KHNPDCDRAIsPEm Resource

From: Ciocco, Jeff
Sent: Tuesday, October 27, 2015 8:06 AM
To: apr1400rai@khnp.co.kr; KHNPDCDRAIsPEm Resource; Harry (Hyun Seung) Chang; Andy Jiyong Oh; Erin Wisler
Cc: Zhang, Deanna; Jackson, Terry; Ward, William; Lee, Samuel
Subject: APR1400 Design Certification Application RAI 274-8277 (07.01 - Instrumentation and Controls - Introduction)
Attachments: APR1400 DC RAI 274 ICE1 8277.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 response time for the RAI questions. We may adjust the schedule accordingly.

07.01-34: 60 days
07.01-35: 45 days
07.01-36: 45 days
07.01-37: 45 days
07.01-38: 45 days
07.01-39: 45 days
07.01-40: 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: 321

Mail Envelope Properties (9d11f6693b514ffbb29b2af8035fe02b)

Subject: APR1400 Design Certification Application RAI 274-8277 (07.01 - Instrumentation and Controls - Introduction)
Sent Date: 10/27/2015 8:06:00 AM
Received Date: 10/27/2015 8:06:02 AM
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

Post Office: HQPWMSMRS07.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	791	10/27/2015 8:06:02 AM
APR1400 DC RAI 274 ICE1 8277.pdf	120228	
image001.jpg	5040	

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

REQUEST FOR ADDITIONAL INFORMATION 274-8277

Issue Date: 10/27/2015
Application Title: APR1400 Design Certification Review – 52-046
Operating Company: Korea Hydro & Nuclear Power Co. Ltd.
Docket No. 52-046
Review Section: 07.01 - Instrumentation and Controls - Introduction
Application Section: Section 7.1, 7.3, and 10.2

QUESTIONS

07.01-34

Provide additional descriptions and clarifications to the response to RAI 43-7887, Question 07.01-18 to demonstrate how the safety-related portion of the radiation monitoring system (RMS) meets the independence requirements and quality requirements of IEEE Std 603-1991.

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. Clause 5.3, "Quality," of IEEE Std. 603-1991 requires 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 pre-scribed quality assurance program. 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.”

In RAI 43-7887, Question 07.01-18, the staff requested for the applicant to demonstrate how standalone system, such as the safety-related portion of the Radiation Monitoring System (RMS) meet the requirements of IEEE Std 603-1991. In the response to this RAI, the applicant states that the RMS consists of two channels, the Safety Related Divisionalized Cabinet (SRDC) and the non-safety related RMS computer cabinet, as shown in Figure 7.3-23. The safety portion of the RMS consists of the radiation element, the local unit, and the SRDC. The divisional SRDC transmits the engineered safety feature actuation system (ESFAS) initiation signals to the dedicated ESFAS measurement channels, as described in Subsection 7.3.1.1. The safety portion of the RMS is part of the engineered safety feature (ESF) system as described in the Subsection 7.1.1.3. Therefore, the safety portion of the RMS is a part of ESF system and designed to comply with ESF System applicable criteria in the APR1400 FSAR Tier 2, Table 7.1-1, “Regulatory Requirements Applicability Matrix.” The ESF system, including the safety portion of the RMS, complies with the requirements of IEEE Std 603-1991, Clauses 5.1, 5.3, 5.5, and 5.6, as described in Subsection 7.3.3.2, is addressed in the Appendix A, “Conformance to IEEE Std 603-1991” of Technical Report, APR1400-Z-J-NR-14001, Rev. 0 “Safety I&C System." Based on the staff’s review of APR1400 FSAR Tier 2, Sections 7.3.1.1 and 7.1.1.3, and Appendix A of the Safety I&C System Technical Report, the staff finds that additional information is needed to clarify the design description of the RMS as described below:

a. APR1400 FSAR Tier 2, Section 7.3.1.1, states the balance of plant (BOP) ESFAS receives process variable signals from the safety portion of the RMS, manual ESF system-level actuation switches, and manual channel bypass switches. The BOP ESFAS consists of 1-out-of-2 logic taken twice except for the Fuel handling area emergency ventilation actuation signal (FHEVAS), which has one 1-out-of-2 logic. APR1400 FSAR Tier 2, Figure 7.3-23, shows the RMS measurement channel functional diagram, but design descriptions or reference to this figure were not provided in FSAR Tier 2, Section 7.3. Based on this figure, it is not clear how many divisions are in the RMS SRDC. In addition, it is not clear whether the RMS computer cabinet is safety-related or non-safety. If the RMS processor in the computer

