FINAL SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

TOPICAL REPORT WCAP-17867-P, REVISION 1,

"WESTINGHOUSE SSPS BOARD REPLACEMENT LICENSING SUMMARY REPORT"

PRESSURIZED WATER REACTOR OWNERS GROUP

TAC NOS. MF3550 AND MF4655

1.0 INTRODUCTION

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

The NRC staff conducted an audit at the Westinghouse Electric Company (Westinghouse or WEC) facilities in New Stanton, Pennsylvania during the week of April 7-11, 2014 (ADAMS Accession No. ML14183B483). As part of this audit, a sample set of requirements was traced and it was identified that the documented traceability analysis should be augmented and supplemented with a technical requirements traceability matrix. In addition, the PWROG agreed to implement and document a more detailed regulatory compliance analysis.

By letter dated May 7, 2014 (ADAMS Accession No. ML14111A320), the NRC requested additional information from the PWROG. By letter dated June 20, 2014 (ADAMS Accession Nos.: Letter – ML14176A096, Non-Publically Available Enclosure – ML14176A097), the PWROG responded to the information request.

The NRC staff conducted an audit at the Westinghouse facilities in Rockville, Maryland during the week of July 15-17, 2014 (ADAMS Accession No. ML14227A928). A revised regulatory compliance matrix was examined and comments were provided. The PWROG further revised the regulatory compliance matrix based on these comments. During the audit, the NRC staff also provided the PWROG with a description of the NRC staff needs for identifying and documenting the bases for all the detailed qualification criteria and summary of qualification tests performed within the text portion of the final TR.

By letter dated August 25, 2014 (ADAMS Accession No. ML14245A490), the PWROG amended its application by docketing Revision 1 of the TR.

ENCLOSURE

The continued operation of the SSPS depends on the availability of replacement circuit boards (a.k.a., new design boards) that contain logic devices that will be available or easily replaced until the scheduled end of plant life including the NRC-approved plant license renewals. The original design SSPS circuit boards have been redesigned and the technology in most of the new designs use programmable logic devices (i.e., a Complex Programmable Logic Device (CPLD)).

In general, the new design boards can be used to replace the original design boards. However, because each plant's configuration and operating conditions are unique, a licensee must confirm (before installing the new design boards) that the tested qualification levels envelope the extreme conditions expected at its plant. The unique configuration of each plant makes it imperative that each licensee analyze whether the new design boards can be installed under 10 CFR 50.59. Therefore, this safety evaluation (SE) addresses only the generic issues associated with installing the new design boards. Licensees may reference this SE, as applicable, when performing a 10 CFR 50.59 Evaluation.

The NRC staff's evaluation of the processes implemented during the development and production of the new design boards described herein represents a modification to the NRC staff's evaluation process currently applied to the review of digital safety systems. The NRC staff recognizes that the development processes that were applied to the new design boards (performed during the 2003 through 2009 time frame) began prior to the full establishment of the NRC staff's current positions (2007 time frame) regarding the application of safety system software development review guidance for most digital technologies. As described within Section 3.4 below, the NRC staff's positions have broadened during the time that the new design boards were being developed. This is with regard to the identification and application of appropriate industry standards describing the degree of rigor that must be applied to different digital technologies during software development and software/hardware integration, which is to be considered as a high-quality development process. Therefore, the NRC staff's evaluation, as described herein, focused on a review of the evidence provided by the supplier of the development processes employed. The NRC staff's review is to make a determination as to whether the regulatory requirements for a high-quality development process have been adequately addressed, rather than to perform a review of compliance with the applicable clauses within the current versions of the appropriate industry standards. For this reason, this SE cannot be used as an example or precedent for referencing in future topical reports associated with digital instrumentation and control (DI&C) upgrades that are submitted to the NRC for review and approval.

The NRC staff believes it is beneficial to use public meetings to discuss proposed applications; particularly where DI&C upgrades or the initial submittals to the NRC by licensing organizations are involved. These two-way discussions are intended so that the staff can provide feedback regarding its positions on critical digital technology and licensing aspects. Digital aspects include the types of technology, development processes used, and diversity and defense-in-depth philosophy. Critical licensing aspects include meeting with organizations which have not submitted previous applications and whose meetings with the NRC include a discussion of applicable regulatory requirements and the staff guidance that should be addressed within the application. All of these issues may likely affect the NRC staff's evaluation process and the schedule for the review. Hence, the use of Phase 0 meetings has been emphasized in DI&C-ISG-06.

2.0 REGULATORY EVALUATION

NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," provides the acceptance criteria for the review of topical reports. Specifically, Standard Review Plan (SRP) Chapter 7, "Instrumentation and Controls," addresses the requirements for instrumentation and control (I&C) systems in nuclear power plants based on light-water reactor designs. SRP Chapter 7 and NRC Interim Staff Guidance (ISG), which augments and supplements SRP Chapter 7, establish the review criteria for DI&C systems, which the NRC staff applied in this evaluation.

SRP Chapter 7, Table 7-1, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety," identifies design criteria and regulations in 10 CFR Part 50 that are applicable to I&C systems and relevant to the general review of the suitability of a digital circuit board for use in safety-related applications. Some review criteria within the SRP depend on the design of an assembled system for a particular application; whereas the TR presents elements of hardware and board-level CPLD programming that constitute the circuit boards, that will be used as replacements for the Motorola High Threshold Logic-based (MHTL) SSPS circuit boards (original design boards). As such, this SE is necessarily limited to the evaluation of compliance with the applicable regulations and guidance documents to the degree that they can be met at the board level, because the TR scope does not involve a plant-specific safety system application. In other words, this SE does not directly evaluate regulations and guidance at the system level, but only evaluates the capabilities and characteristics of the new design boards on a generic basis with respect to supporting 10 CFR 50.59 Evaluations associated with replacing the original design boards with the new design boards.

Determination of full compliance with the applicable regulations remains subject to a plant-specific licensing review of a full system design that is associated with replacing the original design boards with the new design boards. Plant-specific action items have been established to identify criteria that should be addressed by applicants and licensees referencing this SE (see Section 4.2). The plant-specific action items identified in Section 4.2 do not obviate an applicant's or licensee's responsibility to adequately address new or changed design basis or regulations that apply, in addition to those considered in this SE.

The following regulations are applicable to the TR:

> The regulation at 10 CFR 50.55a(a)(1), "Quality Standards," requires structures, systems, and components be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.
>
> The regulation at 10 CFR 50.55a(h), "Protection and Safety Systems" incorporates, by reference, the 1991 version of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," including the correction sheet dated January 30, 1995.

The NRC staff also considered the following application-specific 10 CFR Part 50, Appendix A, “General Design Criteria [(GDC)] for Nuclear Power Plants,” when evaluating the TR for use in safety systems, as follows:

GDC 1, "Quality Standards and Records"

GDC 1 contains four sentences. The first sentence is addressed along with 10 CFR 50.55a(a)(1), IEEE 603-1991, Clause 5.3, and IEEE 7-4.3.2-2003, Clause 5.3. The second sentence is partially addressed by the NRC's incorporation of standards by reference into 10 CFR 50.55a (e.g., IEEE 279 and 603) or their endorsement (e.g., through Regulatory Guides); other generally recognized codes and standards that are used should be identified and evaluated to determine their applicability, adequacy, and sufficiency and should be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. The third and fourth sentences are addressed by other means and were not specifically evaluated as part of the TR evaluation process.

GDC 2, "Design Bases for Protection against Natural Phenomena"

GDC 2 is generally addressed in Section 3.5, "Environmental Equipment Qualification." The new design boards are mounted within electrical cabinets located within controlled environments in the plant. However, the potential occurrence of the aforementioned design basis external events can present hazards leading to a loss of electrical power or other normal plant services that could lead to the loss of heating, ventilating, and air conditioning (HVAC), or the onset of cabinet acceleration/motion due to seismic effects that can result in off-normal environmental conditions. Section 3.5 describes the NRC staff's evaluation of the qualification testing and analysis to demonstrate reliable performance of the new design boards to withstand the effects of such natural phenomena without loss of capability to perform their safety functions.

GDC 4, "Environmental and Dynamic Effects Bases"

GDC 4 is generally addressed in Section 3.5, "Environmental Equipment Qualification," Section 3.9.1.7, "[IEEE 603] Clause 4.7…", and Section 3.9.1.8, "[IEEE 603] Clause 4.8…"

GDC 13 "Instrumentation and Control"

The new design boards do not process signals for monitoring process variables, but they do process signals for Plant Protections System (PPS) and SSPS status indication; these system-signals are provided to the plant computer and the main control board. No signals for process control are processed by the new design boards. The signals processed by each new design board are the same as those for the original design boards. Since the particular signal processed by a board depends on the board location, it is not possible to explicitly map system-status signals to board functions; therefore no evaluation against this criterion was performed. (See Section 3.9.2.8.2, "[IEEE 603] Clause 5.8.2, 'System Status Indication'," and Section 3.9.2.8.3, "[IEEE 603] Clause 5.8.3, 'Indication of Bypasses,' " for a general evaluation of the status indications.)

GDC 18 “Inspection and Testing of Electric Power Systems"

GDC 18 is addressed in Section 3.5.3, “Response Time Characteristics and Testing.”

GDC 20, "Protection System Functions."

The new design boards process signals for PPS actuation functions, field contact inputs, nuclear instrumentation system (NIS) inputs, and main control board switch inputs. The functions by each new design board are the same as those for the original design boards. Since the particular signal processed by a board depends on the board location, it is not possible to explicitly map actuation functions to board functions; therefore no evaluation against specific actuation functions was performed. However, three of the new design boards can affect the response time for safety-related reactor trip (RT) and engineered safety features (ESF) actuation functions. Section 3.5.3 describes the NRC staff’s evaluation of the testing and analysis to ensure that the response time performance of the new design boards did not significantly increase the response time capabilities of the SSPS system, remained within bounding response times allowed within previous safety analyses, and did not violate any assumptions or alter any conclusions made regarding the justification for eliminating response time testing requirements as described in previous analyses reports approved by the NRC staff.

GDC 21, "Protection System Reliability and Testability"

GDC 21 is generally addressed in Section 3.12, “Secure Development and Operational Environment,” Section 3.9.2.7, “[IEEE 603] Clause 5.7…”, and Section 3.9.1.8, “[IEEE 603] Clause 4.8...”

GDC 22, "Protection System Independence"

Those aspects of GDC 22 related to the effects of natural phenomena are generally addressed in Section 3.5, “Environmental Equipment Qualification.” In addition, Section 3.9.2.6.3 describes the NRC staff’s evaluation of testing performed to demonstrate the capability of new design boards that ensure electrical independence between safety and non-safety signals that interface with the SSPS system.

