AUDIT PLAN

Pressurized Water Reactor Owners Group

Topical Report WCAP-17867-P, Revision 0,
"Westinghouse SSPS Board Replacement Licensing Summary Report"
(TAC NO. MF3550)

Instrumentation and Controls Branch

Background: By letter dated February 21, 2014 (available in the Agencywide Documents Access and Management System (ADAMS) under accession number ML14057A289), Pressurized Water Reactor Owners Group (PWROG) submitted Topical Report (TR), WCAP-17867-P, Revision 0, "Westinghouse SSPS Board Replacement Licensing Summary Report." The PWROG is submitting this TR to the U.S. Nuclear Regulatory Commission (NRC) for review and approval for licensees to reference the NRC approved TR in their *Code of Federal Regulations* (10 CFR) Section 50.59 Screens/Evaluations that will be completed to install the new design Solid State Protection System circuit boards.

The staff of the Instrumentation and Controls Branch has reviewed the instrumentation and controls aspects of the licensee's license amendment request and concluded that an audit, as described below, is needed (April 7 - 11, 2014), to complete the review.

Necessary Material:

- Schematic Diagrams of Boards (new and old)
- Software Development tools for complex programmable logic devices (CPLDs)
- Regulatory Criteria Compliance Traceability or Conformance Matrices
- List of all documents exchanged with each vendor (design & fabrication)
- Westinghouse Electric Company (Westinghouse) Engineers with Electronic Access to all referenced documents
  (Requests will be made on sight for printed copies to work with)

Team Assignments: Norbert Carte: Team Lead

Royce Beacom:
- Regulatory Evaluation of Software Development Processes
  - CPLD Programming Verification and Validation (V&V)
  - Configuration Management
- Lead for Vendor Controls
  - Technical Controls for CPLD Programming

Norbert Carte:
- Review Planned Response to Request for Additional Information
- Requirements Tracing
- Lead for Testing Analysis

Stephen Wyman:
- Circuit Comparisons (new vs. old)
- Independence Analysis

Shavon Edmonds
- Assist with Vendor Controls
    - Vendor Control & Quality Assurance
- Assist with Testing Analysis
- Assist with Requirements Tracing

Logistics: Audit to start 1:00 pm on Monday 4/7/14 (Kickoff, Introductions, & Tour)
Audit to be Completed by noon on Friday 4/11/14.

Special Requests: Support of at least one Westinghouse Licensing Engineer with experience licensing Digital Instrumentation and Controls in accordance with NRC criteria.

Deliverables: An audit report, documenting the findings of the audit, will be issued two months after the completion of the audit.

Audit Guidance: The following guidance will be used to audit the life-cycle design processes and design outputs, with particular emphases on vendor controls, verification and validation, configuration management, quality assurance, and CPLD programming.

Vendor Controls

Review the Vendor Controls of the CPLD-based boards

Since Westinghouse contracts hardware, software, or system development to a vendor; there may be two sets of planning documentation, that of Westinghouse and that of the vendor. Appendix B to 10 CFR Part 50 states that applicants may delegate to others, such as a vendor, the work of establishing and executing the quality assurance program, or any part thereof. Therefore, Westinghouse shall retain responsibility and authority over the duties of persons and organizations performing activities affecting the safety-related functions of the CPLD-based replacement boards. These activities shall be clearly established and delineated in writing.

In the case where Westinghouse has contracted work activities with a vendor, the two sets of planning documents should be reviewed together. This will ensure that not only the vendor performs the appropriate activities, but that Westinghouse also has in place a method of assuring those activities are carried out correctly.

CPLD Programming V&V

Review the V&V program of the CPLD-based boards.

Perform a thread audit of a number of requirements, during which Westinghouse will be asked to track the implementation of various requirements to the board requirements and specifications, and CPLD programming requirements and specifications through each phase of the design process. Use the requirements traceability matrices when performing this thread audit. Demonstrate that the design phase outputs were subject to the V&V process.

Trace the CPLD programming V&V plans for each phase of the programming life-cycle. Evaluate the effectiveness of their implementation during design and design acceptance process. Confirm that the V&V team and its activities are sufficiently independent in terms of cost, schedule, and management.

Configuration Management

Review the configuration management process that was used for the CPLD-based replacement boards. Perform interviews with personnel responsible for performing configuration management activities.

