Audit Report

for Review of Proprietary Technical, Procedural, and Process Information Related to the Component Interface Module and Diverse Actuation Systems

for the

Westinghouse AP1000 Design Certification Amendment Application

March 8 - 11, 2010

Bill Roggenbrodt	NRO/DE/ICE1
Jack Y. Zhao	NRO/DE/ICE1
Ken D. Mott	NRO/DE/ICE1

Table of Contents

1. Background

The Advanced Passive 1000 (AP1000) is a 3,400 MWt pressurized-water reactor (PWR) system designed with passive safety features by Westinghouse Electric Company (Westinghouse), LLC. As included in 10 CFR Part 52, Appendix D, the U.S. Nuclear Regulatory Commission (NRC) issued the final design certification rule (DCR) in January 2006 for the AP1000 design control document (DCD) application submitted by Westinghouse. However, on May 26, 2007, Westinghouse submitted a design certification amendment (DCA) application to amend the AP1000 DCR as described in Revision 16 of the AP1000 DCD. Additionally, by letter dated September 22, 2008 Agency wide Documents Access and Management System (ADAMS) Accession No. ML083220482, Westinghouse updated its DCA application to amend the certified AP1000 DCD by submitting Revision 17 of the DCD in accordance with 10 CFR 52.63, "Finality of Standard Design Certifications." The DCA application lists many design changes, which included Westinghouse's proposed removal of the design descriptions and Inspections, Tests, Analysis, and Acceptance Criteria (ITAAC) associated with the first two phases of development for two key instrumentation and control (I&C) systems, the safety-related Protection and Safety Monitoring System (PMS) and the important-to-safety Diverse Actuation System[1] (DAS).

Audit Scope

The specific areas on which this audit focused dealt with Westinghouse's proposed removal of the first two phases of the development lifecycles for the PMS and the DAS as identified in Revision 17 of the AP1000 DCD. Westinghouse proposed removing the PMS design descriptions in Tier 1, Section 2.5.2, Design Description Items 11.a and 11.b, as well as Design Commitment Items 11.a and 11.b within Inspections, Tests, Analyses and Acceptance Criteria (ITAAC) Table 2.5.2-8. Additionally, Westinghouse proposed to remove descriptions associated with the first two development phases of the DAS in Tier 1, Section 2.5.1 as described in Design Description Items 4.a and 4.b, as well as Design Commitment Items 4.a and 4.b within ITAAC Table 2.5.1-4. The proposed removals affecting the PMS and DAS ITAAC are referenced to Revision 15 of the AP1000 DCD. This report summarizes the NRC staff's observations and conclusions developed during the audit that confirmed whether or not the commitments associated with the first two phases of these I&C systems' development have been adequately addressed and permit closure.

Westinghouse defines these phases of development as the Design Requirements (or Conceptual) phase and System Definition phase of the respective software lifecycle (SLC) or programmable technology development lifecycle for the given I&C system. Branch Technical Position (BTP) 7-14 within Chapter 7 of NUREG− 0800, "Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants: Light-water Reactor Edition," SRP defines these two phases of development as the Planning Activities Phase and the Requirements Activities phase.

The audit was conducted on March 8-11, 2010 at the CS Innovations (CSI) facility in Scottsdale, Arizona. CSI is a wholly-owned subsidiary of Westinghouse and supplies the Component Interface Module (CIM) and the Safety-Related Remote Node Controller (SRNC) systems, which are both part of PMS. CSI also supplies the DAS system. The NRC staff provided an audit plan (Attachment A) to the applicant prior to the audit. The documents

[1] The DAS is designed to function as a diverse backup system to the PMS in the event of a software-based common cause failure of the PMS.

provided by Westinghouseand CSI that were reviewed by the audit team are shown in Section 7 of this report.

Current Safety Evaluation Report Findings

The NRC staff documented its current findings and conclusions with regards to the AP1000 Instrumentation and Control (I&C) system in Safety Evaluation Report (SER) with Open Items (OI) for Chapter 7, "Instrumentation and Control," of NUREG-1793, Supplement 2 – AP1000 Design Certification Amendment (SER/OIs) Agencywide Document Access and Management system (ADAMS) Accession No. ML092800266).

In Section 7.2.5 of the staff's SER/OIs, the NRC determined that removal of the first two ITAAC phases as they relate to the PMS that:

> Based on the review of all proprietary and docketed documentation provided to the NRC that relates to the design requirements and system definition phases of the SLC for the PMS, the staff has not concluded that Westinghouse has adequately completed or addressed the design requirements or system definition phases, from a lack of either technical adequacy or completeness of the given subject matter. Westinghouse did not provide sufficient technical information in Revision 17 of the AP1000 DCD, it's associated TRs (technical reports), or its proprietary documentation (to be made available for audit or inspection) to demonstrate satisfactory completion of these phases. It is, therefore, inappropriate for Westinghouse to remove the design requirements or system definition phases of the SLC.

Additionally, the staff concluded in Section 7.2.8 of the SER/OI that:

> 10 CFR 52.47(b)(1) describes the ITAAC. As Westinghouse has provided insufficient information to satisfy the completion of the design requirements or conceptual phase of the PMS SLC, that issue remains open. **The NRC staff identified this as OI-SRP-7.2-ICE-08.** The staff will not approve the removal of the system definition or requirements phase of the PMS SLC until such time as Westinghouse provides satisfactory information to the staff for review and approval.

In Section 7.8.1.1 of the staff's SER/OIs, the NRC staff concluded the applicant's removal of the first two ITAAC phases for the DAS that:

> While Westinghouse removed portions of the ITAAC, ***it did not provide the corresponding design information that would address those two phases.*** Specifically, Westinghouse has not submitted to the staff design information that would fully address the four points in SRP BTP 7-19. Westinghouse should fully address the four points in order for the staff to approve the removal of the design requirements and system definition phases in the design acceptance criteria (DAC). ***Since Westinghouse has not provided design information sufficient to support removal of Items 4a and 4b from the ITAAC, the staff does not approve their removal.***

The NRC staff also concluded in Section 7.8.2 of the SER/OIs:

> General Design Criteria (GDC) 22 requires, in part, that for protection systems, "design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the

protective function." In the previous certified AP1000 DCD Tier 1, ITAAC Table 2.5.1-4, Item 4, provided sufficient DAC to allow for a conclusion that the D3 design of the AP1000 was adequate. Westinghouse removed Items 4a and 4b of the ITAAC ***without providing sufficient design information.*** Therefore, the staff concludes that Revision 17 of the AP1000 DCD does not meet the requirements of GDC 22.

