AP1000DCDFileNPEm Resource

From: David Jaffe
Sent: Wednesday, April 30, 2008 9:44 AM
To: Seelman, Robert J.
Subject: FW: RESEND of Chapter 7 AP1000 RAIs
Attachments: Chapter 7 AP1000 Phase 1 RAIs Rev 2.doc

Please substitute this list of questions for the one previously sent and acknowledge receipt.

From: Terry Jackson
Sent: Wednesday, April 30, 2008 8:35 AM
To: David Jaffe
Cc: Deanna Zhang; Denise McGovern; Kenneth Mott; Tung Truong; William Roggenbrodt
Subject: Resend of Chapter 7 AP1000 RAIs

Dave,

Attached is a resend of what I sent you yesterday evening. We have added two late coming RAIs (RAI-SRP 7.1-ICE-29 and RAI-SRP 7.1-ICE-30). Let me know if you have any questions.

Terry W. Jackson, Chief
Instrumentation, Controls and Electrical Engineering Branch
Office of New Reactors
U.S. Nuclear Regulatory Commission
Phone: 301-415-7313
Terry.Jackson@nrc.gov

Hearing Identifier: AP1000_DCD_Review
Email Number: 38

Mail Envelope Properties (David.Jaffe@nrc.gov20080430094400)

Subject: FW: RESEND of Chapter 7 AP1000 RAIs
Sent Date: 4/30/2008 9:44:03 AM
Received Date: 4/30/2008 9:44:00 AM
From: David Jaffe

Created By: David.Jaffe@nrc.gov

Recipients:
"Seelman, Robert J." <seelmarj@westinghouse.com>
Tracking Status: None

Post Office:

Files	**Size**	**Date & Time**
MESSAGE	762	4/30/2008 9:44:00 AM
Chapter 7 AP1000 Phase 1 RAIs Rev 2.doc	148986	

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

MEMORANDUM TO: Eileen McKenna, Chief
AP1000 Projects Branch 2
Division of New Reactor Licensing

FROM: Terry Jackson, Chief
Instrumentation, Controls, and Electrical Branch 1
Division of Engineering

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION FOR WESTINGHOUSE AP1000 DESIGN CONTROL AMENDMENT REVISION 16 - CHAPTER 7 AND SECTION 9.5.2

The Instrumentation, Controls, and Electrical Branch 1 (ICE1) has reviewed the Westinghouse submittal of the AP1000 Design Control Amendment (DCA) and associated technical reports. This review covered the following DCA sections for which ICE1 has primary review responsibilities and, in addition, applicable interface documentation referenced in the DCA:

Tier 1: Section 2.5, and

Tier 2: Chapter 7, Section 9.5.2, and Section 14.3.5

The staff has determined that additional information is needed to complete this evaluation. Enclosed is a list of Request for Additional Information (RAI) questions. Please forward these questions to Westinghouse for resolution.

Enclosure: As stated

CONTACT: William Roggenbrodt, ICE1/DE
301-415-0678

REQUEST FOR ADDITIONAL INFORMATION

AP1000 DESIGN CONTROL DOCUMENT, REVISION 16

CHAPTER 7 – INSTRUMENTATION AND CONTROL

RAI-SRP 7.1-ICE-01

Provide an exhaustive road map or table demonstrating what plant-specific action items, generic open items, as well as other open items are addressed via a specific Inspections, Tests, Analysis, and Acceptance Criteria (ITAAC). Identify those items that are not yet completed and at what stage of the software lifecycle these open items to be completed.

The safety evaluation report for the Common Q Platform identified several plant-specific action items and generic open items, of which some have been addressed in the AP1000 Design Control Document (DCD), Revision 16. An example is the following:

> PSAI 6.6 is to be resolved via Item 10 in DCD Tier 1 – This can only be accomplished AFTER final selection of all devices from the sensors to the final actuation devices have been selected and the final setpoint methodology is applied via the final setpoint determination calculation. This activity is not expected to be completed until at least the System Integration phase of Westinghouse's software lifecycle.

RAI-SRP 7.1-ICE-02

Provide access to higher level documents referenced in the eleven documents the applicant has determined completes their "Design Requirements Phase" (Standard Review Plan (SRP), Branch Technical Position (BTP) 7-14 equivalent *Planning Activities Phase*) of the software lifecycle process.

Several references were made to documents for which NRC did not have access during their site visit at Westinghouse's Rockville, MD office. Examples of documents that were referenced in the software plans at the Rockville, MD office include:

- WEC Quality Management Commitments
- WNA-PN-00031 General Program Plan
- AP 3.2 Design Change Procedure
- AP1000 Procedure AP6.3
- Nuclear Automation Edition of the Westinghouse Policies and Procedures Manual

Provide access to the current versions of these documents, and others, referenced in the eleven documents that comprise the design requirements phase.

RAI-SRP 7.1-ICE-03

Provide a roadmap describing the relationship between the eleven documents that comprise Design Requirements Phase.

