KHNPDCDRAIsPEm Resource

From:	Ciocco, Jeff
Sent:	Tuesday, November 17, 2015 12:56 PM
To:	apr1400rai@khnp.co.kr; KHNPDCDRAIsPEm Resource; Harry (Hyun Seung) Chang; Andy Jiyong Oh; Erin Wisler ; Steven Mannon
Cc:	Zhang, Deanna; Jackson, Terry; Ward, William; Lee, Samuel
Subject:	APR1400 Design Certification Application RAI 317-8271 (14.03.05 - Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria)
Attachments:	APR1400 DC RAI 317 ICE1 8271.pdf

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, the following days to respond to the RAI questions. We may adjust the schedule accordingly.

14.03.05-13: 60 days
14.03.05-14: 60 days
14.03.05-15: 60 days
14.03.05-16: 60 days
14.03.05-17: 60 days
14.03.05-18: 45 days
14.03.05-19: 45 days
14.03.05-20: 60 days
14.03.05-21: 30 days
14.03.05-22: 45 days
14.03.05-23: 30 days
14.03.05-24: 90 days
14.03.05-25: 30 days
14.03.05-26: 30 days
14.03.05-27: 45 days
14.03.05-28: 45 days
14.03.05-29: 45 days
14.03.05-30: 90 days
14.03.05-31: 45 days
14.03.05-32: 45 days
14.03.05-33: 45 days

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: 366

Mail Envelope Properties (74d3b0b071114c5682710f2add68ebcc)

Subject: APR1400 Design Certification Application RAI 317-8271 (14.03.05 - Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria)
Sent Date: 11/17/2015 12:56:07 PM
Received Date: 11/17/2015 12:56:10 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
"Andy Jiyong Oh" <jiyong.oh5@gmail.com>
Tracking Status: None
"Erin Wisler " <erin.wisler@aecom.com>
Tracking Status: None
"Steven Mannon" <steven.mannon@aecom.com>
Tracking Status: None

Post Office: HQPWMSMRS07.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	1158	11/17/2015 12:56:10 PM
APR1400 DC RAI 317 ICE1 8271.pdf	148391	
image001.jpg	5040	

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

REQUEST FOR ADDITIONAL INFORMATION 317-8271

Issue Date: 11/17/2015
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

14.03.05-13

Identify the safety functions performed by each safety-related instrumentation and control (I&C) systems in the APR1400 Final Safety Analysis Report (FSAR) Tier 1 descriptions

10 CFR 52.47(b)(1) requires that a design certification application contain the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and should operate in accordance with the design certification, the provisions of the Atomic Energy Act, and the NRC's regulations. NUREG 0800, Standard Review Plan (SRP) Section 14.3, "Inspections, Tests, Analyses, and Acceptance Criteria," (ITAAC) provides guidance on the type of information that should be provided in Tier 1 of the application in order to meet the requirements of 10 CFR 52.47(b)(1), including top-level information that describe the principal performance characteristics and safety functions of the structures, systems and components (SSCs). Based on the description of Tier 1 information included, the staff finds that additional information is needed to demonstrate that safety functions performed by I&C systems are adequately described. Specifically, the staff requests the applicant to include the safety functions performed by each safety-related I&C system in the APR1400 FSAR Tier 1 descriptions.

14.03.05-14

Provide design descriptions and corresponding inspections, tests, analyses, and acceptance criteria (ITAAC) to verify the as-built plant protection system (PPS) is provided with the minimum number and locations of sensors required for protective variables that have spatial dependence.

10 CFR 50.55a(h)(3) states, in part, that an 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 4.6, states that for those variables in Clause 4.4 that have a spatial dependence (that is, where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes shall be identified. The staff could not identify design descriptions and corresponding ITAAC in APR1400 FSAR Tier 1 to verify the as-built PPS is provided with the minimum number and locations of sensors required for protective variables that have spatial dependence to meet the requirements of IEEE Std 603-1991, Clause 4.6. As such, the staff requests the applicant to provide this information in Tier 1 of the APR1400 FSAR.