Audit Team Members

The audit team consisted of the NRC staff members identified in Table 1 below.

Name and Title	Affiliation
Terry Jackson, Branch Chief	NRO/Division of Engineering
William Roggenbrodt, Electronics Engineer, Digital I&C, Audit Team Leader	NRO/Division of Engineering
Jack Zhao, Sr. Electronics Engineer, Digital I&C	NRO/Division of Engineering
Ken Mott, Electronics Engineer	NRO/ Division of Engineering
Sikhindra Mitra, Project Manager	NRO/Division of New Reactor Licensing

Table 1: List of NRC Audit Team Members

CSI / Westinghouse Personnel Present at Audit

Table 2 identifies the applicant's key staff members that participated in the audit over the course of the four days at Scottsdale, Arizona.

Name	Affiliation
Bob Seelman	Westinghouse
John Ewald	Westinghouse
Tom Tweedle	Westinghouse
Kyra Durinsky	Westinghouse
Steve Seaman	Westinghouse
Larry Erin	Westinghouse
Mesut Uzman	Westinghouse
Steen Sorenson	CSI
Dan Dragoon	CSI

Table 2: List of Key WEC/CSI's Staff Members

2. Objective

The objective of the regulatory audit examines, evaluates, and confirms proprietary technical, procedural, and process information associated with the safety-related CIM and important-to-safety DAS systems meets regulatory requirements and satisfactorily addresses regulatory guidance. The team focused on gaining a better understanding related to the applicant's implementation of programs and processes which track ongoing work or completion of development tasks or stages related to the Westinghouse AP1000 DCA application. In particular, this audit focused on the CIM system, which is part of the PMS, and the DAS. Although, CSI is a wholly-owned subsidiary of Westinghouse, its processes and procedures are not the same as Westinghouse's processes and procedures. The team conducted the audit to verify adequate programmatic, planning, and process documentation were being utilized by CSI. The team also identified any additional information which would require docketing to support the reasonable assurance of safety of the PMS, the measure of adequate quality of the DAS, and the demonstration that sufficient diversity exists between the two systems.

3. Regulatory Audit Basis

The requirements of 10 CFR 52.47 state, in part, that the Commission will require, before design certification, or in the case of the AP1000, a DCA, that a sufficient level of information be provided to enable the Commission to judge the applicant's proposed means of assuring that construction conforms to the design and to reach a final conclusion on all safety questions associated with the design before the certification is granted. The information submitted for a design certification must include performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant. The Commission will require, that information normally contained in certain procurement specifications and construction and installation specifications be completed and available for audit if the information is necessary for the Commission to make its safety determination. Hence, regulatory audits are necessary to verify information presented by Westinghouse and its suppliers, in this case CSI, to serve as proof of phase completion for the PMS SLC, the DAS developmental lifecycle, and to verify the associated documentation is being retained in accordance with 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," Criterion XVII, Quality Assurance Records.

The documentation presented by the applicant must demonstrate compliance with 10 CFR 50.55a(a)(1), 10 CFR 50.55a(h), which incorporates by reference Institute of Electric and Electronic Engineers (IEEE) Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," 10 CFR Part 50 Appendix A, General Design Criteria (GDC) 1, 21, 22 and 24, and other relevant portions of 10 CFR Part 50, Appendix B. The audit also verified the design of the DAS satisfies both 10 CFR 50.62, Requirements for Reduction of Risk From Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," and addresses the NRC policy discussed in Staff Requirements Memorandum (SRM) associated with Commission Paper (SECY) 93-087, "Policy, Technical, and Licensing Issues pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." The audit should provide evidence to demonstrate the structures, systems or components (SSCs) were designed and tested to the quality standards required commensurate with the safety-related or important-to-safety function, to be performed. In addition, the applicable guidance for examining and evaluating the DAS is Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related," and its enclosure.

The NRC audit team requested CSI provide information and supportive documentation at their facility located in Scottsdale, Arizona to facilitate a timely review of the documentation related to the first two phases of the CIM and DAS development lifecycles.

4. Regulatory Audit Activities

The NRC audit team conducted the following activities:

Audit Activities Related to the CIM System

- The NRC audit team verified whether adequate information existed in documentation describing the developmental lifecycle for the CIM system. The audit team also evaluated the documents provided for the Planning Activities and Requirements Activities Phases, per BTP 7-14, to determine if the CIM documents are of the same quality and detail to be considered consistent with the guidance within Chapter 7 of the SRP, NUREG/CR 6101, and commitments made in the Common Q Software Program Manual (SPM) and WCAP-15927, "Design Process for the AP1000 Common Q Safety Systems," Revision 2.

- The NRC audit team evaluated the acceptability of the requirements specifications and quality standards related to the development of the CIM system, including the 10 CFR Part 50, Appendix B, requirements and their application within the CSI design and independent verification and validation (IV&V) programs, organizations, and processes based upon the commitments made within the Common Q SPM, WCAP-15927, Revision 2, and the guidance within IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation."

- The NRC audit team conducted an evaluation of computer security attributes of the CIM system to determine if the system meets the requirements of IEEE Std. 603-1991, Clauses 5.6.3 – Independence and 5.9 - Access Control to prevent unwanted activations of the CIM by the non-safety related control system and/or inadvertent operator action that could cause the system to operate outside its design parameters.

- Utilizing the Requirements Traceability Matrix (RTM) (Reference 66) of the PMS provided by the applicant, the NRC audit team attempted to trace several of the CIM functional requirements or design specifications of the device from the function design requirements back to their source documents.

Audit Activities Related to DAS System

- The NRC audit team conducted an evaluation of provided documentation related to the DAS to determine whether sufficient information existed to consider Westinghouse's Design Requirements and/or System Definition phases of the AP1000 design process, as related to the DAS, completed.

- The NRC audit team conducted a diversity evaluation to determine if sufficient diversity exists between the DAS and other AP1000 I&C systems, especially the PMS. The NRC audit team used WCAP 15775, "AP1000 I&C Defense-in-Depth and Diversity (D3) Report" Revision 3; WCAP 17179-P, "AP1000 Component Interface Module Technical Report," and WCAP 17184-P, "AP1000 Diverse Actuation System

Planning and Functional Design Summary Technical Report" and their cited CSI documents as reference material. The NRC audit team utilized 10 CFR Part 50, Appendix A, GDCs 22 and 24, and the guidance of NUREG/CR 6303 as supporting information during the evaluation.

