

December 28, 2010

Redacted Version of the non-concurrence package – (a) Insufficient Diversity and Independence in the Implementation Process for AP1000 Instrumentation and Controls Systems; (b) Response to Non-Concurrence Submitted by William Roggenbrodt.

Redactions are based upon staff acceptance of Westinghouse request for withholding of proprietary information, submitted in a December 20, 2010 letter to NRC (ML103570064).

NON-CONCURRENCE PROCESS

SECTION A - TO BE COMPLETED BY NON-CONCURRING INDIVIDUAL

TITLE OF DOCUMENT SEE BELOW	ADAMS ACCESSION NO. ML103420563
DOCUMENT SPONSOR TERRY JACKSON	SPONSOR PHONE NO. 301-415-7313
NAME OF NON-CONCURRING INDIVIDUAL WILLIAM ROGGENBRODT	PHONE NO. 301-415-0678

DOCUMENT AUTHOR DOCUMENT CONTRIBUTOR DOCUMENT REVIEWER ON CONCURRENCE

TITLE ELECTRICAL ENGINEER - DIGITAL I&C	ORGANIZATION NRO/DE/ICE1
---	------------------------------------

REASONS FOR NON-CONCURRENCE

TITLE OF DOCUMENT:
ADVANCED FINAL SAFETY EVALUATION REPORT FOR THE AP1000 STANDARD DESIGN CERTIFICATION AMENDMENT - CHAPTER 7, "INSTRUMENTATION AND CONTROL"

REASON FOR NON-CONCURRENCE:
SEE ATTACHMENT 1

CONTINUED IN SECTION D

SIGNATURE 	DATE 12/16/2010
--	---------------------------

SUBMIT FORM TO DOCUMENT SPONSOR AND COPY TO YOUR IMMEDIATE SUPERVISOR AND DIFFERING VIEWS PROGRAM MANAGER

NON-CONCURRENCE PROCESS

TITLE OF DOCUMENT SEE BELOW	ADAMS ACCESSION NO. ML103420563
---------------------------------------	---

**SECTION B - TO BE COMPLETED BY NON-CONCURRING INDIVIDUAL'S SUPERVISOR
(THIS SECTION SHOULD ONLY BE COMPLETED IF SUPERVISOR IS DIFFERENT THAN DOCUMENT SPONSOR.)**

NAME
TERRY W. JACKSON

TITLE CHIEF, INSTRUMENTATION, CONTROLS, AND ELECTRICAL ENGINEERING BRANCH 1	PHONE NO. 301-415-7313
---	----------------------------------

ORGANIZATION
NRO/DE/ICE1

COMMENTS FOR THE DOCUMENT SPONSOR TO CONSIDER

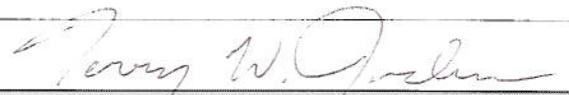
I HAVE NO COMMENTS

I HAVE THE FOLLOWING COMMENTS

**TITLE OF DOCUMENT:
ADVANCED FINAL SAFETY EVALUATION REPORT FOR THE AP1000 STANDARD DESIGN CERTIFICATION
AMENDMENT - CHAPTER 7, "INSTRUMENTATION AND CONTROL"**

SEE ATTACHMENT 2 FOR RESPONSE AND ACTIONS TO ADDRESS NON-CONCURRENCE.

CONTINUED IN SECTION D

SIGNATURE 	DATE 12/16/2010
--	---------------------------

SUBMIT THIS PAGE TO DOCUMENT SPONSOR

NON-CONCURRENCE PROCESS

TITLE OF DOCUMENT SEE BELOW		ADAMS ACCESSION NO. ML103420563
SECTION C - TO BE COMPLETED BY DOCUMENT SPONSOR		
NAME THOMAS BERGMAN		
TITLE DIVISION DIRECTOR		PHONE NO. 301-415-7192
ORGANIZATION NRO/DE		

ACTIONS TAKEN TO ADDRESS NON-CONCURRENCE (This section should be revised, as necessary, to reflect the final outcome of the non-concurrence process, including a complete discussion of how individual concerns were addressed.)

The non-concurrence was withdrawn prior to conclusion of the non-concurrence process. I agree with Messrs. Roggenbrodt and Jackson that the concerns raised by Mr. Roggenbrodt are properly addressed through a vendor inspection. I have confirmed with the Division of Construction Inspection and Oversight Programs that an inspection of CS Innovations is expected to occur in early calendar year 2011 and that two staff from the Division of Engineering will participate on the inspection team, consistent with the recommendations in Sections A and B of this non-concurrence.

I thank Mr. Roggenbrodt for raising his concerns to management and for using the non-concurrence process.

