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.:	**71-7906**
SRP Section:	**14.03.05 – Instrumentation and Controls – Inspections, Tests, Analyses, and Acceptance Criteria**
Application Section:	**14.03.05**
Date of RAI Issue:	**07/15/2015**

Question No. 14.03.05-2

Demonstrate that communications independence requirements will be met for communications between redundant divisions of Class 1E equipment and between non-safety systems and Class 1E equipment. In addition, the design commitment for communication independence and ITAACs needs to include sufficient design descriptions in order to meet the requirements of 10 CFR 52.47(b)(1).

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. IEEE Std. 603-1991, Clause 5.6, "Independence," requires independence between redundant portions of safety systems and between safety and non-safety systems. Digital I&C Interim Staff Guidance (ISG) -04, "Highly-Integrated Control Rooms - Communications Issues," provides guidance for achieving communications independence in order to meet the requirements of IEEE Std. 603-1991, Clause 5.6. 10 CFR 52.47(b)(1) requires an application to contain the proposed inspections, tests, analyses, and acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a facility that incorporates the design certification has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations.

APR1400 FSAR, Tier 1, Section 2.5.1.1, "Design Description," Item 3.c states, "Communication independence is achieved between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1 or between non-safety systems and the Class 1E equipment listed in Table 2.5.1-1." This design commitment implies that communication independence will be achieved either between redundant divisions of Class 1E equipment or between non-safety systems and Class 1E equipment. The staff believes the wording should be modified to "Communication independence is achieved between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1 and between non-safety systems and the Class 1E

equipment listed in Table 2.5.1-1" in order to demonstrate that communications independence will be achieved between redundant divisions of Class 1E equipment and between non-safety systems and Class 1E equipment. Further, the design commitment and the associated ITAACs do not provide sufficient design information to demonstrate how communications independence will be achieved in the as-built system (e.g. types of communications faults that will be mitigated, key safety I&C features that will be used to mitigate these faults) in order to meet the requirements of 10 CFR 52.47(b)(1). For instance, the design description and the ITAAC should be more specific as to how communication independence is achieved for the various interdivisional communication links. The staff did not find ITAACs to verify the uni-directional gateway between the maintenance and test panel (MTP) and the information processing system (IPS), and between the integrated test panel (ITP) and qualified information and alarm system - non-safety (QIAS-N) in order to verify that communications independence is achieved between safety and non-safety systems. Modify Tier 1 of the FSAR, including the ITAAC to resolve these issues.

Response

"A report" described in item 3.c of Acceptance Criteria of Table 2.5.1-5 in DCD Tier 1 means the Safety I&C System Technical Report, which provides the detailed design information on how communications independence between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1 and between Class 1E equipment listed in Table 2.5.1-1 and non-safety systems. Sections C.4.1.5 and C.4.2 of the Safety I&C System Technical Report provide detailed descriptions on communication from the MTP to the IPS and the ITP to the QIAS-N, which is all unidirectional.

Item 3.c of the design description in Section 2.5.1.1 of DCD Tier 1 includes both "between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1" and "between Class 1E equipment listed in Table 2.5.1-1 and non-safety systems."

For clarification, item 3.c of the design description in Section 2.5.1.1 of DCD Tier 1 will be revised to provide the design description only for communication "between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1."

Item 3.d will be added to Section 2.5.1.1 and Table 2.5.1-5 of DCD Tier 1 to provide the design description only for communication "from the MTP to the IPS and from the ITP to the QIAS-N."

Supplemental Response

Section 4.6.2 of the Safety I&C System technical report provides the details on the communications independence between redundant portions of the safety systems and includes the use of fiber optic modems and fiber optic cabling for communication isolation and electrical isolation. Item 3.c of the design description and the design commitment in DCD Tier 1 Section 2.5.1.1 will be modified to provide additional detail of the communications independence.

Item 3.d will be added to DCD Tier 1 Section 2.5.1.1 and Table 2.5.1-5 to provide the design description specific to the communication from the MTP to the IPS through a fiber optic modem and cabling and from the ITP to the QIAS-N through optical isolation.

Response – (Rev. 1)

The previous response as supplemented is being revised to incorporate additional details into the proposed ITAAC. The previously proposed ITAAC verified the communications medium only. This revision is to include verification of key design and software features for ensuring communications independence such as the use of dual port RAM, separate communication and function processor, only accepting predefined messages and error checking.

Impact on DCD

DCD Tier 1 Section 2.5.1.1 and Table 2.5.1-5 will be revised as indicated in the attachment.

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.

3.a Class 1E equipment identified in Table 2.5.1-1 is powered from its respective Class 1E train.

3.b Redundant Class 1E divisions listed in Table 2.5.1-1 and associated field equipment are physically separated and electrically independent from each other and physically separated and electrically independent from non-Class 1E equipment.

3.c Communication independence is achieved between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1 ~~or between non-safety systems and the Class 1E equipment listed in Table 2.5.1-1~~ via fiber optic modem and cabling.

Delete

4.a The PPS provides an automatic reactor trip (RT) and ESF initiation signals, as indicated in Tables 2.5.1-2 and 2.5.1-3, if plant process signals reach predetermined setpoints.

