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:	
Date of RAI Issue:	**07/15/2015**

Question No. 14.03.05-9

Modify the Tier 1 description and the corresponding ITAAC for the engineer safety feature-component control system (ESF-CCS) software development in order to provide inspectable criteria.

10 CFR 50.55a(h)(3) states, in part, that applications 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, requires that components and modules to be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. BTP 7-14 provides guidance for software reviews for safety 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.

The SPM TeR describes the software engineering process for digital computer-based I&C systems of the APR1400. Section 1.1 of this TeR states that this report provides generic guidance for the software program plans based on the BTP 7-14. Section 2.2 of this TeR defines the software lifecycle 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 FSAR, Tier 1, Section 2.5.4.1, Item 15, states “The ESF-CCS software is implemented according to the software lifecycle process.” The staff finds that this section does not describe what this lifecycle process will be (e.g. the different lifecycle phases). The applicant should define the lifecycle phases within this lifecycle process and ensure that they are consistent with the SPM TeR in order to demonstrate compliance to

the requirements of IEEE Std. 603-1991, Clause 5.3. The staff also finds that the design commitment does not state that the output of each lifecycle phase will conform to the requirements of each lifecycle phase. Further, 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 this acceptance criterion does not verify that the output of the phase meet the requirements of each phase. Modify Tier 1 of the FSAR, including the ITAAC to resolve these issues.

Response - (Rev. 1)

Each development phase of the software lifecycle process, as defined in Software Program Manual (SPM), will be identified and added to item #5 of Section 2.5.4.1 and Table 2.5.4-4 of DCD Tier 1 to verify by inspection and analysis that the outputs, including documentation, of each software lifecycle phase conforms to the requirements of that phase.

Impact on DCD

DCD Tier 1, Section 2.5.4.1 and Table 2.5.4-4 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

There is no impact on the Technical/Topical/Environmental Report.

when the BOP ESF actuation signal has been cleared. Once the initiating condition is cleared, the BOP ESF actuation is manually reset.

10. Loss of power in an ESF-CCS division results in the respective ESF-CCS division output assuming fail-safe output condition.

11. Manual ESF actuation switches are provided in the MCR and RSR for the manual ESF actuations identified in Table 2.5.4-3.

12. The operator modules (OMs) in the MCR display ESF actuation status, manual ESF actuation status, and ESF-CCS status information including the test status for ESF actuations identified in Tables 2.5.4-2 and 2.5.4-3.

13. The component interface module (CIM) provides state-based priority logic to prioritize the ESF-CCS and DPS signals.

lifecycle phase in the software development process

14. The CIM provides system-based priority logic for the front panel control switch signals on the CIM, the signals generated by the DMA switches, the signals from the ESF-CCS, and the signals from the DPS. The front panel control switches have the highest priority, and the signals from the DMA switches have priority over signals from the ESF-CCS and DPS.

each ~~development phase of~~

15. The ~~ESF-CCS software~~ is implemented according to ~~the software lifecycle process.~~

application software for the ESF-CCS

16. The ESF-CCS equipment and components identified in Table 2.5.4-1 withstand the electrical surge, electromagnetic interference (EMI), radio-frequency interference (RFI), and electrostatic discharge (ESD) conditions that would exist before, during, and following a design basis event without loss of its safety function for the time required to perform the safety function.

17. Redundant safety equipment and components of the ESF-CCS listed in Table 2.5.4-1 and related field equipment are provided with means of identification.

: concept phase, requirement phase, design phase, implementation phase, test phase, and installation and checkout phase. The outputs ~~of each development phase of the software lifecycle process~~ conform to the requirements of that phase.

