KHNPDCDRAIsPEm Resource

From:	Ciocco, Jeff
Sent:	Wednesday, July 15, 2015 1:37 PM
To:	apr1400rai@khnp.co.kr; KHNPDCDRAIsPEm Resource; Harry (Hyun Seung) Chang; Yunho Kim; Steven Mannon
Cc:	Zhang, Deanna; Jackson, Terry; Ward, William; Lee, Samuel
Subject:	APR1400 Design Certification Application RAI 71-7906 (14.03.05 - Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria)
Attachments:	APR1400 DC RAI 71 ICE1 7906.pdf; image001.jpg

KHNP,

The attachment contains the subject request for additional information (RAI). This RAI was sent to you in draft form. Your licensing review schedule assumes technically correct and complete responses within 30 days of receipt of RAIs. However, KHNP requests, and we grant, 60 days to respond to the RAI question. We may adjust the schedule accordingly.

Please submit your RAI response to the NRC Document Control Desk.

Thank you,

Jeff Ciocco
New Nuclear Reactor Licensing
301.415.6391
jeff.ciocco@nrc.gov

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Hearing Identifier: KHNP_APR1400_DCD_RAI_Public
Email Number: 80

Mail Envelope Properties (a3cd8968dfbf4fa3a19946d9594c867a)

Subject: APR1400 Design Certification Application RAI 71-7906 (14.03.05 - Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria)
Sent Date: 7/15/2015 1:37:20 PM
Received Date: 7/15/2015 1:37:24 PM
From: Ciocco, Jeff

Created By: Jeff.Ciocco@nrc.gov

Recipients:
"Zhang, Deanna" <Deanna.Zhang@nrc.gov>
Tracking Status: None
"Jackson, Terry" <Terry.Jackson@nrc.gov>
Tracking Status: None
"Ward, William" <William.Ward@nrc.gov>
Tracking Status: None
"Lee, Samuel" <Samuel.Lee@nrc.gov>
Tracking Status: None
"apr1400rai@khnp.co.kr" <apr1400rai@khnp.co.kr>
Tracking Status: None
"KHNPDCDRAIsPEm Resource" <KHNPDCDRAIsPEm.Resource@nrc.gov>
Tracking Status: None
"Harry (Hyun Seung) Chang" <hyunseung.chang@gmail.com>
Tracking Status: None
"Yunho Kim" <yshh8226@gmail.com>
Tracking Status: None
"Steven Mannon" <steven.mannon@aecom.com>
Tracking Status: None

Post Office: HQPWMSMRS08.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	638	7/15/2015 1:37:24 PM
APR1400 DC RAI 71 ICE1 7906.pdf	130000	
image001.jpg	5040	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

REQUEST FOR ADDITIONAL INFORMATION 71-7906

Issue Date: 07/15/2015
Application Title: APR1400 Design Certification Review – 52-046
Operating Company: Korea Hydro & Nuclear Power Co. Ltd.
Docket No. 52-046
Review Section: 14.03.05 - Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria
Application Section:

QUESTIONS

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 requirments 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 software-based 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.

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 requirments 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.

14.03.05-3

Within the Tier 1 design description, identify the physical location of RTS and ESF initiation equipment within the auxiliary building and reactor containment building. Modify the corresponding ITAAC to verify that the physical location in the as-built plant meets the design commitment in order to demonstrate compliance to 10 CFR 52.47(b)(1).