Westinghouse provided eleven documents that comprise the design requirements phase of the

AP1000 software development lifecycle. On April 9-11, 2008, the NRC staff conducted a site visit to Westinghouse's Rockville, MD office to review the eleven documents. However, the staff had difficultly navigating through the eleven documents as there were multiple references in a single document to one of the other eleven documents, or references to documents that were not present at the office. Therefore, a roadmap is needed that shows the peer-to-peer relationship, as well as, what documents serve as subordinates to others and what documents serve as supervisory documents to others.

RAI-SRP 7.1-ICE-04

Demonstrate to what quality standards the Westinghouse NPP organization will hold its employees, and any subcontractor organizations, throughout the project plan and design process for any AP1000 safety-related software system.

Several documents listed as proof of completion of the Design Requirements Phase are actually documents detailing the relationship between Westinghouse RRAS and Westinghouse NPP (for example, RRAS AP1000 NuStart I&C Program Project Plan (WNA-PN-00031-GEN) and RRAS AP1000 NuStart I&C Program Project Quality Plan (WNA-PQ-00166-GEN)). While the documents reveal how the subcontractor (Westinghouse RRAS) interfaces with the parent organization (Westinghouse NPP), they do not provide information detailing how Westinghouse NPP interfaces, and holds accountable, Westinghouse RRAS, employees, and other subcontractors. The response to this question should outline the standards used by Westinghouse NPP and how it ensures subordinate organizations, or persons, comply with those standards.

RAI-SRP 7.1-ICE-05

Provide a detailed higher level document which would serve as supervisory document for Testing Process for Common Q Safety Systems (WNA-PT-00058-GEN).

The aforementioned document serves as the testing process, rather than the test plan, as would be expected when dealing in the first phase of the design process for the software life cycle. Per BTP 7-14 which references Regulatory Guide 1.173, which endorses IEEE Standard 1074-1995, an activity to test planned information should be conducted.

RAI-SRP 7.1-ICE-06

Provide via docketing, or make available for review, the *Programming Guidelines for Common Q Systems*, which is listed as Reference 14 within the Common Q Software Configuration Management Guidelines (NABU-DP-00015-GEN).

RAI-SRP 7.1-ICE-07

Provide the current revision of AP1000 NuStart Protection and Safety Monitoring System Project Concept Phase V&V Summary Report.

Based upon a phone conversation on April 18th, 2008, Westinghouse stated that a current revision of the summary report was available and included the final lists of issues raised during the verification and validation portion of design requirements phase of the project, with their

resolution.

RAI-SRP 7.1-ICE-08

In Table 3.3-1, Risk Identification Checklist, of the AP1000 NuStart Protection and Safety Monitoring System Software Project Plan (WNA-PJ-00071-GEN), the risk for superfluous features being added to the software was given a probability, impact, and exposure of "zero". Provide the basis for establishing this risk identification. Specifically, since the risk of having an inexperienced personnel/software developer was identified as "high" in the table, how will Westinghouse ensure no additional superfluous features will be added by inexperienced personnel?

RAI-SRP 7.1-ICE-09

Item 4 of WNA-PJ-00071-GEN, "AP1000 NuStart PMS Software Project Plan," Appendix A, states that the Test/System Integration Phase I V&V is not within the scope of the AP1000 NuStart project. The software project will be frozen at the processor module software test for Division B software.

- Does this mean Division A, C, and D software will not be tested? Thus all software is considered "in-process" and incomplete. Provide the basis for this statement.
- In addition, if the software is considered incomplete, when will the software be completed?
- It appears that Divisions A and D are different from Divisions B and C software because of the interaction between Qualified Data Processing System and Divisions B and C only. How will testing of Division B software validate the software for Divisions A and D?

RAI-SRP 7.1-ICE-10

Westinghouse has requested to remove the reference to WCAP-15927, "Design Process for AP1000 Common Qualified Platform Safety Systems," which was submitted in addition to the Software Program Manual WCAP-16096-NP-A, Revision 1A (previously designated as CES-195, Revision 1) to resolve Requests for Additional Information 420.001 and 420.023, posed during the development and certification of the original AP1000 final safety evaluation report. Demonstrate what measures will be taken to ensure information contained in this report are not removed. If another document covers the same information but is not currently on the docket, submit that document on the docket.

RAI-SRP 7.1-ICE-11

Provide further clarification on the removal of WCAP-16791-P, "AP1000 Cyber Security Implementation," from Chapter 7 to Section 13.6 of the AP1000 DCD. Specifically, how will Westinghouse address cyber security measures within Chapter 7 of the DCD if WCAP-16791-P is removed?

