KHNPDCDRAIsPEm Resource

From: Ciocco, Jeff
Sent: Tuesday, June 23, 2015 9:55 AM
To: apr1400rai@khnp.co.kr; KHNPDCDRAIsPEm Resource; Harry (Hyun Seung) Chang; Yunho Kim; Steven Mannon
Cc: Mott, Kenneth; Jackson, Terry; Ward, William; Lee, Samuel
Subject: APR1400 Design Certification Application RAI 50-7911 (07.02 - Reactor Trip System)
Attachments: APR1400 DC RAI 50 ICE1 7911.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, the following days to respond to the RAI's questions. We may adjust the schedule accordingly.

07.02-1: 60 days
07.02-2: 90 days
07.02-3: 45 days
07.02-4: 60 days
07.02-5: 60 days
07.02-6: 60 days
07.02-7: 90 days
07.02-8: 90 days
07.02-9: 60 days
07.02-10: 60 days
07.02-11: 45 days
07.02-12: 90 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: 55

Mail Envelope Properties (A67A2D233B3FBB4C8B5109AD7C39550715C4EAD991)

Subject: APR1400 Design Certification Application RAI 50-7911 (07.02 - Reactor Trip System)
Sent Date: 6/23/2015 9:54:44 AM
Received Date: 6/23/2015 9:54:47 AM
From: Ciocco, Jeff

Created By: Jeff.Ciocco@nrc.gov

Recipients:
"Mott, Kenneth" <Kenneth.Mott@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: HQCLSTR01.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	899	6/23/2015 9:54:47 AM
APR1400 DC RAI 50 ICE1 7911.pdf	164005	
image001.jpg	5020	

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

REQUEST FOR ADDITIONAL INFORMATION 50-7911

Issue Date: 06/23/2015
Application Title: APR1400 Design Certification Review – 52-046
Operating Company: Korea Hydro & Nuclear Power Co. Ltd.
Docket No. 52-046
Review Section: 07.02 - Reactor Trip System
Application Section: APR1400 RPS and CPCS Reactor Trip Function and Operation

QUESTIONS

07.02-1
For all figures in:

- APR1400 Final Safety Analysis Report (FSAR), Tier 2, Chapter 7, Rev. 0,

- Technical Report APR1400-Z-J-NR-14001, Revision 0, "Safety I&C System," and

- Technical Report APR1400-F-C-NR-14003, Rev. 0, "Functional Design Requirement for a CPCS [Core Protection Calculator System] for APR1400,"

where the figures display only one division/channel (i.e., FSAR, Tier 2, Figure 7.2-10, "PPS Channel A Trip Path Diagram") and where the schematics or diagrams of the figure display differences between the divisions/channels (i.e., FSAR, Tier 2, Figure 7.2-32, "Functional Logic Diagram for CWP"), insert a caption on the figures explaining whether the schematic or diagram shown is identical for all divisions/channels or insert a caption that describes what the differences are between the divisions/channels.

The regulatory requirements of 10 CFR 52.47(a)(2) state that the design "…descriptions shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations." Standard Review Plan (SRP) Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 4, "Safety System Designation," states that the design basis information provided for each design basis item, taken alone and in combination, should have one and only one interpretation and that information provided for the design basis items should be technically accurate. The NRC staff was not able to understand the system design or system functional design requirements for figures displaying differences between divisions/channels and for figures displaying only one division/channel of safety system functionality. Update the FSAR and technical reports accordingly.

07.02-2
Define the reverse order logic trip operation of the reactor protection system (RPS) bistable processors (BP) as software diversity per the software diversity guidance of NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.

10 CFR Part 50, Appendix A, GDC 22, "Protection System Independence" states, in part, that 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 guidance of NUREG/CR-6303, states in Section 3.2.6, "Software Diversity," that software must differ significantly in parameters,

dynamics, and logic, to be considered diverse. Technical Reports APR1400-Z-J-NR-14001-P, Rev. 0, "Safety I&C System," and APR1400-Z-J-NR-14002-P, Rev. 0, "Diversity and Defense in Depth" both state that each BP within a division processes the bistable logic trip function in the reverse order to that of the other BP for software functional diversity (i.e. BP1 in Rack 1 executes sequence 1 through N while BP2 in Rack 2 executes in the reverse sequence, N through 1). NUREG/CR-6303 does not list a diversity category as "software functional diversity," but does identify software diversity and functional diversity. Clarify whether the diversity described is software diversity, functional diversity, or if it accomplishes both, and provide the basis for the determination. In addition, describe how effective the reverse order of operation would be at addressing software faults (e.g., what types of faults does it address and how does the relatively short operational cycles (in the order of milliseconds) impact the effectives of this type of diversity). Update the applicable technical reports accordingly.