14.03.05-15

Provide design descriptions and corresponding ITAACs to verify the as-built reactor protection system (RPS) and Engineered Safety Features Actuation System (ESFAS) provide interlocks when associated conditions are met.

10 CFR 50.55a(h)(3) states, in part, that an 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 4.12, requires the identification of any special design basis that may be imposed on the system design (example: diversity, interlocks, regulatory agency criteria). The staff finds the applicant did not provide design descriptions and corresponding ITAACs to verify that the as-built RPS and ESFAS provide interlocks when associated conditions are met in order to meet the requirements of IEEE Std. 603-1991, Clause 4.12. As such, the staff requests the applicant to provide this information in Tier 1 of the APR1400 FSAR.

14.03.05-16

Provide design descriptions and corresponding ITAAC to verify that failures of the PPS that result in lock-up of the PPS and engineered safety feature-component control system (ESF-CCS) processors would be detected (e.g. via watchdog timers) and the PPS and ESF-CCF would fail in a safe state upon these conditions

IEEE Std 603-1991, Clause 5.5, requires the safety system accomplishes its safety functions under the full range of applicable conditions enumerated in the design basis. 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 23, requires the protection system be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy, or postulated adverse environments are experienced. Based on APR1400 FSAR Tier 1, Section 2.5 descriptions, the staff finds additional information is needed to verify that the as-built PPS and ESF-CCF will fail in a safe state upon conditions indicative of PPS or ESF-CCF processor lock-up. As such, the staff requests the applicant provide design descriptions and corresponding ITAAC in APR1400 FSAR Tier 1, Section 2.5 to verify failures within the as-built PPS and ESF-CCS resulting in lock-up of PPS or ESF-CCF processors would be detected (e.g. via watchdog timers) and the PPS and ESF-CCF would be designed to fail in a safe state upon these conditions.

14.03.05-17

Modify APR1400 FSAR Tier 1, Table 2.5.1-5, "Reactor Trip System and Engineered Safety Features Initiation ITAAC," Items 3.b.ii and 3.b.iii to clarify that qualified isolation devices used between interfaces of redundant Class 1E divisions and between safety and non-safety interfaces are Class 1E as required by IEEE Std 603-1991, Clause 5.6. In addition, amend the inspection, test, and analysis (ITA) and the corresponding acceptance criterion to verify that Class 1E qualified isolation devices exist between redundant portions of safety systems and between safety and non-safety systems.

10 CFR 50.55a(h)(3) states, in part, that an 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 5.6.1, requires redundant portions of safety systems provided for a safety function be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. IEEE Std 603-1991, Clause 5.6.3, requires the safety

system design to be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard. IEEE Std. 603-1991, Clause 5.6.3.1, states, in part, “isolation devices used to effect a safety system boundary shall be classified as part of the safety system.”

APR1400, FSAR, Tier 1, Section 2.5.1.1, "Design Description," Item 3.a and the associated ITAAC state “Class 1E equipment identified in Table 2.5.1-1, "Reactor Trip System and Engineered Safety Features Initiation Equipment Location and Classification," is powered from its respective Class 1E train.” 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 non-Class 1E equipment.” The associated acceptance criterion in FSAR Tier 1, Table 2.5.1-5, Item 3.b.ii states, “A report exists and concludes that independence of as-built redundant Class 1E divisions listed in Table 2.5.1-1 and associated field equipment is achieved by independent power sources and electrical circuits for each division, and by fiber optic cable interfaces, qualified isolation devices at interfaces between redundant divisions, and at interfaces between safety and non-safety systems.” The acceptance criterion for Item 3.b.iii states, "A report exists and concludes that the electrical isolation devices prevent credible faults from propagating into a safety system division."

The staff finds that additional information is needed to clarify whether the qualified isolation devices at interfaces between redundant safety divisions and at interfaces between safety and non-safety systems are Class 1E. In addition, it is not clear that an inspection will be performed as part of this ITAAC to verify that Class 1E qualified isolation devices exist between redundant portions of safety systems and between safety and non-safety systems. As such, the staff requests the applicant to modify the FSAR Tier 1, Table 2.5.1-5, Items 3.b.ii and 3.b.iii to clarify that these qualified isolation devices are Class 1E as required by IEEE Std 603-1991, Clause 5.6, and to amend the ITA and acceptance criterion to verify that Class 1E qualified isolation devices exist between redundant portions of safety systems and between safety and non-safety systems.