10 CFR 50.55a(h)(3) states, in part, that applications filed on or after May 13, 1999, for design certifications must meet the requirments for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. IEEE Std. 603-1991, Clause 5.6.1, "[Independence] Between Redundant Portions of a Safety System," requires physical separation between redundant portions of safety systems, and Clause 5.6.3, "Between Safety Systems and Other Systems," requires physical separation between Class 1E equipment and non-safety systems. RG 1.75, Physical Independence of Electric Systems," provides guidance for meeting the physical separation requirements of IEEE Std. 603-1991, Clause 5.6, "Independence." 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, states, “The RTS and ESF initiation equipment is located in the auxiliary building and reactor containment building.” APR1400, FSAR, Tier 1, Section 2.5.1.1, Item 3.b states, “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 Class 1E equipment." The Table 2.5.1-5, item 3.b.i acceptance criteria states, in part, “The physical separation of as-built redundant Class 1E divisions identified in Table 2.5.1-1 and associated field equipment is provided by distance or barriers in accordance with NRC [Regulatory Guide (RG)] 1.75.” Based on the information presented in APR1400 FSAR, Tier 1, Table 2.5.1-1, the staff could not identify where in the auxiliary building and reactor containment building the redundant divisions of safety equipment will reside in order to demonstrate that sufficient separation exists between the redundant divisions of safety equipment or between safety and non-safety equipment in order to meet the requirements of IEEE Std. 603-1991, Clause 5.6. As such, the staff requests the applicant to include this information in Tier 1 of the FSAR and modify the corresponding ITAAC accordingly to verify that the as-built system meets the design commitment in order to demonstrate compliance to 10 CFR 52.47(b)(1).

14.03.05-4

Clarify the criteria for testing functions within APR1400 FSAR Tier 1, Section 2.5.1.1, for the PPS (Plant Protection System).

10 CFR 50.55a(h)(3) states, in part, that applications filed on or after May 13, 1999, for design certifications must meet the requirments for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. IEEE Std. 603-1991, Clause 5.7, "Capability for Test and Calibration," states, in part, the capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. Branch Technical Position (BTP) 7-17, "Guidance on Self-Test and Surveillance Test Provisions," provides guidance to meet the requirements of IEEE Std. 603-1991, Clause 5.7. 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, Item 20, and the corresponding ITAAC states, “The PPS providing RTS and ESF initiation signals has the testing functions.” It is not clear to the staff what is meant by this design description. Specifically, it is not clear whether this design description intends to state that the capability to test and calibrate the PPS exists or there are self-testing functions within PPS. The design description regarding testing functions does not include criteria for testing features included in the design to meet the requirements of IEEE Std. 603-1991, Clause 5.7 (e.g. ability to detect faults in a manner that meets the design requirements of the PPS). Modify the design description in Tier 1 of the APR1400 FSAR to address these issues (including the acceptance criteria to the corresponding ITAAC) in order to meet the requirements of IEEE Std. 603-1991, Clause 5.7 and 10 CFR 52.47(b)(1).

14.03.05-5

Modify the as-built Diverse Protection System (DPS) and Diverse Indication System (DIS) Tier 1 Description to provide inspectable acceptance criteria following completion of a software lifecycle. Provide Tier 1 design description and ITAAC for the DIS software lifecycle.

GDC 1 states in part that “Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.” Branch Technical Position (BTP) 7-14 provides guidance for software reviews for 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 technical report defines the software life cycle phases for the development of I&C system software, which includes the concept, requirements, design, implementation, test, installation and checkout, and operation and maintenance phases. This TeR applies to both safety-critical (protection) class software and important-to-safety (ITS) software. Appendix A, "The I&C System Software Classes," of this TeR indicates that the DPS and DIS contain ITS software. Tier 1, Section 2.5.2.1, Item 6, and the corresponding ITAAC state, “The DPS software is implemented according to the software lifecycle process.” The staff finds that the design commitment does not state that the output of each life cycle phase will conform to the requirements of that phase. In addition, 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. However, the staff finds that this acceptance criterion does not verify that the output of the phase meet the requirements of that phase. Further no design description and ITAAC exists to verify the DIS is implemented in accordance to a software development lifecycle process, if it contains programmable technology. Modify Tier 1 of the FSAR, including the corresponding ITAAC, to resolve these issues in order to demonstrate compliance to GDC 1 and 10 CFR 52.47(b)(1).