The NRC staff conducted a recent phone conversation (April 9, 2008) with Westinghouse regarding cyber security. The applicant stated during the phone conversation that the reference

to WCAP-16791 will be removed from Chapter 7 to Section 13.6 of the DCD and has requested the NRC staff to stop its Chapter 7, Instrumentation and Controls, review of this technical report. Section 7.1 Appendix D of the SRP, “Guidance for Evaluation of the Application of IEEE Std 7-4.3.2,” states that for digital computer-based systems, controls of both physical and electronic access to safety system and data should be provided to prevent unauthorized changes. In addition, computer-based safety systems (including hardware and software) should be secured against both physical and electronic threats. The consideration of hardware security should ensure there is limited physical access control, and that there are no modems or connectivity to external networks. Security of computer-based system software relates to the ability to survive unauthorized, undesirable, and unsafe intrusions throughout the life cycle of the safety system. Demonstrate how the AP1000 instrumentation and controls design will meet the cyber security criteria within the software and hardware development process as described in Section 7.1 Appendix D of the SRP. Specifically, provide information within the design requirements phase documents, and other associated documents, to demonstrate how cyber security is addressed.

RAI-SRP 7.1-ICE-12

For material associated with the AP1000 Design Certification Amendment, provide a consistent reference of standards and other guidance throughout all docketed and referenced technical documents.

Upon review of various technical reports, several references cited were from different revisions of the same accepted industry standard. For example Technical Report 89 (WCAP 16675-P) references IEEE 7-4.3.2-2003 while Technical Report 42 (APP-GW-GLR-017) references the 1993 version of the standard

RAI-SRP 7.1-ICE-13

Demonstrate how positive control of the reactor is maintained at all times through the use of the Remote Shutdown Room (RSR) transfer switch.

The RSR transfer switch is utilized while in transit from one control location to another, and that switch is located in a hallway, which is in a location other than the main control room or the RSR.

RAI-SRP 7.1-ICE-14

Provide a set of detailed schematic drawings demonstrating a detailed grounding schematic of the electrical distribution system and its relation to all I&C systems. The diagrams should illustrate what type of grounding network is being utilized in all areas of the power plant where I&C monitoring, control, or alarm devices are used.

RAI-SRP 7.1-ICE-15

Provide a detailed listing of all types of open source code or other freeware utilized within the AP1000 I&C system architecture. Utilizing accepted industry standards, standardized reports or other qualified documentation demonstrate that for each of the above affected systems and/or subsystems that no malicious code, hidden backdoors and/or any other unknown functions reside on any freeware or other open source code within the software.

Section 4 of the Software Program Manual for Common Q Systems (WCAP 16096-NP-A, Rev 1A) states that other existing non-commercial software (i.e., freeware) may be used under the following conditions:

- This software can only be qualified as important-to-safety, important-to-availability, or general purpose software.

- The software fulfills a specific requirement identified in the software requirements specification.

- The code is well organized and has adequate design documentation, and source code commentary. If the software has poor, or no documentation, then documentation shall be prepared.

- Will undergo the verification and validation process starting at the implementation phase.

If source code from non-commercial software is used, Westinghouse needs to demonstrate that such code is verified to be free of any unknown vulnerabilities within the given freeware.

RAI-SRP 7.1-ICE-16

Provide a set of detailed schematic drawings of the AP1000 Common Q Platform as it pertains to the Protective and Safety Monitoring System (PMS) clearly showing the system and any ancillary systems connected to the PMS (including any connection(s) to the Diverse Actuation System, if applicable) from sensor, or sensor output devices, through the final actuation devices.

These drawings will enable the NRC Staff to better determine how given components, within given divisions of the system are able to meet the single failure criterion of IEEE Standard 603-1991.

RAI-SRP 7.1-ICE-17

Provide a list of the Component Interface Module (CIM) devices in each division and the components they actuate.

10 CFR Part 50, Appendix A, General Design Criteria (GDC) 21, “Protection system testability and reliability,” requires, in part, that redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in a loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. No documentation has been docketed detailing the minimum number of redundant devices and/or components which will actuate in the presence of a single fault while the system is under maintenance or test to the extent possible, as allowed by Technical Specifications. The references contained within WCAP-16675-P, “AP1000 Protection and Safety Monitoring System Architecture,” were insufficient to render a final determination in this matter.

RAI-SRP 7.1-ICE-18

Provide further information on the physical location of remote I/O modules. Demonstrate that the physical location of the remote I/O modules will be protected from the probability and effect of fires and explosions.

In accordance with 10 CFR Part 50, Appendix A, General Design Criteria 3, “Fire Protection,” structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Noncombustible and heat resistant materials shall be used wherever practical throughout the unit, particularly in locations such as the containment and control room. The NRC staff has reviewed the description of the remote I/O modules within Section 3.2.1 of WCAP-16674-P. However, the NRC staff could not find information on the physical location of the remote I/O modules within the plant. How does Westinghouse meet the location requirements of GDC 3 with respect to the placement of remote I/O modules?

RAI-SRP 7.1-ICE-19

Demonstrate the basis for concluding the Remote Node Controller (RNC) is not performing a safety function and can be defined as an associated circuit per IEEE Standard 603-1991.