14.03.05-18

Provide design descriptions and associated ITAAC to verify that the as-built safety I&C system software is only modified via a physical cable disconnect which can physically open the data transmission circuit to protect safety system software from unintended modifications

10 CFR 50.55a(h)(3) states, in part, that an 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 5.6.3 ,requires the safety system design to be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard. Digital I&C (DI&C) Interim Staff Guidance (ISG) DI&C-ISG-04 Revision 1, “Highly-Integrated Control Rooms – Communications Issues (HICRc)” provides guidance for achieving communications independence to meet the requirements of IEEE Std 603-1991, Clause 5.6. Section 1, "Interdivisional Communications," Staff Position 10 of this ISG states a physical cable disconnect, or a keylock, which can physically open the data transmission circuit or interrupt the hardwired logic connection should be provided to protect software from unintended modifications.

Technical Report APR1400-Z-J-NR-14001, Rev. 0, “Safety I&C System,” Appendix C, Section C.5.1.1 describes how software is physically loaded into the processor module (PM) and when physical connections are disconnected. Based on the staff’s review of the information provided in FSAR Tier 1, Section 2.5, the staff could not locate design descriptions or associated ITAAC to verify that the as-built safety I&C system is normally physically disconnected to protect safety system software from unintended

modifications. In addition, clarify that no other means exist to modify safety I&C system software. Modify Tier 1 of the FSAR to include this information.

14.03.05-19

Clarify whether a reactor trip signal and an engineered safety feature (ESF) initiation signal are automatically initiated for each trip condition listed in APR1400 FSAR Tier 1, Table 2.5.1-2, "Reactor Trip System Variables," and initiation condition listed in FSAR Tier 1, Table 2.5.1-3, "Engineered Safety Features Initiation Variables," respectively.

10 CFR 50.55a(h)(3) states, in part, that an 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 6.1, "Automatic Control," states, in part, that “Means shall be provided to automatically initiate and control all protective actions except as justified in [Clause] 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in [Clause] 4.5 following the onset of each design basis event. APR1400 FSAR Tier 1, Section 2.5.1.1, Item 4a states “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.” The associated acceptance criterion for this design commitment states, “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.”

Based the design commitment and associated ITAAC presented, it is not clear whether a reactor trip signal and an ESF actuation signal are automatically initiated for each trip condition listed in FSAR Tier 1 Table 2.5.1-2 and initiation condition listed in FSAR Tier 1, Table 2.5.1-3, respectively. As such, the staff requests the applicant to clarify this information in the FSAR Tier 1, Section 2.5.1.1, Item 4a, and the corresponding ITAAC in order to demonstrate that the as-built system meets the requirements of IEEE Std 603-1991, Clause 6.1.

14.03.05-20

Demonstrate that the response time for the RT and ESF actuation functions are adequately verified in the as-built RTS and ESFAS.

10 CFR 50.55a(h)(3) states, in part, that an 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 4.10, requires the identification of critical points in time or the plant conditions, after the onset of a design basis event. APR1400 FSAR Tier 1, Section 2.5.1.1, Item 16 states that “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.” The acceptance criterion for the corresponding ITAAC in FSAR Tier 1, Table 2.5.1-5, Item 16a states, “A report exists and concludes that the PPS initiates the RT and the ESF initiation signals identified in Tables 2.5.1-2 and 2.5.1-3 within the response time requirements as described in the design basis.” In addition, the acceptance criterion in FSAR Tier 1, Table 2.5.1-5, Item 16b, states, “The as-built RTS and ESF initiation signals identified as monitored variables in Tables 2.5.1-2 and 2.5.1-3 with response time requirements are bounded by the test.” APR1400 FSAR Tier 1, Section 2.5.4.1, Item 20 states, “The ESF-CCS provides ESF actuation within required response time for ESF functions identified in Table 2.5.4-2 ["Functions Automatically Actuated by the ESF-CCS"] .” The acceptance criterion in the corresponding

ITAAC in FSAR Tier 1, Table 2.5.4-4, [ESF-CCS ITAAC] Item 20a, states, “A report exists and concludes that the ESF-CCS actuates the ESF functions identified in Table 2.5.4-2, within the response time requirements.” The acceptance criterion in the corresponding ITAAC in FSAR Tier 1, Table 2.5.4-4, Item 20b, states, “The as-built ESF actuation function identified in Table 2.5.4-2 with response time requirements are bounded by type tests or a combination of a type test and analysis."

