KHNPDCDRAIsPEm Resource

From: Ciocco, Jeff
Sent: Monday, January 04, 2016 7:53 AM
To: apr1400rai@khnp.co.kr; KHNPDCDRAIsPEm Resource; Harry (Hyun Seung) Chang; Andy Jiyong Oh; Erin Wisler
Cc: Morton, Wendell; Jackson, Terry; Ward, William; Lee, Samuel
Subject: APR1400 Design Certification Application RAI 356-7881 (07 - Instrumentation and Controls - Overview of Review Process)
Attachments: APR1400 DC RAI 356 ICE 7881.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.

07-1: 60 days
07-2: 60 days
07-3: 60 days
07-4: 45 days
07-5: 60 days
07-6: 45 days
07-7: 45 days
07-8: 60 days
07-9: 45 days
07-10: 45 days
07-11: 45 days
07-12: 30 days
07-13: 60 days
07-14: 60 days
07-15: 45 days
07-16: 45 days
07-17: 45 days
07-18: 60 days
07-19: 60 days
07-20: 60 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: 405

Mail Envelope Properties (bb86552e727944bd9b4df65ae546855a)

Subject: APR1400 Design Certification Application RAI 356-7881 (07 - Instrumentation and Controls - Overview of Review Process)
Sent Date: 1/4/2016 7:53:24 AM
Received Date: 1/4/2016 7:53:26 AM
From: Ciocco, Jeff

Created By: Jeff.Ciocco@nrc.gov

Recipients:
"Morton, Wendell" <Wendell.Morton@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: HQPWMSMRS08.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	991	1/4/2016 7:53:26 AM
image001.jpg	5040	
APR1400 DC RAI 356 ICE 7881.pdf	165538	

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 356-7881

Issue Date: 01/04/2016
Application Title: APR1400 Design Certification Review – 52-046
Operating Company: Korea Hydro & Nuclear Power Co. Ltd.
Docket No. 52-046
Review Section: 07 - Instrumentation and Controls - Overview of Review Process
Application Section: Section 7.0

QUESTIONS

07-1

Provide a comprehensive list and description of self-test and self-diagnostic features that will be utilized in the APR1400 safety-related instrumentation and control (I&C) systems and how these features will be verified periodically.

As required in 10 CFR 50.55a(h)(3), IEEE Std 603-1991, Clause 5.5, "System Integrity," states that safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. IEEE Std 7-4.3.2-2003, endorsed by Regulatory Guide (RG) 1.152, provides specific guidance on self-test/self-diagnostic features and their application to computer system integrity. With regard to self-testing features, the Technical Report APR1400-Z-J-NR-14001-P, Rev.0 , “Safety I&C System,” Appendix B, section B.5.5.3, "Fault Detection and Self-Diagnostics," states, in part, the following:

> "A typical set of self-diagnostic functions includes the following:
>
> • Memory functionality and integrity tests (e.g., programmable read-only memory (PROM) checksum and random access memory (RAM) tests)
>
> • Computer system instruction set (e.g., calculation tests)
>
> • Computer peripheral hardware tests (e.g., watchdog timers and keyboards)
>
> • Computer architecture support hardware (e.g., address lines and shared memory interfaces)
>
> • Communication link diagnostics (e.g., cyclic redundancy checksum (CRC) verification)"

The above-quoted information is referred to as "typical" in terms of features but does not address what are the specific set of functions that will be utilized for the APR1400 as a whole, specifically for the safety I&C systems. For example, neither the final safety analysis report (FSAR) (Tier 1 or Tier 2) nor Technical Report APR1400-Z-J-NR-14003-P, Rev.0, “Software Program Manual,” provide a comprehensive listing and description of all self-testing features in the APR1400 design. The design documntation does not provide a comprehensive description of these features.

REQUEST FOR ADDITIONAL INFORMATION 356-7881

1. What are the specific self-test/self-diagnostic features that will be incorporated in the safety I&C systems?

2. Are self-testing/self-monitoring software, as well as any other software-based diagnostic tools, designed under the same controls as the software life-cycle process detailed in the Software Program Manual?

3. Do the FSAR Tier 1 Inspection, Tests, Analyses, and Acceptance Criteria (ITAAC) for the safety I&C systems provide testing and validation for the self-testing and self-diagnostic functions? If not, explain why.