GDC 23, "Protection system failure modes"

The evaluation of the system effects associated with component failure modes is addressed in Section 3.9.2.1.1, “Failure Modes and Effects Analysis.”

GDC 24, "Separation of protection and control systems"

The signals that pass through (or originate in) the SSPS are for protection purposes, and not used for control purposes; therefore there are no shared components within the SSPS.

GDC 25, "Protection system requirements for reactivity control malfunctions"

The new design boards' process signals for PPS actuation functions. The functions by each new design board are the same as those for the original design boards (see Sections 3.1.1-3.1.8). Since the particular signal processed by a board depends on the board location, it is not possible to explicitly map actuation functions to board functions; therefore no evaluation against specific actuation functions was performed.

The NRC staff also considered 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants," when evaluating the development process of the new design boards (see Section 3.4).

Criterion I, "Organization"

Criterion III, "Design Control,"

Criterion V, "Instructions, Procedures, and Drawings"

Criterion VII, "Control of Purchased Material, Equipment, and Services"

Criterion XI, "Test Control"

Criterion XV, "Nonconforming Materials, Parts, or Components"

The NRC staff considered the following guidance when it evaluated the applicant's compliance with the underlying regulations:

Regulatory Guide (RG) 1.22, Revision 0, "Periodic Testing of Protection System Actuation Functions" (ADAMS Accession No. ML083300530), describes a method acceptable to the NRC staff for inclusion of actuation devices in the periodic tests of the protection system during reactor operation.

The testing of the actuation relays does not use the SSPS circuit boards; therefore, no evaluation against the criteria in this RG was performed.

RG 1.47, Revision 1, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems" (ADAMS Accession No. ML092330064), describes a method acceptable to the NRC staff for complying with the regulatory requirements regarding the bypassed and inoperable status indication for nuclear power plant safety systems.

The new design boards process the same signals for display/indication of bypassed status as the original design boards; therefore, no review against these specific criteria

was performed. This criterion was addressed generically by the evaluation that the new design boards perform the same functions as the original design boards. See Sections 3.1.1-3.1.8, and Section 3.9.2.8.3, “[IEEE 603] Clause 5.8.3, Indications of Bypasses.”

RG 1.53, Revision 2, "Application of the Single-Failure Criterion to Safety Systems" (ADAMS Accession No. ML033220006), describes a method acceptable to the NRC staff for meeting the NRC's regulations as they apply to the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems. That is, RG 1.53 states conformance with the normative aspects of IEEE Std. 379-2000, “Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” provides methods acceptable to the NRC staff for satisfying the NRC’s regulations with respect to the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems.

The SSPS addresses the single failure criterion by having two independent redundancies (a.k.a., Trains A and B) with each redundancy being capable of initiating the required safety functions. The new design boards perform the same functions as the original design boards (see Sections 3.1.1-3.1.8); therefore, no review against the criteria in this regulatory guide was performed. See also Section 3.9.2.1, “[IEEE 603] Clause 5.1, Single Failure,” and Section 3.9.2.6, “[IEEE 603] Clause 5.6, Independence.”

RG 1.62, Revision 1, "Manual Initiation of Protective Actions" (ADAMS Accession No. ML101540348), describes methods acceptable to the NRC staff for complying with regulatory requirements in regard to the manual initiation of protective actions.

The SSPS circuit boards do not process signals associated with the manual actuation of the PPS functions; therefore, this RG is not applicable.

RG 1.75, Revision 3, "Criteria for Independence of Electrical Safety Systems" (ADAMS Accession No. ML043630448), describes a method acceptable to the NRC staff for meeting physical independence of the circuits and electrical equipment that comprise or are associated with safety systems. That is, RG 1.75 states conformance with the normative aspects of IEEE Std. 384-1992, “Standard Criteria for Independence of Class 1E Equipment and Circuits,” provides a method that the NRC staff considers acceptable for satisfying the agency’s regulatory requirements concerning physical independence of the circuits and electrical equipment that comprise or are associated with safety systems, subject to the regulatory positions stated.

The Isolation (ISO) board (see Section 3.1.8 for a brief description of the ISO board) is the isolation device in two situations: (1) between redundant portions of the SSPS, and (2) between the SSPS and the non-safety-related systems. The regulatory bases for such isolation is described in Section 3.9.2.6.1, “[IEEE 603] Clause 5.6.1, Between Redundant Portions,” and Section 3.9.2.6.3, “[IEEE 603] Clause 5.6.3, Other Systems,” respectively. The NRC staff’s evaluation of the ISO board testing to address these requirements is described in Section 3.9.2.6.3.

RG 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," describes a method acceptable to the NRC staff for providing instrumentation to monitor variables for accident conditions.

The new design boards do not process signals for monitoring process variables; therefore, no evaluation against the criteria in this RG was performed.

RG 1.100, Revision 3, "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants" (ADAMS Accession No. ML091320468), describes a method acceptable to the NRC staff for meeting the seismic qualification. That is, RG 1.100 states conformance with the normative aspects of IEEE Std. 344-2004 is, in general, acceptable to the NRC staff for the seismic qualification of (1) electrical equipment in new nuclear power plants and (2) new or replacement electrical equipment in operating nuclear power plants, subject to the regulatory positions stated.

The NRC staff's evaluation of compliance with the guidance within RG 1.100 to the degree that it can be met at the circuit board level is addressed in Section 3.5.1.4, "Seismic Qualification."

RG 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems" (ADAMS Accession No. ML003739468), describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to periodic testing of electric power and protection systems. That is, RG 1.118 states conformance with the normative aspects of IEEE Std. 338-1987, "Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," provides a method acceptable to the NRC staff for satisfying the NRC's regulations with respect to periodic testing of electric power and protection systems.

RG 1.118, Revision 3, was issued in April of 1995, at which time the GDC and IEEE 279-1971 contained the applicable regulatory requirements. Subsequently, in 1999, IEEE 603-1991 was incorporated into the regulations by reference, superseding IEEE 279 as noted. RG 1.118 Revision 3 addresses requirements in GDC 18 and 21, IEEE 279-1971, Clauses 4.9 and 4.10, and 10 CFR 50 Appendix B Criterion XI. IEEE 603-1991, Clause 6.5 and 5.7 (see Section 3.9.3.5, "[IEEE 603] Clause 6.5, Capability for Testing and Calibration," and Section 3.9.2.7, Capability for Test and Calibration"), supersede IEEE 279-1971, Clauses 4.9 and 4.10, respectively.

RG 1.152, Revision 3, "Criteria for Use of Computers In Safety Systems of Nuclear Power Plants" (ADAMS Accession No. ML102870022), describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to high functional reliability and design requirements for computers used in safety systems of nuclear power plants. That is, RG 1.152 states conformance with the normative aspects of IEEE Std. 7-4.3.2-2003 is a method that the NRC staff has deemed acceptable for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants, subject to the regulatory positions stated.

RG 1.152 is addressed by Section 3.10 and Section 3.12.

RG 1.153, Revision 1, "Criteria for Safety Systems" (ADAMS Accession No. ML003740022), endorsed IEEE Std. 603-1991 as a method acceptable to the NRC staff for meeting the NRC's regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of the safety systems of nuclear power plants prior to IEEE Std. 603-1991 incorporation by reference into the regulations. That is, RG 1.153 states conformance with the normative aspects of IEEE Std. 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations" (including the correction sheet dated January 30, 1995), provides a method acceptable to the NRC staff for satisfying the NRC's regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of the safety systems of nuclear power plants.

RG 1.153 is addressed by Section 3.9.

RG 1.168, Revision 2, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (ADAMS Accession No. ML13073A210), describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to the verification and validation of safety system software. That is, RG 1.168 states conformance with the normative aspects of IEEE Std. 1012-2004, “IEEE Standard for Software Verification and Validation,” provides an acceptable approach to the NRC for meeting the agency’s regulatory requirements on the verification and validation (V&V) of safety system software with the exceptions and additions listed in the NRC staff regulatory guidance section. That is, RG 1.168 also states conformance methods in IEEE Std. 1028-2008, “IEEE Standard for Software Reviews and Audits,” provides an approach acceptable to the NRC staff for carrying out software reviews, inspections, walkthroughs, and audits, subject to the exceptions and additions listed in the regulatory positions.

The evaluation of the development process was performed against the underlying regulations, rather than using this RG, in part because the new design boards were developed before the NRC staff documented its position that the term “software” is understood to include “logic developed from software-based development systems,” see Section 3.4.

RG 1.169, Revision 2, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (ADAMS Accession No. ML12355A642), describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to the configuration management of safety system software. That is, RG 1.169 states conformance with the normative aspects of IEEE Std. 828-2005, “IEEE Standard for Software Configuration Management Plans,” provides an approach that the NRC staff considers acceptable for satisfying the agency’s regulatory requirements with respect to configuration management plans for safety system software with the exceptions and additions listed in the regulatory positions.

The evaluation of the development process was performed against the underlying regulations, rather than using this RG, in part because the new design boards were developed before the NRC staff documented its position that the term “software” is understood to include “logic developed from software-based development systems,” see Section 3.4.

RG 1.170, Revision 1, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (ADAMS Accession No. ML13003A216), describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to test documentation of safety system software. That is, RG 1.170 states conformance with the normative aspects of IEEE Std. 829-2008, “IEEE Standard for Software and System Test Documentation,” provides an acceptable approach for meeting the agency’s regulatory requirements on the test documentation of safety system software with the exceptions and additions listed in the regulatory positions.

The evaluation of the development process was performed against the underlying regulations, rather than using this RG, in part because the new design boards were developed before the NRC staff documented its position that the term “software” is understood to include “logic developed from software-based development systems,” see Section 3.4.

RG 1.171, Revision 1, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (ADAMS Accession No. ML13004A375), describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to the unit testing of safety system software. That is, RG 1.171 states conformance with the normative aspects of American National Standards Institute (ANSI)/IEEE Std. 1008-1987, “IEEE Standard for Software Unit Testing,” provide an acceptable approach for meeting NRC regulatory requirements on the unit testing of safety system software with the exceptions and additions listed in the regulatory positions.

The evaluation of the development process was performed against the underlying regulations, rather than using this RG, in part because the new design boards were developed before the NRC staff documented its position that the term “software” is understood to include “logic developed from software-based development systems,” see Section 3.4.

RG 1.172, Revision 1, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (ADAMS Accession No. ML13007A173), describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to preparation of software requirement specifications (SRRs) for safety system software. That is, RG 1.172 states conformance with the normative aspects of IEEE Std. 830-1998 provides an approach that the NRC staff considers acceptable for meeting the requirements in 10 CFR Part 50 on the preparation of SRSs for safety system software with the exceptions and additions listed in the regulatory positions.