- The NRC audit team examined documentation related to the DAS to verify the requirements of 10 CFR 50.62 and 10 CFR Part 50, Appendix A, GDCs 1 and 22 and the NRC policy discussed in the SRM associated with Commission Paper SECY 93-087, Policy, Technical, and Licensing Issues pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs were adequately addressed. The SRM associated with SECY 93-087 is considered acceptance criteria in NUREG 0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants" BTP 7-19.

- The NRC audit team evaluated the CSI documentation provided to determine if additional information beyond that contained in the DAS Setpoint Methodology white paper, provided by Westinghouse, would be obtained to more clearly understand the DAS Setpoint Methodology and the basis for the setpoints to be chosen for the DAS.

General Audit Activities

- The NRC audit team conducted a review of CSI's programs tied to nuclear safety.

- The NRC audit team reviewed CSI's IV&V and Testing Program. The audit team based their evaluation upon the requirements of 10 CFR Part 50, Appendix B, Criterion III, Design Control and Criterion XI Test Control. The guidance within NRC Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1, endorses IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation." The commitments made in the Common Q SPM and WCAP-15927 documents were also utilized.

- The NRC audit team conducted a review of CSI's design, document control and change processes, which is based upon the requirements of 10 CFR Part 50, Appendix B, Criterion III, Design Control; Criterion VI, Document Control; and Criterion XVI, Corrective Action. This activity covers both the Design Requirements and System Definition phases for the SLC of the PMS and the programmable technology lifecycle of the DAS.

- The audit team reviewed CSI's training and records management program based upon 10 CFR Part 50, Appendix B, Criterion XVII, "Quality Assurance Records". The commitments made in the Common Q SPM and WCAP-15927 were also utilized.

- The NRC audit team conducted the entrance meeting on March 8, 2010 and the exit meeting on March 11, 2010.

- The NRC audit team conducted daily update meetings with both Westinghouse and CSI representatives in attendance. The meetings were held at the end of the day to discuss observations and insights gained by the audit team while examining

documentation or meeting with CSI/Westinghouse personnel during the day's audit activities.

- The CSI staff invited, and the NRC audit team participated in, a tour of the manufacturing lines constructing the CIM System and the DAS.

5. Observations

Component Interface Module System

For the CIM system, the audit team had the following specific observations during the audit:

- In Westinghouse's document, "Component Interface Module Hardware Requirements Specification," WNA-DS-01271-GEN, Revision 7, Design Requirement R003.1, "Design Tools", requires, "All FPGA design tools and libraries shall be dedicated unless the device directly affected by the tools is 100 percent tested with a different tool before being released." After discussing the issue with CSI, the audit team was informed that the CIM System requirements as written in the Westinghouse document were not achievable. However, CSI's document, "CIM Requirement Traceability Matrix", 6105-20010, Revision 0, shows the above R003.1 requirement is met for the CIM design. In addition, based upon the review of documents provided, the audit team found no document exists describing, in sufficient detail, how the CIM will address either the 100 percent testability criterion within Digital I&C integrated scheduling group Interim staff Guidance 04 or how the high quality processes or programs will adequately address the guidance within BTP 7-14 of the SRP.

- In Westinghouse's document, "Component Interface Module Hardware Requirements Specification," WNA-DS-01271-GEN, Revision 7, Design Requirement R012.1, "Quality Program," requires the supplier shall have a documented Quality Program which meets recognized industry standards, such as ASME NQA-1 or ISO-9000. However, the audit team could not locate any evidence in the documents presented demonstrating that CSI meets the recognized industry quality standards, such as ASME NQA-1 or ISO-9000. After speaking with a CSI staff member, the audit team determined that CSI currently does not possess an ASME NQA-1 or ISO-9000 Quality Program certification. However according to CSI staff; they have been working to obtain the ASME NQA-1 or ISO-9000 Quality Program certificate.

- Design Requirement R003.9, "Module Materials", in Westinghouse's document, "Component Interface Module Hardware Requirements Specification," WNA-DS-01271-GEN, Revision 7 is not consistent with Design Requirement R003.9, "Module Materials", in Westinghouse's document, "Safety System Remote Node Controller Requirements Specification", WNA-DS-01272-GEN, Revision 4.

- In Westinghouse's document, "Safety System Remote Node Controller Requirements Specification," WNA-DS-01272-GEN, Revision 4, design requirement R003.1, "Design Tools", requires all field programmable gate array (FPGA) design tools and libraries shall be validated unless the device directly affected by the tools is 100 percent tested with a different tool before being released. CSI's document, "SRNC Requirement Traceability Matrix", 6105-10010, Revision 1, shows the above R003.1 requirement is met for the SRNC design. However, after talking with a CSI staff member, the audit team found that CSI has not validated all FPGA design tools and libraries nor conducted 100 percent testing for the affected devices.

- The audit team found that Section 5.5.2 of CSI document, "SRNC Architecture Specification," 6105-1002, Revision 2 is not consistent with R011.1 MTBF requirement (100,000 hours) in Westinghouse's document, "Safety System Remote Node Controller Requirements Specification", WNA-DS-01272-GEN, Revision 4; although CSI's document, "SRNC Requirement Traceability Matrix", 6105-10010, Revision 1, claims that the above R011.1 requirement is met for the SRNC design.

- The audit team spoke with CSI about roles of design team members to determine how separation of CIM-SRNC and DAS design personnel requirements were met (refer to Westinghouse document, "Component Interface Module (CIM) and Safety Remote Node Controller (SRNC) Development Project Plan", WNA-PD-00050-GEN, Revision 2 for clarification), the audit team discovered that CSI is relying on Westinghouse to perform critical IV&V functions in Pittsburgh (Cranberry), Pennsylvania. However, after discussion with Westinghouse, no path beyond a document review function and system-based testing function in Pittsburgh (Cranberry) had been offered by Westinghouse and no document describing independent document review and system-based testing functions were provided for review.

- The organizational model described in the document, "Quality Manual", 9000-0000, Revision 3, shows different organizations and the functions they provide, but the company (CSI) is not organizationally based. Rather the company is project based in that first a customer requests a project be performed and then CSI, based upon the project requirements (versus the standardized, procedure-based organizational requirements), develops the process by which each role (design manager, V&V Manager, Configuration Manager, etc.) will be filled. This issue concerns the audit team since, as roles are delineated in CSI document, "CIM-SRNC Management Plan," 6105-00000, Revision 2, the Quality Assurance (QA) Manager also serves as the Configuration Manager. This is not acceptable per 10 CFR Part 50, Appendix B.