CONTINUED IN SECTION D

SIGNATURE - DOCUMENT SPONSOR 	DATE 12/16/10	SIGNATURE - DOCUMENT SIGNER 	DATE 12/16/2010
--	-------------------------	---	---------------------------

NON-CONCURRING INDIVIDUAL (To be completed by document sponsor when process is complete, i.e., after document is signed):

- | | |
|--|---|
| <input type="checkbox"/> CONCURS | <input checked="" type="checkbox"/> WANTS NCP FORM PUBLIC |
| <input type="checkbox"/> NON-CONCURS | <input type="checkbox"/> WANTS NCP FORM NON-PUBLIC |
| <input checked="" type="checkbox"/> WITHDRAWS NON-CONCURRENCE (i.e., discontinues process) | |

December 28, 2010

Attachment 1

Redacted Version of Insufficient Diversity and Independence in the
Implementation Process for AP1000 Instrumentation and Controls Systems

Insufficient Diversity and Independence in the Implementation Process for AP1000 Instrumentation and Controls Systems

Introduction

Based upon the text contained within two secondary references to Chapter 7 of the AP1000 Design Control Document (DCD), "Instrumentation and Controls," Westinghouse (WEC) describes and believes the text explains that a sufficient level of diversity exists between the two instrumentation and controls (I&C) systems able to implement automatic and manual reactor trip and engineered safety features (ESF) functions. The safety-related Protection and Safety Monitoring System (PMS) and the important-to-safety Diverse Actuation System (DAS) are the two I&C systems that are under discussion to determine if a sufficient level of diversity and independence exist between the two systems.

The Component Interface Module Technical Report, WCAP-17179-P discusses diversity between the two I&C systems in Section 2.11, *Diversity*, and the AP1000 Diverse Actuation System Planning and Functional Design Summary Report, WCAP-17184-P, discusses diversity in Section 9, *NUREG/CR 6303 Compliance and Diversity Implementation*. Refer to Attachments A and B respectively.

The component interface module (CIM) subsystem serves as the priority module within the PMS and replaces the loop controllers that serve a safety-related component control function as described in the Common Q Topical Report, WCAP 16097-P-A. The qualification and need for diversity between the loop controllers from the Common Q system was described in the Common Q Topical Report as generic open item 7.8.

The CIM subsystem utilizes a programmable logic-based device known as a field programmable gate array (FPGA) for both the CIM itself and the safety remote node controller (SRNC) that receives inputs from the [Common Q portion of the PMS. The CIM and SRNC are the major FPGA-based components of the CIM subsystem]. The CIMs are capable of being controlled from either the non-safety-related Plant Control System (PLS) or the PMS.

Beginning in Revision 16 of the AP1000 DCD Westinghouse chose to amend its certified design by utilizing a field programmable gate array (FPGA) as the logic-based device for its DAS. This decision raised the issue of diversity between the CIM subsystem portion of the PMS and the DAS as WEC explained that both the CIM and DAS would be developed by CS Innovations of Scottsdale, AZ, now a small subsidiary of WEC.

Chapter 7 of the AP1000 Advance Final Safety Evaluation Report (AFSER) determined that sufficient diversity exists in the AP1000 I&C systems, specifically between the safety-related PMS and the important-to-safety DAS based upon the information supplied in Attachments A and B and via a response from WEC deemed acceptable by the staff reviewer related to the issue. Refer to Attachment C for the AFSER finding related to I&C system diversity.

Chapter 7 of the AP1000 AFSER also determined that, via the documentation supplied in the AP1000 DCD and other secondary references, that a sufficient level of independence for the CIM, CIM testing and DAS development processes had been adequately demonstrated.

Issues Under Discussion

However, beyond the written licensing commitments in the text of the AP1000 DCD, which have been deemed acceptable by the staff, it is the implementation of the regulations and associated guidance via Westinghouse commitments that are in question. CS Innovations (CSI) the CIM and DAS supplier, unsuccessfully demonstrates several requirements of 10 CFR 50 Appendix B, *Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants*, along with 10 CFR 50 Appendix A, General Design Criteria (GDC) 22, *Protection System Independence*.

Of particular concern are the issues listed below:

- Demonstration that a sufficient level of diversity exists between the PMS and the DAS, in accordance with 10 CFR 50, Appendix A, GDC 22, *Protection System Independence*
- Demonstration that an effective and independent QA organization has been created and implemented at CS Innovations in accordance with 10 CFR 50 Appendix B, Criterion I, *Organization*
- Demonstration that the CIM Development Process is being conducted in accordance with 10 CFR 50 Appendix B, Criterion III, *Design Control*
- Demonstration that an adequate inspection program and commercial grade dedication process exists for materials received from subcontractors in accordance with 10 CFR 50 Appendix B, Criterion IV, *Procurement Document Control* and Criterion VII, *Control of Purchased Material, Equipment and Services*
- Demonstration of adequate independent verification and validation (IV&V) testing program or process in accordance with 10 CFR 50 Appendix B, Criterion XI, *Test Control*

Relevant Regulations

10 CFR 50 Appendix A, GDC 22, requires, in part that, "*Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical...*" Based upon the observations made and conclusions drawn in the March and April 2010 audit reports a lack of evidence was located that demonstrates an adequate level of diversity exists between the CIM and DAS development teams.

10 CFR 50 Appendix B, Criterion I, *Organization* requires in part that, "*The persons and organizations performing quality assurance functions shall have sufficient authority and organizational freedom to identify quality problems... There persons and organizations performing quality assurance functions shall report to a management level so that the required authority and organizational freedom, including sufficient independence from cost and schedule when opposed to safety considerations, are provided.*" Based upon the observations made and conclusions drawn in the March and April 2010 audit reports a lack of evidence was located to demonstrate that sufficient independence exists within the QA program at CS Innovations related to the CIM development process.

