KHNPDCDRAIsPEm Resource

From: Ward, William
Sent: Thursday, December 24, 2015 1:51 PM
To: apr1400rai@khnp.co.kr; KHNPDCDRAIsPEm Resource; Harry (Hyun Seung) Chang; Andy Jiyong Oh; Erin Wisler (erin.wisler@aecom.com)
Cc: Lee, Samuel; Ciocco, Jeff; Truong, Tung; Jackson, Terry; Ward, William
Subject: APR1400 Design Certification Application RAI 348-8279 (7.9 - Data Communication Systems)
Attachments: APR1400 DC RAI 348 ICE 8279.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 RAI question response times. We may adjust the schedule accordingly.

07.09-8 : 45days
07.09-9 : 60days
07.09-10 : 45days
07.09-11 : 60days
07.09-12 : 60days
07.09-13 : 90days
07.09-14 : 60days
07.09-15 : 60days
07.09-16 : 60days
07.09-17 : 45days
07.09-18 : 45days
07.09-19 : 45days

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

Hearing Identifier: KHNP_APR1400_DCD_RAI_Public
Email Number: 403

Mail Envelope Properties (bd2ab5c147024099b74d4573924cb22b)

Subject: APR1400 Design Certification Application RAI 348-8279 (7.9 - Data Communication Systems)
Sent Date: 12/24/2015 1:51:20 PM
Received Date: 12/24/2015 1:51:23 PM
From: Ward, William

Created By: William.Ward@nrc.gov

Recipients:
"Lee, Samuel" <Samuel.Lee@nrc.gov>
Tracking Status: None
"Ciocco, Jeff" <Jeff.Ciocco@nrc.gov>
Tracking Status: None
"Truong, Tung" <Tung.Truong@nrc.gov>
Tracking Status: None
"Jackson, Terry" <Terry.Jackson@nrc.gov>
Tracking Status: None
"Ward, William" <William.Ward@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)" <erin.wisler@aecom.com>
Tracking Status: None

Post Office: HQPWMSMRS05.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	1069	12/24/2015 1:51:23 PM
APR1400 DC RAI 348 ICE 8279.pdf	95814	

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

REQUEST FOR ADDITIONAL INFORMATION 348-8279

Issue Date: 12/24/2015
Application Title: APR1400 Design Certification Review – 52-046
Operating Company: Korea Hydro & Nuclear Power Co. Ltd.
Docket No. 52-046
Review Section: 07.09 - Data Communication Systems
Application Section:

QUESTIONS

07.09-8

In Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, “Safety I&C System,” clarify that the Maintenance Test Panel (MTP) is not used for maintenance and software loading.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, "Redundant portions of a safety system provided for a safety function shall 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," and Clause 5.6.3, states, in part, "The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." Section C.5.1 of Technical Report APR1400-Z-J-NR-14001-P, DI&C-ISG-04, Position 10, states conformance to DI&C-ISG-04, Interdivisional Communications, Staff Position 10, and in "SDL Compliance," it states that "...software is loaded into the...” The compliance of the platform is provided in Reference 12 [Common Qualified Topical Report]." Section 5.6.10, "ISG-4 Position 10," of the Common Q Topical Report states "When the reboot occurs…”. It was not clear to the staff if the MTP is used for maintenance and software loading as discussed in the Common Q Topical Report. At a public meeting in August 2015, the applicant said that the MTP is not used for maintenance and software loading.

Staff requests applicant update Technical Report APR1400-Z-J-NR-14001-P to clarify the MTP and its relation with maintenance and software loading.

07.09-9

Describe the interconnections between Division A/B and C/D for shutdown cooling pump start on CS pump trouble and demonstrate the functional dependency will not challenge the independence between the divisions.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, "Redundant portions of a safety system provided for a safety function shall 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," and Clause 5.6.3, states, in part, "The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." Digital I&C Interim Staff Guidance (DI&C-ISG)-04 provides acceptance criteria for communication and functional independence between redundant divisions of safety for meeting the independence requirements of IEEE Std 603-1991, Clause 5.6. The containment

spray actuation signal (CSAS) is used to actuate the containment spray system (CSS). The logic diagram for CSAS is provided in APR1400 FSAR Tier 2, Figure 7.3-5, and it shows four divisions. However, there are only two containment spray pumps. Staff requests the applicant to describe the control logic for the two spray pumps, to describe the interconnections between Division A/B and C/D for shutdown cooling pump start on CS pump trouble, and to demonstrate that the functional dependency will not challenge the independence between the divisions.