IEEE Standard 603-1991 defines associated circuits as non-Class 1E circuits that are not physically separated or are not electrically isolated by acceptable separation distance, safety class structures, barriers or isolation devices. Since the RNC is powered by the safety system and Figure 3-1 of WCAP 16675-P shows the device to be within the Class 1E boundary (i.e. safety-related side of the electrical isolation device), the RNC does not appear to meet the definition of an associated circuit.

RAI-SRP 7.1-ICE-20

Provide a detailed description of the functions, architecture, construction, and implementation of the RNC.

Section 4 of IEEE 603-1991 requires, in part, that the design basis be available as needed to facilitate the determination of the adequacy of the safety system. The description of the RNC provided in Section 3.3.5 of WCAP-16675-P was not sufficient to determine how the RNC meets the various requirements of IEEE 603-1991 and its associated guidance, including IEEE 7-4.3.2-2003. Provide sufficient information describing the RNC such that a determination of adequacy could be made. At a minimum, the following aspects of the RNC should be addressed in detail:

- Functions implemented by the RNC
- Devices and/or components with which the RNC can interface and how the interface is implemented.
- Incoming and outgoing signals to/from the RNC

- Major hardware and logic components within the RNC
- Communication protocols with safety and non-safety systems; including mechanisms to prevent the interference of safety functions by non-safety communications
- Physical separation and electrical isolation between the safety and non-safety components
- RNC operation for various plant/equipment modes (i.e., normal, abnormal, accident conditions and manual, testing, and maintenance modes)
- Power supplies
- Cyber-security for the RNC
- How maintenance is performed on the RNC
- Reliability of the RNC
- Description of how the state of the RNC following power-up and initialization will correspond to the current plant state
- Operating history of the RNC
- Applicable regulations, guidance, testing measures and standards used in RNC design

RAI-SRP 7.1-ICE-21

Provide a detailed description of the functions, architecture, construction, and implementation of the CIM.

Section 4 of IEEE 603-1991 requires, in part, that the design basis be available as needed to facilitate the determination of the adequacy of the safety system. The description of the CIM provided in Section 5.1.5 of WCAP-16675-P, "Protection System Architecture," Rev. 0, was not sufficient to determine how the CIM meets the various requirements of IEEE 603-1991 and its associated guidance, including IEEE 7-4.3.2-2003. Provide sufficient information describing the CIM such that a determination of adequacy could be made. At a minimum, the following aspects of the CIM should be addressed in detail:

- Priority scheme and logic implemented in the CIM
- Actuators that the CIM can control and how the configuration for those actuators is implemented with the CIM
- Incoming and outgoing signals to the CIM
- Major hardware and logic components within the CIM
- Communication protocols with safety and non-safety systems; including mechanisms to prevent the interference of safety functions by non-safety communications
- Physical and electrical isolation between the safety and non-safety components
- CIM operation for various plant/equipment modes (i.e., normal, abnormal, accident conditions and manual, testing, and maintenance modes)
- Identification of how automatic (if applicable) and periodic testing is performed on the CIM, including the ability of the CIM to perform its safety function during testing
- Time response
- Power supplies
- Control of the CIM from locations other than the main control room
- Cyber-security for the CIM
- How maintenance is performed on the CIM
- Reliability of the CIM
- Description of how the state of the CIM following power-up and initialization will correspond to the current plant state

- Operating history

- Applicable regulations, guidance, testing measures and standards used in CIM design

RAI-SRP 7.1-ICE-22

Provide sufficient information on the docket for the NRC staff to determine the quality of the logic within the CIM.

Section 5.1.5 of WCAP-16675-P describes the CIM as a non-software based Class 1E device that is not considered to be susceptible to a software common-cause failure. However, insufficient information has been provided on the docket for the NRC staff to conclude that the CIM is not susceptible to a software common-cause failure. The applicant needs to address all of the criteria in Section 2, “Command Prioritization” of NRC ISG, “Highly-Integrated Control Rooms – Communication Issues,” as it is the current guidance the NRC staff uses to conclude the absence of software common-cause failures in digital systems. If an alternate method to the interim staff guidance is proposed, provide a detailed basis for how the alternate method achieves the same outcome as the guidance.

RAI-SRP 7.1-ICE-23

Describe the hardware qualification of the CIM. Provide on the docket the test plans and results and/or the analysis for seismic, environmental, electromagnetic/radio-frequency interference, and other hardware qualification testing.

Clause 5.4 of IEEE 603-1991 requires, in part, that safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Section 5.1.5 of WCAP-16675-P provides a description of the CIM but does not provide any information regarding hardware qualification for the CIM device. The NRC staff needs detailed information on the hardware qualification of the CIM in order to approve the device for use in a Class 1E application.

RAI-SRP 7.1-ICE-24

Section 1.4 of WCAP-16675-P, last sentence on Page 1-5, the term ***hardwired*** is used. Provide additional detail via various examples or lists explaining what is considered a ***hardwired*** connection and what is not considered a hardwired connection. For example, does hardwired apply to a single point-to-point termination to which no other devices have access or control (non-multiplexed communication)? Or, is hardwired to mean the transfer medium is of a certain type (e.g., copper)?