10 CFR 50 Appendix B, Criterion III, *Design Control* requires in part that, “*The verifying or checking process shall be performed by individuals or groups other than those who performed the original design, but who may be from the same organization.*”

In this case, the text offered in Appendix B, Design Criterion III refers only to safety-related systems, however once that requirement is combined with the independence requirement of the protection system that contains a provision for diversity, the separation between those who design the safety-related system and those who review and test the safety system independently IV&V team, must be different than those who design and test the control systems, especially the control system that is credited with I&C system diversity. Additionally, given the commitments stated in the AP1000 CIM Technical Report (Attachment A) and the Diverse Actuation System Planning and Functional Design Summary Report, (Attachment B) related to human diversity and the conclusions drawn in the March 2010 CS Innovations audit and the April 2010, Westinghouse audit, no evidence can be offered to support the claim of adequate human diversity when applied to the CIM and DAS development processes. Furthermore, the conclusion drawn related to the assignment of one individual serving as both the QA Manager and the Configuration Manager for the CIM-SRNC development project casts serious doubt on the organization’s ability to ensure an independent QA program has been implemented at CSI.

10 CFR 50 Appendix B, Criterion IV, *Procurement Document Control*, requires that, “*Measures shall be established to assure that applicable regulatory requirements, design bases, and other requirements which are necessary to assure adequate quality are suitably included or referenced in the documents for procurement of material, equipment, and services, whether purchased by the applicant or by its contractors or subcontractors. To the extent necessary, procurement documents shall require contractors or subcontractors to provide a quality assurance program consistent with the pertinent provisions of this appendix.*”

In addition, 10 CFR 50 Appendix B, Criterion VII, *Control of Purchased Material*, requires, in part, that, “*Measures shall be established to assure that purchased material, equipment, and services, whether purchased directly or through contractors and subcontractors, conform to the procurement documents. These measures shall include provisions, as appropriate, for source evaluation and selection, objective evidence of quality furnished by the contractor or subcontractor, inspection at the contractor or subcontractor source, and examination of products upon delivery... This documentary evidence shall be retained... and shall be sufficient to identify the specific requirements, such as codes, standards, or specifications, met by the purchased material and equipment. The effectiveness of the control of quality by contractors and subcontractors shall be assessed by the applicant or designee at intervals consistent with the importance, complexity, and quantity of the product or services.*”

With regard to 10 CFR 50 Appendix B, Criteria IV and VII it can be demonstrated that CS Innovations is using a subcontractor to provide printed circuit boards for the CIM subsystem with no documentation of the vendor’s adherence to a 10 CFR 50 Appendix B Program and no commercial dedication process for components that are procured external to the system developer [CSI] that will be utilized as a part of a safety-related protection system.

Additionally, 10 CFR 50 Appendix B, Criterion XI, *Test Control*, requires, in part, that, “A test program shall be established to assure that all testing required to demonstrate that structures, systems, and components will perform satisfactorily in service is identified and performed in accordance with written test procedures which incorporate the requirements and acceptance limits contained in applicable design documents.” Based upon the observations made and conclusions drawn in the March and April 2010 audit reports a lack of evidence to demonstrate any IV&V program had been adequately created or implemented at CSI could be located.

Evidentiary Basis

The foundation for the above statements concerning non-compliance with AP1000 I&C system diversity is based upon two criteria, the first is information discovered during two audits, one conducted at CS Innovations (CSI) in Scottsdale, AZ (a subsidiary of Westinghouse) and an April 2010 audit conducted at Westinghouse in Warrendale, PA. While realizing that an audit is not an activity conducted against a license, CSI is an approved 10 CFR 50 Appendix B vendor and a demonstration of various inadequacies of their policies, programs, and procedures and adherence to them must be appropriately addressed.

The second basis for the determination that an insufficient level of diversity between the AP1000 I&C systems, resides in an evaluation of the guidance of NUREG/CR 6303, Method of Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems.

The basis for the determination that a lack of evidence, pertaining to the independence of the CIM development process and CSI QA program can be located in the conclusions drawn in the two audit reports.

The March 2010 CSI audit conducted at CS Innovations (ADAMS ML101410395), in part, contained the following observations and conclusions as listed in Section 5 and Section 6 of the audit report respectively:

Relevant March 2010 Audit Observations

CSI-OBS1. 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.

CSI-OBS2. 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.

CSI-OBS3. 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-OBS4. 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.

CSI-OBS5. 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.

Relevant March 2010 Audit Conclusions

CSI-CON1. 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.

CSI-CON2. 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.

Based upon the observations cited and conclusions drawn during the March 2010 audit the audit team determined a lack of roles and responsibilities for both design and test personnel for both the safety-related CIM and the important-to-safety DAS exist at CSI, thereby potentially affecting the independence of both the CIM and DAS development processes. This is of particular concern as several members of the CSI technical staff developed both the Advanced Logic System, the system upon which the DAS is based, and the CIM subsystem. This casts serious doubt in relation to how a claim of adequate human diversity can be substantiated, especially that given the roles of designer(s), design verifier, independent tester must be fulfilled and a similar but separate team of individuals must be created for the important-to-safety DAS. There was no demonstration that a sufficient number of technical and managerial team members who would oversee the design, IV&V and Quality Assurance (QA) programs for both programs, the CIM and DAS development teams, were present during either system's development process. Related to the IV&V process the audit team members were directed to understand that several of the concerns related to "unanswered questions" related to diversity between the PMS and DAS and PMS IV&V process would be answered at the following month's Warrendale, PA audit, held at CSI's parent company, Westinghouse.