4. Does the applicant intend to provide a FSAR Tier 1 ITAAC for the safety I&C systems that verifies the fail-safe behaviors (e.g. control output to safety actuators fail to a predefined state and a restoration of power or system reinitialization, does not cause a change of state in the actuators) of the Plant Protection System (PPS) and Engineered Safety Features – Component Control System (ESF-CCS) that would demonstrate system integrity is maintained during such events as a loss of power or component failures?

07-2

Clarify whether automated self-testing/self-monitoring features in APR1400 I&C systems is being credited in the Technical Specifications in lieu of performing periodic surveillance testing.

As required in 10 CFR 50.55a(h)(3), IEEE Std 603-1991, Clause 5.7, states, in part, that capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. In the Technical Specification Bases, Section B 3.3.1 for reactor protection system (RPS) Instrumentation, states, in part, that channel functional test surveillance requirement (SR) 3.3.1.10 for the core protection calculator system (CPCS) testing frequency will be 18 months and the basis for the 18-month frequency is the CPCs perform a continuous self-monitoring function that eliminates the need for more frequent testing. This section also states the channel functional test essentially validates self-monitoring function and checks for, "....a small set of failure modes that are undetectable by the self-monitoring function." This would imply that automated fault detection features are being used to justify a lowered frequency of surveillance testing for the CPCs but there is no technical basis provided for why this is an acceptable approach, such as tying the bases to the CPCS watchdog timer implementation shown in Figure 4-11 in Technical Report APR1400-Z-J-NR-14001-P, Rev.0, "Safety I&C System." In addition, Technical report APR1400-Z-J-NR-14001-P, Rev.0, Section A.5.7, "Capability for Test and Calibration," states, in part, that diagnostics functions check hardware integrity through CRC checksum comparison but does not specifically state that memory containing the self-testing software is verified by this functionality.

1. Clarify whether the applicant is actually crediting automated self-testing/self-monitoring features to reduce maintenance/surveillance frequencies for any I&C components or systems? If so, identify the specific I&C systems/components and the maintenance/surveillance activities that are reduced in frequency due to the presence of automated self-testing/self-monitoring features.

2. For the self-testing/self-monitoring features being credited for testing in lieu of periodic surveillance testing, identify these functions, what purpose they achieve, their limitations, and the basis for why this is an acceptable approach. In other words, describe the degree of self-testing coverage for potential failures and why using the self-testing in lieu of periodic surveillance testing provides as good or better identification and resolution I&C system failures.

3. How does the applicant intend to periodically verify the self-testing feature functionality per the guidance in Branch Technical Position (BTP) 7-17? Would the self-testing features be verified in

conjunction with other forms of periodic testing? Does the safety I&C system memory containing the self-testing features have its integrity verified by CRC checks?

4. Does the APR1400 have any failure modes that are identifiable but undetectable?

5. What specific failure modes are undetectable by the self-monitoring functions? Are these failures detectable through other forms of testing?

6. What I&C components in the Technical Specifications do not have automated self-testing/self-diagnostic capabilities and can only be verified through periodic testing?

07-3

Describe the diagnostic programs used to test digital computer channels in the APR1400 design.

As required by 10 CFR 50.55a(h)(3), IEEE Std 603-1991, Clause 5.7, states, in part, that capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. APR1400 FSAR Tier 2, Chapter 16, Section 1.1, "Definitions" states with regard to the Channel Functional Test, in part,

> *"Digital Computer channels - the use of diagnostic programs to test digital computer hardware and the injection of simulated process data into the channel to verify OPERABILITY, including alarms and trip functions."*

1. Describe the diagnostic programs used for testing. Specifically, what are these programs? How do they help to ensure operability of safety system components?

2. Describe the testing process or describe where in the application the testing process is explained in detail.

3. How does the design ensure that there is adequate independence such that injected signals are only received by the channel being tested and not to other channels on the safety system data network?

4. How does the design ensure that online testing does not result in an unplanned component or spurious actuation of a component(s) while testing is being performed?

07-4

Provide clarification on the term “Non-DCS” on Table 4.5-2 of Technical Report APR1400-Z-J-NR-14012-P, Rev.0, “Control System CCF Analysis.”

10 CFR 50.55a(h)(3) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.3, states, in part, the safety system design shall be such that credible failure in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. Table 4.5-2 of Technical Report APR1400-Z-J-NR-14012-P, describes the control groups of the non-safety I&C architecture that were arranged through functional and component segmentation. The turbine bypass system is described as being part of the non-safety I&C distributed control system (DCS) platform. The turbine control system is designated as non-DCS. This designation is consistent with Table 5.2-1 of Technical Report APR1400-

Z-J-NR-14012-P. In addition, for the control group, “Miscellaneous BOP control”, the platform is designated as DCS/Non-DCS. The applicant does not appear to define the term “non-DCS” in this technical report or in Chapter 7 of the APR1400 DCD.