cabinet is non-safety, then how is it isolated from the SRDC processor to meet the independence requirements of IEEE Std. 603-1991, Clause 5.6.3? If the RMS processor is safety-related, how is it meeting independence requirements of IEEE Std. 603-1991, Clause 5.6.3 when transmitting information to the IPS and QIAS-N?

b. Appendix A of the Safety I&C System Technical Report, Section A.5.3, "Quality," states the platform to be used for the safety I&C system is qualified as described in WCAP-16097-P-A, “Common Qualified Platform Topical Report”, Rev. 3, February 2013. However, APR1400 FSAR Tier 2, Section 7.1 under "Safety Systems," states the safety-related portion of the RMS is implemented on an independent platform that is different from the Common Q platform. Further, Technical Report APR1400-Z-J-NR-14003, Rev. 0, “Software Program Manual,” does not appear to address standalone safety-related systems such as the RMS. As such, it is unclear how the requirements of IEEE Std 603-1991, Clause 5.3, are met for the safety-related portion of the RMS.

c. Clarify in the APR1400 FSAR that the RMS is the only standalone safety-related I&C system.

07.01-35

Provide additional clarification to the response for RAI 43-7887, Question 07.01-19 (ML15224B643), to demonstrate how the turbine generator (TG) I&C system interfaces with the safety I&C system to meet the independence requirements of IEEE Std 603-1991, Clause 5.6.3.

IEEE Std 603-1991, Clause 5.6.3, "[Independence] Between Safety Systems and Other Systems," 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.” In RAI 43-7887, Question 07.01-19, the staff requested the applicant to provide information on the design of the TG I&C system interfaces with the safety-related I&C systems to meet the requirements of IEEE Std. 603, Clause 5.6.3. In response to this RAI, the applicant stated the turbine control system (TCS) interfaces with the plant protection system (PPS) in the safety I&C systems for the turbine trip function on reactor trip. APR1400 DCD, Tier 2, Subsection 7.2.1.4, "Reactor Trip Initiation Signals," Item l, "Turbine trip," and Figure 7.2-14, "[PPS] Interface Logic Diagram for Division D," provide information about the turbine trip function and functional logic. The PPS transmits the turbine trip signal via hardwired connection to the TCS when the reactor trip initiation signal is generated as indicated on the right side of Figure 7.2-14. APR1400 non-safety, standalone I&C systems include the TCS, seismic monitoring system (SMS), vibration monitoring system (VMS), NSSS integrity monitoring system (NIMS), and fixed in-core detector amplification system (FIDAS). This response includes a table (Table 07.01-19-1, "Interface Summary") that summarizes the interfaces between the non-safety standalone I&C systems with safety I&C systems. In addition, this response states that that the PPS and excore neutron flux monitoring system (ENFMS) do not receive any signals from non-safety systems but only send signals to non-safety systems. Electrical isolation is provided in the PPS and ENFMS through isolation devices.

Based on the response to RAI 43-7887, Question 07.01-19, the staff requests the following additional information to determine whether the requirements of IEEE Std 603-1991, Clause 5.6.3, have been met for the interfaces between safety and standalone non-safety systems:

1. Include in the APR1400 FSAR the description from the RAI response regarding the interface between safety-related I&C systems and non-safety standalone system. This includes the statement that the PPS and ENFMS do not receive any signals from non-safety systems but only send signals to non-safety systems. The applicant stated that electrical isolation is provided in the PPS and ENFMS through isolation devices. The applicant should include in the APR1400

FSAR a clarification on whether these isolation devices are Class 1E qualified. In addition, include the information from Table 07.01-19-1 of this RAI response into the APR1400 FSAR.

2. APR1400 FSAR Tier 2, Figure 7.2-14, only shows the PPS system interface logic diagram for Division D. It is unclear to the staff whether the interfaces depicted in this figure also apply to the other three PPS divisions. Clarify in the APR1400 FSAR whether this figure applies to the other PPS divisions. If there are differences between these interfaces for different divisions, provide a description of the differences in the APR1400 FSAR.