The evaluation of the development process was performed against the underlying regulations, rather than using this RG, in part because the new design boards were developed before the NRC staff documented its position that the term “software” is understood to include “logic developed from software-based development systems,” see Section 3.4.

RG 1.173, Revision 1, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (ADAMS Accession No. ML13009A190), describes a method acceptable to the NRC staff for complying with the

NRC's regulations as they apply to the development processes for safety system software. That is, RG 1.173 states conformance with the normative aspects of IEEE Std. 1074-2006, “IEEE Standard for Developing a Software Project Life Cycle Process,” provides an approach that the NRC staff considers acceptable for meeting the requirements in 10 CFR Part 50 and the guidance in RG 1.152, as they apply to development processes for safety system software with the exceptions and additions listed in the regulatory positions, is acceptable for meeting regulatory requirements.

The evaluation of the development process was performed against the underlying regulations, rather than using this RG, in part because the new design boards were developed before the NRC staff documented its position that the term “software” is understood to include “logic developed from software-based development systems,” see Section 3.4.

RG 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems" (ADAMS Accession No. ML032740277), describes a method acceptable to the NRC staff for design, installation, and testing practices to address the effects of electromagnetic interference/radio frequency interference (EMI/RFI) and power surges on safety-related I&C systems. That is, RG 1.180 states conformance with the normative aspects of the various standards identified therein, with the exceptions and additions listed in the regulatory positions, provides an approach deemed acceptable to the staff for identifying and documenting EMI/RFI compatibility.

The NRC staff’s evaluation of compliance with the guidance within RG 1.180 to the degree that it can be met at the circuit board level is addressed in Section 3.5.1.5.

RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants" (ADAMS Accession No. ML070190294), describes a method acceptable to the NRC staff for meeting the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants. That is, RG 1.209 states conformance with the normative aspects of IEEE Std. 323-2003 is appropriate for satisfying the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants, with the exceptions and additions listed in the regulatory positions.

The NRC staff’s evaluation of compliance with the guidance within RG 1.209 to the degree that it can be met at the circuit board level is addressed in Section 3.5.1.1.

Digital Instrumentation and Control – Interim Staff Guidance, DI&C-ISG-04, Revision 1, "Task Working Group #4: Highly-Integrated Control Rooms-Communications Issues (HICRc)" (ADAMS Accession No. ML083310185), describes methods acceptable to the NRC staff to prevent adverse interactions among safety divisions and between safety-related equipment and equipment that is not safety-related.

This ISG is addressed in Section 3.7. There is no digital communication while the system is in operation or while the SSPS is in test.

The NRC staff also considered applicable portions of the Branch Technical Positions (BTPs) in accordance with the review guidance established within NUREG-0800, "U.S. Nuclear Regulatory Commission Standard Review Plan," Chapter 7, "Instrumentation and Controls", in accordance with 10 CFR 50.34(h)(3), as follows:

Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603" (ADAMS Accession No. ML070550088),

See Section 3.9, “Review of System and IEEE Std. 603 requirements.”

Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2" (ADAMS Accession No. ML070660327),

See Section 3.10, “Review IEEE Std. 7-4.3.2”

BTP 7-11, "Guidance on Application and Qualification of Isolation Devices" (ADAMS Accession No. ML070550080),

See Section 3.9.2.6.3, “[IEEE 603] Clause 5.6.3, Other Systems.”

BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" (ADAMS Accession No. ML070670183),

All major Sections.

BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions" (ADAMS Accession No. ML070550075),

See Section 3.9.2.7, “[IEEE 603] Clause 5.7, Capability for Test and Calibration,” and Section 3.9.3.5, “[IEEE 603] Clause 6.5, Capability for Testing and Calibration.”

BTP 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems" (ADAMS Accession No. ML110550791),

See Section 3.6, “Defense-in-Depth and Diversity.”

BTP 7-21, "Guidance on Digital Computer Real-Time Performance" (ADAMS Accession No. ML070550070),

Section 3.5.3 describes the NRC staff’s evaluation of the testing and analysis to ensure that the response time performance of the new design boards did not significantly increase the response time capabilities of the SSPS system, remained within the bounding response times, and did not violate any assumptions or alter any conclusions made regarding the justification for eliminating response time testing requirements as described and approved by the NRC staff in WCAP-14036-P-A, Revision 1.

3.0 TECHNICAL EVALUATION

This technical evaluation section documents the NRC staff's evaluation of the TR against the relevant criteria identified in Section 2.0 above. The twelve subsections below were chosen to correspond to the twelve areas of DI&C-ISG-06 (ADAMS Accession No. ML110140103):

- System Description (Section D.1 of DI&C-ISG-06)
- Hardware Development Process (Section D.2)
- Software Architecture (Section D.3)
- Software Development Process (Section D.4)
- Environmental Equipment Qualifications (Section D.5)
- Defense-in-Depth & Diversity (Section D.6)
- Communications (Section D.7)
- System, Hardware, Software, and Methodology Modifications (Section D.8)
- Compliance with IEEE Std. 603 (Section D.9)
- Conformance with IEEE Std. 7-4.3.2 (Section D.10)
- Technical Specifications (Section D.11)
- Secure Development and Operational Environment (Section D.12)

3.1 SSPS System Description

The SSPS is a product line in use in Westinghouse designed nuclear power plants. The salient features of the SSPS are summarized as follows:

1. The system is comprised of redundant, identical Trains (A and B) that are physically and electrically independent. Each train is capable of being locked to allow for administrative control of access. For a 3-bay SSPS, each train consists of three cabinets: Input, Logic, and Output. For a 4-bay SSPS, each train consists of four cabinets: Input, Logic, and two Output. Additionally, each train is provided with a Demultiplexer cabinet to interface with the main control board and plant computer (if applicable). The new design boards will be installed into the Logic and Demultiplexer cabinets.

2. The system performs reactor trip and engineered safety features actuation functions as well as non-protective control and equipment protection type functions.

3. Redundant channel inputs derived from the process analog equipment or directly from sensor contacts operate input relays which are located in the solid state Input cabinet. Contacts of the input relays are then applied to the voting logic portion (i.e., universal logic boards (ULBs)) of the system which is located in the adjacent Logic cabinet. Electrical and physical isolation between redundant channels is maintained through the Input cabinets. The separation between coil and contacts of the input relays (1200V root-mean-squared (rms) breakdown) provides electrical isolation between the trains and between the trains and the external systems. Additional inputs which carry the train designation enter the logic directly from switches and pushbuttons on the control board.

4. The undervoltage driver (UVD) board receives input signals from the ULB voting logic circuits. The undervoltage coils of the reactor trip breakers are supplied directly from the UVD board located in the logic bay of the associated train. A bypass breaker in parallel with each trip breaker enables on line testing of the trip breakers. The Train A logic de-energizes the Train A trip breaker and the Train B bypass breaker, the Train B logic de-energizes the Train B trip breaker and the Train A bypass breaker. The bypass breakers are interlocked to prevent simultaneous closure thus preventing both trains from being bypassed simultaneously.

5. The safeguards driver (SGD) board receives input signals from the ULB voting logic circuits. The SGD boards operate master relays which then operate slave relays for engineered safety features actuation. The master and slave relays are located in the Output cabinet which is adjacent to the Logic cabinet.

6. System status information is transmitted from the logic to the control board status lamps and annunciators as well as to the plant computer via photocoupled diode pair isolation devices and multiplexing circuits. Multiplexing is used to simplify and reduce field wiring requirements. The isolation circuitry is designed for 1200V AC rms, the isolation device is rated at 2500V DC breakdown.

7. Testing of the complete SSPS can be performed with the plant at power or shutdown. The process instrumentation portion of the protection system, the logic, and the reactor trip and engineered safety features actuation circuits are tested separately but with sufficient overlap to provide a complete system test. Major test features include:

    a. Protection inhibits and test time. During testing of the logic portion of the system including the undervoltage coils and master slave relays, the reactor trip (RT) and Engineered Safety Features (ESF) safeguards actuation functions of the train under test are inhibited. The typical time to complete a logic test is about two – three hours. The time allowed to complete logic testing is defined by the plant-specific Technical Specifications.

    b. Logic testing. The logic is tested semi-automatically, one trip or ESF protection function at a time, using fast pulse testing techniques. Means are provided for testing the logic manually. This mode also inhibits the protection functions of the train under test and it greatly increases the time required for testing. In addition, means are provided for testing the operability of the semi-automatic tester prior to performing the logic test.

c. Status monitoring inhibits. Status information transmitted to the main control board, to the main control board annunciators, or to the plant computer from the train under test is inhibited to avoid confusion to the operator.

d. Critical status monitoring. Means are provided in each train for monitoring test switch positions, multiplexing and input inhibit switch positions, circuit board connector seating, bypass breaker position, and master relay testing configuration.

8. A system status alarm for each train is annunciated in the control room. The alarm is generated by the associated train General Warning circuit. If a General Warning condition should develop simultaneously in both trains, the General Warning circuits will automatically trip the reactor. This design feature is in addition to the bypass breaker interlock trip feature discussed in No. 4.

9. Power distribution is in accordance with the split bus concept throughout. The zero voltage circuit common buses (i.e., logic ground) of Trains A and B are not connected. The ac that feeds the dc power supplies in the logic cabinet are run through noise line filters.

10. Testability of all engineered safety features that can be operated at power (i.e., without an undesired effect on plan operation), is incorporated in the design.

The TR proposes eight replacement circuit boards for the Logic cabinet and associated communications to the main control board and plant computer Demultiplexers. The new design boards also contain some enhancements which include board edge light emitting diodes (LEDs) for enhanced status and diagnostics indication. The rest of the SSPS remains unchanged. The sub-sections below describe the functions of the eight new design boards.

The purchase orders for the design of the new design boards required that the new design boards implement the functions of the original design boards. The fact that these requirements were achieved was confirmed by testing and analysis. A sample of these purchase orders and test procedures were examined as part of the audit of the Westinghouse facilities in New Stanton, Pennsylvania in April of 2014 (ADAMS Accession No. ML14183B483).

3.1.1 Universal Logic Board

The Universal Logic Board (ULB) function in the SSPS is to provide voter logic to generate Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) signals based on PPS inputs, NIS inputs, field contact inputs (e.g., reactor coolant pump undervoltage relays) and main control board switch inputs. The TR contains a description of the new design board in the following sections:

Section 2.1, Universal Logic Board
Section 5.1.1, “Universal Logic Board Simple Logic”
Section A.1, Universal Logic Board

The TR also contains an evaluation of the functionality of the new design board as compared to the original design board. That is, TR Section 2.1.2, "New Design ULB Board Operations and Enhancements," states:

> "The new design ULB is designed as a drop-in, one-for-one replacement for the original design boards. All the basic functions and interfaces of the new design board are the same as those of the original design board."