Additionally, during the March audit, the audit team recognized that the QA Manager for the CIM-SRNC Project also served as the Configuration Manager for the CIM-SRNC project. This issue was identified as a potential non-compliance with the independence requirements associated with an approved QA program.

In addition, although CSI utilized a subcontractor to supply the PCB for the CIM-SRNC system, there was no commercial dedication process in place nor had there been any measures taken, including audits or receipt inspections, to ensure that the supplied material met any and all procurement requirements.

The April 2010 WEC audit at the WEC Automation Services facility in Warrendale, PA (ADAMS ML101380259), in part, contained the following observations and conclusions as listed in Section 5 and Section 7 of the audit report respectively:

Relevant April 2010 Audit Observation

WEC-OBS1. Westinghouse did not provide documentation or a technical report to demonstrate the establishment of a DAS setpoint methodology. **Specifically, Westinghouse has not provided an adequate methodology or design requirement to show the DAS automatic and manual actuations are sufficient and adequate to meet the diversity requirements** of 10 CFR Part 50, Appendix A, GDC 22, and address the diversity and defense-in-depth (D3) guidance in SECY-93-087. The lack of formal DAS setpoint methodology would prevent closure of DAS ITAAC related to the DAS Design Requirements phase of DAS development.

Relevant April 2010 Audit Conclusion

WEC-CON1. As no additional relevant planning, development, or design information related to the CIM developmental lifecycle or the third party IV&V process review being conducted by CSI or Westinghouse was offered to the audit team beyond that reviewed at the March 2010 CSI audit, the conclusions developed in the March 2010, audit relating to the CIM, which is an integral portion of the PMS remain

Based upon the observations and conclusions drawn in the April 2010 audit, no additional information other than those provided in the March 2010 CSI audit related to the demonstration of adequate diversity and independence between the CIM, the CIM's IV&V process and the DAS were offered by WEC during or after the April 2010 audit.

However, it should be noted that the issues related to the demonstration of an adequate DAS setpoint methodology have been resolved. Additionally, as the staff determined that additional detailed design submissions were required prior to concluding the CIM Development Process was conducted in a high quality fashion, WEC chose to add an Inspection, Test, Analyses and Acceptance Criteria (ITAAC), to Tier 1, Chapter 2, Section 2.5.2, Table 2.5.2-8, ITAAC, that ensures the staff will conduct the necessary engineering review of the planned and implemented CIM Development Process, prior to its acceptance by the staff. The staff found the addition of the ITAAC, which will be treated as Design Acceptance Criteria, acceptable.

NUREG/CR 6303 Conformance

In Section 9 of the AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report, WCAP-17184-P, WEC discussed its compliance with NUREG/CR 6303. That Section is included in the report as Attachment B.

While NUREG 6303 is a guidance document, rather than a document containing regulatory requirements, an analysis of its content provides a useful tool in assisting the reviewer in reaching a determination as to whether or not a case can be made that sufficient diversity exists (or does not exist) between the two systems.

From Section 3.2. of NUREG/CR 6303 Guideline 2 – Determining Diversity

For purposes of this guideline and convenience in assessment, diversity will be assumed to be separable into six attributes, listed in alphabetical order:

- Design diversity
- Equipment diversity
- Functional diversity
- Human diversity
- Signal diversity
- Software diversity

3.2.1. Design Diversity

Factors increasing diversity between two designs meeting the same requirements—excluding the effects of human diversity—are listed here **in decreasing order of effect**.

- Different technologies (e.g., analog versus digital)
- Different approaches within a technology (e.g., transformer-coupled AC instrumentation versus DC coupled instrumentation)
- Different architecture (i.e., arrangement and connection of components)

When CIM-DAS diversity is compared to design diversity guidance, [

], minimizes any appreciable amount of design diversity applied to the two I&C systems. The designers are expected to utilize the same approach in the application of a given technology, however it is expected that different architecture be utilized for the two systems.

3.2.2. Equipment Diversity

Factors increasing equipment diversity between two groups or items of equipment are listed here **in decreasing order of effect**:

- Different manufacturers of fundamentally different designs
- Same manufacturer of fundamentally different designs
- Different manufacturers making the same design
- Different versions of the same design

Again, when CIM-DAS diversity is compared to equipment diversity guidance, the use of [

], utilizing highly similar designs it would be extremely difficult to develop a reasonable case for demonstrating that sufficient equipment diversity exists between the two systems.

3.2.3. Functional Diversity

Factors increasing functional diversity between two independent subsystems are listed here **in decreasing order of effect**:

- Different underlying mechanism (e.g., gravity convection versus pumped flow, rod insertion versus boron poisoning).

- Different purpose, function (e.g., normal rod control versus reactor trip rod insertion), control logic, or actuation means.
- Different response time scale (e.g., a secondary system may react if accident conditions persist for a time).

When CIM-DAS diversity is compared to functional diversity guidance, a case can be made both for and against the claim of sufficient functional diversity between the two systems. The use of the logic-based FPGAs to provide safety-related component control in both systems lends itself to the position that an insufficient level of functional diversity exists between the two systems. However, given that one device receives its input from a singular component control distribution device (the Integrated Logic Processor of the PMS) and the other receives its input from sensors and performs a logic or decision-based function a case can be made demonstrating that CIM-DAS diversity may be acceptable, however, that system characteristic may be more attributable or resemble signal, rather than functional diversity. The net result of these two cases results, at best, in a neutral finding for the case of sufficient CIM-DAS functional diversity.