Based on the design commitment and the associated ITAAC provided, it is not clear to the staff where the response time will be measured from (e.g. from output of sensors to the RTSS breakers and the output of the component interface module (CIM)). The staff requests the applicant to clarify where the response time will be measured from in order to verify this design commitment. In addition, it is not clear whether there is sufficient overlap coverage between FSAR Tier 1, Table 2.5.1-5, Item 16, and FSAR Tier 1, Table 2.5.4-4, Item 20, to cover the entire ESFAS actuation path. Specifically, it is unclear where the data communication links between the ESFAS portion of the PPS to the input of the ESF-CCS are included in these two response time verification ITAACs. As such, the staff requests the applicant to modify these ITAACs to demonstrate full coverage of the ESFAS actuation path.

14.03.05-21

Provide design information in APR1400 FSAR, Tier 2 to support the design commitment in APR1400 FSAR, Tier 1, Section 2.5.1.1, Item 23.

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.” APR1400 FSAR Tier 1, Section 2.5.1.1, Item 23, states that two sets of reactor trip switchgear system (RTSS) which consist of four reactor trip switchgear (RTSG)s are diverse [from] each other. The acceptance criterion for the corresponding ITAAC identified in APR1400 FSAR Tier 1, Table 2.5.1-5, Item 23, states, "Two sets of the as-built RTSS which consists of four RTSGs are diverse [from] each other: One set of RTSGs is supplied from a different manufacturer than the other set of RTSGs." APR1400 FSAR Tier 2, Section 7.2.1.9, states that for additional diversity, the RTSS consists of one set of four RTSGs (RTSS 1) and another set of four RTSGs (RTSS 2) with diverse design features. However, this section does not provide description of the attributes that make the design diverse (e.g. RTSGs supplied by different manufacturer). As such, the staff requests the applicant to provide descriptions of the attributes that make the design diverse in APR1400 FSAR Tier 2 to support the design descriptions in APR1400 FSAR Tier 1. Further, the staff requests the applicant to define the acronym “RTSG” as it is not defined in Tier 1 of this application.

14.03.05-22

Clarify how the requirements of 10 CFR Part 50, Appendix A, GDC 19 regarding the provision of equipment outside the control room to shutdown the reactor are verified in the as-built design.

GDC 19 states, in part, “A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents…Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and

(2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures."

The following design descriptions and corresponding ITAAC were provided in APR1400 FSAR Tier 1:

- Section 2.5.1.1, Item 8, and the corresponding design commitment in FSAR Tier 1, Table 2.5.1-5, Item 8, state, "Each PPS division is controlled from either the MCR [(main control room)] or RSR [(remote shutdown room)], as selected from MCR/RSR master transfer switches." The ITA of this ITAAC states, "A test of the as-built PPS will be performed to demonstrate the transfer function between the MCR and RSR." The acceptance criteria for this ITAAC states, "The as-built master transfer switches transfer controls between the MCR and RSR separately for each as-built PPS division, as follows: [1] Controls at the RSR are disabled when controls are active in the MCR. [2] Controls at the MCR are disabled when controls are active in the RSR."

- Section 2.5.4.1, Item 8 and the corresponding design commitment in FSAR Tier 1, Table 2.5.4-4, Item 8, state, "Each ESF-CCS division is controlled from either the MCR or RSR, as selected from MCR/RSR master transfer switches." The ITA of this ITAAC states, "A test of the as-built system for one control within each ESF-CCS division will be performed to demonstrate the transfer of control capability between the MCR and RSR." The acceptance criteria for this ITAAC states, "The as-built master transfer switches transfer controls between the MCR and RSR separately for each as-built ESF-CCS division, as follows: [1] Controls at the RSR are disabled when controls are active in the MCR. [2] Controls at the MCR are disabled when controls are active in the RSR."