1. Define the term “Non-DCS” and what it means in terms of control system implementation.

2. Explain what miscellaneous BOP controls are implemented through the DCS and which BOP controls are non-DCS.

3. Identify the miscellaneous BOP controls.

4. Are there any control groups that do not have separate controllers, as shown on Table 5.2-1?

07-5

Describe the I&C and its supporting features (e.g. location of equipment, power sources, etc.) for the remote control center (RCC) in the APR1400 design.

General Design Criteria (GDC) 19 requires, in part, that equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

Regarding the RCC, the applicant states in APR1400 FSAR Tier 2, Section 7.7.1.1, "Conrol Systems," subsection o.3)c), the RCC has minimum equipment necessary to maintain the plant for 24 hours to accomplish hot standby. The applicant also states that the RCC is located separately from the main control room (MCR) so that aircraft impact to the MCR does not adversely affect the RCC. The applicant goes on to state that the RCC panels have divisionalized control of safety and non-safety controls to achieve plant hot shutdown. In Section 7.7.1.2, "Main Control Room Facility," the applicant states the MCR and remote shutdown room (RSR) both meet the requirements of GDC 19, but makes no mention of the RCC. In Section 7.7.1, "Description," of FSAR Tier 2, the applicant states that the RSR is subject to the human factors engineering process described in Chapter 18 of the APR1400 FSAR Tier 2 but does not mention a similar design commitment for the RCC.

The applicant mentions that the RCC has safety and non-safety related controls available but does not state that RCC complies with any other applicable requirements for this configuration such as independence. The RCC is not depicted on Figure 7.1-1, “APR1400 I&C System Overview Architecture,” therefore, there is no physical depiction of how the functionality of the RCC is taken into account within the overall I&C architecture or how its implemented. The acronym for the remote control center is also not defined in the acronym and abbreviation list in Section 7.0 of FSAR Tier 2. It cannot be determined what the difference is between the RCC and RSR.

1. Describe the RCC including all instrumentation, controls, and displays available at the RCC, all communications and architectural details used to implement the RCC, how the RCC addresses all the applicable requirements to the RCC (i.e. Independence), the specific design functions the RCC is intended to meet, the locations of RCC equipment (i.e. I&C cabinets, if applicable).

2. What is the difference between the RCC and the RSR?

3. Have the controls and displays available at the RCC been designed using the human factors engineering process as described in Chapter 18?

07-6

Define the term “standby” as used in APR1400 FSAR Tier 2, Chapters 7 and 16.

As required by 10 CFR 50.55a(h)(3), IEEE Std 603-1991, Clause 5.7, states, in part, that capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. FSAR Tier 2, Section 7.7.1.1, states, for the digital rod control system (DRCS), there are five modes of control. One of these modes of controls is designated “standby.” For the staff, the word implies this control mode would be comparable to the system being available but not in active operation. However, the applicant does not appear to define this term with respect to operation of the DRCS. This terms also appears in Technical Specifications with regard to the DRCS, but is not defined in that portion of the application either.

1. Define the term "standby" and state which safety and non-safety I&C systems can be placed in standby.

2. Is a system/component placed in standby considered inoperable?

3. How is a standby control mode initiated and how does this control mode affect the operation of the system/component in standby mode?

07-7

Identify and explain the basis for the specific plant components that are contained within control groups as show on Tables 4.5-2, "Control Group," and 5.1-1, "Shared Signals," of Technical Report APR1400-Z-J-NR-14012-P, Rev. 0, "Control System CCF Analysis."

10 CFR 50.55a(h)(3) requires compliance to IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, the safety system design shall be such that credible failure in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. Technical Report APR1400-Z-J-NR-14012-P, Table 5.2-1, "Control Group Segmentation," documents the segmented control groups for the APR1400 non-safety control systems. The table also states whether these control groups have separate controllers. However, the table does not itemize the physical plant components that are controlled by, and part of, each control group. As a result, this requires further analysis of the material provided by the applicant later in the report, such as Tables 5.1-1 and 5.1-2 (thru 5.1-19), "Multiple Failure due to a Single Failure of Shared Signals." As a result, it is more difficult to understand and ascertain whether an entire control group is affected by a single failure or only a single component is affected. In addition, Tables 5.1-2 thru 5.1-19 documents the single failure of shared signals. In the column labeled “Evaluation Result”, the applicant cites various Chapter 15 events as bounding analyses for a particular failure identified on the table. For example, the failure mode of “Reactor power signal fails low”, the applicant states in the evaluation result column that “This failure is bounded by DCD Ch. 15.2.3 (Loss of condenser vacuum)”. There does not appear to be any further explanation on the table as to why this particular failure is bounded by the loss of condenser vacuum event.