The NRC staff compared a sample of the new design board functions to the original design board functions and did not find any discrepancies.

3.1.2 Safeguards Driver Board

The Safeguards Driver (SGD) board function in the SSPS provides eight driver stage outputs that can operate master relays that implement ESFAS actuations when demanded by the ULB voting logic. The TR contains a description of the new design board in the following sections:

Section 2.2, Safeguards Driver Board
Section 5.1.2, "Safeguards Driver Board Logic"
Section A.2, Safeguards Driver Board

The TR also contains an evaluation of the functionality of the new design board as compared to the original design board. That is, TR Section 2.2.2, "New Design SGD Board Operations and Enhancements," states:

> "The new design SGD is designed as a drop-in, one-for-one replacement for the original design boards. All the basic functions and interfaces of the new design board are the same as those of the original design board."

The NRC staff compared a sample of the new design board functions to the original design board functions and did not find any discrepancies.

3.1.3 Undervoltage Driver Board

The Undervoltage Driver (UVD) board functions in the SSPS to provide voltage drive to the undervoltage relay coils in the reactor trip breaker assembly. When the inputs to the ULB indicate that a reactor trip is required, the UVD board turns off the output voltage driver circuits that provide the hold-up voltage to the reactor trip breaker undervoltage coil. This action initiates a reactor trip actuation. The TR contains a description of the new design board in the following sections:

Section 2.3, Undervoltage Driver Board
Section 5.1.3, "Undervoltage Driver Board Simple Logic"
Section A.3, Undervoltage Driver Board

The TR also contains an evaluation of the functionality of the new design board as compared to the original design board. That is, TR Section 2.3.2, "New Design UVD Board Operations and Enhancements," states:

> "The new design UVD is designed as a drop-in, one-for-one replacement for the original design boards. All the basic functions and interfaces of the new design board are the same as those of the original design board."

The NRC staff compared a sample of the new design board functions to the original design board functions and did not find any discrepancies.

3.1.4 Semi-Automatic Tester Board

The Semi-Automatic Tester (SAT) board function in the SSPS is to provide the correct sequence of test signals into logic for testing the logic operation of the SSPS. Clock counter inputs are gated into four possible test pulse signals for routing to the logic circuits being tested. The SAT monitors the results of the logic test and determines if the test is successful or if it has failed. A special circuit on the SAT board, called the general warning, monitors cabinet self-health conditions, test switch positions, and board status conditions, and alerts the operator that a train may be less than fully operational. The TR contains a description of the new design board in the following sections:

Section 2.4, Semi-Automatic Tester Board
Section 5.1.4, "Semi-Automatic Tester Board Simple Logic"
Section A.4, Semi-Automatic Tester Board

The TR also contains an evaluation of the functionality of the new design board as compared to the original design boards. That is, TR Section 2.4.1.1, "New Design SAT Board Operations and Enhancements," states:

> "The new design SAT is designed as a drop-in, one-for-one replacement for the original design boards. All the basic functions and interfaces of the new design board are the same as those of the original design board."

The NRC staff compared a sample of the new design board functions to the original design board functions and did not find any discrepancies.

3.1.5 Clock Counter Board

The Clock Counter Board (CCB) in the SSPS has two functions in the system. The first function is to provide the basic timing clock-counter signals to generate the multiplexing addresses to pass trip and ESFAS actuation status from the logic boards to the main control board status and plant computer. The second function of the clock counter is to provide the basic clock and counter inputs to the SAT to generate the test pulse sequences to allow for testing of all the logic in the SSPS. The TR contains a description of the new design board in the following sections:

Section 2.5, Clock Counter Board
Section 5.1.5, "Clock Counter Board Simple Logic"
Section A.5, Clock Counter Board

The TR also contains an evaluation of the functionality of the new design board as compared to the original design board. That is, TR Section 2.5.2, "New Design CCB Operations and Enhancements," states:

> "The new design CCB is designed as a drop-in, one-for-one replacement for the original design boards. All the basic functions and interfaces of the new design board are the same as those of the original design board."

The NRC staff compared a sample of the new design board functions to the original design board functions and did not find any discrepancies.

3.1.6 Decoder Board

The Decoder (DEC) board function in the SSPS is to convert the clock counter bits to address signals used by the ULB in the train to pass data to the multiplexing portion of the ULB and in the Demultiplexer cabinets to generate the address to store the data in the memory boards. The TR contains a description of the new design board in the following sections:

Section 2.6, Decoder Board
Section 5.1.6, "Decoder Board Simple Logic"
Section A.6, Decoder Board

The TR also contains an evaluation of the functionality of the new design board as compared to the original design board. That is, TR Section 2.6.2, "New Design DEC Board Operations and Enhancements," states:

> "The new design DEC is designed as a drop-in, one-for-one replacement for the original design boards. All the basic functions and interfaces of the new design board are the same as those of the original design board."

The NRC staff compared a sample of the new design board functions to the original design board functions and did not find any discrepancies.

3.1.7 Memory Board

The non-safety Memory (MEM) board function in SSPS is to receive the multiplex data from the ULB in the train and store the data bits on trip and ESF actuations into single bit memory locations for display on the main control board and plant computer. The TR contains a description of the new design board in the following sections:

Section 2.7, Memory Board
Section 5.1.7, "Memory Board Simple Logic"
Section A.7, Memory Board

The TR also contains an evaluation of the functionality of the new design board as compared to the original design board. That is, TR Section 2.7.2, "New Design MEM Board Operations and Enhancements," states:

> "The new design MEM is designed as a drop-in, one-for-one replacement for the original design boards. All the basic functions and interfaces of the new design board are the same as those of the original design board."

The NRC staff compared a sample of the new design board functions to the original design board functions and did not find any discrepancies.

3.1.8 Isolation Board

The Isolation (ISO) board function in the system is to provide a Class 1E barrier between the safety-related logic and actuation signals and the non-safety indication signals used by the main control board and the plant computer. In addition the ISO board provides the Class 1E barrier between redundant SSPS trains. The TR contains a description of the new design board in the following sections:

Section 2.8, Isolation Board
Section 5.1.8, "Isolation Board Simple Logic"
Section A.8, Isolation board

The TR also contains an evaluation of the functionality of the new design board as compared to the original design board. That is, TR Section 2.8.2, "New Design ISO Board Operations and Enhancements," states:

> "The new design ISO is designed as a drop-in, one-for-one replacement for the original design boards. All the basic functions and interfaces of the new design board are the same as those of the original design board."

The NRC staff compared a sample of the new design board functions to the original design board functions and did not find any discrepancies.

The evaluation of the adequacy of this board as an isolation device is found in Section 3.9.2.6.3, "[IEEE 603] Clause 5.6.3, Other Systems."

3.2 Hardware Development Process

The NRC staff used the following regulations and guidance to review the development processes implemented in the design and production of the new design boards:

> The code at 10 CFR Part 50, Appendix B, Criterion VII, requires, in part, that measures shall be established to assure 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, objective evidence of quality furnished by the contractor or subcontractor, inspection at the contractor or subcontractor source and examination of products upon delivery.
>
> The code at 10 CFR Part 21 requires, in part, that the dedicated commercial equipment be deemed equivalent to equipment produced under a 10 CFR Part 50 Appendix B program.

The NRC Generic Letter (GL) 89-02 (ADAMS Accession No. ML031140060), "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products," provided the NRC's conditional endorsement of industry standard Electric Power Research Institute (EPRI) NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications" (ADAMS Accession No. ML14239A523).

This SE follows the form prescribed by DI&C-ISG-06, which includes separate sections for hardware and software development. This partitioning is the result of the process that is typical for computer based applications, where the hardware used is general purpose hardware (i.e., circuit cards) that was developed independently of the application software. For the new design boards, both hardware and software (i.e., used to configure the CPLD logic) were developed concurrently; therefore, the hardware development process is addressed as part of the software development process described in Section 3.4 below.

The new design boards were developed under Westinghouse's 10 CFR Part 50, Appendix B program. The Westinghouse Commercial Grade Dedication (CGD) process was used to address commercial components that were purchased and used in the new design boards. The adequacy of Westinghouse's CGD program has been previously addressed (outside of the TR evaluation). Some CGD documents associated with the new design boards were examined during the April 2014 audit (ADAMS Accession No. ML14183B483).

The following two subsections (3.2.1 and 3.2.2) document how Westinghouse audit activities addressed vendor controls with regard to the design vendor of the circuit boards, as well as the manufacturing vendors of the circuit boards. The NRC staff expected these vendor activities to be performed under the Westinghouse 10 CFR Part 50 Appendix B program. However, the NRC staff noted the design vendor produced commercial products and operated under Westinghouse's approved 10 CFR Appendix B program while the manufacturer vendors operated under their own 10 CFR Appendix B program. Components purchased for the fabrication of the new design boards were purchased commercially and dedicated under Westinghouse commercial dedication instructions (CDI) and various design and test procedures which were delivered though purchase orders to the manufacturer vendor. Also, in the case of the new design boards, the TR credits the interactions with these vendors as part of the commercial grade dedication process of EPRI NP-5253 as endorsed by Generic Letter (GL) 89-02 and the digital computer quality life cycle process of IEEE Std. 7-4.3.2 as endorsed by RG 1.152. The NRC staff also reviewed multiple receipt inspections of various new design boards to ensure that Westinghouse has a method in place to assure that commercial grade dedication activities are carried out correctly.

3.2.1 Design Vendor

Westinghouse considers the development of the prototypes of the new design boards to be a hardware design service and the design service was commercially dedicated in accordance with EPRI NP-5652. Westinghouse performed Commercial Grade Surveys (CGSs) and assessed the design vendor. A CGS is defined by EPRI NP-5652, as conditionally accepted by GL 89-02, as a means by which the purchaser can take credit for the commercial controls that the supplier exercises on an item, or service, to be commercially dedicated.

During the April 2014 audit (ADAMS Accession No. ML14183B483), the NRC staff examined the Westinghouse documented interactions with the design vendor. The NRC staff examined the documentation for the commercial grade surveys and design reviews.

The NRC staff made an observation regarding the hold points as identified in Section 4.5.2, "Design Hold Points," of Revision 0 of the TR. Westinghouse was not able to provide the NRC staff with auditable documentation of these particular hold points. These steps are design vendor hold points which are being credited as part of the life cycle management process as required by IEEE Std. 7-4.3.2 as endorsed by RG 1.152. In response to the audit, the PWROG updated the TR to refer to the hold points as “informal” to indicate that no credit for these activities is intended.