- The audit team determined that on page 15 of CSI document, "CIM-SRNC Management Plan", 6105-00000, Revision 2, it states that no training for the personnel working on the CIM-SRNC project is required, but on Page 31 of CSI document, "CIM-SRNC Test Plan", 6105-00005, Revision 2, it requires special training and certification. However, after talking with a CSI staff member and reviewing the training records, the audit team determined that CSI had provided some training sessions for the personnel working on the CIM-SRNC project. But, in all the documents provided, the audit team was unable to locate any training plan for people working on the CIM-SRNC project for the AP1000.

- The NRC audit team found no appreciable programmable technology developmental lifecycle, SPM or other similar document for the CIM-SRNC development process other than a brief discussion in the CIM Technical Report.

- During the audit, the NRC audit team found that the Westinghouse staff presumes that a "hold-up" resistor exists to ensure that the Z port on the CIM system will always be disabled in the CIM. A CSI staff member described the circuit and informed the NRC audit team that no hold up resistor is utilized. The NRC audit team deems that further explanation detailing how exactly the Z port for the CIM is disabled is required. Westinghouse staff members at CSI recommended this action occur at the upcoming Cranberry, Pennsylvania audit scheduled for April 2010.

- After reviewing all documents provided by the applicant and CSI, the audit team couldn't locate any formal programmable technology Development Plan, Integration Plan, and/or Safety Plan created for the CIM-SRNC project, although those plans have been referenced in the CSI's Document, "CIM-SRNC Management Plan," 6105-00000, Revision 2.

- The Altium Design tool for SRNC schematic and PCB software were used for the CIM-SRNC project and from discussions with CSI personnel, it appeared that the tools would be used to detect logic errors (i.e., serve as a verification and validation tool). However, the audit team was unable to locate any dedication or evaluation documentation describing a process these products would undergo to satisfy the dedication requirements for these commercial design tools and software. SRP BTP 7-14 refers to the criteria within IEEE Std. 7-4.3.2-2003, which states that software tools should be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

- During the audit, the audit team determined CSI has been using a subcontractor to provide the commercial printed circuit board (PCB) product for the CIM-SRNC Project. However, the NRC audit team couldn't locate any evidence in all the documents provided to demonstrate that CSI has developed a commercial dedication process for the PCB board or quality program in order to be able to audit for the PCB subcontractor.

- In documents provided by both Westinghouse and CSI, the NRC audit team discovered there was no mention of meeting the guidelines in RG 1.180 for the electromagnetic compatibility. After discussing with Westinghouse's and CSI's staff members, the CIM and SRNC will be installed as components within Westinghouse's cabinets which will be tested to meet the EMC requirements in RG 1.180. However, the audit team was unable to locate the above information in the documents provided.

- After conducting a sampling check on documents provided by the applicant, the NRC audit team had the following additional observations related to design document quality control for the CIM-SRNC project. Neither Westinghouse nor CSI provided any "in-house" corrective action documents to demonstrate the formal correction process captured these issues before the audit team finished the audit. Westinghouse and CSI have been asked to provide corrective action documents to show that necessary corrective actions have been taken.

    - Appendix D of CSI document, "SRNC FPGA Specification," 6105-10004, Revision 0, is not consistent with CSI document, "SRNC Requirement Traceability Matrix," 6105-10010, Revision 1.

    - Appendix D of CSI document, "CIM FPGA Specification", 6105-20004, Revision 3 does not match with CSI document 6105-20010, "CIM Requirement Traceability Matrix," Revision 0.

    - Appendix D of CSI document, "ASE-SRNC Test Simulation Environment Specification", 6105-10020, Revision B, is not consistent with CSI document, "SRNC Requirement Traceability Matrix," 6105-10010, Revision 1.

    - Appendix D of CSI document, "ASE-CIM Test Simulation Environment Specification", 6105-20020, Revision B, does not match with CSI document 6105-20010 "CIM Requirement Traceability Matrix," Revision 0.

    - It was found in CSI document, "ASE-SRNC Test Simulation Environmental Specification", 6105-10020, Revision. B, that the ALS platform is used for the SRNC, but the SRNC module does not use the ALS platform. The audit team confirmed this fact with a Westinghouse staff member.

    - Actel ProASIC II APA450 FPGA is used in CSI document, "SRNC Hardware Specification", 6105-10003, Revision. 1, but Actel ProASIC3 FPGA is used in CSI document, "SRNC Architecture Specification", 6105-10002, Rev. 2.

    - Many page numbers used on Page 9 of CSI document, "CIM Hardware Specification", 6105-20003, Revision. 0, do not match with the actual page numbers used in the document.

    - In Figure A-1, "Priority Logic," in Westinghouse's document, "Component Interface Module Hardware Requirements Specification", WNA-DS-01271-GEN, Revision 7, "Priority Logic" is used for "Block Overload" cross-reference, but the audit team determined the "Priority Logic" should be changed to "Component Control Logic" for this priority logic diagram to make sense.

    - The audit team determined several document text reference errors, as well as text based or editorial errors (i.e., requirements tracing from applicant to vendor incorrect; training manual listed as 9000-00100, however, actually identified as 9000-00200) existed between different CSI documents and required correction.

- 10 CFR Part 50, Appendix B, Criterion XVII, "Quality Assurance Records," states, "…records shall also include closely-related data such as qualifications of personnel…." The audit team was unable to locate documentation demonstrating the applicable qualifications of the requisite personnel who work on the CIM or DAS project.

Diverse Actuation System

Per Westinghouse, CSI will implement the DAS according to the DAS system requirements provided by WEC. The audit team found that, at the time of the audit, Westinghouse recently provided the DAS System Requirements to CSI. Therefore, CSI has not yet developed or created all of its development plans and design requirements specifications for the DAS. As a result of the recent Westinghouse submission to CSI:

- The audit team observed the Westinghouse requirement specifications for the CIM were delivered to CSI. However, due to the current state of the design, the team was unable to examine and evaluate any CSI quality and functional developmental requirements for the DAS that were generated from the Westinghouse DAS system requirements specifications. During the audit, there were several questions raised about correctness of requirements traceability between the applicant Westinghouse and its DAS subcontractor/supplier (CSI).

- The audit team requested that CSI explain how they will meet the DAS diversity requirements stated within the Westinghouse system requirements specifications. CSI stated the specified ALS components were approved during the Wolf Creek Main Steam and Feedwater Isolation System (MSFIS) and that evaluation would help to ensure that diversity would be met. The audit team was unclear as to how the use of that document reference would aid in determining sufficient diversity exists between the DAS and CIM Systems.