1. Identify the physical plant components (i.e. pumps, valves, etc.) controlled by each control group or identify where in the application this information is located.

2. Provide the basis for why the cited Chapter 15 analysis sections are adequate for each failure mode in Tables 5.1-2 thru 5.1-19.

3. Clarify whether the current approach adequately captures failure modes and effects on control groups beyond shared signals.

07-8

Clarify the design statement regarding embedded digital devices in both safety and non-safety components.

10 CFR 50.55a(h)(3) requires compliance to IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, the safety system design shall be such that credible failure in, and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. The applicant makes a statement with regard to embedded devices in field equipment in the second paragraph of Section 4.10, "CCF Analysis of Embedded Devices in Field Eqiupment," of APR1400-Z-J-NR-14012-P, "Control System CCF Analysis," Revision 0.

1. Does the applicant imply that embedded devices contained in non-safety components are diverse from the embedded devices contained within safety-related components?

2. Provide analysis or further descripition demonstrating that embedded devices within non-safety components are different or diverse from embedded devices in safety-related components.

3. Provide a summary of all types of components that will have embedded digital technology. Identify the functionality provided by the embedded technology for these components.

4. For embedded digital devices contained within safety-related components, has the applicant evaluated the potential consequences of a software CCF for these components? If so, provide this information or point to the area in the application where this information is contained.

07-9

Clarify how systems are selected to be within the scope of Technical Report APR1400-Z-J-NR-14012-P, Rev. 0, “Control System CCF Analysis Technical Report.”

10 CFR 50.55a(h)(3) requires compliance to IEEE Std 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, the safety system design shall be such that credible failure in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. In Section 4.1, second to last paragraph, of Technical Report APR1400-Z-J-NR-14012-P, the applicant makes a statement with regard to monitoring systems such as NIMS [NSSS integrity monitoring system] and RMS [radiation monitoring system].

The applicant does not specifically call out the exact number and/or types of systems that are considered for this evaluation. It must be assumed that, based upon this quote, the only criterion used to determine whether a system is included in the scope of this evaluation is if the system is responsible for controlling variables within pre-defined operational ranges. This criterion would appear to be arbitrary as the applicant does not provide any further evidence to support this criterion. The applicant also states, in part, in Section 4.1 of the technical report that control systems under the scope of evaluation are included because they can affect critical safety functions. The applicant does not concisely identify the criterion or methodology that determines which systems can affect critical safety functions.

What is the criterion or methodology used to determine what systems and components are included within the scope of the control system CCF analysis? Provide information to support why this criterion is the most appropriate way to determine the scope of systems included.

07-10

Discuss whether shared signals are the only failure mechanisms considered when determining the four failure categories listed in Section 4.3, "Credible Failure Types of Control System CCF," of Technical Report APR1400-Z-J-NR-14012-P, Rev. 0.

10 CFR 50.55a(h)(3) requires compliance to IEEE Std 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, the safety system design shall be such that credible failure in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. Table 5.1-1, “Shared Signals” of Technical Report APR1400-Z-J-NR-14012-P presents a list of common signals from specific primary/secondary controls systems and interfacing systems that receive the common shared signal. The analysis in Section 5, "Evaluation Method and Results," appears to limit initiators of CCF to that of shared signals. The applicant does not necessarily provide a basis as to why this failure mode is the sole means to cause a CCF, even if it is the more likely vector. For example, upon reviewing the technical report, the applicant does not appear to consider other potential failure modes such as EMI/RFI, seismic movement, etc. It is possible that the four failure categories, supporting design constraints, and analysis bound all failure modes beyond that of shared signals, but the applicant does not make this claim or arguments to support this premise within the technical report. Explain why failures of shared signals is the only failure mode that was used to develop all the failure types in Technical Report APR1400-Z-J-NR-14012-P, Rev. 0.

07-11

Describe conformance of the Diverse Actuation System (DAS) to the guidance of Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment That is Not Safety-Related."

