KHNPDCDRAIsPEm Resource

From:	Ward, William
Sent:	Friday, December 18, 2015 4:59 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; Kalathiveettil, Dawnmathews; Jackson, Terry; Ward, William
Subject:	APR1400 Design Certification Application RAI 342-8291 (7.8 - Diverse Instrumentation and Control Systems)
Attachments:	APR1400 DC RAI 342 ICE 8291.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.

07.08-6 : 45days
07.08-7 : 90days
07.08-8 : 45days
07.08-9 : 45days
07.08-10 : 45days
07.08-11 : 45days
07.08-12 : 45days
07.08-13 : 45days
07.08-14 : 60days
07.08-15 : 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: 391

Mail Envelope Properties (d6e9468b395b42c48dce875848b6836c)

Subject: APR1400 Design Certification Application RAI 342-8291 (7.8 - Diverse Instrumentation and Control Systems)
Sent Date: 12/18/2015 4:59:17 PM
Received Date: 12/18/2015 4:59:19 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
"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
"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	1010	12/18/2015 4:59:19 PM
APR1400 DC RAI 342 ICE 8291.pdf	115486	

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

REQUEST FOR ADDITIONAL INFORMATION 342-8291

Issue Date: 12/18/2015
Application Title: APR1400 Design Certification Review – 52-046
Operating Company: Korea Hydro & Nuclear Power Co. Ltd.
Docket No. 52-046
Review Section: 07.08 - Diverse Instrumentation and Control Systems
Application Section:

QUESTIONS

07.08-6

Verify whether the statement made in Technical Report APR1400-Z-J-NR-14002-P, Rev.0, regarding the Component Interface Module (CIM) being fully tested, is true or not.

10 CFR Part 50, Appendix A, General Design Criteria (GDC) 22, requires design techniques such as functional diversity or diversity in component design and principles of operation. Item II.Q of the Staff Requirements Memorandum (SRM) to SECY-93-087, Position 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 4.2.2, "Available I&C Functions," of Technical Report APR1400-Z-A-NR-14019-P, Rev.0, “CCF [common-cause failure] Coping Analysis,” states, “Command inputs ... are received from three sources to the CIM; two I&C subsystem (ESF-CCS and DPS) commands and DMA switches.” Earlier, the section states, “The CIM is a non-software-based qualified nuclear safety grade module. Therefore the CIM is not subjected to the same CCF with ESF-CCS which is implemented by qualified PLC platform.”

Technical Report APR1400-Z-J-NR-14002-P, Rev.0, “Diversity and Defense in Depth,” Appendix A, "Conformance to BTP 7-19," Section 1.9, “Design Attributes to Eliminate Consideration of CCF,” states, “In addition, the sections of the CIM that are relied upon for both the safety systems and the diverse systems are fully tested.” Staff expected to see a similar statement in Technical Report APR1400-E-J-NR-14001-P, Rev. 0, "Component Interface Module," regarding fully testing or 100% testing of CIMs. However, since we did not, please verify whether the statement made in Technical Report APR1400-Z-J-NR-14002-P, Rev.0, regarding the CIM being fully tested is true or not.

Other areas in the application also refer to the CIM being fully tested, so the applicant is requested to ensure consistency throughout the application regarding CIM testing. In addition, if 100 percent testing will be performed on the CIM, describe how it will be 100 percent combinatorial testing as described in BTP 7-19.

07.08-7

Clarify how the applicant knows when a software CCF has occurred within the safety system, including the Plant Protection System (PPS) and Engineered Safety Features - Component Control System (ESF-CCS).

10 CFR Part 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, Position 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.” NRC NUREG-800, Section 7.8, “Review Procedures,” states in part, “Information should be available in the control room to indicate the operation of the diverse I&C systems. This aspect of the review may involve considerations included in emergency operating procedures.”

Clarify how operators will be alerted when a software CCF has occurred within the safety system, including the PPS and ESF-CCS. Clarify whether there are any indications or annunciators for a software CCF condition. Also clarify what indications prompt the operators to use the Diverse Actuation System (DAS), and what indications are available in the control room to indicate the operation of the diverse I&C systems. Update the FSAR documents and/or technical reports accordingly.

07.08-8

Clarify in APR1400 FSAR, Tier 2 how the reactor trip switchgear (RTSG) is diverse from reactor trip circuit breaker (RTCB).

10 CFR Part 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, Position 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.”

Technical Report APR1400-Z-J-NR-14002-P, Rev.0, “Diversity and Defense in Depth,” Section 5.1, “Diverse Protection System,” states, “The DPS is designed to transmit reactor trip signals to a total of eight shunt trip devices of the RTSS-1 and RTSS-2 reactor trip breakers. The PPS transmits reactor trip signals to a total of eight undervoltage trip devices of the RTSS-1 and RTSS-2 reactor trip circuit breakers. Four trip circuit breakers of RTSS-1 are diverse from four trip circuit breakers of RTSS-2. This arrangement ensures the capability of the Diverse Protection System (DPS) to interrupt power to the control element drive mechanisms (CEDMs) regardless of the PPS failure to trip the reactor.” Describe the level and types of diversity between the RTSG and the RTCB. Update FSAR documents accordingly.

07.08-9

Clarify why the Diverse Manual ESF Actuation (DMA) input is missing to the CIM priority logic for Divisions B and D in APR1400 FSAR, Tier 2, Figure 7.3-5, "ESFAS Functional Logic Diagram, (CSAS)."

