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. 14.03.05-1

Demonstrate how the as-built Reactor Trip System (RTS) and Engineered Safety Feature (ESF) system meet the quality requirements of IEEE Std. 603-1991, Clause 5.3 and the inspectability requirements of 10 CFR 52.47(b)(1). Specifically, the Tier 1 description and the corresponding Inspection, Test, Analysis and Acceptance Criterion (ITAAC) for the plant protection system (PPS) software development need to be clarified to demonstrate consistency with Tier 2 information and provide sufficient acceptance criteria.

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 5.3, "Quality," requires, in part, components and modules to be of a quality that is consistent with minimum maintenance requirements and low failure rates. This clause also states that "Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program." Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," provides guidance on performing reviews for softwarebased safety-related, instrumentation and control (I&C) systems. 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.

Technical Report (TeR) APR1400-Z-J-NR-14003-P, Rev. 0, "Software Program Manual [SPM]," describes the software engineering process for digital computer-based I&C systems of the APR1400. Section 1.1, "Purpose," of this TeR states this report provides generic

guidance for the software program plans based on the BTP 7-14. Section 2.2, "Software Life Cycle," of this TeR defines the software life cycle phases for the development of safety I&C system software, which includes the concept, requirements, design, implementation, test, installation and checkout, and operation and maintenance phases. APR1400 Final Safety Analysis Report (FSAR), Tier 1, Section 2.5.1.1, Item 11, states “RTS and ESF initiation software is implemented according to the software life cycle process.” The staff finds that this section does not describe what lifecycle process (e.g. specific lifecycle phases of the lifecycle process) the RTS and ESF initiation software follow. The staff requests the applicant to:

1. Identify and define the lifecycle phases for the lifecycle process in Tier 1 (design descriptions and ITAAC) of the APR1400 FSAR and verify that these phases are consistent with the SPM TeR in order to demonstrate compliance to the requirements of IEEE Std. 603-1991, Clause 5.3, and 10 CFR 52.47(b)(1).

2. Ensure the Tier 1 design description and ITAAC address all RTS and ESF software. The current description implies that the design commitment on following the software lifecycle development process only applies to the RTS and ESF initiation software and not all system software of the RTS and ESF system (e.g. self-diagnostic software, communications software).

3. For the Tier 1 design description and ITAAC, state that the output of each life cycle phase will conform to the requirements of that phase. The acceptance criterion for the corresponding ITAAC states that a summary report with the results of each phase exists and this summary report will conclude that the phase activities are performed. The staff finds that the acceptance criterion does not verify that the output of each phase meets the requirements of that phase.

Response – (Rev. 1)

1. Each software lifecycle phase in the software development process, as defined in the Software Program Manual (SPM), will be identified and added to item #11 of Section 2.5.1.1 and Table 2.5.1-5 of DCD Tier 1.

2. The RTS and ESF initiation software implies the application software portion of the safety system. The initiation software utilizes the platform software, which has already been qualified, including self-diagnostic and communication in order to generate reliable reactor trip and ESF initiation signals and accomplish the intended safety functions within the safety system. The term, “RTS and ESF initiation software”, will be modified to “The application software for RT and ESF initiation”.

3. Item #11 of Section 2.5.1.1 and Table 2.5.1-5 will be revised to verify by inspection and analysis that the outputs, including documentation, of each lifecycle phase in the software development process conforms to the requirements of that phase.

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.

APR1400 DCD TIER 1

7.c The PPS provides indications of the bypassed or inoperable status indication (BISI) on the OM in the MCR for the variables identified in Tables 2.5.1-2 and 2.5.1-3 for RT and ESF initiation.

8. Each PPS division is controlled from either the MCR or the RSR as selected from master transfer switches.

9. The PPS utilizes a 2-out-of-4 coincidence logic when no channels are in trip channel bypass. The PPS converts to a 2-out-of-3 coincidence logic whenever a trip channel bypass is present.

10. Accuracy, response time testing, surveillance testing, and maintenance are applied to determine setpoints for variables of RT and ESF initiation.

11. ~~RTS and ESF initiation software~~ is implemented according to ~~the software life cycle process.~~ The application software for RT~~S~~ and ESF initiation

12. The cabinets listed in Table 2.5.1-1 have key locks and door open alarms, and are located in a vital area of the facility.

13. The RT logic of the PPS is designed to fail to a safe state such that loss of electrical power to a division of PPS results in a trip condition for that division but the ESFAS logic of the PPS is designed to fail to a safe state such that loss of electrical power to a division of PPS does not result in ESF initiation for that division.

14. Redundant safety equipment listed in Table 2.5.1-1 is provided with means of identification.

15. The input signals of PPS through APC-S or ENFMS are derived from RT and ESF measurement instrumentation that measures monitored variables identified in Tables 2.5.1-2 and 2.5.1-3.

16. The PPS provides RT and ESF initiation signals to meet the required response time for trip and initiation conditions identified in Tables 2.5.1-2 and 2.5.1-3.

each lifecycle 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.

APR1400 DCD TIER 1

Table 2.5.1-5 (6 of 10)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11. RTS and ESF initiation software is implemented according to the software lifecycle process.	11.a An inspection will be performed for the requirements phase result summary report.	11.a The requirements phase result summary report exists and concludes that the plant requirements phase activities o are performed.
	11.b An inspection will be performed for the design phase result summary report.	11.b The design requirements phase result summary report exists and concludes that the design phase activities are performed.
	11.c An inspection will be performed for the implementation phase result summary report.	11.c The implementation phase result summary report exists and concludes that the implementation phase activities are performed.
	11.d An inspection will be performed for the test phase result summary report.	11.d The test phase result summary report exists and concludes that the test phase activities are performed.
	11.e An inspection will be performed for the installation and checkout phase result summary report.	11.e The installation phase result summary report exists and concludes that the installation and checkout phase activities are performed.

To be revised as shown on the next page.

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11. The application software for RTS and ESF initiation is implemented according to each lifecycle 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.	11.a An inspection and analysis of the outputs including documentation of the concept phase will be performed.	11.a The concept phase outputs including documentations exist and conclude that the concept phase activities are performed and these activities conform to the requirements of the concept phase.
	11.b An inspection and analysis of the outputs including documentation of the requirements phase will be performed.	11.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.
	11.c An inspection and analysis of the outputs including documentation of the design phase will be performed.	11.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.
	11.d An inspection and analysis of the outputs including documentation of the implementation phase will be performed.	11.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.
	11.e An inspection and analysis of the outputs including documentation of the test phase will be performed.	11.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.
	11.f An inspection and analysis of the outputs including documentation of the installation and checkout phase will be performed.	11.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.