10 CFR 50.62 states, in part, that each pressurized water reactor must have equipment from sensor output to final actuation device, that diverse equipment credited to perform reactor trip, and automatic initiation of auxiliary feedwater and initiation of a turbine trip under ATWS conditions, must be designed to perform its function in a reliable manner. GL 85-06 provides quality assurance guidance for those systems implementing ATWS mitigation functions. In addition, NUREG-0800, BTP 7-19, Section B, 1.4, Point 3, states, "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 (D3) Technical Report,” Section 5, states the following with regard to quality:

> “The DAS consists of the DPS, DIS, and the DMA switches. Each subsystem is described in the following subsections. The DAS is implemented on a platform that is diverse from the common safety PLC platform. The DAS is designed to meet the quality assurance guidance of Generic Letter 85-06. Any software associated with the DAS is qualified as ITS.”

FSAR Tier 2, Table 15.0-13, "NRC Generic Letters and Bulletins," lists various NRC generic letters and bulletins and their disposition for the APR1400 design. Under GL-85-06, the applicant states this generic letter is not applicable to the APR1400 and is not included with the APR1400 design requirements. This would appear to contradict design commitments made in both FSAR Tier 2, Section 7.8, and Technical Report APR1400-Z-J-NR-14002-P. If GL 85-06 is not part of any design requirements in the APR1400 design, then it is not clear how the DAS has been design with sufficient quality in order to perform its design functions in a reliable manner.

1. Verify the DAS has been designed to conform to the guidance of GL 85-06. If not, provide an explanation on the quality assurance process used to design and operate the DAS that would ensure a sufficient level of quality such that it can perform its design functions in a reliable manner.

2. Regarding the diverse manual ESF actuation switches (DMAs), provide an explanation on how the applicant intends to verify that the DMAs meet the design commitments in FSAR Tier 2, Section 7.8, regarding Class 1E hardware, power and seismic qualification.

07-12

Provide an explanation on the software safety classification of the core operating limit supervisory system (COLSS) and standalone non-safety I&C systems.

General Design Criteria 13 states, in part, that appropriate controls shall be provided to maintain plant process variables and systems within prescribed operating ranges. NUREG-0800, Section 7.7, III.1, 7th bullet, states, in part, the software for the control systems should be developed in a structured way similar to that of safety system software. Table A-1, "Assignment of Software for the I&C Systems to Classes," of Technical Report APR1400-Z-J-NR-14003-P, Rev. 0, “Software Program Manual,” lists the safety classification of software used in various I&C systems. The software package, COLSS (described in Technical Report APR1400-F-C-NR-14002-P, "Functional Design Requirements for a Core Operating Limit Supervisory System," Rev. 0), is not listed on this table for software components that are part of the information processing system (IPS). COLSS is designed to assist operators in instituting technical specification requirements upon entering limiting conditions of operation (LCOs) for the following reactor core aspects: Departure from nucleate boiling (DNBR) margin, linear heat rate margin, azimuthal tilt and axial shape index. COLSS performs numerous computations to monitor these core attributes to help the operators maintain steady state operations and initiate alarms when necessary. COLSS is listed under APR1400 FSAR Tier 2, Section 7.7.1.4.d, "Application programs." Application programs (i.e. nuclear application programs) are classified as [withheld] safety class. However, other application programs in Section 7.7, such as the computer-based procedure system (CPS), is listed in Table A-1 of the SPM as being [withheld] software. Given the COLSS’ significance to plant operations, it is not clear why this software is not described in the SPM, and subsequently not clear that COLSS software will be developed in a structured process to provide reliable operation.

1. Describe the software development processes used to develop COLSS and provide the basis for the software safety classification of the COLSS, based upon the criteria established in the SPM.

2. How does the applicant intend to verify the design functionality of COLSS (e.g. indications and alarms) to provide its intended functions per Technical Report APR1400-F-C-NR-14002-P, Rev. 0?

3. Does COLSS initiate any control system actions beyond providing indications and alarms in the main control room?

4. COLSS is not mentioned in Chapter 18, “Human Factors Engineering”, of the APR1400 FSAR Tier 2. The applicant states in FSAR Tier 2, Section 7.7.1.4.d, COLSS provides distinct operational advantages. Provide an explanation for how COLSS has been evaluated through human factors engineering practices to ensure design claims about its benefit to operators.

5. Provide a summary of the interface and/or interactions between COLSS and the core protection calculator system (CPCS). The relationship between these two systems is not clear based on design information in Technical Report APR1400-F-C-NR-14002-P, Rev. 0.