RAI-SRP 7.1-ICE-25

Provide a comprehensive and exhaustive listing of all abbreviations and their meanings within WCAP 16675-P and all associated or referenced documents.

Several abbreviations referenced in WCAP 16675-P are not defined. For example FOM (*fiber optic* module?) and several abbreviations on Figure 3-1 are utilized. However those same abbreviations are not captured in the List of Acronyms and Abbreviations listed on pages xi and xii.

RAI-SRP 7.1-ICE-26

In Section 2.2 of WCAP 16675-P, with regards to Numbers 8 and 9, the Qualified Data Processing Subsystems (QDPS) displays are listed as being installed for compliance with Regulatory Guide 1.97. Are these separate displays from the Division B and Division C main control room safety displays, or are they built into the Division B and C safety displays?

RAI-SRP 7.1-ICE-27

Demonstrate what guidelines, procedures etc. will be implemented to ensure operators understand all compensatory measures which must be taken when control of a safety system will be out of their control and out of their sight?

Per WCAP 16675-P, the Maintenance and Test Panel and the Integrated Test Processor will be located in a room other than the main control room. Per 10 CFR 50.54(k), an operator or senior operator licensed pursuant to Part 55 of this chapter shall be present at the controls at all times during the operation of the facility.

RAI-SRP 7.1-ICE-28

Demonstrate how the PMS System meets 10 CFR Part 50, Appendix A, GDC 21, “Protection System Reliability and Testability,” and Clause 5.1 of IEEE-603-1991.

Although the Westinghouse report WCAP-16438-P - FMEA of AP1000 Protection and Safety Monitoring System, provides a good starting point detailing failure modes from a fully operational system, it lacks detailed analysis from a less than fully operational system (i.e., a division in maintenance). Additionally, the FMEA does not detail all possible initial system states which are required for a comprehensive and complete single failure analysis.

RAI-SRP 7.1-ICE-29

Describe how module testing will be performed for the AP1000 safety I&C systems.

The safety evaluation report for the Common Q Software Program Manual did not approve the module testing that was proposed within that report. Rather, it was left as Generic Open Item 7.7. The description as to how the proposed module testing addresses acceptance criteria in Regulatory Guides 1.152, 1.168, and 1.70 should be provided on the docket.

RAI-SRP 7.1-ICE-30

Discuss the control of safety-related components from non-safety and safety displays and

controls in the main control room.

In reading WCAP-16675-P, it appears that safety-related components that do not have onerous consequences cannot be controlled from safety-related displays and controls in the main control room. If this is true, describe how manual control of such components would be performed if the non-safety related displays and controls are lost (i.e., loss-of-offsite power and other design basis events). If the above statement is not true, provide clarification in WCAP-16675.

RAI-SRP 7.2-ICE-01

In Section 2.2.1.3, 2nd paragraph, 3rd sentence, of WCAP 16675-P the sentence declares that, "Any nuclear instrumentation (NI) channel is capable of being removed from service without affecting the other ***two*** channels. To what is the "two" channels referring, since there are greater than three safety related NI channels?

RAI-SRP 7.2-ICE-02

In Section 2.2.3, of WCAP 16675-P reference is made to the term *bypass function*. Provide additional detail which delineates how the bypass function operates including its permissive and other interlocks.

RAI-SRP 7.2-ICE-03

In Section 2.2.3, of WCAP 16675-P sub-point #1, a reference is made to a "*failsafe trip*". Provide additional detail by defining more exactly, what plant condition(s) constitute(s) a "failsafe" trip?

RAI-SRP 7.2-ICE-04

Is the manual reactor trip function, mentioned in Section 2.2.3.1.3, of WCAP 16675-P, entirely software based, entirely hardware based, or a combination of the two types of technology. For example, is there a physical button (or set of buttons) that physically (electrically) open a switch contact or is this function software based?

Regulatory Position Point 4 in Regulatory Guide 1.62, "Manual Initiation of Protective Actions," reads, "*The amount of equipment common to both manual and automatic initiation should be kept to a minimum*." Furthermore, Section 6.2.1 of IEEE Standard 603-1991 reads, "*The means provided [for manual initiation of a safety system] shall…* ***depend on the operation of a minimum of equipment consistent with the constraints of*** *[Section]* ***5.6.1*** *[Independence]*." The NRC staff needs a more detailed description of the manual reactor trip function to determine how the AP1000 PMS address this criteria.

RAI-SRP 7.2-ICE-05

In Section 2.2.5 of WCAP 16675-P (Page 2-18) states, *"**[**To reduce wear on the breakers through excessive tripping, and to avoid a potential plant trip resulting from a single failure while testing is in progress, the test sequence is designed so that the actual opening of the trip*

*breakers is only required when the trip breaker itself is being tested.**]***" Explain exactly how this activity is being accomplished. Include in the explanation exactly when during testing and other maintenance activities the Reactor Trip Circuit Breakers will actually be opened and at what periodicity.