- APR1400 FSAR Tier 1, Section 2.5.5.1, Item 3, and the corresponding design commitment in FSAR Tier 1, Table 2.5.5-2, Item 3, state, "The PCS [(power control system)] and P-CCS [(process-component control system)] are controlled from either the MCR or RSR, as selected from master transfer switches." The ITA of this ITAAC states, "A test of the as-built system will be performed to demonstrate the transfer of control capability between the MCR and RSR." The acceptance criteria for this ITAAC states, "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: [1] Controls at the RSR are disabled when controls are active in the MCR for the as-built PCS and P-CCS. [2] Controls at the MCR are disabled when controls are active in the RSR for the as-built PCS and P-CCS."

Based on the above descriptions, it is unclear whether this ITAAC is intended to verify that the RSR will have controls for the PPS, ESF-CCS, PCS and P-CCS to meet the requirements of the GDC 19 since the design description and corresponding ITAAC only focuses on verifying the operation of the transfer switch. As such, the staff requests the applicant to provide design descriptions and corresponding ITAACs to verify that the as-built RSR contain sufficient controls to meet the requirements of GDC 19.

14.03.05-23

Clarify how verification of adequate physical separation and electrical independence of the as-built Qualified Information and Alarm System-Safety (QIAS-P) are achieved as required by the IEEE Std 603-1991, Clause 5.6.

10 CFR 50.55a(h)(3) states, in part, that an 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 5.6.1, requires redundant portions of safety systems provided for a safety function be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any

design basis event requiring that safety function. IEEE Std 603-1991, Clause 5.6.3, requires that the safety system design to be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard. IEEE Std. 603-1991, Clause 5.6.3.1, states, in part, “Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.”

APR1400 FSAR Tier 1, Section 2.5.3.1, Item 3.b, states that the Class 1E equipment identified in Table 2.5.3-1, and associated equipment are physically separated and electrically independent from each other and physically separated and electrically independent from non-Class 1E equipment. APR1400 FSAR Tier 1, Table 2.5.3-1, lists QIAS-P Processors for Divisions A and B, and QIAS-P Flat Panel Display (FPD), Division A and B. It is not clear, based on the design commitment, which equipment within Table 2.5.3-1 will be physically separated and electrically independent from one another (e.g. whether redundant divisions of QIAS-P equipment listed in Table 2.5.3-1 are physically separated and electrically independent from each other). In addition, the acceptance criterion provided for the corresponding ITAAC in APR1400 FSAR, Table 2.5.3-3, Item 3.b.i states, “the physical separation of as-built redundant Class 1E equipment identified in Table 2.5.3-1 and associated field equipment is provided by distance or barriers.” The staff finds that this acceptance criterion does not provide criteria for the amount of distance or barrier that would be adequate to meet the physical separation requirements of IEEE Std 603-1991, Clause 5.6. The acceptance criteria for verifying that physical separation requirements are met for the PPS and the ESF-CCS references RG 1.75 as the guidance for demonstrating that the provided distance or barriers is acceptable. In addition, this acceptance criterion also does not address physical separation of QIAS-P equipment from non-Class 1E equipment. The acceptance criterion provided for the ITAAC in APR1400 FSAR, Table 2.5.3-3, Item 3.b.ii states, “a report exists and concludes that independence of as-built redundant Class 1E equipment identified in Table 2.5.3-1, and associated field equipment is achieved by independent power sources and electrical circuits for each channel, and by fiber optic cable interfaces, conventional isolators, or other proven isolation methods or devices at interfaces between redundant divisions, and at interfaces between safety and non-safety systems.” It is not clear to the staff what is meant by “conventional” isolators, or other “proven” isolation methods or devices. Specifically, are these “conventional” isolators, or other “proven” isolation methods or devices Class 1E qualified as required by IEEE Std 603-1991, Clause 5.6.3. As such, the staff requests the applicant to provide the following:

1. Clarify whether the design commitment in APR1400 FSAR Tier 1, Section 2.5.3.1, Item 3.b are intended to address physical separation and electrical isolation requirements for redundant divisions of safety equipment identified in APR1400 FSAR Tier 1, Table 2.5.3-1.