6. Technical Report APR1400-F-C-NR-14002-P, Rev. 0, Section 1.2, "Scope," states that COLSS is implemented within the plant monitoring system. Define what the applicant considers is the plant monitoring system as this term does not appear to exist within Chapter 7 of the APR1400 FSAR Tier 2 or other technical reports related to Chapter 7.

7. Describe how operators would be able to determine if COLSS has failed such that an LCO would need to be entered.

07-13

Describe the environmental protections (e.g. high temperature equipment alarms or cooling) for the Power Control System (PCS), Process – Component Control System (P-CCS) and DAS.

10 CFR 50.55a(h)(3) requires compliance to IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, that the safety system design shall be such that credible failure in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. Standard review plan Section 7.7 states, in part, that I&C systems should include protection from environmental extremes. APR1400 FSAR Tier 2, Section 7.7.1.4.c, states that, for Information Processing System (IPS) cabinets, temperature switches and alarms exists to protect against high temperature conditions and to alert operators to the potential high temperature condition. Section 7.7 does not address similar design functionality for cabinets containing equipment that comprises the PCS, P-CCS and DAS. FSAR Tier 2, Section 9.4, "Heating, Ventilation and Air Conditioning Systems," does not appear to provide specific information on the cabinets for these systems as well.

1. Describe the environmental protection design attributes for the cabinets (and rooms that contain these cabinets) for the PCS, P-CCS and DAS systems (i.e. high temperature protections and alarms).

2. Do the safety I&C systems have similar equipment cabinet environmental protective design features as the non-safety equipment cabinets?

07-14

Describe the specific design and implementation of the watchdog timers (WDTs) for the APR1400 design.

As required by 10 CFR 50.55a(h)(3), IEEE Std. 603-1991, Clause 5.5, states the safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. APR1400 FSAR Tier 2, Table 7.2-7, "Failure Modes and Effects Analysis for the Plant Protection System," refers to the WDT for core protection calculator (CPC) processor module (PM), the auxiliary CPC PM and the control element assembly calculator. WDT functionality is also mentioned for the local coincidence logic (LCL) processors responsible for performing reactor trips on Item 10 of Table 7.2-7. For this item, the stated effect of the WDT action is that the open WDT contact trips one-half of the safety division reactor trip initiation circuit. This is for LCL failures modes such as application program memory failure or failed program execution. Chapter 7 of the APR1400 FSAR Tier 2 does not provide specific details on the implementation of the WDT design, such as that the WDTs are non-programmable hardware.

Section 4.2.2, "Design Features," of Technical Report APR1400-Z-J-NR-14001-P, Rev.0, “Safety I&C System” states that each LCL reactor trip processor has a built-in WDT. Section 4.2.2 also states that the

outputs of the WDT are hardwired in series to the RPS initiation circuits to ensure appropriate trip signals are generated, as shown on Figure 4-7, "Watchdog Timer for PPS," of this report. The applicant also points to "Common Qualified Platform Topical Report" for detailed information on WDT configuration. The applicant makes similar assertions regarding the CPCS on Figure 4-11, "Watchdog Timer for CPCS." Figure 4-16, "Watchdog Timer for ESF-CCS," depicts the WDT configuration for the ESF-CCS. Figure 4-7 does not appear to show the actual wiring of the WDT and how it initiates a RT. Figure 4-16 does not appear to show how the WDT initiates a fail-safe condition for ESF-CCS components. Section 4.2.2 of technical report APR1400-Z-J-EC-13001-P, revision 0, “Safety I&C System”, states the following:

> “Each PPS LCL RT processor is supervised by the PLC watchdog timer.”

According to the acronym definition list in APR1400-Z-J-NR-14001-P, Rev. 0, “PLC” stands for programmable logic controller. This would imply that, for the LCLs, the WDTs are implemented with programmable technology and it is not clear that this is only applicable to LCLs, based upon the applicant’s description. This implementation would run counter to the guidance of SRP 7.1-D, which describes an acceptable methodology for meeting the criterion set forth in IEEE Std. 7-4.3.2-2003, which the applicant states the APR1400 design complies with. SRP 7.1-D, Section 5.7, states, in part, that a non-software WDT is critical in the overall diagnostic scheme of a computer system. A software-based WDT may be subject to the similar failure modes as the operating system it is intended to monitor, such as CCF, as described in BTP 7-19, for which the applicant states the APR1400 design complies.

1. Is the trip path for the WDT design, for both reactor trip and ESF-CCS, include any portion of the PPS or supporting systems that is dependent on software or other programmable technology to initiate a fail-safe condition?