07.09-10

Beside the MTP, clarify whether there are any other safety systems that send data to the DCS gateway.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, "Redundant portions of a safety system provided for a safety function shall 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," and Clause 5.6.3, states, in part, "The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." Digital I&C Interim Staff Guidance (DI&C-ISG)-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6. Section 7.9.1.4 of the FSAR Tier 2 states "the MTP sends data to the IPS through the DCS gateway server using fiber-optic cable uni-directionally... The DCS gateway server receives data from safety systems with fiber-optic isolation." Besides the MTP, it is not clear to the staff if there are any other safety systems that send data to the DCS gateway. Clarify whether there are additional safety systems that send data to the DCS gateway and update the FSAR as appropriate.

07.09-11

Describe the measures used to prevent data going from non-safety systems to safety-related systems.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, "Redundant portions of a safety system provided for a safety function shall 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," and Clause 5.6.3, states, in part, "The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." Digital I&C Interim Staff Guidance (DI&C-ISG)-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

Section 4.1.1.4 of Technical Report APR1400-Z-J-NR-14001-P states "The QIAS-P also transmits the sensor signals and their calculated variables to the IPS and QIAS-N through the MTP and ITP, respectively. In the case of the IPS, this data communication is a uni-directional protocol from the MTP. In the case of the ITP, the SDL data communication is used to transmit data to the QIAS-N." The first paragraph of section 4.2.3.4 of the same report also discusses the MTP, its capabilities, displays, interfaces, and data transmission details.

Section 4.3.1.5 of the same report states "This MTP interface is a unidirectional point-to-point Ethernet datalink from the MTP to the DCN-I gateway." In addition, Figure 4-22 of the technical report shows that the MTP to IPS link is a one way fiber optic cable. Section C.4.2 of the report contains the following, "...(no receiving connection)..."

Describe the uni-directional interface between MTP and IPS and clarify what is meant by "no receiving connection," since a typical Ethernet connector has 4 pairs of wires. It is not clear to staff if a standard Ethernet cable is used or a modified cable/connectors with TX pairs/pins on the non-safety end removed and RX pairs/pins on the safety end removed.

07.09-12

Demonstrate how the effects of data storms are addressed for this connectivity in order to provide reliable data transmissions to support safety system functions.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, "Redundant portions of a safety system provided for a safety function shall 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," and Clause 5.6.3, states, in part, "The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." Digital I&C Interim Staff Guidance (DI&C-ISG)-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6. 10 CFR 50, Appendix A, Criterion 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.

To comply with DI&C-ISG-04, Section 1, Position 4, in section C.5.1.5(4) of technical report APR1400-Z-J-NR-14001-P, the applicant stated “The EP [Ethernet Processor] checks the integrity of the received data by ..." This section goes on to discuss actions taken "...over a certain number of cycles,..." Since the ESCM is connected to 4 IFPDs, the applicant is requested to identify the “certain number of cycles” and the how much erroneous data the Ethernet Communication Module can handle.

To comply with DI&C-ISG-04, Section 1, Position 19 (section C.5.1.5(19), the applicant stated “…even if incorrect data are broadcasted or a broadcast data storm occurs on a network causing an excess of data traffic...” The staff also request the applicant to demonstrate how the effects of data storms are addressed for this connectivity in order to provide reliable data transmissions to support important to safety functions as required by GDC 13.

07.09-13

Discuss how the Information Flat Panel Display (IFPD) communications to ESF-CCS Soft Control Module (ESCM) support or enhance the performance of the safety functions.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, “Redundant portions of a safety system provided for a safety function shall 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,” and Clause 5.6.3, states, in part, “The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.” DI&C-ISG-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6. Technical Report, APR1400-Z-J-NR-14001-P, Section C.5.1.5(3), states conformance to DI&C ISG-04, Section 1, Position 3, and defines the purpose of the IFPD to ESCM interdivisional communication. DI&C ISG-04, Section 1, Position 3 states, in part, “A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function.” It is not clear to the staff how the IFPD interdivisional communication as described in the technical report meets DI&C ISG-04, Section 1, Position 3. Specifically, how do the described IFPD interdivisional communications support or enhance the performance of the safety functions? The staff requests the applicant to address this portion of DI&C ISG-04 and update the FSAR accordingly.

07.09-14

Discuss how response times will be verified for IFPD to ESCM interdivisional communication.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, "Redundant portions of a safety system provided for a safety function shall 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," and Clause 5.6.3, states, in part, "The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." Digital I&C Interim Staff Guidance (DI&C-ISG)-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

To comply with DI&C-ISG-04, Section 1, Position 20, for IFPD to ESCM interdivisional communication, in APR1400-Z-J-NR-14001-P, section C.5.1.5(20), the applicant describes how the maximum delay time is calculated, including the time components involved in the calculation. Discuss the testing and analysis that will be performed to demonstrate how these response times will be verified for IFPD to ESCM interdivisional communication; particularly for those manual actions that are credited to implement a safety function.

