

KHNPDCDRAIsPEm Resource

From: Ciocco, Jeff
Sent: Tuesday, June 23, 2015 8:00 AM
To: apr1400rai@khnp.co.kr; KHNPDCDRAIsPEm Resource; Harry (Hyun Seung) Chang; Yunho Kim; Steven Mannon
Cc: Truong, Tung; Jackson, Terry; Ward, William; Lee, Samuel
Subject: APR1400 Design Certification Application RAI 45-7883 (07.09 - Data Communication Systems)
Attachments: image001.jpg; APR1400 DC RAI 45 ICE1 7883.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.

07.09-1: 60 days
07.09-2: 90 days
07.09-3: 90 days
07.09-4: 60 days
07.09-5: 45 days
07.09-6: 90 days
07.09-7: 60 days

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

Thank you,

KHNP can answer each question of the RAI with the schedule as follows:

Jeff Ciocco
New Nuclear Reactor Licensing
301.415.6391
jeff.ciocco@nrc.gov



Hearing Identifier: KHNP_APR1400_DCD_RAI_Public
Email Number: 50

Mail Envelope Properties (A67A2D233B3FBB4C8B5109AD7C39550715C4EAD88A)

Subject: APR1400 Design Certification Application RAI 45-7883 (07.09 - Data Communication Systems)
Sent Date: 6/23/2015 7:59:32 AM
Received Date: 6/23/2015 7:59:34 AM
From: Ciocco, Jeff
Created By: Jeff.Ciocco@nrc.gov

Recipients:

"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
"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	875	6/23/2015 7:59:34 AM
image001.jpg	5020	
APR1400 DC RAI 45 ICE1 7883.pdf		128116

Options

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



REQUEST FOR ADDITIONAL INFORMATION 45-7883

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: 07.09 - Data Communication Systems

Application Section:

QUESTIONS

07.09-1

Describe how the isolation devices between redundant safety-related instrumentation and control (I&C) divisions and between safety-related and non-safety-related I&C systems are qualified and how they conform to NRC guidance for isolation devices.

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." Regulatory Guide (RG) 1.75 provides guidance on the physical separation requirements of IEEE Std. 603-1991, Clause 5.6. Branch Technical Position (BTP) 7-11 provides guidance on application and qualification of isolation devices to meet the electrical isolation requirements of IEEE Std. 603-1991, Clause 5.6. 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.

Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, "Safety I&C System," describes the design features of the APR1400 digital I&C system and how the design complies with NRC regulation. Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, Section 4.1.3.1, states, in part, "...DPS ESF [Diverse Protection System Engineered Safety Features] actuation signals are hardwired to the CIM [Component Interface Module] through the isolation device," and Section 4.1.3.3 states, in part, "The DMA [Diverse Manual Action] switches signals are hardwired to the CIM through the isolation device." The current application does not describe how these isolation devices are qualified to provide isolation between safety-related and non-safety-related I&C systems. Describe how these isolation devices address the isolation guidance in BTP 7-11, RG 1.75, and DI&C-ISG-04 in order to demonstrate compliance to IEEE Std. 603-1991, Clause 5.6. The staff also requests the applicant to address independence criteria and isolation guidance for other sections of the technical report where other isolation devices are discussed. Update the final safety analysis report (FSAR) to include the description for how isolation devices are qualified.

07.09-2

List all safety system to safety system interfaces and their connection types and all safety system to non-safety system interfaces and their connection types.

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." RG 1.75 provides guidance on the physical separation requirements of IEEE Std. 603-1991, Clause 5.6. BTP 7-11 provides guidance on application and qualification of isolation devices to meet the electrical isolation requirements of IEEE Std. 603-1991

REQUEST FOR ADDITIONAL INFORMATION 45-7883

Clause 5.6. 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, Rev. 0, "Safety I&C System," describes the design features of the APR1400 digital I&C system and how the design complies with NRC regulations. Section 4.2.4 of the technical report, "System Interfaces," discusses Plant Protection System (PPS) cabinet interfaces. The applicant provided description for some of the system interfaces and their type (e.g. Auxiliary Process Cabinet - Safety connects to PPS cabinets via hardwire cables, Core Protection Calculator System connects to PPS cabinets via hardwire cables, and PPS sends initiation signals to Engineered Safety Features-Component Control System Group Controllers through fiber optic Serial Data Link). It is not clear how other safety systems and non-safety systems are connected. List all safety to safety system interfaces and their interface type, and to list all safety to non-safety system interfaces and their interface type, and provide information on how these interfaces meet the requirements of IEEE Std. 603-1991, Clause 5.6, or provide a reference to sections of the FSAR or technical reports where this information resides. Update the FSAR with the requested information.

07.09-3

Address multidivisional control and display stations staff guidance for the data communication interface between the Information Flat Panel Display (IFPD) and Engineered Safety Features-Component Control System Soft Control Module (ESCM).

