switches and the PPS/ESF-CCS are combined in the CIM that are not affected by a software CCF. Therefore, signal diversity is provided between the DMA switches and PPS/ESF-CCS.

Software diversity – The PPS/ESF-CCS uses the software of the PLC for digital logic processing, whereas the DMA switches do not use the software.

Equipment diversity – The PPS/ESF-CCS use the common safety PLC platform for the digital logic processing, whereas the DMA switches are implemented by the conventional analog devices. Therefore, significant equipment diversities are provided between the DMA switches and the PPS/ ESF-CCS.

Human diversity – The DMA switches are designed and tested by different design and test team from the PPS/ESF-CCS design and test team. Therefore, human diversity is provided between the DMA switches and the PPS/ESF-CCS.

6.2.4 Diversity Evaluation between the Actuators/Sensors and Safety I&C Platform

Detailed analysis results of diversity attributes between actuators/sensors and the safety I&C platform are as follows:

Design diversity – Diverse equipment platform based on different technology is applied to the actuators/sensors compared with the safety I&C platform. The actuators/ sensors use the analog technology, whereas the safety I&C platform uses the common safety PLC technology for the signal processing. Therefore, design diversity is provided between the sensors/ actuators and the safety I&C platform.

Functional diversity – There is no functional diversity between the sensors/ actuators and the safety I&C platform. Sensors and actuators provide the functions closely related with the safety I&C systems.

Signal diversity – There is no signal diversity between the sensors/actuators and the safety I&C platform. The safety I&C systems get inputs from various sensors, and provide their outputs to related actuators.

Software diversity – The sensors/actuators do not use the software, whereas the safety I&C platform uses the software for PLC. Therefore, software diversity is not provided between the sensors/actuators and the safety I&C platform.

Equipment diversity – The sensors/actuators are analog type equipment, whereas the safety I&C systems are digital type PLC equipment. Therefore, equipment diversity is provided between the sensors/actuators and the safety I&C platform.

Human diversity – Compared with the safety I&C systems, the sensors/actuators are designed and tested by different design and test team. Therefore, human diversity is provided between the sensors/actuators and the safety I&C platform.

Insert “A” on the next page.

Page intentionally blank