3. APR1400 FSAR Tier 2, Section 10.2.2.3.3, states that each trip input is applied to a triple redundant protection module, where 2-out-of-3 majority voting is conducted within the protection system where possible to prevent spurious turbine trips and enhance protection system operation on an actual turbine trip. The turbine includes instrumentation for a trip on excess vibration and a remote trip input signal from the plant control system on a reactor trip. Since there are four divisions of PPS, and the turbine protection system only has triple redundancy, how does each PPS division interface with the turbine protection system to produce a turbine trip? Provide this information in the APR1400 FSAR.

07.01-36

Incorporate by reference specific technical and topical reports referenced in the APR1400 FSAR.

10 CFR 52.47(a)(2) requires, in part, 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.

The submittal letter by Korea Electric Power Corporation and Korea Hydro & Nuclear Power Co., Ltd for the application for design certification of the APR1400 Standard Design, dated December 23, 2014 (ML15006A037), provides a list of technical reports that contain analyses and other information that supplement the materials included in the DCD, with certain technical reports shown as incorporated by reference. APR1400 FSAR, Tier 2, Tables 1.6-1, "List of Topical Reports," and 1.6-2, "List of Technical Reports," provide a list of topical and technical reports. However, these two lists in the APR1400 FSAR do not correspond to the list provided in the APR1400 design certification submittal letter. Further, APR1400 FSAR, Tier 2, Tables 1.6-1 and 1.6-2, do not indicate which of the technical or topical reports are incoporated by referenced. As such, the staff requests the applicant to ensure that these two lists are consistent and to indicate which technical or topical reports are incoporated by referenced in APR1400 FSAR, Tier 2, Tables 1.6-1 and 1.6-2. In addition, the staff requests the applicant to incorporate by reference additional technical and topical reports currently not listed as IBRed in the APR1400 design certification submittal letter. Specifically, APR1400 FSAR, Tier 2 Chapter 7 references several technical and topical reports that the staff uses to as bases in their safety evaluation. These reports include:

- APR1400-A-J-NR-14003, “APR1400 Disposition of Common Q Topical Report NRC Generic Open Items and Plant Specific Action Items”
- APR1400-A-J-NR-14004, “Common Q Platform Supplemental Information in Support of APR1400 Design Certification”
- APR1400-E-J-NR-14001, “Component Interface Module”
- APR1400-F-C-NR-14003, “Functional design Requirements for a Core Protection Calculator System for APR1400”

- APR1400-Z-A-NR-14019, “CCF [(Common Cause Failure)] Coping Analysis”
- APR1400-Z-J-NR-14002, “Diversity and Defense-in-Depth”
- APR1400-Z-J-NR-14012, “Control System CCF Analysis”
- APR1400-Z-J-NR-14013, “Response Time Analysis of Safety I&C System”
- WCAP-10697-P-A, Revision 3, “Common Qualified Platform Topical Report”

The staff requests these technical and topical reports be incorporated by reference in APR1400 FSAR Tier 2, Tables 1.6-1 and 1.6-2.

07.01-37

Clarify how the Core Protection Calculator System (CPCS) responds to failures in order to meet the requirements of 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 23.

GDC 23 requires the protection system to 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 (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced. Section C.5.1.3.7, “DI&C-ISG-04 Staff Positions,” of Technical Report APR1400-Z-J-NR-14001, Revision 0, “Safety I&C System”, last paragraph at the bottom of page C24 discusses reed switch position transmitter (RSPT)1 and RSPT2 failure, penalty factors (PF) and plant trips.

Based on the staff’s review of the CPCS, the staff requests the applicant to clarify the following:

1) During normal plant operation, explain how the predetermined control element assembly (CEA) PF value provides assurance that it will be a PF value that is an accurate representation of the actual core CEA PF.

2) Discuss why, after sensing that both RPST1 and RSPT2 signals have failed, the safety system would not automatically place the affected channel(s) in trip. By not placing the affected channel in trip how are the requirements of GDC 23 met?