The initial CGS did not document the identification of the CPLD device or the identification and control of the CPLD and its associated application design tools, which the NRC staff believes to be critical attributes in the evaluation of this design vendor’s quality controls. This shortfall may have been because the initial specification by the design vendor envisioned the only on-board programmable logic device to be a CPLD. After initial CGS, Westinghouse began to actively monitor tool manufacturers for notification of error reporting and updates as stated in the TR.

TR Section 4.7 describes the design vendor involvement to be a service; however, the NRC staff considers the design vendor to be providing a product and these were the prototypes built by the design vendor in addition to the engineering services that interpreted the circuit board requirements to specify the CPLDs and the circuit board prototypes. Nonetheless, the NRC staff observed the three general characteristics of effective procurement and dedication programs as described by GL 89-02 which conditionally endorsed EPRI NP-5652. The three characteristics are: (1) engineering involvement in the procurement process; (2) product acceptance programs and utilizing appropriate testing; and (3) engineering-based program for the review, testing and dedication of commercial grade products.

However, the NRC staff also found documentation inconsistencies in confirming the critical characteristics, personnel qualifications, the design tools and the qualifications of the personnel using specific tools within the CGS of the design vendor versus what was identified by the TR and which should be done by the guidance of EPRI NP-5652. Since the current design phase is complete, as is the manufacturing phase (including testing) of many of the new design boards by a separate vendor, documentation becomes less of a concern. However, the need for complete documentation becomes important if a redesign of the CPLD becomes necessary—including its impact on the process for selection of another commercial design vendor.

3.2.2 Manufacturing Vendors

During the April 2014 audit (ADAMS Accession No. ML14183B483), the NRC staff reviewed the Westinghouse documented interactions with the manufacturing vendors. The NRC staff examined the commercial dedication instruction, qualified supplier listings, corrective actions, non-conformances, supplier quality program audit report and samples of purchase orders and certificates of compliance.

The TR Section 4.7, describes the comprehensive testing that was performed on the new design boards and this testing is equivalent to a Method 1, "Special Tests and Inspection," used

in the commercial grade dedication process. Section 4.7 of the TR identifies five critical characteristics to be verified. These are product identification verification; physical inspection; performance characteristics; environmental conditions qualification; and configuration control. Also, there are five critical characteristics (CCs) listed in Westinghouse's CDI document sent to the manufacturing vendor of the circuit boards through purchase orders for each type of new design board. The manufacturing vendor of the circuit boards is responsible for performing "product verifications," "physical inspection," and evaluation of "performance characteristics" of the new design boards. The last of the five CCs is "configuration control" which is verified by Westinghouse through a Method 2, "Commercial Grade Survey," of the manufacturing vendor of the circuit boards, which verifies that their manufacturer practices have acceptable supplier controls.

3.3 Software Architecture

Appendix C, "Westinghouse CPLD Operations White Paper," of the TR contains a description of the architecture of the CPLD and a description of the way that it is configured/programmed in order to be able to perform its application-specific functions. There are no application-specific architectural aspects of the CPLDs that require application-specific evaluations. The CPLD was evaluated by Westinghouse to determine its suitability for its intended use and was commercially dedicated by Westinghouse (see Section 3.2.2).

The evaluation of the software tools used for the CPLD development is addressed under the evaluation against IEEE 7-4.3.2 Clause 5.3.2 (see Section 3.10.1.1.2, "[IEEE 7-4.3.2] Clause 5.3.2, Software Tools").

3.4 Development Process

For the TR, the NRC staff used the following regulatory requirements and guidance to evaluate the development process:

> The regulations in 10 CFR 50.55a(a)(1) addresses Quality Standards for Systems Important to Safety: "Structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed."
>
> The regulations in 10 CFR 50.55a(h)(3), "Safety Systems," incorporate IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995 into the federal regulations by reference.
>
> The regulations in GDC 1, "Quality Standards and Records," state: "Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed…"
>
> The regulations in 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants," Criterion I, "Organization," require in part that the applicant shall be responsible for the establishment and execution of the quality assurance program.

The regulations in 10 CFR Part 50, Appendix B, Criterion III, "Design Control," require, in part that, for safety-related structures, systems, or components (SSCs), quality standards be specified and that design control measures shall provide for verifying or checking the adequacy of design.

The regulations in 10 CFR Part 50, Appendix B, Criterion V, "Instructions, Procedures, and Drawings," require, in part that, for safety-related SSCs, activities affecting quality shall be prescribed by documented procedures of a type appropriate to the circumstances.

The regulations in 10 CFR Part 50, Appendix B, Criterion XI, "Test Control," require, in part, that a test program be established to demonstrate that safety-related systems and components will perform satisfactorily in service.

The regulations in 10 CFR Part 50, Appendix B, Criterion XV, "Nonconforming Materials, Parts, or Components," require in part that measures be established to control materials, parts, or components which do not conform to requirements in order to prevent their inadvertent use or installation.

RG 1.152, “Criteria for Use of computers in Safety Systems of Nuclear Power Plants,” endorsed IEEE Std. 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Clause 5.3.1 of IEEE Std. 7-4.3.2, “Software Development,” provides guidance.

RG 1.173, Revision 1, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to the development processes for safety system software.

BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems.”

Additional Guidance on NRC staff positions regarding Programmable Logic Devices is contained in DI&C-ISG-04 Revision 1, “Highly-Integrated Control Rooms – Communication Issues,” and DI&C-ISG-06, “Licensing Process,” provides review criteria.

Background on the SSPS Circuit Board Redesign Regarding Software:

In June of 1997, the NRC staff issued Revision 4 of Human Factors Instrumentation and Control Branch 14 (predecessor to BTP 7-14, Revision 5) “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems” (ADAMS Accession No. ML052500547). By letter dated July 17, 1997, the NRC staff issued a SE of the EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" (ADAMS Accession No. ML12205A284). The NRC staff determined that EPRI TR-106439 contains an acceptable method for dedicating commercial grade digital equipment. This guidance also applied to “the dedication of replacement parts for a piece of equipment when those parts contain digital components.” In the SE on EPRI TR-106439, the NRC staff stated:

> "The NRC staff considers verification and validation activities common to software development in digital systems to be critical characteristics that can be verified as being performed correctly following the completion of the software development by conducting certain dedication activities such as audits, examinations, and tests."

Subsequently, in September of 1997, the NRC staff issued six new RGs (Nos.: 1.168, 1.169, 1.170, 1.171, 1.172, and 1.173). These six new regulatory guides endorsed eight IEEE Computer Society standards on the software life cycle process for software used in safety systems.

By letter dated April 10, 2001 (ADAMS Accession No. ML011130215), the Westinghouse Owners Group docketed the approved version of WCAP-15413-A, Revision 0, "Westinghouse 7300A ASIC-Based Replacement Module Licensing Summary Report." This report includes the NRC staff SE of the report that was docketed by letter dated June 21, 2000. Neither the TR nor the NRC staff SE referenced any software related guidance.

During the review (March 2007 – March 2009) of the Wolf Creek Generating Station license amendment regarding the Main Steam and Feedwater Isolation System controls (ADAMS Accession No. ML090610317), the NRC staff documented its position that logic development using software should be treated in accordance with high quality software development processes. Further, in the initial issuance of DI&C-ISG-02 in September of 2007 (ADAMS Accession No. ML072540118), the NRC staff clearly documented its position that the term software is understood to include "logic developed from software-based development systems."

The only referenced digital standard in Revision 0 of the TR was IEEE Standard 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

3.4.1 NRC Staff Approach to the Evaluation of the Development Process

The NRC staff's initial review and audit of the TR information identified a significant inconsistency between the perceived need within the industry for use of DI&C development standards and those endorsed and viewed as appropriate by the NRC staff. This dichotomy posed a challenge for the review by comparison of DI&C guidance and standards to a development process that was not considered to be a digital technology component, and therefore, not intended to meet the DI&C standards at the time of development.

The most critical source of objective evidence available for the NRC staff's review of the new design boards was the comprehensive testing conducted during the design and manufacturing activities. An evaluation of this evidence was included in the NRC staff review of the scope of the design and manufacturing tests (see Section 3.4.3.2, "Testing Activities") and the review by the NRC staff of eliminating consideration of common cause failure (CCF) in (see Section 3.6, "Defense-in-Depth and Diversity").

Based on the NRC staff's initial evaluation of the limited degree of conformance to DI&C guidance and standards, the NRC staff determined that further pursuit of "docketable" information in support of consistency with these standards and guidance documents would provide limited results. However, it was found that the applicant's development program

included a testing program of comprehensive scope and volume, as described in the TR. In order for the NRC staff to be able to reach a final safety determination, the NRC staff considered that careful evaluation of the applicant's comprehensive testing program could serve to compensate for the limited information found during the NRC staff's qualitative evaluation of the development process to demonstrate consistency with the DI&C review guidance documents. Although the NRC staff's normal evaluation process is to evaluate the applicant's description of the compliance of the development process against current guidance and endorsed industry standards, for this unique situation, the NRC staff evaluated the applicant's program against the underlying regulations. This was done by applying judgment in the evaluation of each of the significant developmental activity groups, with their associated characteristics, to make a compliance determination as to whether a careful and deliberate development process was employed for the digital technologies adopted. This approach should also be applicable to any careful and deliberate development process, regardless of the technology, that results in a high-quality product suitable for use in safety-related systems in nuclear power plants.

The NRC staff considers three groups of activities to be applicable, regardless of the technology or degree of software involved that will result in a high quality product. The NRC staff's determination was constructed upon (1) confirmation that acceptable plans were prepared to control development activities, (2) evidence that the plans were implemented in an acceptable process, and (3) evidence that the process produced acceptable design outputs. The acceptance criteria used by the NRC staff for its evaluation process is divided into three activity groups: planning; implementation; and design outputs. The NRC staff's evaluation of the development process was conducted in those three major areas as described in the subsections below (i.e., Sections 3.4.2, 3.4.3, and 3.4.4). Within this evaluation, the specific issues or concepts drawn from the review of software development processes and determined to be applicable are sometimes identified as "(digital)" or "(software)." Characteristics within those activity groups which are maintained from the software-centered reviews are highlighted based on NRC staff justification that these characteristics are also applicable to any careful and deliberate development process, regardless of the technology implemented. This effort to identify such key characteristics by the NRC staff was necessitated due to the unique situation of performing a licensing evaluation for a product that had already been developed and manufactured without using the endorsed standards within the staff's applicable Regulatory Guides or generally recognized codes and standards for the technology employed.

3.4.2 Planning Documentation

A (software) life-cycle is a project-specific, sequenced mapping of activities per RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." The purposes of the mapping are to permit execution of related activities and portions of activities and to provide staged points at which product and process characteristics are verified during the development process. In this case, it is expected that although a "software life cycle" was not intended, many product and process characteristics were similar as they are not technology specific but consistent with NRC staff guidance. Test planning activities, when found to be acceptable, provide the reviewer with additional criteria for reviewing the testing process activities, as discussed below.

