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.:	**317-8271**
SRP Section:	**14.03.05 - Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria**
Application Section:	
Date of RAI Issue:	**11/17/2015**

Question No. 14.03.05-32

Provide design descriptions, including corresponding ITAACs regarding the system development of the IFPD.

10 CFR Part 50, Appendix A, GDC 1, requires SSCs important to safety to be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. GDC 13 states, "Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges." Technical Report APR1400-Z-J-NR-14001, Rev. 0, "Safety I&C System Technical Report," Section 4.4.2 states “The ESCM provides the operators with [withheld as proprietary .] The ESCMs on the operator consoles work [withheld as proprietary .]” It appears that the IFPD is used as the primary control and indication (including alarms), during normal, abnormal, and accident conditions. As such, the staff considers the IFPD important-to-safety. Thus, the staff requests the applicant to provide design descriptions, including corresponding ITAACs regarding the system development of the IFPD in APR1400 FSAR Tier 1, Section 2.5, in order to demonstrate that the requirements GDC 1 and GDC 13 are met for the as-built IFPD. In addition, the staff requests the applicant to modify the APR1400 FSAR to provide a description of what augmented quality is associated with the IFPD, including its classification in Technical Report, APR1400-Z-J-NR-14003, Rev. 0, "Software Program Manual."

Response – (Rev. 2)

TS

TS

Impact on DCD

DCD Tier 1, Section 2.5.5.1 and Table 2.5.5-2 will be revised as indicated in the attachment 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-14001-NP, Rev. 0, “Safety I&C System,” Subsection 4.4.2 and Technical Report APR1400-Z-J-NR-14003-NP, Rev. 0, “Software Program Manual,” Table A- 1 will be revised as indicated in the attachment associated with this response.

TS

A.2 Software Classification for the Safety I&C Systems

The software for the safety I&C systems is classified as one of the two software classes: SC class and ITS class. Both classes of the software for the safety I&C systems are implemented on Class 1E hardware.

IEEE Std. 603 (Reference 15), Clause 5.3 requires that components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates. RG 1.152 (Reference 4) endorses IEEE Std. 7-4.3.2 (Reference 14) which supplements IEEE Std. 603 for computer-based safety I&C systems. IEEE Std. 7-4.3.2, Clause 5.3.3, “Verification and validation” states that software V&V effort shall be performed in accordance with IEEE Std. 1012 (Reference 21) and the IEEE Std. 1012 V&V requirements for the highest integrity level (level 4) apply to systems developed using IEEE Std. 7-4.3.2. Performing adequate V&V is a critical part of ensuring a high quality development process for safety I&C systems.

In the safety I&C system design, for ITS class software, V&V activities are not performed in accordance with the V&V requirements for the highest integrity level as stated in IEEE Std. 7-4.3.2. However, the assurance is given to demonstrate that ITS class software is of sufficient quality and reliability to maintain the safety function of the software and does not present a hazard on SC class software.

TS

TS

TS

4.4.3 Architecture Description

Page intentionally blank

2.5.5 Control System Not Required for Safety

2.5.5.1 Design Description

Control system which is not required for safety consists of power control system (PCS) and process-component control system (P-CCS).

The PCS includes the reactor regulating system (RRS), the digital rod control system (DRCS), and the reactor power cutback system (RPCS). The P-CCS includes nuclear steam sypply system (NSSS) process control system (NPCS) and balance of plant (BOP) control systems. The NPCS consists of the feedwater control system (FWCS), the steam bypass control system (SBCS), the pressurizer pressure control system (PPCS), the pressurizer level control system (PLCS), and other miscellaneous NSSS control systems which include reactor makeup control function of the chemical and volume control system (CVCS).

The PCS and P-CCS provide control of functions to maintain the plant within its normal operating range for all normal modes of plant operation.

Control and display interface devices for the PCS and P-CCS are provided in the main control room (MCR) and in the remote shutdown room (RSR) for control and monitoring of the PCS and P-CCS.

1. The major controllers of the PCS and NPCS are arranged in separate controller groups as identified in Table 2.5.5-1.

2. The digital equipment and software used in the PCS and P-CCS are independent from those of the plant protection system (PPS) and the engineered safety features-component control system (ESF-CCS).

Insert "B" on the next page

3. The PCS and P-CCS are controlled from either the MCR or RSR, as selected from master transfer switches.

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..