- CSI stated by using the components specified in Table 5.5-1 of Westinghouse's document, APP-DAS-J4-001, "AP1000 Diverse Actuation System Design Specification," Revision C, these components would ensure that diversity between the DAS and the CIM-SRNC are met (specifically, ALS-101 FPGA chip board). However, a review of the SER for Wolf Creek MSFIS (ADAMS) Accession No. ML090580520 shows that ALS board ALS-101 was used, instead of ALS-102 that is being described for use in the DAS. Section 3.1.1.4.2 of the SER for Wolf Creek MSFIS states, "The Core Logic Board (ALS-101-1) performs the MSFIS application-specific control logic. The core logic board is responsible for the MSFIS safety functions and is the bus master for the safety signal bus." For any changes, it states in Section 4.2.2 of the SER for the Wolf Creek MSFIS, the staff listed the applicable ALS hardware that

  > *"…has been reviewed by the staff and has been determined to be suitable for reference in future use of the ALS platform in safety-related applications in nuclear power plants. Modification of these documents to new revision levels will require review of the changes, to determine that those changes do not invalidate the staff's acceptance."*

  The ALS-102 core logic board, which is currently slated to be used for the DAS is not listed as a component reviewed by the NRC staff.

- Neither the applicant Westinghouse nor its supplier (CSI) provided adequate documentation or a formal report demonstrating the "establishment of setpoint methodologies." Specifically, the applicant has not provided an adequate methodology or design requirements demonstrating the DAS actuations are sufficient and adequate to meet the diversity requirements of GDC 22 and address the NRC's Policy as it relates to Diversity and Defense-in-Depth contained within the SRM related to SECY-93-087.

- CSI presented no documentation supporting the human diversity claim within WCAP 15775, **"**AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," Revision 3, WCAP-17179, "AP1000 Component Interface Module Technical Report," Revision 0 or WCAP 17184-P, "AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report," Revision 0. As CSI's tasks involve construction of both the CIM-SRNC, which is part of the protection system and the diverse backup system to the PMS, 10 CFR Part 50, Appendix A, GDC 22 applies. Additionally, no documentation demonstrating how CSI specifically addressed NUREG/CR 6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," could be located.

6. Conclusions

The NRC audit team informed Westinghouse and CSI at the exit meeting that the audit team considered the following items pertinent issues. Based upon the issues identified and potential resolution paths discussed among the audit team and Westinghouse/CSI personnel, some issues may require formal action if satisfactory responses are not offered.

During the audit, Westinghouse personnel stated that several issues below should be deferred to the Cranberry, Pennsylvania audit scheduled for April 2009. While the staff understands WEC's position in that it believes some of the issues below may be resolved in Cranberry, Pennsylvania the issues will be captured, until such time as the identified items are addressed adequately at the forthcoming audit or through another mechanism.

Component Interface Module System

- CSI demonstrated no clear CIM-SRNC Programmable Technology Development Plan, Integration Plan, Safety Plan and/or IV&V Plan for CIM-SRNC development process. Without this key information, the future lack of these critical planning documents for the CM-SRNC would prevent the staff from concluding the CIM-SRNC system was developed and constructed in accordance with previously approved Westinghouse commitments

- The staff identified a lack of separation of the assigned duties of design and test personnel that were inconsistent with 10 CFR Part 50 Appendix B requirements.

- The audit team did not identify processes or procedures related to IV&V as defined in 10 CFR Part 50 Appendix B and discussed in BTP 7-14 of the SRP. The staff's concern lies in the fact that under the current CSI process for verification and validation of programmable technology devices, no current process exists requiring a separate and independent function-based or module-based testing be conducted in accordance with the commitments Westinghouse made to satisfy IEEE Std. 1012-2004. Additionally, FPGA testing devices, which CSI claims meet IV&V requirements, used during the

design process (by CSI) were developed in parallel by CSI design personnel. This process offers no mechanism to independently validate the testing process at CSI or at Westinghouse's Cranberry, Pennsylvania facilities. During the close-out meeting for the audit, the CSI staff explained how the critical IV&V functions were to be performed. However, the information conveyed in the verbal CSI explanation was not documented.

- Due to inconsistencies in requirement specifications between documents from Westinghouse and CSI for the CIM-SRNC system, the information within documentation concerning "hand-off" points between Westinghouse and CSI should clearly demonstrate not only what requirement needs to be met, but how each requirement will be met by the respective organization. This issue should be addressed when hand-offs occur from either Westinghouse or CSI.

- CSI referenced the Wolf Creek MSFIS topical report and the staff's associated safety evaluation (SE) (ADAMS accession number ML090580520) in several documents and discussions. However based upon the audit team's research, the software management plan and other referenced documents within the Wolf Creek SE, the plans were deemed application specific, that is for the MSFIS only, and other "generic approval" documents were to be referenced for prior approval only as it applied to a safety-related Advanced Logic System (ALS), such as the system used at Wolf Creek. Since the CIM-SRNC System is not ALS-based, references to the Wolf Creek SE may not be valid for some technical areas.

Diverse Actuation System

- The audit team informed Westinghouse and CSI that without providing additional documentation beyond the informal Westinghouse DAS setpoint white paper the staff would be unable to reach a determination of acceptability of the DAS setpoint methodology.

- CSI failed to demonstrate an adequate strategy in process or practice that CSI team members utilized appropriate methods with regard to separation of task assignments as they relate to the design or testing of safety-related systems. Therefore it is not possible to determine if sufficient measures are in place to ensure adequate diversity exists between different CSI staff members, or their contractors, demonstrating that those who work on the CIM-SRNC System have no part in the development of the DAS and vice versa.

General Audit Activities

- CSI and Westinghouse should provide corrective actions to address textual errors associated with documents as these errors serve as an indicator when measuring overall quality control as it relates to the design process.

- The audit team informed Westinghouse and CSI of their expectation that CSI submit corrective action documentation for the action items listed previously in this report on the docket or make the corrective action documentation available for the staff to review at the upcoming audit, currently scheduled for April 12 -16, 2010 at WEC office in Cranberry, Pennsylvania and at the Westinghouse Rockville Office.