07.02-3

Provide diagrams and figures that graphically display and demonstrate the relationship between (1) regulating Control Element Assembly (CEA), (2) shutdown CEAs, (3) part-strength CEAs, (4) full-strength CEAs, (5) 4 finger CEAs, (6) 12 finger CEAs, (7) CEA groups (as listed in Technical Report APR1400-F-C-NR-14003-P, Rev. 0, “Functional Design Requirements for a Core Protection Calculator System for APR1400”), (8) CEA control groups, and (9) CEA subgroups. In addition, the diagrams and figures should demonstrate how CEAs are operated and positioned as a unit.

10 CFR Part 50, Appendix A, General Design Criterion (GDC) 25, “Protection System Requirements For Reactivity Control Malfunctions,” states that the protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal. SRP Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std. 603,” Section 4, “Safety System Designation,” states that the design basis information provided for each design basis item should be complete and sufficient to enable the detailed design of the I&C system to be carried out. The NRC staff was not able to identify diagrams or figures that would graphically demonstrate CEA functional design and operation as it relates to Core Protection Calculator System (CPCS) operation and safety system failure mode and effects analysis. Provide diagrams and figures to demonstrate CEA functional design in accordance with CPCS safety system operation and failure mode analysis and update the application accordingly.

07.02-4

Describe:

a) How the validity of each CPCS program’s execution interval and dynamic adjustments to the parameters is determined and

b) The actions that occur if the CPCS determines that the execution interval or programs’ dynamic adjustments to the parameters are not valid.

10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.10, "Repair," requires safety systems to be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. SRP Branch Technical Position 7-17, "Guidance on Self-Test and Surveillance Test Provisions" provides guidance regarding the use of fault detection and self-diagnostics. Section 4.3.2.3, “Program Structure,” of the Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, states the CPCS will group detailed calculations of departure from nucleate boiling ratio (DNBR) and peak linear heat rate into different programs and will determine if the execution interval over which the dynamic adjustments to the parameters, calculated in each program, are valid. The NRC staff

was not able to identify design descriptions that would explain how the execution interval and dynamic adjustments to parameters are determined to be valid and what protective actions would occur if the execution interval or dynamic changes of the programs were found to be invalid. Explain how the validity of the execution interval and dynamic changes of CPCS programs is determined and the actions performed if the execution interval of the programs or dynamic changes were found to be invalid. Update the application accordingly.

07.02-5

Explain why the Local Coincidence Logic (LCL) processor schematic boxes are different in Figure 4-5 of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, and Figure 7.2-10 of APR1400 FSAR, Tier 2, Rev. 0.

10 CFR 52.47(a)(2) requires, in part, the FSAR design descriptions be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 4, "Safety System Designation," states that the information provided for the design basis items should be technically accurate and should have one and only one interpretation. Figure 4-5 of Technical Report APR1400-Z-J-NR-14001-P displays "OR" gates for all LCL processors while Figure 7.2-10 in the FSAR displays several empty LCL processor schematic boxes (i.e., LCL processor's A4 and A3). Discuss the differences between the two figures and update the application as necessary.

07.02-6

Explain why the CPCS would allow a safety limit to be exceeded before transmitting a trip signal.

10 CFR 50.36(c)(1)(ii)(A) requires, in part, where a limiting safety system setting is specified for a variable on which a safety limit has been placed, the setting must be so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded. Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, Section 4.1.1.3, "Core Protection Calculator System," states:

> *The CPCS compares the DNBR and LPD values against setpoints to determine if fuel design limits are exceeded. When these values* ***exceed a safety limit****, a trip signal is transmitted to the PPS using hardwired cables.*

Initiating a protective action after a safety limit is exceeded does not comply with the requirements of 10 CFR 50.36. Modify the application to describe how the CPCS and other APR1400 safety-related instrumentation and control (I&C) systems will initiate an automatic reactor trip prior to exceeding a safety limit.

07.02-7

a) Define and explain the differences and similarities between the following terms used in Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, describing the CEAs:

I. CEA number 1
II. CEA 1 (referred to as the center CEA)
III. CEA01 (as listed in Table C.5.1-1)

b) Explain why the design descriptions state the center CEA is assigned to only CPCS Channel B (i.e., 70 CEA's to Channel B versus 69), yet, figures and tables of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, demonstrate that the center CEA is going to both CPCS Channels B and C (for a total of 70 CEAs to both channels).

10 CFR 50.55a(h)(3) requires compliance to IEEE Std 603-1991. IEEE-603-1991, Clause 5.6.1, requires redundant portions of a safety system provided for a safety function to 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. SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.6, "Independence," states that the safety system design precludes the use of components that are common to redundant portions of the safety system or any other features that could compromise the independence of redundant portions of the safety system.

Section C.5.1.3.2, "Divisional Independence," in Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, states that the twenty-third subgroup consists of 4 CEAs distributed to the four quadrants of the reactor core with CEA number 1 being located at the center of the core and that the center CEA is assigned to Channel B (thus, 70 CEA's to Channel B versus 69). However, Table C.5.1-1, "RSPT1 and RSPT2 Channel Assignment" and Figure 4-8, "CPCS Block Diagram," of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, show the center CEA is going to both CPCS Channels B and C (for a total of 70 CEAs to both channels - 3 quadrants times 23 CEAs equals 69, plus the center CEA would equal 70). Correctly define the acronym for the center CEA and consistently apply center CEA terminology. Also, clarify the assignment of the center CEA to the CPCS channels that would demonstrate compliance to the applicable safety system independence requirements of IEEE-603-1991. Update the application as necessary.

07.02-8
Provide design information that would:

a) Define the conditions resulting in unavailable CEA position data.

b) What are the failures that cause CEA position data to become unavailable?

c) Describe what system, component, and/or processor senses and makes the determination that CEA position data is unavailable?

d) Explain all system actions and the component(s) and/or device(s) that control those actions that are performed when switching from using the preferred CEA position data to the alternate source.

e) Include failure mode entries into APR1400 FSAR, Tier 2, Revision 0, Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System," describing safety system actions performed after CEA position data becomes unavailable.

10 CFR Part 50, Appendix A, General Design Criteria (GDC) 21, "Protection System Reliability and Testability," requires, in part, that redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function, and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.5, "System Integrity,' states, in part, that the review of system integrity should confirm that the design provides for safety systems to fail in a safe state, or into a state that has been demonstrated to be

acceptable on some other defined basis. In addition, SRP Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std. 603,” Section 4, “Safety System Designation,” states that the design basis information provided for each design basis item should be complete and sufficient to enable the detailed design of the I&C system to be carried out.

Section 4.3.3.2, “CEA Calculator Rack,” of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, states that, should the preferred source of CEA position data become unavailable, the alternate source will be used. However, the staff was not able to find information that describes: (a) The conditions resulting in unavailable CEA position data; (b) what failures would cause CEA position to become unavailable; (c) what portion of the I&C system determines CEA position is unavailable; (d) what actions would occur to transfer CEA position data to the alternate source; and (e) identification of CEA position unavailability in the Plant Protection System failure modes and effects analysis. Explain and describe the complete safety system actions performed to detect and mitigate against the unavailability of preferred CEA position data. Update the application accordingly.

07.02-9

Define, describe, and provide logic diagrams, if applicable, to explain the following terms used in the column titled “Effect on PPS,” of Table 7.2-7, “ Failure Mode and Effects Analysis for the Plant Protection System,” in Chapter 7 of the APR1400 FSAR, Tier 2, Rev. 0:

a) “…trip logic changes to…”

b) “…logic of RPS are converted to….”

10 CFR 50.55a(h)(3) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 4.2, requires the documentation of the safety functions and corresponding protective actions of the execute features for each design basis event. SRP Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std. 603,” Section 4, “Safety System Designation,” states that the design basis should demonstrate completeness and should address all system functions necessary to fulfill the system's safety intent.