3) Discuss why, after sensing that both CEAC1 and CEAC2 are inoperable, the safety system would not automatically place the affected channel(s) in trip. By not placing the affected channel in trip how are the requirements of GDC 23 met?

The staff requests the applicant to include this clarification in the APR1400 FSAR or its referenced documents.

07.01-38

Define terminology used when discussing the CPCS and ensure the consistency of these terms among the APR1400 FSAR sections and the referenced documents.

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. Clause 5.1 of IEEE Std. 603-1991 states, in part, “The safety systems shall perform all safety functions required for a DBE in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused

by the single failure; and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions.

APR1400 FSAR Tier 2, Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System," No. 2-12 a), states “Affected CPC uses the last valid PF from the failed CEAC or the current PF from the operable CEAC, whichever is larger.” However, Technical Report (TeR) APR1400-F-C-NR-14003, Rev. 0, “Functional Design Requirements for CPCS,” Section 4.2.4 uses the term “last good” DNBR and LPD PFs. It is not clear to the staff whether these terms refer to the same PF. It is also not clear to the staff what is meant by “last good” or “last valid” PF. In addition, the Functional Design Requirements for CPCS TeR refers to DNBR and LPD PFs from the CEAC which is not used in the APR1400 FSAR or other referenced document. For example, the TeR APR1400-Z-J-NR-14001, “Safety I&C System” states that the CEAC processor module calculates the magnitude of CEA deviation PFs and does not refer to the DNBR and LPD PFs. Further APR1400 FSAR Tier 2, Table 7.2-7, No. 2-12 a), states, “If the other CEAC is failed/declared inoperable/or in test, a large pre-assigned PF is assumed in that CPC.” While the Functional Design Requirements for CPCS TeR, Section 4.2.4 states, “Both CEACs are considered inoperable. Use the pre-determined DNBR and LPD penalty factors...” It is not clear to the staff whether the terms “pre-assigned” and “pre-determined” have the same meaning. Definitions were also not provided for these terms. As such, the staff requests the applicant to review the design descriptions of the CPCS in the APR1400 FSAR and its referenced documents to ensure consistency of the terminology used and to provide definitions for terms used.

07.01-39

Describe what happens to the output of safety-related I&C system processors when the processor is declared inoperable.

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. Clause 5.1, "Single-Failure Criterion," of IEEE Std. 603-1991 states, in part, “The safety systems shall perform all safety functions required for a [DBE] in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the [DBE] requiring the safety functions."

AR1400 FSAR Tier 2, Table 7.2-7 provides the system level failure modes and effects analysis (FMEA) for the PPS. For several of the entries in this table, the applicant states that the effect on the PPS will be the respective safety-related I&C system processor (e.g. CEAC) is declared inoperable. The staff could not find a description of what happens to the output of this processor (e.g. forced to a predefined value of 0 or 1) when it is declared inoperable per technical specification. As such, the staff requests the applicant to modify the APR1400 FSAR to describe what happens to the output of safety-related I&C system processors when the processor is declared inoperable.

07.01-40

Clarify the terms used in APR1400 FSAR Tier 2, Table 7.2-7, “Failure Mode and Effects Analysis for the Plant Protection System,” Item 2-14, and clarify why an improper CEA position renders a CPC inoperable and changes the voting logic.

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. Clause 5.1 of IEEE Std. 603-1991, states, in part, “The safety systems

shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

For the APR1400 FSAR Tier 2, Table 7.2-7, “Failure Mode and Effects Analysis for the Plant Protection System,” Item 2-14, Failure Mode Item b), identifies the following failure terms:

a. Unrecognized software malfunctions

b. Erroneous control element assembly (CEA) position transmission and indication

c. Improper CEA position

It is unclear to the staff what these terms mean with respect to the failure analysis. In addition, it is unclear to the staff how an improper CEA position renders a core protection calculator (CPC) channel inoperable and changes the logic to 2-out-of-2 coincidence. Describe and define the failure terms used: software malfunction, erroneous CEA position, erroneous CEA indication, and improper CEA position. In addition, clarify why an improper CEA position renders a CPC inoperable, and changes the logic to 2-out-of-2 coincidence (e.g. does the voting logic change to 2-out-of-2). Provide diagrams regarding the operation of the CPCS in the APR1400 FSAR to support these clarifications.


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