Discuss a postulated change to controlled documents (to include at least one procedure and one design product). Ask the responsible personnel to describe the documentation for each postulated change and to walk through the processes used to manage the changes. This discussion is intended to include the entire process down to the final approvals of the changed product.

Audit an example of an actual finding that required a subsequent CPLD programming change and that was completed during the development of the CPLD-based replacement boards. Review the generated documentation and the conclusion that demonstrates the resultant change adequately resolved the finding.

Discuss with the configuration control librarian the methods used to:
(1) control access to only authorized personnel,
(2) ensure inadvertent changes to the configuration baseline do not occur,
(3) ensure that multiple individuals do not inadvertently check out a particular version of a controlled item for parallel modification that cannot be reconciled, and to demonstrate the methods used to maintain and control the resulting versions.

CPLD Programming Quality Assurance

Review the process with the Quality Assurance (QA) manager responsible for CPLD programming QA. Perform an evaluation to determine that the QA program is effective in controlling the CPLD programming development process to assure quality of the CPLD programming.

Identify the methods by which the QA manager assesses the effectiveness of the processes that affect quality of the CPLD programming.

Postulate an issue indicative of an ineffective process that could be adverse to the quality of the CPLD programming. Ask the QA manager to describe the paperwork for the postulated ineffective process and to walk through the way it would be processed if this were a real quality issue. This discussion is intended to include the entire process down to the final approvals and changes.

Audit an example of an actual QA finding that required a subsequent process change and that was completed during the development of the CPLD-based replacement boards. Review the generated documentation and the conclusion that demonstrates the resultant process change adequately addressed the QA finding.

CPLD Programming Safety

Determine if the CPLD programming safety plans and procedures, to the extent applicable to the platform, are used or in place for use during CPLD programming safety analysis activities.

Where applicable to the platform, verify that the CPLD programming safety plans and associated procedures are adequate to determine that the CPLD programming is suitably safe for use in future nuclear power plant safety applications.

Review the process with appropriate representatives from the QA and V&V organizations.

Review any CPLD-based replacement board's safety analysis to determine its effectiveness in detection of CPLD programming hazards.

Planned RAI Responses

The NRC staff review of the TR has identified issues that will present significant challenges toward completing a comprehensive review and identifying a robust review schedule of the TR. These issues have been expressed previously in a request for additional information. There are three main issues that are not being addressed as part of the regulatory basis and appear to be focused on the life cycle process development. These main issues are: 1) all applicable NRC staff regulatory guides have not been identified; 2) for the guidance that has been identified, adequate evaluations are not included presenting consistency with the NRC staff's positions; 3) if there are alternatives to the NRC staff guidance, these differences should be identified and thoroughly explained as an acceptable alternative approach complying with the Commission's regulations.

In order to make the application complete, the NRC staff requests that PWROG supplement the application to address the information requested below by April 30, 2014. Since acceptance review is not as detailed as the technical review, there may be instances in which issues that impact the NRC staff's ability to complete the detailed technical review are identified. It is highly recommended that a thorough review of the regulatory basis be conducted prior to submittal of the additional information given the issues the staff has identified with this matter. You will be advised of any further information needed to support the NRC staff's detailed technical review by separate correspondence.

1) Section 3, "Regulatory Compliance", of the TR needs to be significantly augmented and supplemented, for example:
   a. Section 3.5 of the TR states that the software life cycle follows the guidance specified in Branch Technical Position (BTP) 7-14, as described in Section 4, "Design Process." However, Section 4 does not describe how the design process is consistent with BTP 7-14, nor does it provide an alternative to BTP 7-14.
   b. Inherent to the review of the life cycle development process is an evaluation of the TR against the six associated Regulatory Guides (RGs) and the ten Institute of Electrical and Electronics Engineers (IEEE) standards endorsed within them. Those RGs are 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173. Only RG 1.169 is identified as a reference within the TR. The TR does not provide an adequate demonstration of compliance with the criteria within these regulatory guides. Similarly, only one of the ten IEEE standards is referenced, which is IEEE Standard (Std) 1012; however, consistency with the criteria in the standard is not presented.
      i. Section 3.3.8 of the TR states that V&V in accordance with IEEE Std 1012 is required; however, the TR does not describe how compliance with IEEE Std 1012 has been achieved, nor does it describe why the described design process provides comparable assurance of compliance with the regulations.

ii. Section 3.3.9, of the TR states that the design and life cycle meets the technical independence, managerial independence, and financial independence criteria for independent verification and validation; however, the TR does not describe how the technical, managerial, and financial independence criteria of RG 1.168 are met.

c. The TR should reference and address the RGs, and not solely the IEEE standard endorsed, because the NRC staff regulatory positions provide additions to (or differ from) the criteria of the referenced standard(s). This includes not only the six RGs identified above but also RG 1.152 which endorses IEEE Std 7-4.3.2.