7. References – (List of Documents Reviewed)

Reference No.	Document No.	Title	Revision
CSI Documents			
1		Team Member List	
2	6105-00000	CIM-SRNC Management Plan	2
3	6105-00001	CIM-SRNC QA Plan	1
4	6105-00002	CIM-SRNC CM Plan	1
5	6105-00003	CIM-SRNC VV Plan	1
6	6105-00004	CIM-SRNC EQ Plan	2
7	6105-00005	CIM-SRNC Test Plan	2
8	6105-00090	CIM-SRNC VV Report	A
9	6105-01000	D105 Board Assembly Procedure	0
10	6105-01001	CIM-SRNC BP and TP Assembly Procedure	0
11	6105-01002	Inspection Procedure, D105	A
12	6105-10002	SRNC Architecture Specification	2
13	6105-10003	SRNC Hardware Specification	1
14	6105-10004	SRNC FPGA Specification	0
15	6105-10008	SRNC Reliability Analysis	B
16	6105-10010	SRNC Requirement Traceability Matrix	1
17	6105-10011	SRNC Test Traceability Matrix	
18	6105-10020	ASE-SRNC Test Simulation Environment Specification	B
19	6105-10021	ASE-SRNC Test Design Specification	C
20	6105-10031	ATB-SRNC Test Design Specification	C
21	6105-10033	ATB-SRNC Test Procedure	B
22	6105-10042	SRNC Module Assembly Procedure	A
23	6105-10070	SRNC Board Initial Power-On Test Procedure	0
24	6105-10071	SRNC Isolation Test Procedure	A
25	6105-10072	SRNC ESD Test Procedure	A
26	6105-10073	SRNC Acceptance Test Procedure	0
27	6105-20002	CIM Architecture Specification	3
28	6105-20003	CIM Hardware Specification	0
29	6105-20004	CIM FPGA Specification	3
30	6105-20008	CIM Reliability Analysis	0
31	6105-20010	CIM Requirement Traceability Matrix	0
32	6105-20011	CIM Test Traceability Matrix	
33	6105-20020	ASE-CIM Test Simulation Environment Specification	B
34	6105-20021	ASE-CIM Test Design Specification	B
35	6105-20031	ATB-SNRC Test Design Specification	C
36	6105-20033	ATB-CIM Test Procedure	B
37	6105-20042	CIM Assembly Module Procedure	0
38	6105-20070	CIM Board Initial Power-On Test Procedure	0
39	6105-20071	CIM Isolation Test Procedure	A
40	6105-20072	CIM ESD Test Procedure	A
41	6105-20073	CIM Acceptance Test Procedure	0
42	6105-01011	CIM Burn-in Procedure	A

Reference No.	Document No.	Title	Revision
CSI Documents (cont)			
43	6105-30032	CIM Base Plate, Test Procedure	A
44	6105-40000	CIM-SRNC ATE Design Specification	B
45	6105-40001	CIM-SRNC ATS Design Specification	A
46	6105-40002	CIM-SRNC ATU Design Specification	A
47	5105-10000	BOM, SRNC Module	0
48	5105-20000	BOM, CIM Module	0
49	4105-20300	Schematic and Assembly Drawing, CIM Output Board	1
50	9000-00000	Quality Manual	3
51	9000-00001	QCP	4
52	9000-00300	Design	3
53	9000-00311	Electronics Development Procedure	3
54	9000-00316	HDL Coding Guideline	1
55	9000-00200	Indoctrination and Training	
56	9000-01001	Qualification and Certification of Inspection and Test Personnel	
57	9000-00301	Commercial Grade Dedication	
Westinghouse Documents			
58	WNA-DS-01271-GEN	Component Interface Module Hardware Requirements Specification	7
59	WNA-DS-01272-GEN	Safety System Remote Node Controller Requirements Specification	4
60	WNA-TP-01835-GEN	Component Interface Module (CIM) System Test Plan	0
61	WNA-PD-00050-GEN	Component Interface Module (CIM) and Safety Remote Node Controller (SRNC) Development Project Plan	2
62	APP-DAS-J1-001	AP1000 Diverse Actuation System Functional Requirements	0
63	APP-DAS-J4-001	AP1000 Diverse Actuation System Design Specification	C
64	WNA-PN-0056-WAPP	Project Plan Titled Nustart/DOE design Finalization Diverse Actuation System	1
65	APP-DAS-GEH-001	AP1000 Diverse Actuation System Design Process	0
66	APP-PMS-J0R-001	Protection and Safety Monitoring System Requirements Traceability Matrix	0

Audit Plan

Purpose

The regulatory audit examines and evaluates technical, procedural, and process information at the applicant's facility. The intent is to gain understanding regarding the applicant's implementation of programs and processes which track ongoing work or completion of development tasks or stages relating to Westinghouse Electric Company's (WEC) AP1000 nuclear power plant. In particular this audit focuses on the safety-related (SR) Instrumentation and Controls (I&C) system responsible for Reactor Trip and Engineering Safety Features Actuation System (ESFAS) functions, known as the Protection and Safety Monitoring System (PMS) and the important-to-safety Diverse Actuation System (DAS). The audit will be conducted at the CS Innovations (CSI) facility in Scottsdale, Arizona. CSI is a wholly-owned subsidiary of Westinghouse whose processes and procedures have not yet been combined with Westinghouse processes. The audit will verify proprietary information and review programs and processes utilized by the applicant's supplier, as well as, identify any additional information which requires docketing to support the reasonable assurance of safety of the PMS, the measure of adequate quality of the DAS and the demonstration that sufficient diversity exists between the two systems. The audit's expected length is five days from Monday, March 8, 2010 through Friday, March 12, 2010. If the audit team's evaluation results in no significant findings during the first several days of the audit, the audit may end prior to March 12, 2010.

Regulatory Audit Basis

An audit is required to verify information presented by Westinghouse and its suppliers, in this case CSI, to serve as proof of phase completion for the PMS software lifecycle (SLC), the DAS developmental lifecycle and to verify the associated documentation is being retained in accordance with 10 CFR 50.71.

The presented documentation must demonstrate compliance with 10 CFR 50.55a(a)(1), 10 CFR 50.55a(h), which incorporates by reference IEEE Standard 603 – 1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," 10 CFR 50 Appendix A, General Design Criteria (GDC) 1, 22 and 24 and 10 CFR 50 Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," thus providing evidence to demonstrate the structures, systems or components (SSCs) were designed and tested to the quality standards required commensurate with the SR or important to safety function to be performed.

Regulatory Audit Scope

The NRC requests CSI provide information and supportive documentation at their facility located in Scottsdale, Arizona to facilitate a timely review of the documentation related to the first two phases of the PMS and DAS developmental lifecycles, namely the Design Requirements (Planning Activities phase per Branch Technical Position (BTP) 7-14 within Chapter 7 of NUREG -0800 Standard Review Plan) and System Definitions (Requirements Activities phase per BTP 7-14) phases of the PMS SLC.