3.4.2.1 Test Planning Documentation

This subsection addresses acceptance criteria for the test planning activities. The acceptance criterion for a (software) test plan is contained in the Standard Review Plan, BTP 7-14, Section B.3.1.12, "Software Test Plan," and in Section B.3.2.4, "Acceptance Criteria for Testing Activities." The acceptance criteria that the NRC staff uses in reviewing plans are divided into three sets: management characteristics; implementation characteristics; and resource characteristics. Each of these is further divided into specific characteristics as the NRC staff evaluation below indicates.

The test planning portion of the process from development through manufacturing of the new design boards can be divided into two sections as they are discussed here. The first is the plan to cover the testing performed by Westinghouse of the prototypes which were designed and built by the design vendor; this is identified in the "Design Test Planning" section below. The second section is the "Manufacturing Testing" which was performed by the manufacturing vendor for the CGD of the manufactured new design boards.

3.4.2.1.1 Design Test Planning

The following documentation was relied upon for reference to the activities associated with the design test planning. In particular, this information represents the test planning and procedure hierarchy for the ULB circuit board. The test planning and procedure hierarchy for the ULB circuit board is representative of the type and scope of the test planning and procedure documents for the eight circuit boards included in this upgrade effort. Only TDH-121803-001, Revision 2, "Project Plan SSPS Circuit Boards Re-Design," is common to all circuit boards.

Table 3.4.1.1 Docketed SSPS Re-design Test and Test Planning Documentation

Document ID	Title	Reference
418A49, Revision 4	Design Specification Universal Logic Board Redesign	1
TDH-121803-001, Revision 2	Project Plan SSPS Circuit Boards Re-Design	2
UL-TP-TDH-001, Revision 2	Universal Logic Board Design Test Plan	3
1TS2870, Revision 1	ULB Functional Test Procedure	4
1TS2868, Revision 0	ULB 6D30225 Test Decomposition Procedure	5
1TS2871, Revision 0	ULB System Tests Procedure	6

The NRC staff considers the management characteristics of the (Software) Test Plan should exhibit the purpose, organization and responsibilities. The "Project Plan SSPS Circuit Boards Re-Design" as well as providing a general project purpose and overview for the design (not manufacturing activities) identified the general design and testing tasks (i.e., design, qualification, and Electromagnetic Compatibility (EMC)) of all the circuit boards as well as the organization of teams or groups responsible for those activities. This document also provided a

two-phased approach to the testing process. The first phase was the test (and design) of the Protection Function boards which are those boards used to pass the safety-related actuation signals through the SSPS. The second phase was the test (and design) of the Non-Protection Function boards which are those boards used to provide indication of the system status and testing interface. The plan assumed the design organization was ultimately responsible for and sole implementer of the design and testing with the exception of the environmental qualification testing which was identified for a different group. There was no identification of a V&V organization or individuals selected to perform the V&V functions.

The implementation characteristics of the test plan should identify the means of measurement (i.e., criteria), procedures and record keeping capabilities. The testing strategy is described in the individual circuit board test plans, using the ULB plan as an example. These plans discuss the test topics of functional and system test procedures, how they were generated and what the intentions of the tests were. The requirements in the "Design Specification for the Universal Logic Board Redesign" are decomposed into specific test cases in the "ULB 6D30225 Test Decomposition Procedure." This test decomposition document determines which of the requirements listed in the design specification are testable, assigns a requirement number to the requirement, and provides guidance for type of test required to ensure the board functions as stated in the design specification.

Once the "ULB 6D30225 Test Decomposition Procedure" was completed, the test procedures were developed using the guidance from this document. The type test can be either a functional test or it can be assigned as a system test as each circuit board had a functional test procedure. For the ULB the type test is the "ULB Functional Test Procedure" executed at the circuit board level as well as a system test procedure, "ULB System Tests Procedure" for testing each circuit board in an SSPS system. The functional test uses a static input test box and is used to verify the circuit board's fundamental operations. SSPS system schematics were used to determine every possible arrangement of new design and original design boards in the system. From those combinations the test cases were developed to generate the system functional test procedure. The system tests are those tests where board interfaces and interaction within the system are tested. Not only are the board functions re-tested in the system, but the test is performed in the same operating environment and with the same interfaces as seen during plant operation. These system type tests include all the requirements that the board must be able to operate with and with any new or original design board operating in the system.

During the initial audit in New Stanton, Pennsylvania, the NRC staff reviewed the functional test procedure for the ULB circuit board to verify that all test criteria are specified for each testing task.

Also part of the record keeping characteristics should be a description of the testing record requirements for control and managing test cases and the procedures involved so that the revision history of each item may be retrieved, and the latest revision of each item may be easily identified. The NRC staff review found the documents are archived in the Enterprise Document Management System (EDMS) per Westinghouse Level 2 procedures WEC 17.1 (Records) and WEC 6.1 (Document Control).

The resource characteristics that the Test Plan should exhibit include the methods and tools to facilitate the performance of the testing as well as any standards and guidelines to be followed by the testing organization. The ULB Test Plan explains that as part of the design vendor deliverables Westinghouse received a test box, which is the primary tool used to perform the functional test procedure. The Test Plan document includes the discussion of the facility to complete the individual circuit board system tests that had to be done on equipment that required simulation of system input trip conditions, as well as methods to view outputs from the system. The project plan, design specification or testing documents did not reference the necessary external standards or guidelines such as IEEE standards endorsed, or incorporated by reference (e.g. IEEE Std. 603 or IEEE Std. 279), by the NRC which are necessary to meet regulatory requirements. This reference to standards and regulatory requirements should be done at the planning stage so that the necessary traceability is documented and verified for regulatory requirements, not just technical requirements. This point is also discussed in Section 3.4.4, “Design Outputs.”

3.4.2.1.2 Manufacturing Test Planning

The following documentation was relied upon for reference to the activities associated with the manufacturing test planning.

Document ID	Title	Reference
418A49, Revision 4	Design Specification Universal Logic Board Redesign	7
TDH-121803-001, Revision 2	Project Plan SSPS Circuit Boards Re-Design	2
UL-TP-TDH-001, Revision 2	Universal Logic Board Design Test Plan	3
CDI-3015, Revision 3	Commercial Dedication Instruction for the Universal Logic Board 6D30225	8
1TS2958, Revision 3	Universal Logic Board 6D30225G01/ G02 G03/ G04 Configuration Procedure For Manufacturing and Repair	9
1TS2963, Revision 4	Universal Logic Board 6D30225G01/ G02 G03/ G04 Functional Test Procedure for Manufacturing and Repair	10

The planning documents and the associated implementation activities of the various vendors should be coordinated in one complete plan. The “Project Plan SSPS Circuit Boards Re-Design,” and the “Universal Logic Board Design Test Plan,” discussed only activities associated with the design vendor and the related testing activities. The “Design Specification for the Universal Logic Board Redesign,” describes the general specifications and activities for both the initial development phase done by the design vendor, as well as the production phase for the manufacturing vendor.

The manufacturing process includes a commercial grade dedication instruction that is completed by the Westinghouse-approved Appendix B supplier that manufactures the circuit boards. The NRC has inspected the New Stanton, Pennsylvania facility in the past for appropriate use of inspection and commercial supplier acceptance methods involved in commercial grade dedication. There was no planning documentation describing the manufacturing process.

The NRC staff has provided an SE (ADAMS Accession No. ML12205A284) on the use of EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," as a description of an acceptable method that licensees or applicants may use dedicating commercial grade digital equipment for use in nuclear power plant safety applications and meets the requirements of 10 CFR Part 21. The NRC staff's SE is consistent with the industry's recommendation that three of the four methods, from EPRI NP-5652, should be the basis for commercial dedication of digital devices. They are: (1) special tests and inspections, (2) commercial grade survey of supplier, and (4) acceptable supplier/item performance record.

Westinghouse chose not to reference EPRI TR-106439 primarily because the company believes conformance to critical characteristics can be verified strictly by Method 1 (Special Test and Inspection) and Method 2 (Commercial Grade Survey of Supplier). Method 4 was believed to be strictly categorized as "Dependability." The NRC staff does not agree with the strict categorization of Method 4 and does not agree that the processes described in EPRI TR-106439 should not be applicable. As the industry document states, this method also included characteristics related to problem reporting and configuration control. These types of characteristics and the basis of engineering judgment, to use them or not, should be documented by the dedicating organization during the process.

If this were a matter of a review of the plans to minimize risk before the product was manufactured and tested, thorough documentation of not only the vendor performance record but the product operating history and the use of EPRI TR-106439 would be recommended by the NRC staff. During the planning process, risk should be minimized as much as possible for commercially developed digital devices. These considerations are applicable for future redesigns of these circuit boards. Risk is further discussed in Section 3.10.1.1.6, Clause 5.3.6, "Software Project Risk Management."

The purchase order is the governing document for the requirements to the manufacturing vendor. The purchase order includes the assembly drawing, artwork Gerber files, configuration file for the CPLD, the CDI (Reference 8) and all of the controlled procedures to build, configure, test, burn-in, then re-test and dedicate the board for use as a safety-related item. The CDI (Reference 8) includes five critical characteristics: identification, inspection, equipment qualification, performance characteristics and configuration control. The performance characteristics include the manufacturing test, then burn-in, and then performing the manufacturing test again. To minimize infant mortality issues, the new design boards are burned in at power and load for 100 hours at 60 degrees Celsius (ºC). The burn-in loads all inputs to the low level for 50 hours and then loads all the inputs to the high level for 50 hours. When burn-in is completed, the manufacturing test is repeated. Data sheets from both pre-burn-in and post burn-in manufacturing tests become part of the quality assurance (QA) package for the manufactured board.

The test planning should describe the method of reporting and resolving anomalies, including the standards for reporting an anomaly and the authority for resolving anomalies as well as the procedures that govern the process. Each new manufactured circuit board is commercially dedicated per Westinghouse Level 2 procedure WEC 7.2 (Dedication of Commercial Grade Item). Non-conformances are addressed through Westinghouse Level 3 procedure Repair and Replacement Service Center (RRSC)-415 (Control of Material Deficiencies) and Level 2 procedure WEC 15.1 (Deviation Notices). Per RRSC-415, where the nonconformance relates to boards returned from a customer, a review will be made by Engineering to determine whether a significant deficiency, unreviewed safety question or substantial safety hazard exists and is documented in the Corrective Action Program Level 2 procedure WEC 16.2. All required documentation is retained per WEC 17.1 (Records) in the Westinghouse EDMS.