14.03.05-6
Provide a design commitment and corresponding ITAAC to verify that the response time of the as-built DPS.

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. GDC 22 states “The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.” The SRM to SECY-93-087 (ML003708056), Item II.Q, "Defense Against Common Mode Failures in Digital I&C Systems," provides requirements for addressing software common cause failures within safety I&C systems. Point 3 of this item states, “If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.”

Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," provides guidance on meeting the requirements of GDC 22 and SRM to SECY-93-087, Item II.Q. Section 3.1 of BTP 7-19 states, “For each anticipated operational occurrence [(AOO)] in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic assumptions should not result in radiation release exceeding 10 percent of the applicable siting dose guideline values or violation of the integrity of the primary coolant pressure boundary.” The staff reviewed APR1400 FSAR Tier 1, Section 2.5.2, and could not identify design commitments or corresponding ITAACs that verify the response time of the as-built DPS will be sufficient to demonstrate that the plant response will not result in radiation release exceeding 10 percent of the applicable siting dose guideline values or violation of the integrity of the primary coolant pressure boundary. Modify Tier 1 to provide a design commitment and corresponding ITAAC to verify that the as-built DPS response time from sensor output through equipment actuation is less than the value required to satisfy the diverse actuation function response time assumptions.

14.03.05-7
Provide design commitments and corresponding ITAACs in APR1400 FSAR, Tier 1, to verify that the as-built DIS is diverse and independent from the Quality Indication and Alarm System Safety (QIAS-P). In addition, demonstrate that the as-built DIS provides indications of the necessary plant variables and parameters.

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. GDC 22 states “The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of

operation, shall be used to the extent practical to prevent loss of the protection function." The SRM to SECY-93-087, Item II.Q provides requirements for addressing software common cause failures within safety I&C systems. Point 4 of this item states "A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above." BTP 7-19 provides guidance on meeting the requirements of GDC 22 and SRM to SECY-93-087, Item II.Q.

Section 5.2, "Diverse Indication System," of Technical Report APR1400-Z-J-NR-14002-P, Rev. 0, "Diversity and Defense-in-Depth [D3]," states, "The DIS is a single channel of non-safety equipment to meet the requirements of BTP 7-19, Point 4, position on D3 for the safety I&C systems." This section of the TeR states that the DIS is diverse from the QIAS-P and QIAS-N. In addition, this section of the TeR states that the typical DIS variables are listed in Appendix C of this TeR and the display parameters include inadequate core cooling monitoring information, accident monitoring information, and emergency operation-related information. The DIS independently calculates a representative core exit temperature, saturation margins and reactor vessel levels for the display. It also provides the heated junction thermo-couple heater power control function for the reactor vessel level detector as a backup of the QIAS-P calculated function which is potentially lost due to a postulated CCF of the safety I&C systems. The staff reviewed APR1400 FSAR, Tier 1, and could not find any design commitments and corresponding ITAACs to verify that the as-built DIS performs the functions stated in the D3 TeR. The staff also could not find design commitments and corresponding ITAAC to verify that the as-built DIS is diverse and independent from the QIAS-P and QIAS-N to address the SRM to SECY-93-087 and GDC 22. Provide design commitments and ITAACs in Tier 1 of the APR1400 FSAR to verify that the as-built DIS performs these functions and is diverse and independent QIAS-P and QIAS-N to meet the requirements of 10 CFR 52.47(b)(1).

14.03.05-8

Modify the Tier 1 description and the corresponding ITAAC for the QIAS-P 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 requirments 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 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. These lifecycle phases apply to both safety-critical (protection) class software and important-to-safety software. Appendix A of this TeR states that the QIAS-P contains important-to-safety software. APR1400 FSAR, Tier 1, Section 2.5.3.1, Item 5, states "The QIAS-P software is implemented according to the software lifecycle process." However, this Tier 1 section does not describe what this lifecycle process will be (e.g. the different lifecycle phases). The applicant should define the

specific lifecycle phases within this lifecycle process and this information should be consistent with the SPM TeR in order to demonstrate compliance to the requirements of IEEE Std. 603-1991, Clause 5.3. The staff 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 each phase meets the requirements of that phase. Modify Tier 1 of the FSAR, including the ITAAC to resolve these issues.