2. Provide a clear consolidated figure that depicts the specific internal design of the WDT and its external connections and demonstrates how it is physically integrated into the systems that are applicable to its function (e.g. LCLs for reactor trip function) to perform its safety function, from detection of a system fault to outputs to reactor trip breakers for fail-safe actuation for ESF-CCS components.

3. Regarding WDT physical design, does the applicant consider the WDTs within the APR1400 design to be hardware components or software components, considering the WDTs for the LCLs are implemented using programmable technology?

4. Identify whether WDTs used in the APR1400 design are implemented with programmable technology or not. What technologies are used to implement WDTs that are not implemented with PLCs?

5. If the WDTs are implemented with programmable technology, has the applicant accounted for potential failure modes of the WDTs in the D3 analysis or control system CCF analysis?

07-15

Clarify the design information presented on Figures 4.5-5 and 4.5-6 of Technical Report APR1400-Z-J-NR-14012-P, Rev. 0, “Control System CCF Analysis.”

10 CFR 50.55a(h)(3) requires compliance with IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. Technical Report APR1400-Z-J-NR-14012-P, Rev. 0, Section 4.5, "Segmentation," describes the segmentation arrangements for the APR1400 design. The segmenting of control functions and components is intended to supplement quantitative analyses provided in the technical report as well as add additional diversity within the non-safety I&C DCS. The controllers that comprise the DCS have very specific arrangements

in terms of the application software that is allocated to various controllers. Figures 4.5-5, "Component Segmentation 1 for SBCS Turbine Bypass Control," and 4.5-6 "Component Segmentation 1 for High Pressure FW Heater," show a bi-directional communication path between controllers, but do not specify the exact type of communications that are taking place.

1. What type of communication is taking place between controllers in the in Figures 4.5-5 and 4.5-6 of Technical Report APR1400-Z-J-NR-14012-P, Rev. 0, and is this representative of communications between all other controllers in the DCS?

2. What is meant when Figure 4.5-5 states, “Signal transmission is limited for Failure Type 2 to be bounded by DCD Ch.15 AOO?” How is the signal transmission limited?

3. Are the interlocks/permissives described in Section 4.7, "Interlock/Permissive Functions by Separate Control Group or Safety system," of Technical Report APR1400-Z-J-NR-14012-P, Rev. 0, the only interlocks/permissives that exist and will be implemented within separate controllers from the control functions, as shown on Figure 4.5-6?

07-16

Explain the redundant controller arrangement for non-safety control functions listed in the Technical Report APR1400-Z-J-NR-14012-P, Rev.0, “Control System CCF Analysis.”

10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.3 states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. In Section 4.6, "Redundant Controller for Availability Enhancement," of Technical Report APR1400-Z-J-NR-14012-P, Rev.0, the applicant identifies the following functions as having completely redundant control loops with redundant controllers and two I/O modules, with the I/O modules operating concurrently for each control loop:

- Control logic for reactor coolant pumps

- Control logic for non-Class 1E 13.8 kV switchgear power circuit breakers

- Control logic for non-Class 1E 4.16 kV switchgear power circuit breakers

The applicant states this portion of the DCS architecture is for enhanced availability. The applicant does not mention other control functions having this type of communications configuration and it is unclear why these specific functions were acknowledged and others appear to be omitted. The applicant also does not present an argument or criteria that would suggest that these particular functions were necessary to implement in this format, or why other functions may not be implemented in this format.

1. Is the design description in Section 4.6 of Technical Report APR1400-Z-J-NR-14012-P, Rev.0, “Control System CCF Analysis,” applicable to only the three control logic functions mentioned in this section?

2. Explain the basis for the three control functions in Section 4.6 having the stated level of controller redundancy. It is not clear the criterion the applicant uses to determine that these three functions require enhanced availability versus other non-safety functions, such as, pressurizer pressure/level control or feedwater control.

07-17

Describe the criteria used to determine the level and types of segmentation for specific functions and components as described in Technical Report APR1400-Z-J-NR-14012-P, Rev.0, “Control System CCF Analysis.”

10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. Section 4.5.3 of Technical Report APR1400-Z-J-NR-14012-P, Rev.0, states, in part, in additional to functional segmentation, additional segmentation maybe applied in order to bound the failures of the particular function or component that is being segmented. The applicant does not provide any criteria that would suggest how the determination of how much additional segmentation, is needed.

1. What is the criteria that determines when additional segmentation is needed after the functional segmentation is applied?