, including documentation, of each lifecycle phase in the software development process

Table 2.5.4-4 (5 of 7)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
13. The component interface module (CIM) provides state-based priority logic to prioritize the ESF-CCS and DPS signals.	13. A test will be performed using simulated input signals concurrently to the CIM.	13. When the CIM receives conflicting component control input signals from the ESF-CCS and DPS, the CIM prioritizes the signals so that one direction of component control always has priority over the opposite direction, regardless of which system is commanding the priority direction.
14. The CIM provides system-based priority logic for the front panel control switch signals on the CIM, the signals generated by the DMA switches, the signals from the ESF-CCS, and the signals from the DPS. The front panel control switches have the highest priority, and the signals from the DMA switches have priority over signals from the ESF-CCS and DPS.	14. A test will be performed using simulated input signals concurrently to the CIM.	14. When the CIM receives input signals from the front panel control switch and DMA switches concurrently, the CIM prioritizes signals so that the signal of the front panel control switch has priority over signals of the DMA switches. The DMA switches have priority over signals from the ESF-CCS and DPS.
15. The ESF-CCS software is implemented according to the software lifecycle process.	15.a An inspection will be performed for the requirements phase result summary report of ESF-CCS software.	15.a The requirements phase result summary report exists and concludes that the plant requirements phase activities of ESF-CCS software are performed.
	15.b An inspection will be performed for the design phase result summary report of ESF-CCS software.	15.b The design requirements phase result summary report exists and concludes that the design phase activities of ESF-CCS software are performed.
	15.c An inspection will be performed for the implementation phase result summary report of ESF-CCS software.	15.c The implementation phase result summary report exists and concludes that the implementation phase activities of ESF-CCS software are performed.

APR1400 DCD TIER 1

To be revised as shown on the next page.

Table 2.5.4-4 (6 of 7)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
15. (cont.)	15.d An inspection will be performed for the test phase result summary report of ESF-CCS software.	15.d The test phase result summary report exists and concludes that the test phase activities of ESF-CCS software are performed.
	15.e An inspection will be performed for the installation and checkout phase result summary report of ESF-CCS software.	15.e The installation phase result summary report exists and concludes that the installation and checkout phase activities of ESF-CCS software are performed.
16. The ESF-CCS equipment and components identified in Table 2.5.4-1 withstand the electrical surge, electromagnetic interference (EMI), radio-frequency interference (RFI), and electrostatic discharge (ESD) conditions that would exist before, during, and following a design basis event without loss of its safety function for the time required to perform the safety function.	16.a A type test, analysis, or a combination of a type test and analysis will be performed.	16.a A report exists and concludes that the ESF-CCS equipment identified in Table 2.5.4-1 withstand the electrical surge, EMI, RFI, and ESD conditions that would exist before, during, and following a design basis event without loss of its safety function, for the time required to perform the safety function.
	16.b An inspection and analysis of the as-built Class 1E equipment and components installation configuration and environment will be performed identified in Table 2.5.4-1.	16.b The as-built Class 1E equipment, components, and the associated wiring, cables, and terminations identified in Table 2.5.4-1 are bounded by a type test or a combination of a type test and analysis.
17. Redundant safety equipment and components of the ESF-CCS listed in Table 2.5.4-1 and related field equipment are provided with means of identification.	17. An inspection of the as-built equipment for conformance with the identification requirements will be performed.	17. The as-built equipment and components listed in Table 2.5.4-1 and related field equipment comply with the labeling and the color coding requirements.

Replacement ITACC for Design Commitment 15.

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
15. The ~~ESF-CCS software~~ application software for the ESF-CCS is implemented according to each ~~development phase of the software lifecycle process~~: lifecycle phase in the software development process: concept phase, requirements phase, design phase, implementation phase, test phase, and installation and checkout phase. The outputs~~, of each development phase of the software lifecycle process~~ including documentation, of each lifecycle phase in the software development process conform to the requirements of that phase.	15.a An inspection and analysis of the outputs, including the documentation, of the concept phase will be performed ~~for the outputs of the concept phase~~.	15.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.
	15.b An inspection and analysis of the outputs, including documentation, of the requirements phase will be perfor~~med for the outputs of~~ the ~~requirements phase~~.	15.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.
	15.c An inspection and analysis of the outputs, including documentation, of the design phase will be performed ~~for the outputs of the design phase~~.	15.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.
	15.d An inspection and analysis of the outputs, including documentation, of the implementation phase will be performed ~~for~~ the ~~outputs of the implementation phase~~.	15.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.
	15.e An inspection and analysis of the outputs, including documentation, of the test phase will be performed ~~for the outputs of the test phase~~.	15.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.
	15.f An inspection and analysis of the outputs, including documentation, of the installation and checkout phase will be performed ~~for the outputs of the installation and checkout phase~~.	15.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.