10 CFR Part 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, Position 4, states, “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.” Clarify why the DMA input is missing to the CIM priority logic for Divisions B and D in APR1400 FSAR, Tier 2, Figure 7.3-5. Update the FSAR documents accordingly.

07.08-10

Clarify that the ATWS mitigation logic and DAS is designed such that, once initiated, the mitigation function will go to completion.

10 CFR Part 50.62, “Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants,” requirement (c)(1) states, “Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.” Item II.Q of the SRM to SECY-93-087, Position 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.”

Clarify whether the ATWS mitigation logic and DAS is designed such that, once initiated, the mitigation functions will go to completion. Update the FSAR documents and/or technical reports accordingly.

07.08-11

Clarify why any system in the APR1400 design that doesn't have a "functional programmable unit," is not susceptible to a software CCF.

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, Position 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, "Diverse Instrumentation and Control Systems," 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, "Diverse Indication System," (DIS) 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, "Auxiliary Process Cabinet - Safety," 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." (Staff acknowledges that the response to Question 07.08-5, see below, will modify this statement.) 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 programmable devices versus non-programmable devices.

In the response to RAI 7880 dated 7/16/15 (ML15197A290), Question 07.08-5, the term "functional programmable unit" was introduced, including a definition for it. The term was defined as a computer that consists of one or more associated processing units and a peripheral equipment, as defined in Section 3.1.8 of IEEE Std 7-4.3.2-2003. The question response explains that if the equipment doesn't have any functional programmable units, it is not susceptible to a software CCF. The definition of functional programmable unit provided in the question response is vague. For instance, what is classified as a computer? As defined, one could interpret functional programmable unit to exclude programmable logic technology, such as field programmable gate arrays or programmable logic devices. Branch Technical Position 7-19 of NUREG-0800, Section B.1.4, states "In this guidance, common software includes software, firmware, and logic developed from software-based development systems." Provide further clarification with regards to the APC-S and its non-susceptibility to software common cause failure in comparison to the definition used by the staff to consider components that are

susceptible to software common cause failure. Inclusion of a diagram explaining the logic within the APC-S would be helpful. Update the FSAR documents and/or technical reports accordingly.

07.08-12

Clarify whether the Diverse Indication System (DIS) manual transfer switch for heated junction thermocouple (HJTC) control is safety or non-safety related and address the potential for a software CCF of the QIAS-P to affect the transfer of HJTC control to the DIS.

10 CFR Part 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, Position 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." Position 4, states, "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."

Based on the staff's evaluation, clarify whether the DIS manual transfer switch for HJTC control is safety or non-safety related equipment. Explain whether a software CCF of the QIAS-P could adversely affect the manual switch or the transfer of HJTC control to the DIS. In other words, could such a failure adversely affect the DIS from performing its diverse functions? Provide diagram(s) illustrating the interface between QIAS-P and DIS with the manual transfer switch to illustrate such design aspects as safety classification, signal flow and type of signals. Update the FSAR documents and/or technical reports accordingly.

07.08-13

Clarify whether a software CCF of a safety-related I&C system could result in a loss of power to the DAS and consequently prevent the DAS from performing its diverse functions.

10 CFR Part 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, Position 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." Position 4, states, "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."

Discuss the potential for a software CCF in a safety-related I&C system to compromise the ability of the safety-related I&C system to perform its function and simultaneously result in a loss of power to the DAS and consequently prevent the DAS from performing its diverse functions. In other words, provide analysis demonstrating that the DAS power supply is protected in all cases of a software CCF of the safety-related I&C systems. The response should include clarification as to how the DAS will be powered in a loss-of-offsite power scenario, alternate power sources that are available to power the DAS, and why they are not susceptible to a software CCF of any safety-related I&C system in the plant. Update the FSAR documents and/or technical reports accordingly.

07.08-14

Clarify whether the Diverse Manual ESF [Engineered Safety Features] Action (DMA) enable switch is susceptible to a software CCF the safety system (including the PPS and ESF-CCS) and consequently prevent the DMA switches from performing their diverse functions.

10 CFR Part 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 Staff Requirements Memorandum (SRM) to SECY-93-087, Position 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." Position 4, states, "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."

Describe why the DMA enable switch is not susceptible to a software CCF in the safety I&C systems (including the PPS and ESF-CCS) and consequently prevents the DMA switches from performing their diverse functions. In the description, provide analysis and diagrams as necessary to illustrate the independence and the interface between the DMA enable switch and the safety-related I&C systems. In addition, is the DMA enable switch credited for the mitigation of a design bases event which occurs concurrent with a software CCF of the safety system? Update the FSAR documents and/or technical reports accordingly.

07.08-15

Describe why a safety injection into the RCS due to a spurious Diverse Protection System (DPS) safety injection actuation, and during reactor coolant system (RCS) heatup and cooldown conditions, does not cause any significant risk to plant safety.

10 CFR Part 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 Staff Requirements Memorandum (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.”

Technical Report APR1400-Z-J-NR-14002-P, Rev.0, “Diversity and Defense in Depth,” Appendix A, Section 1.8, “Potential Effects of CCF: Failure to Actuate and Spurious Actuation,” describes the effects and details of a spurious DPS safety injection actuation during the RCS normal operating condition and during the RCS heatup and cooldown conditions.

The guidance of NUREG-800, Section 7.8, states, in part, the diverse I&C systems design should limit the potential for inadvertent actuation and challenges to safety systems. Describe why a safety injection into the RCS due to spurious DPS safety injection actuation, for RCS heatup and cooldown conditions, does not cause any significant risk to plant safety. Is this situation bounded by the safety analysis or another analysis? Update the FSAR documents and/or technical reports accordingly.