3.2.4. Human Diversity

Factors increasing the human diversity of a design ***in decreasing order of effect are:***

- Different design organization (i.e., company).
- Different engineering management team within the same company.
- Different designers, engineers, or programmers.
- Different testers, installers, or certification personnel

Based upon the observations made and conclusions drawn during the March 2010 CSI audit, no acceptable level of human diversity was made in relation to a sufficient level of diversity between the CIM and DAS. To reiterate, WEC chose to utilize the same company with a singular design organization and possessed no organization to conduct IV&V processes. Additionally, the parent organization, WEC, provided no demonstration of how the CIM or DAS will be tested at the elemental, module, channel and other higher level tests to verify proper operation at each stage of module, (whether that be the CIM, SRNC or DAS) development as is the case for the Common Q portion of the PMS.

3.2.5. Signal Diversity

Factors increasing signal diversity between two signal sources are listed here ***in decreasing order of effect:***

- Different reactor or process parameters sensed by different physical effects (e.g., pressure or neutron flux).

- Different reactor or process parameters sensed by the same physical effect (e.g., pressure versus water level or flow sensed by differential pressure sensors).
- The same reactor or process parameter sensed by a different redundant set of similar sensors (e.g., a set of four redundant water level sensors backed up by an additional set of four redundant water level sensors driving a diverse design of protective equipment).

A case can be made supporting signal diversity for the two I&C systems since the CIM subsystem performs a priority function from the PLS or PMS to control safety-related components whereas the DAS receives and processes sensor inputs, performs logic functions and then, if necessary, conducts command and control features over safety-related components. Due to this level of “difference” of signal path, it is reasonable to conclude the level of diversity between the CIM-DAS is acceptable.

3.2.6. Software Diversity

Factors increasing diversity between software designs meeting the same requirements, excluding the effects of human diversity, are listed here in decreasing order of effect:

- Different algorithms, logic, and program architecture
- Different timing, order of execution
- Different operating system
- Different computer language

Based upon the factors considered when compared to Section 3.2.6, a case can be made for adequate software diversity, based on WEC’s continuing commitment in Revision 18 to utilize different algorithms, logic, program architecture, executable operating system, and executable software/logic.

Conclusion

Based upon the lack of documentation provided to the staff and the observations made and conclusions drawn in the March and April 2010 audit reports by the audit team, there exists a great deal of uncertainty when discussing CSI’s ability to produce two critical AP1000 I&C systems that satisfy all applicable diversity, independence, programmatic and other requirements of 10 CFR Part 50 Appendices A and B. Additionally, when taken as a whole, it is considered highly unlikely that a relatively new and small company with extremely limited experience in the development and construction of safety-related I&C systems that purchased highly similar devices utilizing the same technology from the same manufacturer while also utilizing its project driven, versus process driven culture is still able to appropriately satisfy all regulatory requirements without additional scrutiny appears improbable. Additionally, based upon the audit team’s determination that several members of the same design team developed both the safety-related CIM subsystem and the ALS (Advanced Logic System) that is the

blueprint for the DAS, provides a strong case for the likelihood that the critical I&C systems for the AP1000 were developed with insufficient diversity metrics applied to each.

Further beyond the results of the two audits, and several follow-up meetings held in the WEC office in Rockville, MD no responses were offered, by either WEC or CSI, that precluded the conclusion that only two of six diversity attributes as delineated in Section 3 of NUREG/CR 6303 can be easily substantiated as acceptable, nor that the independence requirements for the CIM development process can be met.

Recommendations

Based upon the large amount of discrepancies that exist between the written language of the AP1000 DCD and its secondary references and the "as built" field-based implementation of undefined personnel roles and responsibilities and equipment resources as it relates to I&C system diversity at CSI, the most conservative course of action would be to postpone issuance of Chapter 7 of the AP1000 AFSER until such time as it can be demonstrated that CSI, or another equipment or system supplier, has the ability to implement and apply a sufficient level of independence and diversity commensurate with the amount of differentiation required for a safety-related and important-to-safety I&C system.

A more liberal approach would encompass contacting the Office of New Reactors Quality and Vendor Branch (CVQA) in writing and offer the conclusions drawn in the two audits as it relates to CSI's status as an approved 10 CFR 50 Appendix B supplier. The CVQA staff would rely on CSI's ability to institute an acceptable independence and diversity program for the two I&C systems. CVQA would then schedule an inspection at a time convenient to both organizations.

However, given the all the scheduling constraints placed upon the regulator and the applicant, a more prudent and balanced approach would be to allow the AP1000 AFSER for Chapter 7 to be issued, unhampered by this non-concurrence, and have a team from the Division of Engineering's CQVA and Instrumentation Controls and Electrical Engineering Branch One (ICE1) conduct an inspection in the near future (two to three months) at CS Innovations in Scottsdale, AZ in a stand-alone format allowing primarily the CSI organization, along with WEC assistance, to demonstrate the improvements it has undertaken and implemented based upon the conclusions drawn in the March and April 2010 audits. To ensure team and issue continuity, it is suggested that at least two of the three participants from the ICE1 March 2010 audit be available to serve on the forthcoming inspection team.

