KHNPDCDRAIsPEm Resource

From: Ciocco, Jeff
Sent: Tuesday, October 20, 2015 2:02 PM
To: apr1400rai@khnp.co.kr; KHNPDCDRAIsPEm Resource; Harry (Hyun Seung) Chang; Andy Jiyong Oh; Erin Wisler
Cc: Taneja, Dinesh; Jackson, Terry; Ward, William; Lee, Samuel
Subject: APR1400 Design Certification Application RAI 261-8253 (07.01 - Instrumentation and Controls - Introduction)
Attachments: APR1400 DC RAI 261 ICE 8253.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.

07.01-26: 30 days
07.01-27: 30 days
07.01-28: 60 days
07.01-29: 30 days
07.01-30: 30 days
07.01-31: 30 days
07.01-32: 30 days
07.01-33: 45 days

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: 300

Mail Envelope Properties (9125d1fbfb7a4fbaa0a1c9e0c9529c15)

Subject: APR1400 Design Certification Application RAI 261-8253 (07.01 - Instrumentation and Controls - Introduction)
Sent Date: 10/20/2015 2:01:55 PM
Received Date: 10/20/2015 2:01:56 PM
From: Ciocco, Jeff

Created By: Jeff.Ciocco@nrc.gov

Recipients:
"Taneja, Dinesh" <Dinesh.Taneja@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
"Andy Jiyong Oh" <jiyong.oh5@gmail.com>
Tracking Status: None
"Erin Wisler " <erin.wisler@aecom.com>
Tracking Status: None

Post Office: HQPWMSMRS07.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	805	10/20/2015 2:01:56 PM
image001.jpg	5040	
APR1400 DC RAI 261 ICE 8253.pdf	106464	

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


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

REQUEST FOR ADDITIONAL INFORMATION 261-8253

Issue Date: 10/20/2015
Application Title: APR1400 Design Certification Review – 52-046
Operating Company: Korea Hydro & Nuclear Power Co. Ltd.
Docket No. 52-046
Review Section: 07.01 - Instrumentation and Controls - Introduction
Application Section: 7.1.3 Digital I&C Systems Software Design Process & SPM Technical Report

QUESTIONS

07.01-26

10 CFR Part 50, Appendix A, General Design Criterion (GDC) 1 requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. In addition, 10 CFR 50.55a(h)(3) incorporates by reference IEEE Std 603-1991. Clause 5.3 of IEEE Std. 603-1991 requires that components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

Based on review of the technical report APR1400-Z-J-NR-14003, “Software Program Manual” (SPM), Rev. 0, Section 2.1, “Software Classification and Categorization,” Tables 4-2, “Tasks required for Software Categories,” & 4-3, “Software tasks and Responsibilities,” and Appendix A, “The I&C System Software Classes,” the applicant is asked to provide following additional information:

1. Appendix A, Section A.2, of the SPM includes information to justify the use of Important-to-Safety (ITS) class software and states that an software hazard analysis is provided. The applicant is asked to provide this analysis.

2. SPM Table A-1, Assignment of Software for the I&C Systems to Classes,” outlines assignments of I&C systems' software to specific classes. However, the software class for subsystems Control Panel Multiplexer (CPM), Control Channel Gateway (CCG), and Component Interface Module (CIM) is not specified. The applicant is asked to provide software classification for CPM, CCG, and CIM subsystems.

3. Table 4-2, Footnote 2, and the section in Table 4-3 applicable to Table 4-2, Footnote 2, have opposing statements. The applicant is asked to resolve this discrepancy.

07.01-27

Provide a combined license (COL) information item for the COL referencing the APR1400 design certification to provide the Software Installation Plan (SInstP), Software Training Plan (STrngP), and Software Operation and Maintenance Plan (SOMP).

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. IEEE Std 603-1991, Clause 5.3, states, in part, that safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. In addition, 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 1 states, in part, that structures, systems, and components (SSCs) important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Technical Report (TeR) APR1400-Z-J-NR-14003, “Software Program Manual [(SPM)],” Table 4-3, indicates that the SInstP, SOMP, STrngP will be the responsibility of the utility. The staff could not identify a COL information item in APR1400 FSAR Tier

2, Table 1.8-2, specifying these plans are the responsibility of the COL applicant. Provide a COL information item to address this issue.

07.01-28

Identify the relationship between the TeR APR1400-Z-J-NR-14003, “Software Program Manual” and the Common Q Software Program Manual.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. IEEE Std 603-1991, Clause 5.3, states, in part, that safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. The APR1400 design certification application (see TeR APR1400-Z-J-NR-14001, "Safety I&C System," Rev. 0, Section 8, "Safety I&C System Platform") identifies Common Q as the digital platform that will be used to implement safety-related instrumentation and control (I&C) systems, such as the Plant Protection System. The NRC approved Topical Report WCAP-16096-NP-A, Revision 4, “Software Program Manual for Common Q Systems,” dated Feb. 2013. What is the relationship between the APR1400 Software Program Manual and WCAP-16096?