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." RG 1.75 provides guidance on the physical separation requirements of IEEE Std. 603-1991, Clause 5.6. BTP 7-11 provides guidance on application and qualification of isolation devices to meet the electrical isolation requirements of IEEE Std. 603-1991 Clause 5.6. 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, Rev. 0, "Safety I&C System," describes the design features of the APR1400 digital I&C system and how the design complies with NRC regulation. Technical Report, Appendix C, Section C.3, "Data Communication Systems" states, in part, "DI&C-ISG-04 Section 3 is not applicable as described in Section C.5.3." Section C.5.1.5 discusses communication between IFPD and ESCM, and that data sent from IFPD to ESCM are used to support operator's manual action.

Although the ESCM may not be used to perform a credited safety function, it appears to the staff that the component data from IFPD (non-safety control) to ESCM (safety-related) may be used to control safety-related equipment. Section 3.1.1 of DI&C-ISG-04 provides guidance on the control of safety-related equipment from a non-safety workstation. Based on the staff's understanding of the interface between ESCM and the IFPD, the staff finds that the non-safety IFPD is used to indirectly control safety-related equipment. Thus, the guidance of DI&C-ISG-04 applies. The staff requests the applicant to address the staff positions in ISG-04, Section 3, for this interface. Also, it is not clear if it is possible to bypass or lockout any safety functions from the non-safety IFPD via the ESCM. Identify and describe the various types of commands that ESCM could send to the Engineered Safety Features - Component Control System (ESF-CCS) Loop Controller (LC). The staff requests applicant to clarify, and update the FSAR with this information.

REQUEST FOR ADDITIONAL INFORMATION 45-7883

07.09-4

Discuss how the Integrated Test Panel interdivisional (ITP) communications to display Containment Isolation Valve (CIV) positions 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." RG 1.75 provides guidance on the physical separation requirements of IEEE Std. 603-1991, Clause 5.6. BTP 7-11 provides guidance on application and qualification of isolation devices to meet the electrical isolation requirements of IEEE Std. 603-1991 Clause 5.6. 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, Rev. 0, "Safety I&C System," Section C.5.1.4, "SDL [Serial Data Link] communication between ITPs," states conformance to DI&C ISG-04, Section 1, Position 3, and defines the purpose of the ITP-to-ITP 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 ITP interdivisional communication as described in the technical report meets DI&C ISG-04, Section 1, Position 3. Specifically, how do the described ITP 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.

07.09-5

Clarify what is meant by "the Qualified Indication and Alarm System - non-safety (QIAS-N) network is implemented by the Safety System Data Network (SDN)."

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." RG 1.75 provides guidance on the physical separation requirements of IEEE Std. 603-1991, Clause 5.6. BTP 7-11 provides guidance on application and qualification of isolation devices to meet the electrical isolation requirements of IEEE Std. 603-1991 Clause 5.6. DI&C-ISG-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

APR1400 FSAR, Tier 2, Section 7.9.1.4, "Data Communication from Safety System to Non-Safety System" states, in part, "The QIAS-N network is implemented by the SDN." It is not clear what is meant by "is implemented by the SDN." Is the applicant trying to say QIAS-N network will be implemented using AF100 network communication system, which is discussed in the Common Q topical report? The staff requests applicant to clarify and update the FSAR accordingly.

REQUEST FOR ADDITIONAL INFORMATION 45-7883

07.09-6

Provide summary of how communication independence requirements are met between redundant portions of the safety system.

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." RG 1.75 provides guidance on the physical separation requirements of IEEE Std. 603-1991, Clause 5.6. BTP 7-11 provides guidance on application and qualification of isolation devices to meet the electrical isolation requirements of IEEE Std. 603-1991 Clause 5.6. DI&C-ISG-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

APR1400 FSAR, Tier 2, Section 7.2.2.3, "Independence" states, "Independence between redundant portions of the safety system. The routing of Class 1E and associated cabling and sensing lines from sensors meets the guidance of NRC RG 1.75 (Reference 7) and NRC RG 1.151 (Reference 8). The cablings for the four safety divisions are routed separately. The PPS divisions receive ac power from the vital bus power supply system. The PPS does not share the power between divisions." This section of the FSAR does not discuss how data communication independence between redundant portions of the Plant Protection System (PPS) is achieved to meet the requirements of IEEE Std. 603-1991, Clause 5.6.1. Provide either a summary of how communications independence requirements are met or reference the particular section of the Safety I&C System Technical Report where data communication independence between redundant portions of the safety system is being analyzed.

07.09-7

Clarify what is meant by "any errors", and describe potential data communication faults and mitigating measures.

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." RG 1.75 provides guidance on the physical separation requirements of IEEE Std. 603-1991, Clause 5.6. BTP 7-11 provides guidance on application and qualification of isolation devices to meet the electrical isolation requirements of IEEE Std. 603-1991 Clause 5.6. 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 12, states, in part, "Communication faults should not adversely affect the performance of required safety functions in any way...", and lists examples of credible communication faults. APR1400 FSAR, Tier 2, Section 7.1, Page 7.1-3, states, in part, "Data communications within or between I&C systems are designed to provide reasonable assurance that any error in data communication will not cause inadvertent actuations or prevent the safety functions from being performed." Clarify whether the applicant really meant "any" errors as this goal is typically difficult to achieve except on simple communication schemes. Also, per DI&C ISG-04, Section 1, Position 12, describe the potential data communication faults between IFPD and ESCM and the mitigating measures for each fault.