2. For Type 1 and Type 2 failures, explain the types of segmentation that would be applicable and how this segmentation choice benefits the analysis.

07-18

Describe the mechanisms in place that would allow operators to determine whether the QIAS-N and IFPDs have undergone a failure.

10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, that the safety system design shall be such that credible failure in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. The QIAS-N and IFPDs, located in the main control room (MCR) provide alarm, display and controls for operators. In Section 7.7.1.4 of APR1400 FSAR Tier 2, regarding the IFPDs, the applicant states that, “If a data communication error occurs, an appropriate message is generated.” For information displays, the applicant does not appear to state in the licensing documentation how an operator can determine whether a failure such as a common cause failure has occurred such that the displays are frozen up or affected by some other means. Therefore, it is not apparent that an appropriate error message could be generated to alert the operator(s) to a random or common cause failure, for non-safety or safety-displays. Failures of the IFPDs are addressed in Technical Report APR1400-Z-J-NR-14012-P, Rev.0, “Control System CCF Analysis.” However this document does not address how operators would make the initial determination that IFPDs have experienced a failure of some type.

Describe the mechanisms, procedures, or processes in place for the APR1400 design that would allow operators to be alerted to a failure of either the QIAS-N or the IFPDs (e.g. frozen displays or controls).

07-19

Address potential discrepancies in equipment qualification information for safety I&C systems in the APR1400 FSAR.

10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991. IEEE Std. 603-1991, Clause 5.4, states, in part, that safety system equipment shall be qualified to substantiate that it be capable of continuously meeting performance requirements as specified in the design basis. SRP Section 7.1-C states, in part, that lightning protection should be addressed as part of the electromagnetic compatibility (EMC) review and conforms to the guidance of Regulatory Guide (RG) 1.204, “Guidelines for Lightning Protection of Nuclear Power Plants.

Section 3.4.22 of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, “Safety I&C System” states the safety system I&C design complies with the guidance of RG 1.204. APR1400 FSAR Tier 2, Table 7.1-1, describes the applicability of regulations and guidance the safety and non-safety I&C systems of the APR1400 design. RG 1.204 is listed on this table, but the applicant does not state that this document applies to any I&C systems (it refers to Chapter 8 of the DCD). APR1400 FSAR Tier 1, Table 2.5.1-5, for example, has an ITAAC Item for EMC compliance, but does not incorporate lightning protection, nor does any other item on this table. APR1400 FSAR Tier 2, Table 7.1-1, does not include 10 CFR 50.49 as part of the applicable requirements for the safety I&C systems and is not actually listed on this table. Appendix Section C.5 of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, states that, with regard to DI&C-ISG-04 compliance to applicable aspects of the safety I&C design to 10 CFR 50.49, refer to Reference 12 of this technical report. Reference 12 is WCAP-16097-P-A, “Common Qualified Platform Topical Report,” Rev. 3. This document has not been incorporated by reference into the APR1400 DCD in Section 1.6.

1. Verify that design attributes with regard to lightning protection for the safety I&C systems are accounted for with the APR1400 FSAR Tier 1 ITAAC. If such information is already in Tier 1, point out where this information is captured.

2. Explain the discrepancy between ARP1400 FSAR Tier 2, Table 7.1-1, and Section 3.4.22 of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, “Safety I&C System,” regarding conformance with the guidance of RG 1.204.

3. Provide an explanation for why 10 CFR 50.49 is not included as an applicable requirement on ARP1400 FSAR Tier 2, Table 7.1-1.

4. Does APR1400 FSAR Tier 1, Table 2.5.1-5, Item 19, provide testing and verification of the safety I&C cabinets HVAC systems such as cooling fans, etc.?

07-20

Provide the unavailability analysis as described in Technical Report APR1400-Z-J-NR-14001-P, Rev.0, “Safety I&C System.”

10 CFR 50.55a(h)(3) requires compliance with IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.15, requires, in part, systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. Technical Report APR1400-Z-J-NR-14001-P, Rev.0, Section 7.2, "Unavailability Analysis," describes analysis that assesses the availability of the safety I&C systems that, along with the individual system FMEAs, addresses reliability requirements for the APR1400 design. The applicant does not present the analysis within this report, nor does the applicant provide information on where this analysis may reside within the application.

REQUEST FOR ADDITIONAL INFORMATION 356-7881

1. Provide the unavailability analysis, as described in Section 7.2 of Technical Report APR1400-Z-J-NR-14001-P, Rev.0.

2. Is this analysis applicable to all safety I&C systems?