07.09-15

Address DI&C-ISG-04, "Highly Integrated Control Room - Communication," Rev. 1, Positions 12, 13, 14, 15 and 17 for the IFPD to ESCM interface.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, "Redundant portions of a safety system provided for a safety function shall 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," and Clause 5.6.3, states, in part, "The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." Digital I&C Interim Staff Guidance (DI&C-ISG)-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

For DI&C-ISG-04, Section 1, Positions 12, 13, 14, 15, and 17, in technical report APR1400-Z-J-NR-14001-P, section C.5.1.5, the applicant stated that DI&C-ISG-04 position is not applicable to the communication between IFPD and the ESCM. The staff disagrees. DI&C-ISG-04 states "vital communication as used are communications that are needed to support a safety function," and based on the discussions in Technical Report APR1400-Z-J-NR-14001-P, the IFPD and ESCM connectivity supports a safety function (e.g., steam generator tube rupture manual actions). Address DI&C-ISG-04 Positions 12, 13, 14, 15, and 17 for the IFPD to ESCM interface.

07.09-16

Identify whether there are any data communication failures that are APR1400 architecture specific.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, "Redundant portions of a safety system provided for a safety function shall 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," and Clause 5.6.3, states, in part, "The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." Digital I&C Interim Staff Guidance (DI&C-ISG)-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

Sections C.5.1.1, C.5.1.2, C.5.1.3, and C.5.1.4 of Technical Report APR1400-Z-J-NR-14001-P state, "The compliance of the platform is provided in Reference 12 [Common Qualified Platform Topical Report.]" for DI&C-ISG-04, Section 1, Position 12. Identify and discuss if there by any data communication failures that are APR1400 architecture specific or related to the APR1400 application (including the APR1400 software).

07.09-17

Discuss if there are operational limits for message transfer.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. Clause 5.5 of IEEE Std. 603-1991 requires safety systems be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. In addition, Clause 4.10 of IEEE Std. 603-1991 requires, as a part of the design basis, identification of the critical points in time or the plant conditions, after the onset of a design basis event. To meet IEEE Std. 603-1991, Clause 5.5 and Clause 4.10, data communications systems in support of the protection system should demonstrate real-time performance in accordance with SRP Branch Technical Position (BTP) 7-21, “Guidance on Digital Computer Real-Time Performance.”

REQUEST FOR ADDITIONAL INFORMATION 348-8279

Section 4.6.1.3 of Technical Report APR1400-Z-J-NR-14001-P discusses real-time, deterministic behavior of the SDL and SDN data communication networks and states message transfer is non-deterministic. Since message transfer is not performed cyclically, but only when one or more of the attached communication interfaces have data to send, the staff requests the applicant to discuss if there are operational limits for message transfer and how message transfer would not impact any safety functions.

07.09-18
Discuss how the CPP and CEAC/CPP interdivisional communications support or enhance the performance of the safety functions.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, “Redundant portions of a safety system provided for a safety function shall 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,” and Clause 5.6.3, states, in part, “The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.” DI&C-ISG-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

DI&C ISG-04, Section 1, Position 3, states, in part, “A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function.” It is not clear to the staff how the CPP and CEAC/CPP interdivisional communication as described in Section C.5.1.3 of Technical Report, APR1400-Z-J-NR-14001-P, meets DI&C ISG-04, Section 1, Position 3. Specifically, how do the described CPCS interdivisional communications support or enhance the performance of the safety functions? The staff requests the applicant to address this portion of DI&C ISG-04 and update the FSAR and/or technical reports accordingly.

07.09-19
Discuss failures which have been identified through analysis but cannot be detected through equipment or diagnostics, and how those undetectable failures are addressed.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, “Redundant portions of a safety system provided for a safety function shall 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,” and Clause 5.6.3, states, in part, “The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.” DI&C-ISG-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

Section C.5.1.3.7(2) of Technical Report, APR1400-Z-J-NR-14001-P states conformance to DI&C ISG-04, Section 1, Position 2, and discusses failures modes for Reed Switch Position Transmitter (RSPT) which are detectable by CPCS and through diagnostics. Staff requests applicant to discuss failures that have been identified through analysis but cannot be detected through equipment or diagnostics, and how those undetectable failures are addressed.