ATTACHMENT A (Page 1 of 2)

Section 2.11 Diversity – from Component interface Module Technical Report WCAP-17179-P
Revision 1 – May 2010

2.11 DIVERSITY

[

]

2.11.1 Design Diversity

Design diversity is the use of different methods to solve similar problems. [

]

2.11.2 Equipment Diversity

Equipment diversity is the use of different hardware to perform similar safety functions. [

]

ATTACHMENT A (Page 2 of 2)

Section 2.11 Diversity – from Component interface Module Technical Report WCAP-17179-P
Revision 1 – May 2010

2.11.3 Functional Diversity

Two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects. [

]

2.11.4 Human Diversity

The purpose of human diversity is to reduce the chance of common errors in similar designs. [

]

2.11.5 Signal Diversity

Signal diversity is the use of different sensed parameters to initiate protective action. [

]

2.11.6 Software Diversity

Software diversity is the use of different programming or algorithms to perform the same or similar functions. [

]

2.11.7 Diversity Summary

All of the elements must be evaluated to determine if adequate diversity is provided. [

]

ATTACHMENT B (Page 1 of 2)

Section 9 NUREG/CR 6303 Compliance and Diversity Implementation –
from AP1000 Diverse Actuation System Planning and Functional Design Summary Report
WCAP-17184-P, Revision 2 – June 2010

**9 NUREG/CR 6303 COMPLIANCE AND DIVERSITY
IMPLEMENTATION**

NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection System” (Reference 12) provides a method for analyzing computer-based nuclear reactor protection systems that discovers and identifies vulnerabilities to common-mode failure. []

9.1 []
[]

9.2 []
[]

9.3 []
[]

]

ATTACHMENT B (Page 2 of 2)

Section 9 NUREG/CR 6303 Compliance and Diversity Implementation –
from AP1000 Diverse Actuation System Planning and Functional Design Summary Report
WCAP-17184-P, Revision 2 – June 2010

[

]

9.4 []

The design, verification, and validation programs for I&C systems, [

] and
the DAS Design Process (Reference 15), require and specify the use of independent review. It is a
requirement of the DAS that different people (personnel not assigned to safety system engineering) will
be responsible for its design and fabrication.

[

]

9.5 []

[

]

9.6 []

[

]

Software diversity between the DAS and PMS will be achieved through the use of different algorithms,
logic, program architecture, executable operating system and executable software/logic.

ATTACHMENT C (Page 1 of 2)

AP1000 Advance Final Safety Evaluation Report, Chapter 7 Section 7.8.2 - Diverse Actuation System Assessment (pg 7-54-55)

In AP1000 DCD, Revision 17, the applicant changed the microprocessor-based implementation of the DAS to be a special purpose logic processor-based system. This special purpose logic processor-based DAS is further described as a Field Programmable Gate Array (FPGA) digital platform-based system in technical report WCAP 17184-P. The applicant also made changes to use the FPGA technology for the Component Interface Module (CIM) in the safety-related PMS in WCAP 17179-P, "AP1000 Component Interface Module Technical Report" and APP-GW-GLR-071 (WCAP 16775-P), "AP1000 Protection and Safety Monitoring System Architectural Technical Report." According to the above reports, the CIM and DAS systems will be designed and manufactured by the same company at a common design and manufacturing facility. 10 CFR Part 50, Appendix A, GDC 22, "Protection System Independence," requires, among other things, that design techniques such as functional diversity or diversity in component design and principles of operation shall be used to the extent practical to prevent loss of the protection function. BTP 7-19 provides guidance for evaluating an applicant's D3 assessment to ensure conformance with the NRC position on D3 for digital I&C systems. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" provides diversity analysis methods and strategies to demonstrate that adequate and sufficient diversity should be included within the design. The staff found that the applicant did not provide design descriptions that can demonstrate adequate and sufficient diversity between the DAS and CIM systems in accordance with the guidance listed above. Hence, the staff issued RAI-SRP-7.8-DAS-04 requesting the applicant to describe in detail how the DAS equipment (i.e., hardware, software) will be diverse from the safety-related CIM in PMS. The staff also issued another RAI-SRP-7.8-DAS-05 requiring the applicant to identify the criteria, practices, and processes that will ensure adequate diversity in the development of the CIM and the DAS at the common design and manufacturing facility, including the diversity with respect to human, software, and equipment diversity.

In response to the above RAIs, the applicant states, in part, that diversity is a principle in instrumentation of sensing different variables, using different technology, using different logic or algorithm, or using different actuation means to provide different ways of responding to postulated plant conditions. The applicant also revised WCAP 15775, the AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report, to Revision 4 to address the specific requirement of diversity between CIM and DAS. The applicant demonstrated in Section 2.11 of Technical Report WCAP 17179-P, draft Revision 2, and Section 9 of Technical Report WCAP 17184-P, draft Revision 2, how the requirements of diversity are met between CIM and DAS. For example, for the human diversity, the applicant states in the two technical reports that different designers are used for the CIM and DAS designs. In addition, the different design teams and different test teams will be used to test the CIM and DAS designs. In order to achieve the software diversity between the DAS and PMS (i.e. CIM), the applicant will use different algorithms, logic, program architecture, executable operating system and executable software/logic. The staff concludes that the applicant has provided sufficient information

ATTACHMENT C (Page 2 of 2)

AP1000 Advance Final Safety Evaluation Report, Chapter 7
Section 7.8.2 - Diverse Actuation System Assessment (pg 7-54-55)

demonstrating conformance with regulatory policies and criteria concerning diversity. The AP1000 DCD Tier 1 and Tier 2 will also be updated accordingly to address the software diversity. Therefore, the staff finds the responses to RAI-SRP-7.8-DAS-04 and RAI-SRP7.8-DAS-05 acceptable and the commitments to modify the technical reports will be tracked as **CI-SRP-7.8-ICE-03**.