Attachment A

Regulatory Audit Plan CS Innovations PMS Software Lifecycle and DAS Developmental Lifecycle Documentation Validation
March 8th – 12th, 2010, Scottsdale, Arizona

Regulatory Audit Team

Terry Jackson, NRO/DE/ICE1	**Branch Chief**
Kenneth Mott, NRO/DE/ICE1	Electronics Engineer
William Roggenbrodt, NRO/DE/ICE1	Electronics Engineer, Digital I&C, **Team Lead**
Jack Zhao, NRO/DE/ICE1	Senior Electronics Engineer, Digital I&C

Location / Dates

Scottsdale, Arizona – CS Innovations facility
7400 East Tierra Buena Lane, Suite 101, Scottsdale, Arizona 85260

Information and Other Material Necessary for the Regulatory Audit

Documentation Requirements

At a minimum the audit team requires the current revisions of the Westinghouse and CSI documentation and other recognized standards listed in the **Attachment 1** to be present in the designated review area for the NRC Staff members. Additionally, if the documents listed have been revised since their original issue, the staff requires the previous revisions of the documents.

The team requests the information for the currently revised documents produced by CSI or WEC are available in the following formats:

- One (1) electronic copy housed on a CD or other portable storage medium, and,
- One (1) paper copy of each of the following CSI and Westinghouse documents (or their descendent documents) neatly compiled and in a logical order or sequence to enable a technical reviewer to easily locate given subject matter.
- One (1) paper copy of previous revisions of a given CSI or Westinghouse document contained within Attachment 1 will be sufficient.

NOTE:

Two copies of the referenced documents in the CIM Technical Report and DAS Planning and Functional Design Summary Technical Report, produced by CSI, are not listed in Attachment 1, but are expected to be available for review during the audit.

The audit team prepared a list of questions related to several of the technical reports currently under review by the NRC that will be discussed during the audit. The questions are not considered formal requests for aditional information (RAIs); rather they serve as clarifying questions and queries to stimulate additional discussion related to the design detail of the material provided in the technical reports and white paper.

As the listing of questions contains proprietary information, it will be delivered in a separate enclosure to the Westinghouse licensing agent prior to the audit.

CSI/WEC Personnel Requirements

The following CSI/Westinghouse personnel are required to be available, in person, to answer the staff's questions during the audit. It is hoped these individuals will be available during both the documentation review periods from Monday, March 8th through March 11, 2010 and, if requested by the NRC staff, they should attend the NRC/Westinghouse interface meetings. It is also requested those individuals attend the entrance and exit meetings at the beginning of and completion of the audit.

The following subject matter experts are required to be available during the audit period.

CSI CIM System Project Team Lead

CSI CIM System Lead Designer/Design Team Leader

CSI CIM System Independent Verification and Validation (IV&V) Team Leader

CSI DAS System Project Team Lead

CSI DAS Lead Designer/Design Team Leader

Additionally, the following personnel are requested to be present during the audit.

WEC AP1000 Licensing Project Manager

WEC PMS Project Team Lead/Subject Matter Expert

WEC PMS System Design Subject Matter Expert

WEC DAS Project Team Lead/ Subject Matter Expert

WEC DAS System Design Subject Matter Expert

It should be noted that one person may fill more than one role on the lists above.

Room Requirements

The NRC staff request the use of a climate controlled, well-lit conference room, or other suitable room, of sufficient size to accommodate four NRC personnel and the review of all requested documentation (See Attachment 1).

The room shall be separate from the meeting room where the CSI/Westinghouse/NRC interface meetings occur in order to afford sufficient privacy to the audit team when requested.

Regulatory Audit Plan CS Innovations PMS Software Lifecycle and DAS Developmental Lifecycle Documentation Validation
March 8th – 12th, 2010, Scottsdale, Arizona

Regulatory Audit Activities and Assignments

Pre-Trip Activities

Team members located at headquarters will review docketed documentation related to the CIM System and DAS and their discussion of programs and other oversight guidelines to determine if sufficient information exists to warrant an audit team visit to the Scottsdale, Arizona facility.

Trip Activities

1. Evaluate provided documentation to determine if sufficient information exists to consider the Design Requirements phase, or Phase 1 (Planning Activities phase per BTP 7-14) and/or System Design (Requirements Activities per BTP7-14) of the AP1000 design process complete as the process relates to the CIM.

   1a. Verify adequate information exists in documentation describing the developmental lifecycle for the CIM System. Information provided should be of the same quality and detail to be considered consistent with the guidance of BTP 7-14, NUREG/CR 6101 and commitments made in the Common Q Software Program Manual (SPM) and WCAP-15927, "Design Process for the AP1000 Common Q Safety Systems", Revision 2 (both of which are Tier 2* documents).
   (Planning Activities/Requirements Phases)
   (Zhao)

   1b. Evaluate the acceptability of the requirements specifications and quality standards related to the development of the CIM System, including the 10 CFR 50 Appendix B requirements and their application within the CSI design and independent verification and validation (IV&V) programs, organizations, and processes based upon the commitments made within the Common Q SPM, WCAP-15927 Revision 2, (both are Tier 2* documents) and the guidance within IEEE Standard 1012.
   (Requirements Activities)
   (Zhao)

   1c. Evaluate computer security attributes of the CIM System to determine if the system meets the requirements of IEEE Standard 603-1991, Clause 5.9 – Access Control to prevent inadvertent operator action that could cause the system to operate outside its design parameters.
   (Planning Activities/Requirements Phases)
   (Zhao)

   1d. Utilizing the Requirements Traceability Matrix (RTM) of the PMS provided by WEC, trace several of the CIM functional requirements or design specifications of the device from the function design requirements back to requirements of 10 CFR 50 Appendix A General Design Criteria (GDC) [specifically GDCs 21-24] and 10 CFR 50.55a(h) which incorporates IEEE Standard 603-1991. The RTM is expected to provide guidance explaining the device's traceability to the higher level AP1000 I&C Architecture documents, and finally to the regulatory requirements.
   (Requirements Phase)
   (Zhao)

2. Evaluate provided documentation to determine if sufficient information exists to consider the Design Requirements phase and/or System Design phases of the AP1000 design process as related to the DAS as satisfactorily complete.