2. Provide criteria for determining what amount of distance or barrier (e.g. in accordance with RG 1.75, "Physical Independence of Electrical Systems") is adequate to meet the physical separation requirements of IEEE Std 603-1991, Clause 5.6.

3. Amend the acceptance criteria for physical separation to address physical separation of QIAS-P equipment from non-Class 1E equipment.

4. Clarify whether the conventional isolators, or other prevent isolation methods or devices used will be qualified as Class 1E isolation devices.

14.03.05-24

Provide design descriptions and corresponding ITAAC to address Type A variables.

10 CFR 50.55a(h)(3) states, in part, that an 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 5.8.1, states that the display instrumentation

provided for manually controlled actions for which no automatic control is provided and the display instrumentation required for the safety systems to accomplish their safety functions shall be part of the safety systems."

In RAI 38-7878, Question 07.05-1, the staff requested the applicant to justify why Type A variables are not required for this design when it appears that manually controlled actions were credited for cases where no automatic controls exist during several events analyzed in Chapter 15. As such, if the applicant determines that Type A variables are needed in response to this RAI, the staff requests the applicant to provide design descriptions and a corresponding ITAAC to verify that the as-built design provides indications for manually controlled actions for which no automatic control is provided as required by IEEE Std 603 1991, Clause 5.8.1.

14.03.05-25

Demonstrate how control of access features are verified in the as-built QIAS-P.

10 CFR 50.55a(h)(3) states, in part, that an 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 5.9, states "The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof." The staff could not identify any design descriptions or corresponding ITAACs to verify that the control of access features exist for the QIAS-P equipment identified in APR1400 FSAR Tier 1, Table 2.5.3-1 (e.g. cabinet keylocks). As such, the staff request the applicant to clarify whether any control of access features are employed to prevent unauthorized or unintended access of QIAS-P equipment identified in APR1400 FSAR Tier 1. If such features exists, the staff requests the applicant to provide an ITAAC that verify that these control of access features exist for the as-built QIAS-P equipment identified in APR1400 FSAR Tier 1. Otherwise, the staff requests the applicant to justify why such features are not required.

14.03.05-26

Provide design descriptions and a corresponding ITAAC to verify that the as-built QIAS-P equipment are distinctly identified for each redundant portion of the QIAS-P.

10 CFR 50.55a(h)(3) states, in part, that an 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 5.11, requires, in part that safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1981 and IEEE Std 420-1982. The staff could not identify any design descriptions or corresponding ITAACs to verify that the as-built QIAS-P equipment are distinctly identified for each redundant portion of the QIAS-P to meet the requirements of IEEE Std 603-1991, Clause 5.11. As such, the staff requests the applicant to provide design descriptions and a corresponding ITAAC to verify that the as-built QIAS-P equipment are distinctly identified for each redundant portion of the QIAS-P.

14.03.05-27

Provide design descriptions and ITAACs to verify that the as-built ESF-CCS meets completion of protection requirements for all ESFAS functions.

10 CFR 50.55a(h)(3) states, in part, that an 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 5.2, states that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. APR1400 FSAR Tier 1, Section 2.5.4.1, Item 9, and the corresponding ITAAC states "Once a BOP [(Balance of Power)] ESF actuation has been actuated (automatically or manually), the ESF actuation logic is latched in the actuated state and is not reset automatically." The corresponding ITAAC in FSAR Tier 1, Table 2.5.4-4, Item 9, verifies this design commitment in the as-built ESF-CCS. This ITAAC verifies that the as-built ESF-CCS meet completion of protective action requirements for BOP ESF functions. However, the staff could not find design descriptions and corresponding ITAACs to verify the as-built ESF-CCS meets completion of protection requirements for other ESFAS functions (e.g. nuclear steam supply system (NSSS) ESF actuation functions identified in FSAR Tier 1, Table 2.5.4-2). As such, the staff requests the applicant to provide design descriptions and ITAACs to verify that the as-built ESF-CCS meets completion of protection requirements for these other ESFAS functions.