Please be prepared to discuss the plans to augment and supplement regulatory analysis.

2) In Section 4.7, the TR draws a parallel to the dedication process described in EPRI NP-5652. In the NRC staff safety evaluation (SE) of EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," (ADAMS accession number ML092190664), the staff determined that TR 106439 contains an acceptable method for dedicating commercial grade digital equipment. In the SE, the staff reiterated that methods described in EPRI NP-5652 "are applicable to many of the safety-related components in a nuclear power plant but do not provide specific guidance for dedication of digital equipment."

   Please be prepared to discuss the plans to provide a description of the evaluations methods and evaluate them against the TR-106439 guidelines for digital applications.

3) The TR contains mostly proprietary information, and a non-proprietary version would not be very readable; however, the NRC is obligated to keep the public informed about the activities that it performs.

   Please be prepared to discuss the plans to provide a non-proprietary summary of the material in the TR.

4) During the Phase 0 meetings for this TR, the PWROG stated that it had analyzed the logic implementation on the Complex Programmable Logic Devices that perform safety functions **[ ]** The PWROG also stated that an appendix would be added which provided an example of the tracing used in this analysis. However, neither the added appendix nor the body of the TR contains a summary regarding the tracing **[ ]** (Revision 6 of BTP 7-19.)

   Please be prepared to discuss the plans to provide a summary regarding the tracing **[ ]**

5) The TR addresses eight (8) replacement boards **[ ]** Additional analyses of these **[ ]** boards are performed since their failure to operate correctly could directly impact the system's ability to perform the safety function. The TR asserts, but does not demonstrate, that failures **[ ]** will not impair the system's ability to perform the safety function.

   Please be prepared to discuss the plans to provide adequate information to demonstrate that the proper operation **[ ]** is independent of failures/miss-operation **[ ]**

References: The following references are representative of the life-cycle design process by subject and content that may be audited for regulatory compliance and also identifies the regulatory evaluation criteria and industry guidance against which the audit will be performed.

NRC Guidance:

The following guidance will be applied with adjustments appropriate to accommodate minor regulatory basis differences between the CPLD and digital computer technologies:

Standard Review Plan (NUREG-0800), Chapter 7, "Instrumentation and Controls" with a focus on Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," and BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems."

Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"

Regulatory Guide 1.168, Revision 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

Regulatory Guide 1.169, dated September 1997, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

Regulatory Guide 1.170, dated September 1997, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

Regulatory Guide 1.171, dated September 1997, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

Regulatory Guide 1.172, dated September 1997, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

Regulatory Guide 1.173, dated September 1997, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

Safety Evaluation by the office of Nuclear Reactor Regulation, on the EPR TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," ML092190664.

Corresponding Industry Standards:

The following Industry Standards correspond to the previously identified Regulatory Guides that will be applied with adjustments appropriate to accommodate minor regulatory basis differences between the CPLD and digital computer technologies:

IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Regulatory Guide 1.152)

IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation" (Regulatory Guide 1.168)

IEEE Std 1028-1997, "IEEE Standard for Software Reviews and Audits" (Regulatory Guide 1.168)

IEEE Std 828-1990, "IEEE Standard for Software Configuration Management Plans" (Regulatory Guide 1.169)

ANSI/IEEE Std 1042-1987, "IEEE Guide to Software Configuration Management" (Regulatory Guide 1.169)

IEEE Std 829-1983, “IEEE Standard for Software Test Documentation” (Regulatory Guide 1.170)

ANSI/IEEE Std 1008-1987, “IEEE Standard for Software Unit Testing” (Regulatory Guide 1.171)

IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" (Regulatory Guide 1.171)

IEEE Std 830-1993, “IEEE Recommended Practice for Software Requirements Specifications” (Regulatory Guide 1.172)

IEEE Std 1074-1995, “IEEE Standard for Developing Software Life Cycle Processes (Regulatory Guide 1.173)