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 requirments 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.

14.03.05-10

Clarify the criteria for testing functions within APR1400 FSAR Tier 1, Section 2.5.4.1 for the as-built ESF-CCS.

10 CFR 50.55a(h)(3) states, in part, that applications filed on or after May 13, 1999, for design certifications must meet the requirments for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. IEEE Std. 603-1991, Clause 5.7, states, in part, the capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. BTP 7-17 provides guidance on self-test and surveillance test provisions to meet the requirements of IEEE Std. 603-1991, Clause 5.7. 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 2.5.4.1, Item 21, and the corresponding ITAAC states, “The ESF-CCS has the testing functions.” It is not clear to the staff what is meant by the design description, "the testing functions." Specifically, it is not clear whether this design description intends to state that the capability to test and calibrate the ESF-CCS exists or the ESF-CCS system has self-testing functions within it. Further, the design description does not include criteria for the testing features included in the ESF-CCS (e.g. ability to detect faults in a manner that meets the design requirements of the ESF-CCS). Modify the design description and corresponding ITAAC in APR1400 FSAR Tier 1 to address these issues.

14.03.05-11

Modify the APR1400, Tier 1, to provide design descriptions and ITAAC that address communications independence between redundant divisions of the ESF-CCS and between the ESF-CCS and non-safety systems.

10 CFR 50.55a(h)(3) states, in part, that applications filed on or after May 13, 1999, for design certifications must meet the requirments for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. IEEE Std. 603-1991, Clause 5.6, requires independence between redundant portions of safety systems and between safety and non-safety systems. Digital I&C Interim Staff Guidance (ISG) -04 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.

Technical Report APR1400-Z-J-NR-14001, Rev. 0, "Safety I&C System," Section 4.2.4, "System Interfaces," states, “The PPS sends the ESFAS [engineered safety features actuation system] initiation signals to the ESF-CCS GCs [group controllers] in all ESF-CCS divisions through the fiber optic SDL [safety data link].” In addition, Section 4.4.2, "Design Features," of this TeR states “The ESCM [ESF-Soft Control Module] provides the operators with primary manual control means for other safety components as well as ESF components. There is one ESCM per division at each operator console in the MCR [main control room] and RSR [remote shutdown room] and SC [Safety Console] in the MCR. The divisionalized ESCM has access to all ESF safety components within its division. The ESCMs on the

operator consoles work in conjunction with the IPFDs [Information Flat Panel and Display], but the ESCMs on the SC work independently of the IFPDs. DI&C-ISG-04 compliance for communication between the IFPD and ESCM is described in Appendix C.5.1.5." These design descriptions indicate that data communications exist between redundant divisions of ESF-CCS and between the ESF-CCS and non-safety systems. However, the staff could not identify any Tier 1 descriptions or corresponding ITAACs committing to achieve communications independence between these interfaces. As such, the staff requests to modify Tier 1 of the FSAR, including the ITAAC to include this information to verify communication independence in the as-built design. The design commitment and associated ITAAC should include sufficient information regarding the types of data communications faults that the system will be protected from and software features to mitigate these faults.

14.03.05-12

Demonstrate that the inspectability requirements of 10 CFR 52.47(b)(1) are met for standalone safety I&C systems. Specifically, provide Tier 1 design descriptions and corresponding ITAACs to verify that the as-built system meets the design commitments for standalone 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 staff reviewed the Tier 1 descriptions and ITAACs and could not find information regarding the standalone safety I&C systems such as the radiation monitoring system (RMS) and the essential chiller condenser system. Modify Tier 1 of the APR1400 FSAR to include this information.


U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment