## KHNPDCDRAIsPEm Resource

**From:** Ward, William
**Sent:** Friday, July 10, 2015 5:50 PM
**To:** 'apr1400rai@khnp.co.kr'; KHNPDCDRAIsPEm Resource; 'Chang, Harry'; 'Yunho Kim (yshh8226@gmail.com)'; 'Mannon, Steven (steven.mannon@aecom.com)'
**Cc:** Ciocco, Jeff; Lee, Samuel; Morton, Wendell; Jackson, Terry
**Subject:** APR1400 Design Certification Application RAI 68-7892 (7.7 Control Systems)
**Attachments:** image001.jpg; APR1400 DC RAI 68 ICE1 7892.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's questions. We may adjust the schedule accordingly.

07.07-1: 45 days
07.07-2: 90 days
07.07-3: 90 days
07.07-4: 90 days
07.07-5: 45 days
07.07-6: 90 days
07.07-7: 90 days
07.07-8: 60 days

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

Thank you,

**William R. Ward, P.E.**
**Senior Project Manager**
**U.S. Nuclear Regulatory Commission**
**m/s T6-D38M**
**Washington, DC, 20555-0001**
NRO/DNRL/Licensing Branch 2
ofc T6-D31
ofc (301) 415-7038 fax (301) 415-6350

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

Please consider the environment before printing this email.

**Hearing Identifier:** KHNP_APR1400_DCD_RAI_Public
**Email Number:** 77

**Mail Envelope Properties** (5810f58b8fd54af7bf083e5627382ff6)

**Subject:** APR1400 Design Certification Application RAI 68-7892 (7.7 Control Systems)
**Sent Date:** 7/10/2015 5:49:39 PM
**Received Date:** 7/10/2015 5:49:41 PM
**From:** Ward, William

**Created By:** William.Ward@nrc.gov

**Recipients:**
"Ciocco, Jeff" <Jeff.Ciocco@nrc.gov>
Tracking Status: None
"Lee, Samuel" <Samuel.Lee@nrc.gov>
Tracking Status: None
"Morton, Wendell" <Wendell.Morton@nrc.gov>
Tracking Status: None
"Jackson, Terry" <Terry.Jackson@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
"'Chang, Harry'" <hyunseung.chang@gmail.com>
Tracking Status: None
"'Yunho Kim (yshh8226@gmail.com)'" <yshh8226@gmail.com>
Tracking Status: None
"'Mannon, Steven (steven.mannon@aecom.com)'" <steven.mannon@aecom.com>
Tracking Status: None

**Post Office:** HQPWMSMRS05.nrc.gov

| **Files** | **Size** | **Date & Time** |
|---|---|---|
| MESSAGE | 956 | 7/10/2015 5:49:41 PM |
| image001.jpg | 4205 | |
| APR1400 DC RAI 68 ICE1 7892.pdf | 107613 | |

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


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

# REQUEST FOR ADDITIONAL INFORMATION 68-7892

Issue Date: 07/10/2015
Application Title: APR1400 Design Certification Review – 52-046
Operating Company: Korea Hydro & Nuclear Power Co. Ltd.
Docket No. 52-046
Review Section: 07.07 - Control Systems
Application Section: Section 7.7

QUESTIONS

**07.07-1**

Clarify whether the intent of APR1400 Final Safety Analysis Report (FSAR), Tier 1, Table 2.5.5-2, Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Item No. 2, is to verify diversity between safety and non-safety-related instrumentation and control (I&C) equipment and software.

10 CFR 52.47(b)(1) states in part that if the inspections, tests and analyses are performed and the acceptance criteria met, a facility that incorporates the design certification has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations. In ITAAC Item No. 2, the design commitment states, "The digital equipment and software used in the PCS and P-CCS are independent from those of the plant protection system (PPS) and the engineered safety features-component control system (ESF-CCS)." Independence is a safety attribute established by such requirements as General Design Criteria 24 and IEEE Std. 603-1991, Clause 5.6, as incorporated by reference in 10 CFR 50.55a(a)(2). The manner in which this ITAAC item is written would imply the PCS and P-CCS are diverse from the PPS and ESF-CCS because it states the equipment and software are independent between systems rather than simply stating the systems are independent.

Verify the intent of this ITAAC is actually to establish and verify diversity between the subject systems or to verify independence between safety and non-safety I&C systems.

**07.07-2**

Explain the differences in controller group arrangements between the APR1400 FSAR, Tier 1, Table 2.5.5-1, and Table 5.2-1 of Technical Report APR1400-Z-J-NR-14012-P, Rev. 0, "Control System CCF [common cause failure] Analysis."

10 CFR 52.47(b)(1) requires, in part, that if the inspections, tests, and analyses are performed and the acceptance criteria met, a facility that incorporates the design certification has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations. Standard Review Plan (SRP) Section 7.7 states, in part, the failure of any control system component or any auxiliary supporting system for control systems should not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the safety analysis report (SAR).

The content of APR1400 FSAR Tier 1, Table 2.5.5-1, “Controller Group Arrangement of The PCS and NPCS”, and Table 5.2-1, “Control Group Segmentation” of Technical Report

APR1400-Z-J-NR-14012-P do not align. Table 5.2-1 has a wider scope of design detail, while the Table 2.5.5-1 does not seem to be updated to match the number of systems described in the technical report. For example, Table 5.2-1 of the "Control System CCF Analysis" technical report contains information about controller groups such as the Turbine Control System (TCS), Condenser Vacuum control and Non-1E AC power. Table 2.5.5-1 does not contain these individual controller groups. Though the technical report would be expected to convey are larger amount of detailed design information, Table 2.5.5-1 of the Tier 1 FSAR would be an incomplete representation of the non-safety control system controller arrangement.

1. Is the intent of APR1400 FSAR, Tier 1, Table 2.5.5-1, to convey the total number of control groups within the non-safety I&C architecture or only a limited set?

2. Explain why the APR1400 FSAR, Tier 1, Design Description, does not contain a table that establishes all of the control groups (essentially the control group segmentation), which would align with Technical Report APR1400-Z-J-NR-14012-P to adequately describe the design of the control system architecture.

**07.07-3**

Provide an ITAAC that verifies the implementation of functional segmentation and component segmentation arrangements as described in Technical Report APR1400-Z-J-NR-14012-P, Revision 0, "Control System CCF Analysis" technical report.

10 CFR 52.47(b)(1) states, in part, that if the inspections, tests, and analyses are performed and the acceptance criteria met, a facility that incorporates the design certification has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations. SRP Section 7.7 states, in part, that for the effect of control system failures, the failure of any control system component or any auxiliary supporting system for control systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the SAR.

Technical Report APR1400-Z-J-NR-14012-P, Section 4.5 "Segmentation" describes the grouping of control functions and components into segmented arrangements that directly support the quantitative and qualitative analysis provided in this report to address the safety issue of postulated failure(s) in the APR1400 control systems. Table 2.5.5-2, "Control System Not Required for Safety ITAAC," of the APR1400 FSAR, Tier 1, ITAAC Section 2.5.5, "Control System Not Required for Safety," does not provide an ITAAC that verifies that these segmentation arrangements have been adequately implemented to support the safety case made within Technical Report APR1400-Z-J-NR-14012-P. It is essential the programming and implementation of the functional and component segmentation as shown in the technical report be verified in order in order to maintain the validity of the CCF quantitative and qualitative analysis. Provide an ITAAC that verifies the segmentation arrangements for the APR1400 control systems or provide an explanation for why this design commitment is not necessary.

**07.07-4**

Provide information on fault detection capabilities of the non-safety I&C, as mentioned in Technical Report APR1400-Z-J-NR-14012-P, Rev.0 "Control System CCF Analysis."

IEEE Std. 603-1991, Clause 5.6.3 states, in part, that the safety system design shall be such that credible failures in, and consequential actions by other systems, as documented in the design basis per Clause 4.8, shall not prevent the safety systems from meeting the requirements of this standard. Section 4.4.2, "Redundancy," of Technical Report, APR1400-Z-J-NR-14012-P, Rev. 0, states, "A comprehensive set of diagnostics aids in fault detection, locating and repairing problems before they lead to more serious operational concerns. Failure of the primary controller would result in fail-over to the standby controller and an alarm. Failure of the standby controller would only result in an alarm as the primary controller is already controlling." This section goes on to further discuss the redundancy between the primary and standby controllers and the fail-over action. However, the section provides no other details to substantiate the claim of a comprehensive set of diagnostics exists or what these diagnostics are. Section 4.4.4.1, "Design Features to Prevent Spurious Control Commands," of APR1400-Z-J-NR-14012-P, Rev. 0, details some data communications error checking features of the DCS controllers but that would not appear to constitute a comprehensive set of fault detection measures in the non-safety I&C systems within the boundaries of this technical report.

1. Provide the full set of the automated fault detection features implemented in the non-safety I&C that are used to support the control system CCF analysis.

2. What types of faults would require a fail-over from primary to standby controllers? Describe the logic that implements the fail-over function between the controllers.

3. How does the design prevent a faulted controller from continuing to send signals onto data communication network-information (DCN-I) network or any other connected network?

4. For failures of either the primary or standby DCS controller, where does the alarm appear for these failures?

**07.07-5**

Clarify the network architectural arrangements and interfaces for the individual non-safety I&C systems, with specific attention to those cited in the failure boundary portion of Figure 4.1-1 in Technical Report APR1400-Z-J-NR-14012-P, Rev.0, "Control System CCF Analysis Technical Report."

10 CFR 52.47(a)(2) requires, in part, that the description of structures, systems and components shall be sufficient to permit understanding of the system designs. Section 4.4.2 of the Control System CCF Analysis Technical Report states, in part, that, "The non-safety system incorporates network communication configurations that have dual or redundant communications paths." and Section 4.4.6, "Design Features to Cope with Broadcast Storms on the IFPD/ESCM Ethernet Networks," discusses the potential for a broadcast storm on the Ethernet networks. Figure 4.1-1, "Credible Failure Boundary of Control System CCF," of Technical Report APR1400-Z-J-NR-14012-P, Rev. 0, is a general network diagram illustrating the baseline communications paths but does not convey the level of detail

mentioned in the above quotes, thereby making it difficult to understand the non-safety I&C architecture.

1. Are there figures illustrating the internal network architectural layout of specific non-safety I&C systems such as the power control system (PCS), as it is described in APR1400 FSAR, Tier 2, Section 7.7? This is critical as the PCS system contains multiple subsystems such as the reactor regulating system (RRS) and the digital rod control system (DRCS).

2. Describe the interface, along with communication type and logic, facilitating the turbine trip function from a reactor trip signal. APR1400 FSAR, Tier 2, Section 10.2.2.3.3, describes the Turbine Generator Control system as a 2-out-of-3 logic system but the Plant Protection System is a 2-out-of-4 logic system.

3. In Figure 4.1-2, "Control System Overview," of Technical Report APR1400-Z-J-NR-14012-P, the acronym, “RRS” (Reactor Regulating System?) is not defined in the drawing key.

**07.07-6**

Clarify the information given with regards to network data storms in Sections 4.4.5, "Design Features to Prevent CCF Due to Broadcast Storms on the DCN-I Network," and 4.4.6 of Technical Report APR1400-Z-J-NR-14012P, "Control System CCF Analysis Technical Report," Rev. 0.

IEEE Std. 603-1991, Clause 5.6.3, as incorporated by reference in 10 CFR 50.55a(a)(2), states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in the design basis per Clause 4.8, shall not prevent the safety systems from meeting the requirements of this standard.

Sections 4.4.5 and 4.4.6 of Technical Report APR1400-Z-J-NR-14012P state, in part, that, "A broadcast storm could occur on the DCN-I network..." The sections go on to discuss how a broadcast storm is handled and its event type classification, including classification justification. However Section 4.4.5 does not provide an adequate technical basis to substantiate the event classification assigned to broadcast data storms.

NRC Information Notice 2007-15, "EFFECTS OF ETHERNET-BASED, NON-SAFETY RELATED CONTROLS ON THE SAFE AND CONTINUED OPERATION OF NUCLEAR POWER STATIONS," documents a network data storm event that resulted in a loss of multiple reactor recirculation pumps at Brown's Ferry Unit 3. The root cause of the data storm even was determined to be excessive network traffic and not a failure in the software or hardware of any specific component. It is not apparent that in this report that excessive network traffic was considered as a potential failure mode in the DCN-I network or other non-safety networks within this design.