December 28, 2010

Attachment 2

Response to Non-Concurrence Submitted by William Roggenbrodt

Response to Non-Concurrence Submitted by William Roggenbrodt

On December 8, 2010, a non-concurrence was submitted by William Roggenbrodt associated with the Advanced Final Safety Evaluation Report input for Chapter 7 of the AP1000 Standard Design Certification Amendment. The non-concurrence identifies five concerns that can be grouped into two categories:

- Insufficient implementation of a 10 CFR Part 50, Appendix B, Quality Assurance Program by a vendor that supplies safety-related components for the AP1000.
- Insufficient demonstration of diversity by a vendor that supplies components for both the primary protection system and its diverse back-up system.

Mr. Roggenbrodt is the lead technical reviewer for Chapter 7, "Instrumentation and Controls," for the AP1000 design certification amendment, and I am both Mr. Roggenbrodt's supervisor and the document sponsor for the memo titled, "Advanced Final Safety Evaluation Report for the AP1000 Standard Design Certification Amendment – Chapter 7, "Instrumentation and Control." As mentioned in the "Issues Under Discussion" section of the non-concurrence, the issues center on the design implementation aspects versus the licensing commitments provided in the AP1000 Design Control Document (DCD).

Background

In the AP1000 Instrumentation and Control (I&C) design, the Diverse Actuation System (DAS) provides a limited set of back-up reactor trip and engineered safety features actuation functions to the primary reactor protection system, or Protection and Safety Monitoring System (PMS). The PMS is a safety-related digital protection system that is to be designed with high quality and incorporate design principles such as redundancy, independence, and high reliability. Despite the high quality and design principles incorporated in the PMS, there is a low potential for a software common-cause failure to defeat the four redundant divisions. 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 22, "Protection System Independence," requires that protection systems be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in a loss of the safety function. 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 safety function. To meet GDC 22, Westinghouse Electric Corporation (WEC) included the DAS to provide a diverse means to perform the safety functions through a limited set of automatic or manual functions. Since common-cause failure of the PMS is considered beyond design basis, DAS is classified as a non-safety system consistent with the SRM to SECY-93-087.

The PMS includes a component called the Component Interface Module (CIM) that provides for priority logic and individual plant component control and interface. The priority logic allows plant

component control by safety and non-safety systems; however, safety systems are assured priority over the non-safety systems by the CIM priority logic. In the AP1000 design amendment, WEC proposed to develop the CIM and the DAS using field-programmable gate array (FPGA) technology. The concern lies in the diversity of the CIM and DAS, as both are being developed by a company called CS Innovations (CSI), which is a subsidiary of Westinghouse.

The non-concurrence addresses applicable regulations in the “Relevant Regulations” section, which include 10 CFR Part 50, Appendix B, and GDC 22. The introduction to 10 CFR Part 50, Appendix B, states, in part, that the pertinent requirements of this appendix apply to all activities affecting the safety-related functions of those structures, systems, and components. As a safety-related system, the requirements of 10 CFR Part 50, Appendix B, apply to the PMS, including the CIM. Since CIM is required to meet the requirements of 10 CFR Part 50, Appendix B, the quality assurance issues in the audits for CIM are a valid concern. Also, DAS should demonstrate diversity as described in the GDC 22 and committed in the AP1000 DCD. Therefore, adequacy diversity between CIM and DAS is also a valid concern.

CIM and DAS Diversity

The staff uses the guidance in NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” to evaluate adequate diversity within a plant’s I&C design. In addition, the staff recently issued NUREG/CR-7007, “Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems,” to provide guidance to staff regarding the sufficient level of diversity for plant I&C systems. NUREG/CR-6303 describes six types of diversity that could be incorporated into the plant I&C system, including (1) design diversity, (2) equipment diversity, (3) functional diversity, (4) human diversity, (5) signal diversity, and (6) software diversity. In WCAP-17179-P, “AP1000 Component Interface Module Technical Report,” Rev. 2, WEC committed to the six types of diversity between the CIM and the DAS as follows:

- Design Diversity – Different FPGAs are used from the same manufacturer; the FPGAs have different chip geometries and manufacturing lines. Also, the DAS and CIM architecture differ via data communication means (i.e., serial bus communication vs. backplane communication channels)
- Equipment Diversity – Same as design diversity with the addition of different power supplies and no common hardware modules between CIM and DAS.
- Functional Diversity – CIM performs priority logic and interfaces/controls individual plant components. DAS performs limited safety function processing and controls plant components through different paths.
- Human Diversity – Different design and test teams will be used to develop CIM and DAS.

- Signal Diversity – CIM receives digital component command signals from safety and non-safety systems. DAS receives analog plant process signals to determine component actuation.
- Software Diversity – The functionality of the DAS and CIM are different and do not have common algorithms. The output of the software tool for FPGA development is unique to the FPGA. Therefore, the output of the software tool for the CIM and DAS will be different as the FPGAs are different. However, there is no commitment that the FPGA programming language would be different (most likely it will be VHDL for both devices).

