

KHNPDCDRAIsPEm Resource

From: Ciocco, Jeff
Sent: Thursday, June 18, 2015 8:53 AM
To: apr1400rai@khnp.co.kr; KHNPDCDRAIsPEm Resource; Harry (Hyun Seung) Chang; Yunho Kim; Steven Mannon
Cc: Zhao, Jack; Jackson, Terry; Ward, William; Lee, Samuel
Subject: APR1400 Design Certification Application RAI 37-7882 (07.03 - Engineered Safety Features Systems)
Attachments: APR1400 DC RAI 37 ICE1 7882.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 60 days to respond to the RAI. We may adjust the schedule accordingly.

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



Hearing Identifier: KHNP_APR1400_DCD_RAI_Public
Email Number: 43

Mail Envelope Properties (A67A2D233B3FBB4C8B5109AD7C39550715C4DCAE8F)

Subject: APR1400 Design Certification Application RAI 37-7882 (07.03 - Engineered Safety Features Systems)
Sent Date: 6/18/2015 8:52:33 AM
Received Date: 6/18/2015 8:52:47 AM
From: Ciocco, Jeff
Created By: Jeff.Ciocco@nrc.gov

Recipients:

"Zhao, Jack" <Jack.Zhao@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	631	6/18/2015 8:52:47 AM
APR1400 DC RAI 37 ICE1 7882.pdf		94265
image001.jpg	5020	

Options

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

REQUEST FOR ADDITIONAL INFORMATION 37-7882

Issue Date: 06/18/2015

Application Title: APR1400 Design Certification Review – 52-046

Operating Company: Korea Hydro & Nuclear Power Co. Ltd.

Docket No. 52-046

Review Section: 07.03 - Engineered Safety Features Systems

Application Section:

QUESTIONS

07.03-1

Demonstrate how software common cause failure (CCF) is addressed and the quality requirement is met for the component interface modules (CIM) used downstream of both the Engineered Safety Features - Component Control System (ESF-CCS) system and the Diverse Protection System (DPS).

10 CFR 50, Appendix A, General Design Criteria (GDC) 21 states, in part, that the protection system (or safety system) shall be designed for high functional reliability commensurate with the safety functions to be performed. 10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. Clause 5.3 of IEEE Std. 603-1991 requires, in part, that safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum (SRM) (ML003708056) on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs" contains the NRC regulatory guidance and position on the diversity and defense-in-depth (D3). It says, in part, that if a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure as the safety system, shall be required to perform either the same function as the safety system function that is vulnerable to common mode failure or a different function that provides adequate protection. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary functions under the associated event conditions.

Technical Report (TeR) APR1400-E-J-NR-14001-P, Rev. 0, "Component Interface Module," states, in part, that the field programmable gate array (FPGA) portion of the CIM is safety-related for the diagnostic and surveillance features which are used in associated safety functions. As shown in Figure 4.2-1 of the above TeR, several outputs from the FPGA portion of the CIM are sent to the safety-related ESF-CCS Loop Controller. As described in Branch Technical Position 7-19, Rev. 6, the staff considers programmable technology (firmware) to be software. In addition, it appears the FPGA portion of the CIM is potentially involved in safety functions since it sends signals to the safety-related ESF-CCS Loop Controller. Describe how software common cause failure is addressed, and quality requirement met, for the entire CIM including the FPGA. If applicable information is in other portions of the application, provide the necessary references to those sections. Update the final safety analysis report (FSAR) and technical reports accordingly.

07.03-2

Clarify what functions the FPGA portion of the CIM performs.

Both 10 CFR 50.54(jj) and 10 CFR 50.55(i) require structures, systems, and components subject to the codes and standards in 10 CFR 50.55a to be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. As indicated in Figure 4.2-1 of TeR APR1400-E-J-NR-14001-P, Rev. 0, "Component Interface Module," the FPGA portion of the CIM sends outputs to the safety-related ESF-CCS Loop

REQUEST FOR ADDITIONAL INFORMATION 37-7882

Controller. However, Section C.5.2.1 of Appendix C in TeR APR1400-Z-J-NR-14001-P, Rev. 0, "Safety I&C System Technical Report," states the diagnosis section only receives signals from the priority logic section and base section of the CIM. Clarify the inconsistent description of the functions of the CIM FPGA portion.