"B"

The information flat panel displays (IFPDs) provide control means of PCS and P-CCS. The IFPDs are the primary human systems interface (HSI) for normal and abnormal plant conditions. They display information that is used by plant operators, including indications and alarms for critical safety and power production functions, and the performance of the plant's preferred non-safety and safety systems that are used to control those critical 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 IFPD software is implemented according to the software lifecycle process.

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.

Table 2.5.5-2

Control System Not Required for Safety ITAAC

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. The major controllers of PCS and NPCS are arranged in separate controller groups as identified in Table 2.5.5-1.	1. Inspection of the as-built PCS and NPCS will be performed.	1. The as-built PCS and NPCS are arranged in separate controller groups as identified in Table 2.5.5-1.
2. The digital equipment and software used in the PCS and P-CCS are independent from those of the plant protection system (PPS) and ~~the~~ engineered safety features-component control system (ESF-CCS).	2. Inspection of the as-built PCS and P-CCS equipment will be performed. Inspection of the design documentation will be performed to confirm that the software is developed by independent design groups.	2. The as-built digital equipment and software used in the PCS and P-CCS are independent from those of the PPS and ESF-CCS based on: • PCS and P-CCS use a platform which is independent from the platform used in the PPS and ESF-CCS and • The design group(s) which developed the PCS and P-CCS software is independent from the design group(s) which developed the PPS and ESF-CCS software.
3. The PCS and P-CCS are controlled from either the MCR or RSR, as selected from MCR/RSR master transfer switches.	3. A test of the as-built system will be performed to demonstrate the transfer of control capability between the MCR and RSR.	3. The as-built MCR/RSR master transfer switches transfer controls between the MCR and the RSR for as-built PCS and P-CCS, as follows: • Controls at the RSR are disabled when controls are active in the MCR for the as-built PCS and P-CCS. • Controls at the MCR are disabled when controls are active in the RSR for the as-built PCS and P-CCS.

Insert "C" on the next page for Item 4, 5, 6, 7.

~~"C"~~

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
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.	4. Inspection of the as-built IFPDs will be performed.	4. The as-built IFPDs allow monitoring the critical safety functions, and monitoring and selecting components for controlling the preferred emergency success paths for each critical function.
5. The IFPDs are independent from Class 1E HSI devices.	4. Inspection of the as-built IFPDs will be performed.	4. The IFPDs are isolated and are independent from Class 1E systems, including the QIAS-P, ESCMs, and minimum inventory switches.
6. The IFPD software is implemented according to the software lifecycle process.	6.a An inspection will be performed for the requirements phase result summary report of IFPD software.	6.a The requirements phase result summary report exists and concludes that the plant requirements phase activities of IFPD software are performed.
	6.b An inspection will be performed for the design phase result summary report of IFPD software.	6.b The design requirements phase result summary report exists and concludes that the design phase activities of IFPD software are performed.
	6.c An inspection will be performed for the implementation phase result summary report of IFPD software.	6.c The implementation phase result summary report exists and concludes that the implementation phase activities of IFPD software are performed.
	6.d An inspection will be performed for the test phase result summary report of IFPD software.	6.d The test phase result summary report exists and concludes that the test phase activities of IFPD software are performed.
	6.e An inspection will be performed for the installation and checkout phase result summary report of IFPD software.	6.e The installation phase result summary report exists and concludes that the installation and checkout phase activities of IFPD software are performed.
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.

"C (1/2)"

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
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.	4. Inspection of the as-built IFPDs will be performed.	4. The as-built IFPDs allow monitoring the critical safety functions, and monitoring and selecting components for controlling the preferred emergency success paths for each critical function.
5. The IFPDs are independent from Class 1E HSI devices.	5. Inspection of the as-built IFPDs will be performed.	5. The IFPDs are isolated and are independent from Class 1E systems, including the QIAS-P, ESCMs, and minimum inventory switches.
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.	6.a An inspection and analysis of the outputs including the documentation of the concept phase will be performed.	6.a The concept phase outputs including documentation exist and conclude that the concept phase activities are performed and these activities conform to the requirements of the concept phase.
	6.b An inspection and analysis of the outputs including the documentation of the requirements phase will be performed.	6.b The requirements phase outputs including documentation exist and conclude that the requirements phase activities are performed and these activities conform to the requirements of the requirements phase.
	6.c An inspection and analysis of the outputs including the documentation of the design phase will be performed.	6.c The design phase outputs including documentation exist and conclude that the design phase activities are performed and these activities conform to the requirements of the design phase.
	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.

"C (2/2)"

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
	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.