As described in NUREG/CR-7007, software common-cause failures are caused by a combination of latent design faults and concurrent triggering conditions. Triggering conditions that can activate software design faults include human actions (poor design, maintenance, operation), signal trajectory (unexpected combination of inputs and internal system states), external events (plant processes, electromagnetic interference, external system failures), and temporal effects (timing and synchronization issues). Design faults are addressed through high quality development processes, but such processes alone cannot sufficiently address design faults due to the complexity of modern digital systems. Other techniques such as fault management and diversity are incorporated to further eliminate the concern for software common-cause failure.

The safety concern associated with this non-concurrence is the possibility that a triggering condition could activate latent design faults in both the CIM and DAS, preventing the safety function from being accomplished. In other words, the following sequence of events would need to occur to impact public health and safety:

- An accident or transient condition occur
- PMS (including CIM) fails to respond to the event due to a common-cause failure
- DAS fails to respond to the event due to the same or similar common-cause failure
- Operators fail to properly address the event leading to a radiological release

It is acknowledged that CIM and DAS do not have the maximum level of diversity for each of the six categories. For example, both systems use different FPGAs from the same manufacturer, and they will likely use the same programming language (VHDL). However, as acknowledged in NUREG/CR-7007, the maximum level of diversity is not required to achieve sufficient diversity between the CIM and DAS. For example, if a common programming language is being used that contains within itself a latent fault, for a software common-cause failure to occur, the construct of the DAS/CIM algorithms, the inputs and internal states, and the use of the programming language component containing the latent fault would need to be the same, or very similar, to cause a software common-cause failure in both systems. This would be unlikely given the DAS and CIM use different input signals, perform different functions, use different design teams, and commit to different algorithms. Based on the level of diversity committed to in the AP1000 design, and the events needing to occur to arrive at a radiological release, the

staff found in its Chapter 7 FSER input that there was reasonable assurance of adequate protection of the public health and safety.

Quality Assurance Issues at CS Innovations

The non-concurrence also addresses observations at an audit of CS Innovations. During the audit, CS Innovations and Westinghouse were in-process for developing the CIM and the DAS and generating design documents. The audit did reveal the following types of observations:

1. Unclear CIM development lifecycle process (as noted by CSI-OBS1, CSI-CON1, and WEC-CON1 in the non-concurrence)
2. Quality assurance issues related to CIM development (as noted by CSI-OBS2, CSI-OBS5, and CSI-CON1 in the non-concurrence)
3. Insufficient diversity demonstration between CIM and DAS (as noted by CSI-OBS3, CSI-OBS4, CSI-CON2, and WEC-OBS1)

Most of the concerns are associated with the implementation of the CIM and DAS diversity and CIM quality versus issues associated with the AP1000 DCD commitments. In some cases, the observations did impact the staff's review of the AP1000 DCD. For example, WEC proposed the removal of AP1000 DCD, Tier 1, Table 2.5.2-8, Item 11(a), which is the design requirements, or software planning phase, for the PMS (including CIM). Item 11(a) is an Inspection, Tests, Analyses, and Acceptance Criteria (ITAAC) that was also considered to be Design Acceptance Criteria (DAC). The staff determined that WEC did not submit acceptable CIM development plans as part of WCAP-17179. During the audit at CSI and WEC, the staff intended to verify whether sufficient CIM development plans were described in CSI and WEC engineering procedures. However, the staff did not find sufficient CIM development plans at the engineering procedure level during the audits. Since the staff found the software planning for the Common Q portion of PMS to be acceptable in other parts of the review, WEC proposed a new ITAAC/DAC in place of Item 11(a) specifically to call out the CIM development lifecycle process. The staff found their proposal acceptable as WEC would still need to demonstrate acceptable CIM development plans in order to complete the new ITAAC/DAC. With regards to No. 3 above, WEC did submit a DAS setpoint methodology as Appendix A of WCAP-17184-P, "AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report," Rev. 2, following the audit activities. The staff found the DAS setpoint methodology to be acceptable in Section 7.8.2 of the AP1000 Advanced Final Safety Evaluation Report.

Implementation of DAS/CIM diversity and CIM quality are two issues that were identified in the audits and must be adequately addressed by WEC. Since the detailed design of these components is in-process, and the staff found the design commitments in the AP1000 DCD to be acceptable, these design implementation issues can be addressed through various inspection mechanisms, including vendor inspections, engineering design verification inspections, and ITAAC inspections. ITAAC 3.c of Table 2.5.1-4, Tier 1, AP1000 DCD, Revision 18, states that "any DAS algorithms, logic, program architecture, executable operating systems, and executable software/logic are different than those used in the PMS." This ITAAC is currently a targeted ITAAC for NRC inspection and could be used to verify adequate diversity between CIM and DAS once design outputs reach a finalized stage.

Proposed Actions

The non-concurrence proposes a vendor inspection at CSI with at least two of the three participants from the March 2010 audit participating on that inspection team. I agree that a vendor inspection would be appropriate to address the concerns listed in the non-concurrence. Mr. Roggenbrodt and I will engage the NRO vendor inspection branch to arrange for a vendor inspection at the earliest convenience.