KHNPDCDRAIsPEm Resource

From:	Ciocco, Jeff
Sent:	Tuesday, June 16, 2015 10:36 AM
To:	apr1400rai@khnp.co.kr; KHNPDCDRAIsPEm Resource; Harry (Hyun Seung) Chang (hyunseung.chang@gmail.com); Yunho Kim (yshh8226@gmail.com); Steven Mannon
Cc:	Kalathiveettil, Dawnmathews; Jackson, Terry; Ward, William; Lee, Samuel
Subject:	APR1400 Design Certification Application RAI 33-7880 (07.08 - Diverse Instrumentation and Control Systems)
Attachments:	APR1400 DC RAI 33 ICE1 7880.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.

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: 38

Mail Envelope Properties (A67A2D233B3FBB4C8B5109AD7C39550715C4CCD548)

Subject: APR1400 Design Certification Application RAI 33-7880 (07.08 - Diverse Instrumentation and Control Systems)
Sent Date: 6/16/2015 10:36:12 AM
Received Date: 6/16/2015 10:36:19 AM
From: Ciocco, Jeff

Created By: Jeff.Ciocco@nrc.gov

Recipients:
"Kalathiveettil, Dawnmathews" <Dawnmathews.Kalathiveettil@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)" <hyunseung.chang@gmail.com>
Tracking Status: None
"Yunho Kim (yshh8226@gmail.com)" <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	519	6/16/2015 10:36:19 AM
APR1400 DC RAI 33 ICE1 7880.pdf	129305	
image001.jpg	5020	

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

REQUEST FOR ADDITIONAL INFORMATION 33-7880

Issue Date: 06/16/2015
Application Title: APR1400 Design Certification Review – 52-046
Operating Company: Korea Hydro & Nuclear Power Co. Ltd.
Docket No. 52-046
Review Section: 07.08 - Diverse Instrumentation and Control Systems
Application Section:

QUESTIONS

07.08-1
Clarify what is meant by diverse design group.

10 CFR Part 50, Appendix A, General Design Criterion (GDC) 22, "Protection system independence," states, "The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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." Item II.Q of the Staff Requirements Memorandum (SRM) (ML003708056) to SECY-93-087 (ML003708021), Positions 3, states, "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, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions."

Section 5.1 of Technical Report APR1400-Z-J-NR-14002-P, Rev.0, "Diversity and Defense in Depth," states, "The DPS [Diverse Protection System] is designed to mitigate the consequences of a DBE [design basis event] concurrent with a postulated CCF [common-cause failure] of the safety I&C [instrumentation and control] system digital computer." The DPS is part of the Diverse Actuation System. The acceptance criteria for the DPS Inspection, Tests, Analyses, and Acceptance Criteria (ITAAC) Item 2 on Table 2.5.2-5 (2 of 3) of the APR1400 FSAR, Tier 1, states, "The as-built DPS is developed by diverse design group from the design group(s) which developed the PPS [Plant Protection System] and ESF-CCS [Engineered Safety Features - Component Control System] software." Based on the staff's evaluation, the staff requests the applicant to provide definition(s) for diverse design group. Specifically, what criteria would the groups need to meet in order to be considered diverse from one another (e.g., level of communication, organizational separation, etc.) Update final safety analysis report (FSAR) and technical reports accordingly.

07.08-2
Clarify the apparent inconsistency between Tier 1 and Tier 2 information with regards to the purpose and scope of the Diverse Actuation System (DAS).

10 CFR 50, Appendix A, GDC 22, "Protection system independence" states, "The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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." Item II.Q of the SRM to SECY-93-087, Positions 3, states, "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, shall be required to perform either the same function or a

different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions."

APR1400 FSAR, Tier 2, Section 7.8, states, "The diverse actuation system (DAS) consists of the diverse instrumentation and control (I&C) systems that are provided to protect against potential common-cause failure (CCF) of digital safety I&C systems including the plant protection system (PPS) and engineered safety features-component control system (ESF-CCS)." However, APR1400 FSAR Tier 1, Section 2.5.2.1, states, "The diverse actuation system (DAS) is a non-safety system which provides a diverse mechanism to decrease risk from the anticipated transients without scram (ATWS) events. The DAS also assists the mitigation of the effects of a postulated software common cause failure (CCF) within the plant protection system (PPS) and the engineered safety features component control system (ESF-CCS)." There is inconsistency between the information provided within the Tier 1 and Tier 2 documents. As indicated by the Tier 2 statement, DAS mitigates the effects of postulated CCF within the entire digital safety I&C systems, whereas the Tier 1 description is limited to the PPS and ESF-CCS. Based on the staff's evaluation, the staff requests the applicant to correct/update the Tier 1 information wherever applicable, such that Tier 1 information is consistent with Tier 2 information.