RAI-SRP 7.2-ICE-06

In Section 2.2.6, of WCAP 16675-P the fourth bullet discusses "*partial trip mode*". Describe exactly what the term "partial trip mode" means.

RAI-SRP 7.2-ICE-07

Provide basis for changing the term "switches" with the term "controls" in Table 7.2-2 "Reactor Trips" (sheet 2 of 2) for all listed manual trips.

Figure 3 of IEEE Standard 603-1991 provides a text based representation of the general elements of a safety system. Within the *"Sense and Command Features"* portion of the figure, the Reactor Trip and Engineered Safety Features Actuation System (ESFAS) utilizes manual "switches", not "controls", thereby working in concert with Section 6.2.1 "Manual Control" of the same standard. Sub-point 6.2.1 reads, "*The means provided [for manual initiation of a safety system] shall… depend on the operation of a* ***minimum of equipment consistent with the constraints of*** *[Section]* ***5.6.1*** *[Independence]*."

RAI-SRP 7.2-ICE-08

Demonstrate how WCAP-16361-P "Westinghouse Setpoint Methodology for Protection Systems - AP1000" satisfies the requirement of COL Action Item 7.2.7-1 to provide the NRC with a calculation of setpoints for protective functions.

WCAP-16361-P concludes that setpoint calculations cannot be given until the final design of the power plant has been completed. However, in Westinghouse AP1000 DCD, Revision 16, Tier 2, Chapter 7, Subsection 7.1.6.1, states that all requested information on the subject of setpoint methodology and final setpoint calculations have been completely addressed and require no further action by the Combined License Applicant.

RAI-SRP 7.3-ICE-01

In Section 2.2.3.2.2 of WCAP 16675-P, paragraph 4, first sentence, states, "**[***Control of safety components with no onerous consequences is accomplished from the MCR via the operator workstations and the remote I/O bus*."**]** Provide additional detail as to whether or not these ESFAS functions will be conducted via non-safety related control devices or will these components still be operated by a safety related control device(s)?

RAI-SRP 7.3-ICE-02

Provide additional detail of the manual control scheme of the PMS Engineered Safety Features Actuation System (ESFAS) function as described in WCAP 16675-P.

Per WCAP 16675-P, the manual system level actuation uses all automatic PMS components with the exception of the Bistable Processor Logic device. Regulatory Position Point 4 in Regulatory Guide 1.62, "Manual Initiation of Protective Actions," reads, "*The amount of equipment common to both manual and automatic initiation should be kept to a minimum*." Furthermore, Section 6.2.1 of IEEE Standard 603-1991 reads, "*The means provided [for manual initiation of a safety system] shall…* ***depend on the operation of a minimum of equipment consistent with the constraints of*** *[Section]* ***5.6.1*** *[Independence]*." It is currently difficult for the NRC staff to see how the manual actuation of the ESFAS functions meets this criteria.

RAI-SRP 7.5-ICE-01

Why does the Qualified Data Processing Subsystems (QDPS) which is required to be powered from a Class 1E 72-hour source contain variables of the Post Accident Monitoring System which will only be available for 24 hours? Why are the variables not required past 24 hours?

AP1000 Chapter 7, Section 7.5.4 states "*he qualified data processing subsystems are divided into two separate electrical divisions. Each of the two electrical divisions is connected to a Class 1E dc uninterruptible power system with sufficient battery capacity to provide necessary electrical power for at least 72 hours."* Table 7.5-1 of the AP1000 DCD, Revision 16, has several variables, which have been added to the QDPS Indication. These same variables have Note 7 added in the "Number of Instruments Required" column, which reads "*This instrument not required after 24 hours."*

RAI-SRP 7.7-ICE-01

Demonstrate what actions, or outputs, are generated when one or more signals disagree or fall outside a defined parameter field for a given set of inputs (e.g. temperature, pressure, flux) to the Signal Selector Algorithms within the Plant Control System. For example, what alarm, control or indication outputs are processed based upon the logic contained within the Signal Selector Algorithms once a signal originating from the PMS is flagged as "bad" quality?

RAI-SRP 7.8-ICE-01

With regards to Table 14.3-3 of the AP1000 DCD, Revision 16, Tier 2, Chapter 14 (Page 14.3-35), the third table item from bottom of table shows the term "microprocessor" was not replaced with "microprocessor or special purpose logic processor. In Tier 2, Chapter 7 of the AP1000 DCD, the term microprocessor was replaced with "microprocessor or special purpose logic processor". Which wording phrase is correct?

RAI-SRP 7.8-ICE-02

With regards to Table 14.3-6, Sheet 7 of the AP1000 DCD, Revision 16, Tier 2, Chapter 14 (Page 14.3-46), in the second table item from bottom of table, the term “different” was not removed from term “different software”, and replaced with “any” as was done to Section 7.7.1.11, “Diverse Actuation System.” Update and correct as necessary.