14.03.05-28

Clarify how verification of adequate electrical independence of the as-built ESF-CCF is achieved as required by the IEEE Std 603-1991, Clause 5.6.

10 CFR 50.55a(h)(3) states, in part, that an 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 5.6.1, requires redundant portions of safety systems provided for a safety function be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. IEEE Std 603-1991, Clause 5.6.3, requires the safety system design to be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard. IEEE Std. 603-1991, Clause 5.6.3.1 states, in part, "Isolation devices used to effect a safety system boundary shall be classified as part of the safety system."

APR1400 FSAR Tier 1, Section 2.5.4.1, Item 2 states that redundant Class 1E divisions listed in Table 2.5.4-1 and associated field equipment are physically separated and electrically isolated from each other and physically separated and electrically isolated from non-Class 1E equipment. The associated acceptance criteria in FSAR Tier 1, Table 2.5.4-4, Items 2.b and 2.c, state "A report exists and concludes that independence of as-built redundant Class 1E divisions listed in Table 2.5.4-1 and associated field equipment is achieved by independent power sources and electrical circuits for each division, and by fiber optic cable interfaces, qualified isolation devices at interfaces between redundant divisions, and at interfaces between safety and non-safety systems." The staff finds that additional information is needed to clarify whether the qualified isolation devices at interfaces between redundant safety divisions and at interfaces between safety and non-safety systems are Class 1E qualified. In addition, it is not clear whether an inspection will be performed to verify that that Class 1E qualified isolation devices exist between redundant portions of safety systems and between safety and non-safety systems in the as-built ESF-CCS. As such, the staff requests the applicant to modify the FSAR Tier 1, Table 2.5.4-4, Item 2 to clarify that these qualified isolation devices are Class 1E qualified as required by IEEE Std 603-1991,

Clause 5.6.3.1, and to verify via inspection that Class 1E qualified isolation devices exist between redundant portions of safety systems and between safety and non-safety systems.

14.03.05-29

Provide design descriptions and a corresponding ITAAC in APR1400 FSAR Tier 1, Section 2.5.4 to verify the priority scheme of demands from the manual controls and automatic safety system at the ESF-CCF loop controllers (LC).

10 CFR 50.55a(h)(3) states, in part, that an 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 5.6.1, requires redundant portions of safety systems provided for a safety function be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. IEEE Std 603-1991, Clause 5.6.3, requires that the safety system design to be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard. DI&C-ISG-04, Section 2, “Command Prioritization” provides guidance on use of priority modules in safety I&C systems. Position 3 of this section states, “Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a Common-Cause Failure in the primary system that erroneously forces the plant equipment to a state that is different from the designated “safe state.”), and which do not directly support any safety function, have lower priority and may be overridden by other commands.…The priority module itself should be shown to apply the commands correctly in order of their priority rankings, and should meet all other applicable guidance.”

APR1400 FSAR Tier 1, Section 2.5.4.1, Item 13, and the corresponding ITAAC in FSAR Tier 1, Table 2.5.4-4, Item 13 state, “The component interface module (CIM) provides state-based priority logic to prioritize the ESF-CCS and DPS signals.” APR1400 FSAR Tier 1, Section 2.5.4.1, Item 14 and the corresponding ITAAC in FSAR Tier 1, Table 2.5.4-4, Item 14 state “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.” The APR1400 FSAR appears to provide adequate design descriptions and corresponding ITAAC to verify the priority scheme of the as-built CIM to meet the requirements of 10 CFR 52.47(b)(1).

However, the staff could not find any design descriptions or corresponding ITAAC to verify the priority scheme of the ESF-CCS for commands originating from the automatic safety system and the manual controls from the ESF-CCF soft control module (ESCM) and Information Flat Panel Display (IFPD). Technical Report APR1400-Z-J-NR-14001, Rev. 0, "Safety I&C System Technical Report," Section 4.4.2 states, “The priority interlock in the LC [loop controller] is used to [withheld as proprietary]. The ESF actuation signals from the GC [(Group controller] [withheld as proprietary.]” As such, the staff requests the applicant to provide design descriptions and corresponding ITAAC to verify this design feature.