4.b Once RT is initiated (automatically or manually), the reactor trip breakers remain open until completion of the protective action, and do not automatically return to normal after the trip condition is reset.

4.c Manual reactor trip switches are provided in the MCR and the RSR for reactor trip.

5. The OM in the MCR displays the status information for variables listed in Tables 2.5.1-2 and 2.5.1-3.

6. Each local coincidence logic (LCL) receives trip signals from four channels of bistable processors (BPs) and utilizes a 2-out-of-4 coincidence logic to perform RPS and ESF initiation functions identified in Tables 2.5.1-2 and 2.5.1-3.

7.a The PPS provides manual trip bypasses on the MTP switch panel, for RT and ESF initiation identified in non-safety systems and Class 1E equipment listed in Table 2.5.1-1

7.b The PPS automatically removes the operating bypasses listed in Table 2.5.1-4 when permissive conditions are not met.

3.d Communication independence is achieved between ~~the MTP (Class 1E equipment listed in Table 2.5.1-1) and the IPS (non-safety system) through fiber optic modem and cabling and between the ITP (Class 1E equipment listed in Table 2.5.1-1) and the QIAS-N (non-safety system) through optical isolation. The communication is unidirectional~~.

between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1

Table 2.5.1-5 (3 of 10)

Delete

via fiber optic modem and cabling

independence

	Design Commitment		Inspections, Tests, Analyses		Acceptance Criteria
3.c	Communication independence is achieved between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1 ~~or between non-safety systems and the Class 1E equipment listed in Table 2.5.1-1~~.	3.c	Analyses, tests or a combination of analyses and tests of the as-built Class 1E equipment listed in Table 2.5.1-1 will be performed to verify its communication independence.	3.c	A report exists and concludes that ~~data~~ communication between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1 ~~or between non-safety systems and the Class 1E equipment listed in Table 2.5.1-1 does not inhibit the performance of the safety function.~~
4.a	The RTS provides an automatic reactor trip (RT) and ESF initiation signals, as indicated in Tables 2.5.1-2 and 2.5.1-3, if plant process signals reach predetermined setpoints.	4.a	A test of the as-built PPS will be performed using simulated test signals.	4.a	Each as-built RTSS opens upon receipt of the automatic reactor trip signal identified in Table 2.5.1-2 from respective division of the as-built RTS, and as-built ESF initiation signals are sent to ESF-CCS upon receipt of the automatic ESF initiation signal identified in Table 2.5.1-3.
4.b	Once reactor trip is initiated (automatically or manually), the reactor trip breakers remain open until completion of the protective action, and do not automatically return to normal after the trip condition is reset.	4.b.	A test of the as-built RT system will be performed by returning simulated signals to a level within the predetermined limits of plant process signals at the as-built PPS input for RT functions as identified in Tables 2.5.1-2 after the as-built reactor trip breakers are opened.	4.b.	As-built reactor trip breakers remain open upon receipt of simulated signals returned to a level within the predetermined limits of plant process signals for RT functions as identified in Table 2.5.1-2 after the as-built reactor trip breakers are opened.
4.c	Manual reactor trip switches are provided in the MCR and the RSR for reactor trip.	4.c	A test will be performed to verify the actuation of the as-built RTSS using the as-built manual initiation switches in the MCR and RSR.	4.c	Each as-built RTSS opens upon receipt of the corresponding as-built manual reactor trip signal in the MCR and RSR.

Delete

Delete

is provided by:
- The communication process is performed by a communication processor (CP) separate from the function processor (FP) that executes the RPS and ESFAS function.
- Separate send and receive data channels are used for communication.
- The FP and CP interface only by way of the dual-ported random access memory.
- The FP operates in a strictly cyclic manner.
- The CP transmits signals to serial data link in a deterministic transmit cycle, receives only defined messages, and stores them in a predefined shared-memory.
- The FP and CP detect errors through self-diagnostic function.

Insert another line for item 3.d as shown on the next page.

non-safety systems and Class 1E equipment listed in Table 2.5.1-1.

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3.d Communication independence is achieved between ~~the~~ MTP (Class 1E equipment listed in Table 2.5.1-1) and the IPS (non-safety system) through fiber optic modem and cabling and between the ITP (Class 1E equipment listed in Table 2.5.1-1) and the QIAS-N (non-safety system) through optical isolation. The communication is unidirectional.	3.d Analyses, tests or a combination of analyses and tests of the as-built Class 1E equipment listed in Table 2.5.1-1 will be performed to verify its communication independence.	3.d A report exists and concludes that ~~data communication from the MTP to the IPS and from the ITP to the QIAS-N does not inhibit the performance of the safety function since the communication is unidirectional.~~

between non-safety systems and Class 1E equipment listed in Table 2.5.1-1

communication independence between non-safety systems and Class 1E equipment listed in Table 2.5.1-1 is provided by:
- The data flow from the MTP to the IPS and from the ITP to the QIAS-N is unidirectional via fiber optic cable.
- The MTP and the ITP do not receive any data from the IPS and the QIAS-N (no receiving connection).
- The MTP has separate communication modules for communication processing to provide a buffering circuit between the PPS and the IPS.
- The communication process between the ITP and the QIAS-N is performed by the communication processor (CP) in the ITP.