RAI-SRP 7.8-ICE-03

In Table 19.59-18, Sheet 8 (Page 19.59-82), Table Section 3, the word “different” was not removed from term “different software” and replaced with “any” as was done to Section 7.7.1.11, “Diverse Actuation System.” Update and correct as necessary.

RAI-SRP 7.8-ICE-04

What type of microprocessor does the QDPS System utilize and is that type of microprocessor used elsewhere in the AP1000 architecture, including that architecture outside of the PMS? Provide further delineation on this microprocessor equivalent to the level of detail provided for the Common Q based safety system if another system is being utilized.

RAI-SRP 7.8-ICE-05

Provide a detailed schematic and other relevant documentation detailing how the Diverse Actuation System accomplishes its intended function of actuating necessary ESFAS components without interfacing with any portion of the ESFAS System other than the final actuation devices in accordance with AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report (WCAP-15775).

RAI-SRP 7.8-ICE-06

Provide additional detail on how probabilistic risk assessment will be used in selecting functions performed by the Diverse Actuation System and how the approach is comparable to the guidance identified in BTP 7-19 of SRP, Chapter 7.

Technical Report 97, “AP1000 Standard Combined License Technical Report DAS Platform Technology and Remote Indication Change (APP-GW-GLN-022)," stated in Section 7.7.1.11 Diverse Actuation System that the specific functions performed by the diverse actuation system are selected based upon the probabilistic risk assessment evaluation. The diverse actuation system functional requirements are based on an assessment of the protection system instrumentation common mode failure probabilities combined with event probability.

RAI-SRP 7.9-ICE-01

Section 7.1.2.6 of the AP1000 DCD, Revision 16, stated that the Protection and Safety Monitoring System (PMS) does not contain multiplexers to provide a signal path between the protection system equipment and the main control room. Provide the complete basis for removing these multiplexers. Describe the additional or existing component(s) that would provide the signal path between the protection system equipment and the main control room?

RAI-SRP 7.9-ICE-02

Provide further design information of the communication network within the AP1000 PMS. Specifically, in the AP1000 PMS design, what types of network segregation exist between message transfer and process data transfer to prevent the two processes from interfering with each other?

Section 7.9 of the Standard Review Plan, “Data Communication Systems,” defines performance criteria for data communication systems; specifically on system capacity, data rates, and bandwidth requirements. Section 3.1 of WCAP-16675-P states that process data transfers will be of a certain percentage of the maximum capacity of the network and message transfers will use the remainder of the capacity. What mechanisms within the network design prevent interference of process data transfers with message transfers when there is excess network traffic?

RAI-SRP 7.9-ICE-03

WCAP-16675-P stated that the Common Q network (AF100 bus) is not used for engineered safety features actuation system (ESFAS) functions or reactor trip (RT). However, WCAP-16674-P stated that the Common Q Network is used to integrate all the safety functions, including ESFAS and RT. Please clarify how the AF100 bus will be used to integrate the ESFAS and RT.

RAI-SRP 7.9-ICE-04

Provide additional information on access control of AC160 controllers and Flat Panel Display System. What types of access control exist for non-safety, on-site access and for offsite access to the AC160 controllers and PMS?

Section 7.9 of the Standard Review Plan, “Data Communication Systems,” states that the “DCS does not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators.” How does Westinghouse plan to meet the access control criteria in Section 7.9 of the Standard Review Plan? Specifically, Section 4.1.2 of WCAP-16774-P stated that security is maintained within the PMS since the ability to remotely program the AC160 controllers and Flat Panel Display Systems over the AF100 network has been disabled in the PMS. What method is used to remove the ability to remotely program the AC160 controllers (e.g. software, hardware, or combination)?

RAI-SRP 7.9-ICE-05

Provide additional information on the reliability of the Advant/Ovation Interface (AOI) Gateway to support safety to non-safety communication. Specifically, what testing has been completed on the AOI gateway to verify its reliability?

Section 5.1.2 of WCAP-16675-P states that the AOI gateway consists of two subsystems: one safety subsystem, which is part of the PMS division, and one non-safety system, which is part of the non-safety real-time data network. A unidirectional optical fiber (with an optical transmitter on the safety subsystem and optical receiver on the non-safety subsystem) connects the two

subsystems. In accordance with the requirements from 10 CFR 50.55a(a)(1), “Quality Standards for Systems Important to Safety,” structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. What is the basis demonstrating the reliability of the AOI Gateway? Provide additional information on the testing, fabrication, traceability of the AOI Gateway. In addition, is the AOI Gateway considered part of the safety system? If so, submit on the docket information describing how the AOI Gateway meets the requirements of IEEE 603-1991 (for both hardware qualification and software quality).

RAI-SRP 7.9-ICE-06

Provide additional information on the design of the isolation device, including the device’s functional independence and diversity characteristics between safety and non-safety systems. Demonstrate that failures within the non-safety system will not influence or prevent the protection system from completing its safety functions.