14.03.05-30

Provide design descriptions and a corresponding ITAAC to verify means are provided for manual initiation and control of the protective actions that have not been selected for automatic control.

10 CFR 50.55a(h)(3) states, in part, that an 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 6.2.2, states “Means shall be provided in the control room to implement manual initiation and control of the protective actions identified in [Clause] 4.5 that have not been selected for automatic control under 6.1. The displays provided for these actions shall meet the requirements of [Clause] 5.8.1." In RAI 38-7878, Question 07.05-1, the staff requested the applicant to justify why Type A variables are not required for this design when it appears that manually controlled actions were credited for cases where no automatic controls exist during several events analyzed in Chapter 15. As such, if the applicant determines that Type A variables are needed in response to this RAI, the staff requests the applicant to provide design descriptions and a corresponding ITAAC to verify means are provided for manual initiation and control of the protective actions that have not been selected for automatic control as required by IEEE Std 603-1991, Clause 6.2.2.

14.03.05-31

Resolve discrepancies in terminology used between APR1400 FSAR Tier 1, Tier 2, and referenced documents, and provide additional information in Tier 2 to support the Tier 1 descriptions regarding the platforms used for the PCS and P-CCS

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. APR1400 FSAR Tier 1, Section 2.5.5.1, Item 2, and the corresponding design commitment in FSAR Tier 1, Table 2.5.5-1, Item 2 state, “The digital equipment and software used in the PCS and P-CCS are independent from those of the [PPS] and the [ESF-CCS].” The acceptance criteria for this ITAAC will verify that the 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. APR1400 FSAR Tier 2, Section 7.7.1.1, "Control Systems," states that the control systems are implemented on a digital platform that is diverse in both hardware and software from the safety common platform. Section 4.1 of Technical Report APR1400-Z-J-NR-14002-P, Rev. 0, "Diversity and Defense-in-Depth” states, “The plant-wide data networks are composed of safety networks and non-safety networks. The safety network is independent and diverse from the non-safety network. The non-safety network utilizes different communication hardware, software and communication protocol from the safety network.” Section 6.1.2 (under "Diversity") of this technical report states, “In addition, to correspond with the hardware diversity of these fluid/mechanical systems, the APR1400 employs both hardware and software diversity between control and protection I&C systems to eliminate the potential for CCFs.” The staff could not find discussion of how the plant control system platform are diverse from the safety common platform in APR1400 FSAR Tier 2 or its referenced documents. In addition, APR1400 FSAR Tier 2 does not use the term “independent” (which is used in APR1400 FSAR Tier 1) when discussing the differences between platform and software used for the control system and the platform and software used for the PPS and ESF-CCS. As such, the staff requests the applicant to resolve this discrepancy in terminology, and provide additional information in Tier 2 to support the Tier 1 descriptions regarding the platforms used for the PCS and P-CCS.

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."

14.03.05-33

Modify the use of the term "ESF Initiation" to reflect the intent to reference a portion of the ESFAS.

10 CFR 52.47(a)(2) requires, in part, for the applicant to provide a description and analysis of the structures, systems, and components (SSCs) of the facility, with emphasis upon performance requirements, the bases, with technical justification therefor, upon which these requirements have been established, and the evaluations required to show that safety functions will be accomplished. It is expected that the standard plant will reflect through its design, construction, and operation an extremely low probability for accidents that could result in the release of significant quantities of radioactive fission products. The description shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. APR1400 FSAR Tier 1, Section 2.5.1.1 states that the ESF initiation is performed in sensors, the auxiliary processing cabinet-safety (APC-S) and the ESFAS portion of the PPS cabinets. It appears that the term "ESF initiation" is used to reference a portion of the ESFAS from sensors to the output of the PPS. However, the term “initiation” typically refers to a function and not a system. As such, the staff requests the applicant to modify the use of this term to reflect the intent of referencing a portion of the ESFAS.


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