Table 7.2-7 of the APR1400 FSAR, Tier 2, Rev. 0, implies that reactor trip logic will modify during operation. Typically, the reactor trip logic remains static once it is programmed and installed on the reactor protection system. Values of parameters used by the reactor trip logic may change due to plant conditions, but the logic remains static. Describe what is meant by the coincidence logic is “changed” or “converted” as listed in Table 7.2-7 column titled “Effect on PPS.”

07.02-10

Describe what happens to the Reactor Protection System (RPS) channel status when the RPS detects a high steam generator sensor failure.

10 CFR Part 50, Appendix A, GDC 23, "Protection system failure modes," requires protection systems to be designed to fail into a safe state or into state demonstrated to be acceptable on some other defined basis. SRP Appendix 7.1-C, Section 5.5, “System Integrity,” states that computer-based safety systems should, upon detection of inoperable input instruments, automatically place the protective functions associated with the failed instrument(s) into a safe state (e.g., automatically place the affected channel(s) in trip), unless the operator has already placed the affected channel in a bypass mode.

APR1400 FSAR, Tier 2, Rev. 0, Table 7.2-7, single failure entry Item# 1-6, b), states that once the reactor protection system (RPS) detects and activates an alarm for a detected "sensor failure," the RPS trip logic would be changed to a 2-out-of-2 (as listed in the "Effect on PPS" column). The alarm would result from the RPS feature of "comparison of three channels" for the failed steam generator high pressure sensor signal. However, since the logic of the RPS is not designed to provide a trip for a high steam generator pressure, it is not clear why the RPS trip logic would change for a failed high steam generator pressure sensor. Describe other actions initiated by the RPS resulting from an RPS detected high steam generator pressure sensor failure and the basis for the actions described in Table 7.2-7.

07.02-11

Define and explain the meaning of the term "quality margin" as it relates to APR1400 FSAR, Tier 2, Rev. 0, Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System," Item# 2-1, b).

10 CFR 52.47(a)(2) requires the FSAR design descriptions be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 4, "Safety System Designation," states that the information provided for the design basis items, taken alone and in combination, should have one and only one interpretation.

Section 4.5.2, "DNBR/Quality Trip," in Technical Report APR1400-F-C-NR-14003-P, Rev. 0, "Functional Design Requirement for a CPCS for APR1400," states that if "Quality Margin Trip" is violated, a DNBR Trip or Pre-trip signal is issued. However, the NRC staff was not able to identify a definition or design description of the term "quality margin" to understand its usage in the technical report and in Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System," single failure entry Item # 2-1, b), of APR1400 FSAR, Tier 2, Chapter 7, Rev. 0. Define and describe the term "quality margin" and update the FSAR and technical reports accordingly.

07.02-12

For the single failure entry items 2-4a), 2-4b), and 2-4c), of APR1400 FSAR, Tier 2, Chapter 7, Rev. 0, Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System," explain:

a) The difference between a sensor and a finger;

b) Why the plant would shut down due to an in-range 12 finger CEA single failure;

c) Why the plant would not shut down due to an in-range 4 finger CEA single failure; and

d) Why an excessive number of failures, as postulated in single failure entries 2-4b) and 2-4c), do not result in the same reactor protection system (RPS) protective actions.

10 CFR Part 50, Appendix A, GDC 21, requires, in part, redundancy and independence to be designed into the reactor protection system to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy. SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 4, "Safety System Designation," states that the information provided for the design basis items should be technically accurate.

REQUEST FOR ADDITIONAL INFORMATION 50-7911

Table 7.2-7, “Failure Mode and Effects Analysis for the Plant Protection System,” in APR1400 FSAR, Tier 2, Rev. 0, discusses failures and actions associated with CEAs. Specifically, single failure entry items 2-4a), 2-4b), and 2-4c) discuss these items. Provide clarification for: (a) The difference between a sensor and a finger; (b) Why the plant would shut down due to an in-range 12 finger CEA single failure; (c) Why the plant would not shut down due to an in-range 4 finger CEA single failure; and (d) Why an excessive number of failures, as postulated in single failure entries 2-4b) and 2-4c), do not result in the same reactor protection system (RPS) protective actions.


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