The Interim Staff Guidance (ISG) for Highly Integrated Control Rooms- Communications provided guidance to meet GDC 24, “Separation of Protection and Control Systems,” and 10 CFR 50.55a(h). Section 3.3.4 of WCAP-16775-P stated that a qualified isolation device will be used to provide electrical and communication isolation as envisioned in IEEE 603-1991 and IEEE 7-4.3.2-1993, respectively. Demonstrate how the criteria defined in Item 2 of Section 1, “Interdivisional Communication” of the ISG is met. Specifically, demonstrate how the isolation device design ensures that protection will be sustained despite any operation, malfunction, design error, communication error, software error, or corruption from the non-safety system. In addition, the NRC staff finds that it is necessary for the applicant to provide an ITTAC to verify that the isolation device is built as designed.

RAI-SRP 7.9-ICE-07

Demonstrate that the discrete digital signals sent from the non-safety system to the safety system for manual system level actuation of the safety system is sent over a reliable and secure link.

GDC 21, “Protection System Reliability and Testability,” states that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired. Verify that the discrete digital signals sent from the non-safety system to the safety system (as described in Case D of the communication between safety and non-safety systems of WCAP-16775-P) are over a dedicated link, such that any failures from the non-safety system will not impact the safety system.

RAI-SRP 7.9-ICE-08

Provide further information regarding the soft controls used for manual control of non-onerous components from non-safety workstations within the main control room. Specifically, what access control and security measures are in place to prevent unauthorized activation of these soft controls?

Section 7.9 of the SRP, “Data Communication Systems,” states that the “DCS does not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators.” How does Westinghouse plan to meet this access control criterion from Section 7.9? Specifically, Section 3.4.2 of WCAP-16675 states that soft controls will be used for manual control of non-onerous components from non-safety workstations within the main control room. What design features exist to prevent any unauthorized activation of manual soft controls (key stroke control) of safety components without operator knowledge?

RAI-SRP 7.9-ICE-09

Provide additional information on the communication and function processors used within the Component Interface Module (CIM). Specifically, clarify the design of the memory and resource allocation within the function and communication processors.

To meet the independence requirements of IEEE 603-1991, the ISG for Highly Integrated Control Room- Communications provided guidance on safety to non-safety communication. Demonstrate how Westinghouse meets this ISG or a suitable alternative to satisfy the independence requirement? Specifically, do the communication and function processors operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information?

RAI-SRP 7.9-ICE-10

Provide additional information demonstrating how the non-safety data network will meet system capacity, data rates, and bandwidth requirements.

The Standard Review Plan (SRP), Section 7.9, “Data Communication Systems,” defines performance criteria for data communication systems, specifically on system capacity, data rates, and bandwidth requirements. In Section 3.1.2 of WCAP-16774-P, Westinghouse commits to implementing simultaneous communication of general purpose communication and real-time data transmission in such a way as to preserve the design philosophy of guaranteeing the real-time periodic data transmission without loss, degradation, or delay; even during plant upsets. Demonstrate via text and schematics how this is achieved since general purpose communication occurs on the same physical media as the real-time periodic data.

RAI-SRP 7.9-ICE-11

Provide additional information on the implementation of cyber security measures for the non-safety data network. Demonstrate how the network design prevents unauthorized access of the non-safety network.

In Section 3.1.3 of WCAP-16774-P, Westinghouse commits to providing off-site access security via the use of multilayered firewalls, with the Ovation System providing only unidirectional access to higher and higher levels in the hierarchy. Demonstrate via text and schematics how this hierarchy is defined. For example, where are the firewalls placed? What types of firewalls will be used (e.g. stateful, stateless)? How will Westinghouse prevent workstations within higher security levels from downloading malicious code (either intentionally or unintentionally) from devices at lower security levels?

RAI-SRP 9.5.2-ICE-01

In Section 9.5.2.2.3, Private Automatic Branch Exchange (PABX) System, the applicant has changed the PABX interface to Communications System requirements with the following modifications. The applicant states that the hotlines to specified locations (for example, dedicated communication lines with load dispatcher to support and coordinate the system grid) is described in Section 9.5.2.5. The hotline circuits are dedicated channels that provide direct communication between the main control room and the headquarters or other facilities. The NRC staff has reviewed Subsection 9.5.2.5, Combined License Information. The staff cannot find the described requirements in Subsection 9.5.2.5 that the applicant moved from Section 9.5.2.2.3. Clarify which of the specific requirements in Subsection 9.5.2.5 meet the requirements that were removed from Section 9.5.2.2.3.

RAI-SRP 10.4.7-ICE-01

Within the AP1000 DCD Revision 16, Tier 2, Chapter 10, Figure 10.4.7-1, Sheet 4, “Condensate and Feedwater System Piping and Instrumental Diagram,” the notes have been removed from the figure. On page 8 of Technical Report 103, in the first paragraph it states that Note 3 and Note 4 will be revised. Without the notes, Technical Report 103 is referencing notes in Figure 10.4.7-1 that do not exist. Update and/or correct.