Also, test planning should consider appropriate guidance or procedures on regression testing requirements, specifying the conditions (including design changes and repairs) under which all the original acceptance tests should be re-performed, or the criteria for performing a carefully selected and justified subset of the acceptance tests. Westinghouse has procedures, (Nuclear System Protection System 11.1 (Test Control) and Nuclear Automation 4.28 (Request for Engineering Change)), which provide steps for identifying potential design issues and implementing design changes. Regression testing planning is subject to engineering judgment and peer review during the design change process referenced in the above procedures. Engineering must evaluate the extent of testing required for a change on a case by case basis. Any repair under warranty will generate the creation of a correction action issue (WEC 16.2, “Westinghouse Corrective Action Program”). Any plant issue, not necessarily a repair, would be subject to engineering review and corrective actions implemented in accordance with the issue. Evaluation and completion of the corrective action for a design change would follow the process described in the TR in Section 4.5.4.2 and depicted in Figure 4-4.

The TR Section 4.5.4.2, Figure 4-4 (steps 24 – 29) shows the continuous process for possible design change issues being used once the design has been released for production. The figure does not specifically address procedures to follow, but step 28 does specifically state to implement design changes per design change procedures. Westinghouse uses repair reports, issues raised at PWROG I&C Working Group meetings, and direct contact with the licensees to determine if an issue exists.

All changes to the circuit board design require the assembly drawing to be revised per WEC 5.5 (Preparation and Control of Drawings and Sketches) where the following is evaluated:

Ambient Specs	Seismic Specs	Verification Report	System Application
Environmental	EMI/EMC	Time Response	Design Specs

The individual circuit board test plan documents provide the plan outline of the steps required to complete the testing of the design. These documents outline the plan to perform an analysis to develop test case documents, develop functional and system tests, and qualification tests.

All subsequent testing activities such as site acceptance testing and installation or surveillance testing are considered to be the responsibility of the licensee and are therefore not within scope of the testing plan and activities described by the TR or addressed by this SE.

In conclusion, the test procedures and associated documents prescribe the scope, approach and schedule for a plan of the design vendor testing activities and they identify the new SSPS circuit board features and the means to which they are to be tested. The NRC staff found documentation ambiguity in the initial selection of the technology used by the design vendor and the review of that vendor's design tools used. The NRC staff found a deficiency in the organization plans because they did not identify personnel who perform verification and validation functions that were independent to the group that developed the product. Also, throughout the test documents and plans the NRC staff observed an absence of appropriate standards used to meet regulatory requirements. This was particularly evident for standards related to digital technology as was expected given the premise at the beginning of the project that the CPLD was not considered by Westinghouse to be a digital device. These concerns are addressed in the NRC staff's conclusions for this section (Section 3.4.5).

3.4.3 Implementation Documentation

This subsection addresses acceptance criteria for implementation activities. The acceptance criteria address specific (software) life cycle process implementation activities and documentation. These activities and products, when found to be acceptable, provide the reviewer with confidence that the plans have been carried out. A principal measure for the acceptance criteria in the implementation activities is that the NRC staff confirms that the plans have been followed by the (software) developer.

3.4.3.1 V&V Analysis and Reports

Rigorous V&V should be integral to this process to provide reasonable assurance that the resulting system will perform its safety function in a predictable and reliable manner. For the review of this TR, the NRC staff determined direct compliance to the following regulations:

> 10 CFR Part 50, Appendix B. Criterion I, "Organization," requires in part, that individuals and organizations performing QA functions have sufficient authority, organizational freedom, and independence from cost and schedule.
>
> 10 CFR Part 50, Appendix B, Criterion III, "Design Control," imposes in part an independence requirement for the verification and checking of the adequacy of the design, requiring that those who perform the verification and checking be persons other than the designers.

The NRC staff conducted the second audit of the new design activities on July 15-17, 2014 at the Westinghouse office in Rockville, Maryland. Of particular importance related to V&V reviews was the NRC staff observation that there was inconsistent independence of the verifiers performing a V&V activity, as required by 10 CFR 50 Appendix B, involved in both design and testing activities. The PWROG took an action item to provide possible V&V activities that could be credited towards meeting this requirement.

As a result of the audit action item regarding the independence requirement of V&V activities, Section 5.5, "Independent Confirmation of Testing," was added to the TR. In this section a summary of the test methods employed was provided. This is inclusive of the testing done by Westinghouse during the design process and the testing done by the manufacturing vendor

which was previously included in the TR. This section further describes the details of the Utility Beta Test Program as well as the plant post installation and surveillance test procedures that demonstrate operability of the SSPS following installation of the new design boards.

The NRC staff considers the post installation test as an effective means of providing an additional measure of independent testing (i.e., assurance to meeting the requirements). Therefore, the NRC staff has identified a plant specific action item (4.2.4) to require a post installation test is performed to demonstrate proper system function(s) associated with the affected card slots following the installation of one or more new design ULB, UVD, SGD and/or SAT printed circuit boards in either SSPS train. The post installation test is satisfied by the performance of an Actuation Logic Test Surveillance, or an equivalent logic test, which demonstrates the operability of the SSPS, as required by the plant Technical Specifications.

The PWROG has formed the SSPS Replacement PCB Utility Core Group which operates independently from Westinghouse. A subset of the Utility Core Group conducted the new design board beta test program. The beta test program objectives were to fully exercise and challenge each board type in various plant environments and to ensure the accuracy and usability of supporting board assembly and schematic drawings as well as instructions, bulletins and technical manuals. Bench tests were performed using existing site procedures and fixtures used for the original design boards, some with licensee designed test boxes, others were done with the Westinghouse supplied test box. The system tests were organized in various combinations of the new design boards and original design boards but also included the new design boards in actual system operation for several months.

These utility/PWROG reviews and beta tests were self-directed by plants, autonomous of Westinghouse, and therefore provide an additional degree of independence demonstration with respect to verifying the adequacy of the design. Since the consistency of the procedures, acceptance criteria and test environments have not been reviewed by the NRC staff nor can they otherwise be addressed, this can only be considered an additional factor in judging whether there is reasonable assurance for the independence requirement and obviously not the only factor.

Also, as part of a (digital) V&V effort, a traceability analysis should be performed and documented. The traceability analysis documentation should show the linkage between each requirement imposed (on the software) by the system requirements document and system design documents, and one or more requirements in a (software) requirements specification. In the case of the new design boards, Westinghouse decomposed all the circuit board design requirements to identify what requirements are to be verified by test. This would also be considered a part of the (software) validation activities which demonstrate that all validation tests required (usually by a software V&V plan) were successfully completed. The result was the testing process was shown to contain one or more tests for each testable requirement in the design specification, as well as the acceptance criteria for each test. The result of each test showed that the associated requirement had been met.

A summary report of all validation testing was also developed. As recommended by the NRC staff (digital) guidance on the acceptance criteria for V&V activities, this would typically identify any possible errors encountered during testing, the actions taken to correct the problems encountered and any additional analysis that may be required to provide information on the

acceptance or rejection of the testing issues and how they affect the ability of the tests to detect any issues that may have been introduced in the design process. This report included a summary of tests and any additional analysis used to determine the validity and quality of the new design boards to be used in the system. The conclusion was that the validation testing identified no issues that could affect the new circuit board design from meeting the requirements and operating conditions of the original circuit board design.

The NRC staff concludes with reasonable assurance that the V&V effort has adequately traced acceptance criteria for each testable requirement and concluded that no issues have been introduced in the design process that may affect the new design circuit boards from meeting the requirements and operating conditions of the original circuit boards. Also, sufficient independence has been demonstrated with regards to the entities performing the checking function inclusive of the Utility Beta Test Program and the plant specific action item (4.2.4) to demonstrate SSPS operability following the installation of one or more new design ULB, UVD, SGD and/or SAT printed circuit boards in either SSPS train. The post installation test is satisfied by the performance of an Actuation Logic Test Surveillance, or an equivalent logic test, which demonstrates the operability of the SSPS, as required by the plant Technical Specifications.

3.4.3.2 Testing Activities

SRP Chapter 7 BTP 7-14 Section B.3.4 contains SRP acceptance criteria and references to applicable guidance (see also Section D.4.4.1.12):

> RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," with a few noted exceptions, identifies acceptable methods for addressing computer system qualification testing (See: IEEE Std. 7-4.3.2-2003 Clause 5.4.1, “Computer System Testing”).

The (software) development process characteristics listed below should be exhibited by testing activities per BTP 7-14:

Completeness means that all required functionality for all operating modes, including error recovery be tested.

Consistency means that the testing is consistent with the safety system requirements, the safety system design, the (software) requirements specifications, the (software) design specification, and documented descriptions and known properties of the operational environment within which the safety system will operate. Uniform and consistent terminology, notation, and definitions should be used throughout.

Traceability means that traces exist between the requirements, design and the test documentation, which shows how each requirement is tested.

As discussed in the Design Test Planning Section (3.4.2.1.1), Westinghouse conducted a comprehensive set of functional and system operational tests on the prototypes from the design vendor to ensure that the design of the new design boards met the requirements to be used as

circuit board replacements in the SSPS. These tests included sequenced testing of the logic and of the support circuits to ensure they function as intended. The design cannot be changed without affecting the revision level of the controlled file. Once the verification testing and design analysis was complete, the CPLD configuration files were placed into the Westinghouse EDMS.

The results of the manufacturing tests provide reasonable assurance that the manufacturing process has not introduced an error or deficiency that could ultimately affect the safety function of the new circuit board. The manufacturing tests are a subset of the design validation tests and are selected to ensure the circuit board functions as intended and is the same configuration as the one tested by the design validation. Westinghouse provides a comparison of the design functional tests and the manufacturing functional tests procedure in Table 4-2 of Section 4 of the TR. A justification is provided to explain why particular tests were included in the design testing but not in the manufacturing testing. Within the table, there are several design tests which are not performed following manufacturing and Westinghouse recommends as a secondary or second verification, a post installation actuation logic test to demonstrate that different characteristics or requirements are met. This verification is the post installation system test that shall be performed following the installation of one or more new design ULB, UVD, SGD and/or SAT printed circuit boards in either SSPS train. The post installation test is satisfied by the performance of an Actuation Logic Test Surveillance, or an equivalent logic test, which demonstrates the operability of the SSPS, as required by the plant Technical Specifications. This is plant specific action item 4.2.4 (Section 4.2.4). The NRC staff requires the use of post installation tests to demonstrate the manufactured circuit boards have been equivalently tested to the criteria of the design functional testing. This is in support of the same plant specific action item identified above in Section 3.4.3.1, V&V Analysis and Reports.