   2a. Evaluate CSI documentation to determine if additional information beyond that contained in the DAS Setpoint Methodology white paper may be obtained related to the DAS Setpoint Methodology and the basis for the setpoints to be chosen for the DAS.
   (Planning Requirements)
   (Mott)

   2b. Conduct a diversity evaluation to determine if sufficient diversity exists between the DAS and other AP1000 I&C Systems, especially the PMS. Utilize the AP1000 I&C Defense-in-Depth and Diversity Report, the CIM Technical Report and AP1000 DAS System Planning and Functional Design Summary Technical Reports and their referenced documents as reference material. The evaluation should utilize 10 CFR 50 Appendix A, GDCs 22 and 24 and the guidance of NUREG/CR 6303 as references.
   (Diversity Analysis)
   (Mott)

   2c. Examine documentation related to the DAS to verify the requirements of 10 CFR 50.62 and 10 CFR 50 Appendix A, GDC 1 are being met and the guidance of NUREG- 0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants" Branch Technical Position 7-19 continues to be satisfied.
   (Requirements Analysis)
   (Mott)

3. Programmatic Review: The staff expects to conduct a review of CSI's programs tied to nuclear safety.

   3a. A review of CSI's IV&V and Testing Program will be conducted. The staff's evaluation will be based upon the requirements of 10 CFR 50 Appendix B, Criterion III, Design Control and Criterion XI Test Control. The guidance of IEEE Standard 1012, "IEEE Standard for Software Verification and Validation" and the commitments made in the Common Q SPM and WCAP-15927 documents will also be utilized.
   (Planning Activities/Requirements Phases)
   (Roggenbrodt)

   3b. A review of CSI's design and document control and change processes will be conducted based upon the requirements of 10 CFR 50 Appendix B, Criterion III, Design Control and Criterion VI, Document Control.
   (Planning Activities/Requirements Phases)
   (Roggenbrodt)

   3c. A review of CSI's training and records management program will be conducted based upon 10 CFR 50 Appendix B, Criterion III, Design Control. The commitments made in the Common Q SPM and WCAP-15927 will also be utilized.
   (Planning Activities/Requirements Phases)
   (Roggenbrodt)

4. Evaluations, Meetings, and Tours: The staff expects to interface with CSI/Westinghouse personnel via meetings and review activities during the audit period including a tour of the CSI facility.

4a. Evaluations: The staff expects the CSI/Westinghouse subject matter experts to be available to discuss any issues or clarifications that may require explanation during the staff's review of the documentation presented.

4b. Entrance/Exit Meetings: The staff expects the entrance meeting to be held on Monday, March 8, 2010, and the exit meeting on or about March 12, 2010.

4c. Daily Update Meetings: At CSI/Westinghouse's request the staff will conduct daily update meetings typically held at the end of the day to discuss any potential issues discovered during the day's audit activities.

4d. CSI Facility Tour: The CSI tour should incorporate a tour of the manufacturing lines constructing the CIM System and the DAS.

Attachment 1: Audit Documentation Requested for Review or Reference for the CSI Audit
March 8-12, 2010

NO.	WESTINGHOUSE DOC. ID	APPLIES TO	DOCUMENT / DRAWING TITLE
W1	WCAP-16096-NP-A (Revision 1A)	I&C System	Software Program Manual for Common Q Systems
W2	WCAP-15927 (Revision 2)	PMS	Design Process for AP1000 Common Q Safety Systems
W3	WCAP-15775	I&C System	AP1000 I&C Defense in Depth and Diversity Report
W4	WCAP- 13383 (Revision 1)	I&C System	AP600 I&C Hardware and Software Design, V&V Process Report
W5	WCAP-17179-P	PMS	AP1000 Component Interface Module Technical Report
W6	WCAP-17184-P	I&C System	AP1000 DAS Planning and Functional Design Summary Technical Report
W7	WCAP-16674-P	PMS	I&C Data Communications and Manual Control for Safety System Components
W8	WCAP-16675-P	PMS	PMS Architecture Report
W9	WNA-PV-00009-GEN (All Revisions)	PMS	Verification & Validation Process for the Common Q Safety Systems
W10	WNA-PT-00058-GEN	PMS	Testing Process for Common Q Systems
W11	WNA-VR-00213-GEN	PMS	AP1000 PMS Project Concept Phase V&V Summary Report
W12	APP-PMS-JO-001	PMS	AP1000 PMS Architecture 1 Line Diagram
W13	APP-PMS-JO-002	PMS	AP1000 PMS Architecture Division A
W14	APP-PMS-JO-003	PMS	AP1000 PMS Architecture Division B
W15	APP-PMS-JO-004	PMS	AP1000 PMS Architecture Division C
W16	APP-PMS-JO-005	PMS	AP1000 PMS Architecture Division D
W17	APP-PMS-J4-020	PMS	AP1000 System Design Specification for the Protection and Safety Monitoring System
W18	AP 1000 DCD (Revisions 15-17)	AP1000	AP1000 Design Control Document Tier 1 Chapter 2 and Tier 2 Chapter 7
W19	Requirements Traceability Matrix	AP1000	RTM describes Functional Requirements traceable back to Regulations

(continued on next page)

Regulatory Audit Plan CS Innovations PMS Software Lifecycle and DAS Developmental Lifecycle Documentation Validation March 8th – 12th, 2010, Scottsdale, Arizona

Attachment 1: Audit Documentation Requested for Review or Reference for the CSI Audit March 8-12, 2010 (cont.)

NO.	REFERENCE DOC. ID	APPLIES TO	DOCUMENT / DRAWING TITLE
R1	Code of Federal Regulation		Chapter 10 Energy – Parts 1-199
R2	NUREG 0800	Light Water Reactors	Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants
R3	NUREG 1793	AP1000	Final Safety Evaluation Report Related to Certification of the AP1000 Standard Plant Design
R4	NUREG/CR 6101		Software Reliability and Safety in Nuclear Reactor Protective Systems
R5	NUREG/CR 6303		Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems
R6	Regulatory Guide 1.168		Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
R7	Regulatory Guide 1.169		Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
R8	Regulatory Guide 1.170		Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
R9	Regulatory Guide 1.171		Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
R10	Regulatory Guide 1.172		Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
R11	Regulatory Guide 1.173		Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
R11	IEEE Standard 384		IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits -Description
R12	IEEE Standard 603		IEEE Std Criteria for Safety Systems for Nuclear Power Generating Stations
R13	IEEE Standard 1012		IEEE Std 1012-2004 Standard for Software Verification and Validation
R14	IEEE Standard 1074		IEEE Standard for Developing Software Life Cycle Processes