1. Was excessive network traffic considered a potential failure mode in the APR1400 design? If so, where is this information described?

2. What are the design features in place to cope with excessive network traffic and the potential effects on safety and non-safety I&C components?

3. Provide more information on the technical basis/justification for the data storm event classification for the DCN-I and IFPD/ESCM Ethernet networks described in sections 4.4.5 and 4.4.6.

4. Does the applicant intend to verify the adequacy of operator actions to cope with a data storm event through an ITAAC?

5. Has the applicant verified the adequacy of operator actions through human factors engineering or analysis?

**07.07-7**

Clarify the use of the word, "disappeared" in Technical Report APR1400-Z-J-NR-14012-P, Rev. 0, “Control System CCF Analysis.”

10 CFR 52.47(a)(2) requires, in part, that the description of structures, systems and components shall be sufficient to permit understanding of the system designs. Technical Report APR1400-Z-J-NR-14012-P uses the term, "disappeared" in multiple places in Section 5, "Evaluation Method and Results," which is confusing since it would not seem to convey the technical idea that is appropriate for the context in which the term is used. For example, in Sheet 9 of 18 of Table 5.1-10, "Multiple Failure due to a Single Failure of Shared Signals," of the technical report, it states the following, "The above temporary excessive feedwater by ... is disappeared by ..." Given the safety significance of this technical issue, it is essential that the design description be expressed in the most accurate way possible.

Clarify the use of the term "disappeared" in Technical Report APR1400-Z-J-NR-14012-P.

**07.07-8**

Clarify the design information regarding the non-safety control system control capabilities of safety I&C functions or components in Technical Report APR1400-Z-J-NR-14012-P, Rev. 0, “Control System CCF Analysis.”

IEEE Std. 603-1991, Clause 5.6.3, as incorporated by reference in 10 CFR 50.55a(a)(2), states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in the design basis per Clause 4.8, shall not prevent the safety systems from meeting the requirements of this standard. Technical Report APR1400-Z-J-NR-14012-P, Section 4.4.4.1 Rev. 0, last paragraph provides additional important information concerning this issue.

Figure 4.1-1 of Technical Report APR1400-Z-J-NR-14012-P shows network connectivity that potentially leads from the non-isolated information flat panel displays (IFPDs) to their associated ESF-CCS soft control module (ESCM), through the gateways and down to the safety I&C. The networked IFPDs are within the boundary of the CCF analysis. This figure does not appear to imply a limitation on the safety I&C that can be controlled from the IFPDs. Also, DI&C-ISG-04, Section 3.1.5, "Malfunctions and Spurious Actuations," states that, "Multidivisional control and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location." Figure 4.1-1 shows the IFPDs are located

in the main control room (MCR) and the applicant states that control of safety components from non-safety devices exist within this design.

1. Are the safety I&C systems identified in Section 4.9 of Technical Report APR1400-Z-J-NR-14012-P the only safety I&C systems and/or components that can be controlled from non-safety devices (IFPDs and DCS Controllers)? If not, provide a complete list and summary for all safety functions and safety-related devices safety that can be controlled from non-safety components and workstations (e.g. IFPDs).

2. In Figure 4.9-2, "ESF-CCS Control Logic against Non-Safety Signal Failure," are all of the signals shown hardwired signals? What type of isolation is depicted in this figure?

3. Considering that the IFPDs/DCS controllers control safety-related components/functions according to Section 4.9 of the Control System CCF Analysis Technical Report, provide an explanation for why the IFPDs and DCS controllers do not need to address environmental qualification, as stated in Section 3 of DI&C-ISG-04, “Multidivisional Control and Display Stations”, for such things as seismic conditions, EMI/RFI, etc.

4. Provide an explanation on what the applicant means when it states IFPDs and DCS controllers do not "directly" control safety-related components/functions, except those defined in Section 4.9 of the Control System CCF Analysis Technical Report. Is there an indirect means by which other safety functions and components are controlled that are not stated in Section 4.9?