07.01-29

Describe the analysis that is necessary when using existing nuclear power plant software.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Clause 5.3 of IEEE Std 603-1991 requires components and modules of safety-related I&C equipment to be of a quality that is consistent with minimum maintenance requirements and low failure rates. Section 4.1.2, "Scope," of Technical Report APR1400-Z-J-NR-14003, Rev. 0, “Software Program Manual,” describes the criteria for using pre-existing nuclear power plant software in the APR1400. However, the criteria did not describe the analysis of software features/functionality, the application environment/interface the previous software used, and necessary modifications to allow its use in the APR1400. While the use of pre-existing software can provide benefits, without a thorough analysis of its functionality, interface points, and how it will fit in the new application environment, software faults can be introduced. Modify the APR1400 SPM to identify and describe the analysis that will need to be performed on pre-existing software to demonstrate that it can be safely re-used in the APR1400 design.

07.01-30

Describe how the Software Quality Assurance Plan relates to the APR1400 Quality Assurance Manual.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Clause 5.3 of IEEE Std 603-1991 requires safety system equipment to be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Section 4, "Software Quality Assurance Plan," of Technical Report APR1400-Z-J-NR-14003, Rev. 0, “Software Program Manual,” describes the Software Quality Assurance Plan. However, it did not appear to describe the relationship between the Software Quality

Assurance Plan and the APR1400 Quality Assurance Manual. Modify the APR1400 SPM to describe the relationship and interfaces between these two documents.

07.01-31

Describe the software development lifecycle model that will be used to develop APR1400 safety-related I&C software.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Clause 5.3 of IEEE Std 603-1991 requires safety system equipment to be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Section 4.8, "Tools, Techniques, and Methodologies," of Technical Report APR1400-Z-J-NR-14003, Rev. 0, “Software Program Manual,” states the use of the waterfall model of software development and testing techniques shall be employed. However, this is the only statement in the software program manual regarding the waterfall model. Based on recent experiences developing new nuclear power plant software, vendors use a cyclic model that incorporates several baselines of software that go through the various lifecycle phases multiple times versus a once-through development process such as the waterfall model. Will the APR1400 use a true waterfall model for software development or will it use a form of cyclic software development? Modify the APR1400 SPM to describe the type of software development lifecycle model that will be employed for the APR1400 safety-related software development.

07.01-32

Describe the scope of the factory and site acceptance testing.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Clause 5.3 of IEEE Std 603-1991 requires safety system equipment to be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Section 13, "Software Test Plan," of Technical Report APR1400-Z-J-NR-14003, Rev. 0, “Software Program Manual,” describes the software test plan, but does not describe the scope of systems that will be tested in the factory and site acceptance tests. For example, in the factory acceptance test, will the Plant Protection System be tested alone or will it be tested while connected to other I&C systems? Also, will tests be conducted with the safety and non-safety I&C systems connected. Modify the APR1400 SPM to identify the scope of systems that will be connected and tested in an integrated fashion for the factory and site acceptance tests.

07.01-33

Provide additional information on the secure development and operational environment (SDOE) of APR1400 safety I&C systems, including details on the vulnerability assessment and the use of commercial off-the-self (COTS) software.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. IEEE Std 603-1991, Clause 5.9, states, “The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be

supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof." Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" provides guidance on establishing a SDOE in order to meet the requirements of IEEE Std 603-1991, Clause 5.9. Section C.2.1 of this guidance states, the licensee should assess the digital safety system's potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system's life cycle that could degrade its reliable operation. This assessment should identify the potential challenges to maintaining a secure operational environment for the digital safety system and a secure development environment for development life cycle phases. The results of the analysis should be used to establish design feature requirements (for both hardware and software) to establish a secure operational environment and protective measures to maintain it."

Technical Report APR1400-Z-J-NR-14003, "Software Program Manual," Section 14.0, SDOE, provides information on the establishment of SDOE for the digital safety I&C systems during the software life cycle phases. The staff reviewed this SDOE and requests the applicant to provide the following information in order for the staff to determine whether the APR1400 safety I&C systems meet the requirements IEEE Std 603-1991, Clause 5.9:

1. Section 14.1 of the SPM TeR states that "this section provides the guidance for establishment of SDOE for the digital safety I&C systems during the software life cycle phases in accordance with RG 1.152." It is not clear to the staff whether the applicant is committing to the information presented in this section or whether it is just guidance that may not be used during the life cycle phases of safety I&C systems. Clarify that the digital safety systems will follow the criteria established in this section of the SPM TeR.

2. The staff reviewed the summary of the vulnerability assessment in Section 14.5 of the SPM TeR and finds that additional information is needed to evaluate this vulnerability assessment. Specifically, this vulnerability assessment is generic and does not seem to address potential vulnerabilities specific to the APR1400 safety I&C system development and operational environment. In addition, it is unclear how each of the identified vulnerabilities is addressed by the security features described Sections 14.3.1 through 14.3.5 of the SPM TeR. Modify the SPM TeR to provide additional information regarding vulnerabilities specific to the APR1400 safety I&C systems and provide a mapping of how each of these vulnerabilities are addressed in Sections 14.3.1 through 14.3.5 of the SPM TeR.

3. Section 14.4, "Security Processes for [COTS] Software" of the SPM states "This section describes the processes employed to (1) achieve high assurance that COTS software products are free of unwanted code that could degrade the security of the safety I&C system, and (2) to ensure that any unwanted code that may be introduced into the safety I&C system by the COTS software products is detected and eliminated." The staff reviewed the information presented and could not find what measures are employed to ensure that COTS software products are free of unwanted code that could degrade the security of the safety I&C system. Since most COTS software code are not available for review to determine if this code may degrade the security or operation of the safety I&C system, what measures are in place to determine that the COTS software will not adversely impact the safety I&C system.