07.08-3

In case of a potential CCF of the Qualified Indication and Alarm System-P (QIAS-P), demonstrate that the Diverse Indication System (DIS) would still be able to conform to Position 4 of SRM to SECY 93-087 and satisfy the requirements of 10 CFR 50, Appendix A, GDC 22.

10 CFR 50, Appendix A, GDC 22, "Protection system independence" states, "The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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." Item II.Q of the SRM to SECY-93-087, Positions 3, states, "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, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions." Positions 4 states that a set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. These credited displays and controls shall be independent and diverse from the safety-related computer system.

APR1400 FSAR, Tier 2, Section 7.8, states, in part, the DAS consists of the diverse I&C systems that are provided to protect against potential CCF of digital safety I&C systems. APR1400 FSAR, Tier 2, Section 7.8.1.3, states, "The DIS provides functions to monitor critical variables following a postulated software CCF of safety I&C systems." Figure 5-2 "Diversity Features between QIAS and DIS" of the Diversity and Defense in Depth (D3) Technical Report (TeR), shows that the DIS receives Core Exit Thermocouples (CETs)/Heated Junction Thermocouples (HJTCs) hardwired signal inputs from the QIAS-P.

1. Confirm whether the applicant takes credit for CETs/HJTCs signal inputs to the DIS in their CCF Coping Analysis.
2. Explain why the CETs/HJTCs signals are routed through the QIAS-P instead of the APC-S (other DIS input variables come from the APC-S) and demonstrate that by routing the signals through QIAS-P, the DIS would still be able to meet Position 4 of SRM to SECY 93-087 in case of a potential CCF of the QIAS-P.
3. Would the DIS still receive the CETs/HJTCs hardwired signals in case of a postulated CCF of the QIAS-P?
4. Verify the origin of the CETs/HJTCs signals before the signals are received by the QIAS-P.

07.08-4
Demonstrate how the DIS is independent from the APC-S and QIAS-P when it receives signals from those systems.

10 CFR 50, Appendix A, GDC 22, "Protection system independence" states, "The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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." Item II.Q of the SRM to SECY-93-087, Positions 3, states, "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, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions." Positions 4 states that a set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. These credited displays and controls shall be independent and diverse from the safety-related computer system.

The DIS is part of the DAS. APR1400 FSAR, Tier 2, Section 7.8.1.3, states, "The DIS provides functions to monitor critical variables following a postulated software CCF of safety I&C systems. Because the DIS receives its hardwired signal inputs from isolation devices in the auxiliary process cabinet-safety (APC-S) as well as in qualified indication and alarm system – P (QIAS-P), the DIS is independent from the APC-S and QIAS-P." Receiving hardwired signal inputs from isolation devices does not necessarily demonstrate independence; particularly with respect to data that could be corrupted, incorrect, or missing from the receiving systems. In addition, while there may be electrical isolation, there could be functional dependence between the systems. Based on the staff's evaluation, the staff requests the applicant to demonstrate the communication and functional independence between the DIS and the APC-S and QIAS-P.

07.08-5
Define what the applicant considers to be programmable devices and analog equipment.

10 CFR 50, Appendix A, GDC 22, "Protection system independence" states, "The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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." Item II.Q of the SRM to SECY-93-087, Positions 3, states, "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, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions." Positions 4 states that a set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. These credited displays and controls shall be independent and diverse from the safety-related computer system.

APR1400 FSAR, Tier 2, Section 7.8, states, "The diverse actuation system (DAS) consists of the diverse instrumentation and control (I&C) systems that are provided to protect against potential common-cause failure (CCF) of digital safety I&C systems including the plant protection system (PPS) and engineered safety features-component control system (ESF-CCS)." FSAR Tier 2, Section 7.8.1.3, states in part that the DIS receives its hardwired signal inputs from isolation devices in the auxiliary process cabinet-safety (APC-S) as well as in the

qualified indication and alarm system-P (QIAS-P). Section 4.1.1.5 of Technical Report APR1400-Z-J-NR-14001-P, Rev.0, “Safety I&C System,” states, “There are no programmable digital devices in the APC-S.” Provide definition(s) for programmable devices versus non-programmable devices. In addition, Section 5.1 of Technical Report APR1400-Z-J-NR-14002-P, Rev.0, “Diversity and Defense in Depth,” states, “The safety class sensors and APC-S are analog equipment.” Provide definition(s) for analog equipment. Does analog equipment and non-programmable devices mean the same? Update FSAR and technical reports accordingly.


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