In addition, during the initial audit by the NRC staff in New Stanton, Pennsylvania; members of the PWROG performed a peer review of the “Universal Logic Board 6D30225G01/G02/G03/G04 Functional Test Procedure for Manufacturing and Repair.” The objective of the industry peer review was to confirm the manufacturing test procedure includes sufficient functional tests and performance characteristic measurements to demonstrate that each new production ULB performed its design basis functions. The industry peer review confirmed the test procedure in Sections 3.0 - 10.0 included sufficient instructions, functional tests, and voltage measurements to demonstrate the new design ULB protection and information design functions. The review also confirmed the procedure includes sufficient tests and measurements to demonstrate proper operation of the ULB including board edge status indications, and the voting logic self-test failure alarm.

The NRC staff has reasonable assurance that the required functionality of the new design boards has been tested. The reasonable assurance of the testing for the manufactured circuit boards is inclusive of the post installation test as a plant specific action item (4.2.4). The post installation test will be performed following the installation of one or more new design ULB, UVD, SGD and/or SAT printed circuit boards in either SSPS train. The post installation test is satisfied by the performance of an Actuation Logic Test Surveillance, or an equivalent logic test, which demonstrates the operability of the SSPS, as required by the plant Technical Specifications. All functional circuit board testing is complete with regard to the prototypes being tested to the original design circuit board functional requirements. The SSPS system testing was consistent with the existing safety system design description and the new design boards were verified to operate within the same system parameters as the original design

boards. Uniform and consistent terminology, notation, and definitions were used throughout the testing process. Traceability of requirements was established between the new circuit board design specification and the test procedures which demonstrated how each requirement was tested.

3.4.4 Design Outputs

This subsection describes the criteria that should be used to assess whether the product (software) has each of the characteristics for safety system components. Acceptance criteria are divided into two sets for Design Outputs: functional characteristics and process characteristics. Each of these characteristics is subdivided into additional characteristics. However, not all characteristics identified in NRC staff guidance occur for every design output.

For functional characteristics, the NRC staff reviewed functionality and reliability sub-characteristics. The functionality of the proposed system or components should be compared to the system requirements. The design specification included the system requirements from the original SSPS system description, system standard and the circuit board schematic drawings. There is a separate document for each circuit board which decomposes the design specification requirements which can be tested into a functional test or a separate system type test to ensure that the functional requirements are met. The NRC staff has reasonable assurance the functionality of the circuit boards has been evaluated and tested to meet the system requirements.

The reliability of the new design boards has been addressed by separate documents for each circuit board. For the ULB, this is documented within “Failure Mode and Effect Analysis for Solid State Protection System Module Universal Logic Board” and “MTBF [Mean Time Between Failure] Estimate for Solid State Protection System Module Universal logic Board 6D30225.” The NRC staff conducted the first audit on April 7-11, 2014 at the Westinghouse New Stanton, Pennsylvania facility (ADAMS Accession No. ML14183B483). There the audit team examined the MTBF calculations for the each circuit board and confirmed the duty cycle numbers in Table 9-1 of the TR with the values in the corresponding documents. Also, the NRC staff confirmed the calculated MTBF for the new design circuit boards is an improvement over the original design circuit board design.

Based on this review, the NRC staff has reasonable assurance the new design boards are a more reliable upgrade to the original design circuit boards and include the necessary functional characteristics for the safety system to perform its safety function.

There are many process characteristics that can be used for this application to determine that the design outputs have been completed effectively. These included completeness, consistency, correctness style, traceability and verifiability.

Revision 1 of the TR includes a Regulatory Requirements Matrix to ensure that all applicable regulatory requirements were indeed adequately addressed by the application. This has provided a complete and clear method of analysis which will support the NRC staff’s final reasonable assurance determination. The consistency between the tools and testing methods used in the design and manufacturing sections of the project are thorough and understandable to the level of identifying the differences in the type tests done on each circuit board during the

design vs. manufacturing test phases. The consistency between the original and new design circuit boards, and therefore the simplicity of the functional aspects has been maintained. The intent to require no system input or output interface changes and integration of original vs. new design boards has been a controlling point throughout the development and manufacturing process. There are two interfacing issues when the new circuit boards are installed as identified in Section 4.1.2 of the TR. The NRC staff's thorough review and discussions with Westinghouse lead to a conclusion that these are multiplexing technical issues associated with plant-specific operating procedures and computers and there are no safety concerns associated with the installation of original and new design boards in the same system. These technical issues, with regards to replacing the ULB and MEM boards, are also thoroughly described in the updates to the SSPS technical manuals.

The style of design output documentation is generally acknowledged by the planning documents. The style of the planning documents is generally determined by the requirements for those documents, such as IEEE standards endorsed, or incorporated by reference, by the NRC and applicant requirements. The NRC staff identified previously that the planning documents and design specification did not reference any external standards or guidelines including those necessary to meet the appropriate regulatory criteria (e.g., IEEE Std. 603 or IEEE Std. 279) not related to equipment qualification. Again, this was particularly evident for standards related to digital technology as was expected given the premise at the beginning of the project that the CPLD was not considered by Westinghouse to be a digital device.

3.4.5 Regulatory Summary of the Development Process

The application is a unique situation in that digital development process guidance was not considered to be applicable from the beginning of the project and therefore the NRC staff's resulting review approach relied more heavily on NRC staff engineering judgment, as opposed to the use of available NRC staff guidance, in the determination of whether these requirements are met.

As described by Section 2.0, "Regulatory Evaluation," of this SE, the first two sentences of GDC 1 are evaluated and are applicable to the development process as well. The first sentence states, "Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed." At least for the extent of the development process, this is identical to and will be evaluated with 10 CFR 50.55a(a)(1) and IEEE 603-1991, Clause 5.3.

Westinghouse has an NRC-approved 10 CFR 50 Appendix B quality assurance program which was evaluated separately. The NRC staff has reviewed the audits performed by Westinghouse of both the design vendor and the manufacturing vendors prior to placing them on the approved suppliers list during the development and manufacturing processes. In the NRC staff's opinion, the technical enhancements, which the NRC staff has reviewed as well as Section 2.0 of the TR, will contribute to the improvement in reliability and maintainability of the circuit boards resulting in improved quality. These determinations meet the guidance acceptance criteria in SRP Chapter 7, Appendix 7.1-C, Section 5.3, "Quality;" therefore, the SSPS circuit board upgrade conforms to this requirement of GDC 1.

The second sentence of GDC 1 is partially addressed by the NRC's incorporation of standards by reference into 10 CFR 50.55a (e.g., IEEE Std. 603 or IEEE Std. 279) or their endorsement (e.g., through RGs). Other generally recognized codes and standards that are used should be identified and evaluated to determine their applicability, adequacy, and sufficiency.

For this application by reference to 10 CFR 50.55a, IEEE 603 has been invoked and included in the TR only. There are a few endorsed standards or generally recognized codes and standards applicable to the Environmental Equipment Qualification effort (see Section 3.5 below). However, the endorsed standards (those by regulatory guides or NRC staff guidance) that are applicable to digital technologies were not adequately identified as discussed in the front matter of this section.

Consistent with the NRC staff's review approach (see Section 3.4.1, "Staff Review Approach to the Development Process"), the NRC staff concerns identified in the test planning documentation (see Section 3.4.2, "Planning Documentation,") are adequately compensated for by the NRC staff review of the scope of the design and manufacturing tests (see Section 3.4.3.2, "Testing Activities") and the review by the NRC staff of eliminating consideration of CCF (see Section 3.6, "Defense-in-Depth and Diversity"). Therefore, for the purposes of the development process, and with the emphasis on the testing procedures and activities, the NRC staff has determined with reasonable assurance based on the review and audits of the plans, procedures and testing results, as identified above, that the development process has met the requirements of 10 CFR Part 50 Appendix B, Criteria V, "Instructions, Procedures, and Drawings," XI "Test Control," and XV "Nonconforming Materials, Parts, or Components."

10 CFR Part 50 Appendix B, Criterion I, requires that persons and organizations performing quality assurance functions report to a management level such that sufficient authority and organizational freedom exist, including sufficient independence from cost and schedule limitations. Quality assurance functions include verifying, such as by checking, auditing, and inspecting, that activities affecting the safety-related functions have been correctly performed. Criterion III imposes an independence requirement for the verification and checking of the adequacy of the design, requiring that those who perform the verification and checking be persons other than the designers.

The NRC staff considers that the design and testing process within the Westinghouse scope did not have adequate independence of the verifiers performing the V&V activities to meet requirements of 10 CFR 50 Appendix B, Criterion I and III. However, the NRC staff has considered the additional independent activities conducted under the Utility Beta Test Program and the post installation test that shall be performed following the installation of one or more new design ULB, UVD, SGD and/or SAT printed circuit boards in either SSPS train. The post installation test is satisfied by the performance of an Actuation Logic Test Surveillance, or an equivalent logic test, which demonstrates the operability of the SSPS, as required by the plant Technical Specifications. This is plant specific action item 4.2.4 (Section 4.2.4). With these factors the NRC staff has reasonable assurance of adequate independent verification the circuit boards meet the functional requirements and, therefore, the requirements of 10 CFR 50 Appendix, B, Criterion I and III are met.

3.5 Environmental Equipment Qualification

The NRC staff considered the following regulations and guidance to be applicable to this application to evaluate the processes used to qualify the new design boards with respect to environmental equipment qualification:

Regulations and Regulatory Basis

The GDC of Appendix A to 10 CFR Part 50 establishes minimum requirements for the principal design criteria for light water reactors. These principal design criteria establish the necessary design, fabrication, construction testing, and performance requirements for components important to safety, that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.

The GDC 2 provides criteria for "Design Bases for Protection against Natural Phenomena"

> "Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design basis for these structures, systems, and components shall reflect: (1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed."
>
> The NRC staff's evaluation of the SSPS-board design conformance to GDC 2 is addressed in this section. The new design boards are mounted within electrical cabinets located within controlled environments within the plant. However, the potential occurrence of the aforementioned design basis external events can present hazards leading to a loss of electrical power or other normal plant services that could lead to the loss of HVAC, or the onset of cabinet acceleration/motion due to seismic effects that can result in off-normal environmental conditions. This section describes the NRC staff's evaluation of the qualification testing and analysis to demonstrate reliable performance of the new design boards to withstand the effects of such natural phenomena without a loss of the capability to perform their safety functions.

The GDC 4 provides criteria for "Environmental and Dynamic Effects Bases"

> "Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit.

> The NRC staff's evaluation of the new design boards' conformance to GDC 4 is addressed here and briefly within Sections 3.9.1.7 and 3.9.1.8, which address IEEE 603, Clauses 4.7 and 4.8, respectively. As described above, the new design boards are mounted within electrical cabinets located within controlled environments within the plant. However, variations can occur within the performance of the HVAC systems serving those controlled environments. The cabinets are subject to the limits of normal variations of heating and cooling and de-humidification, as well as the temporary failure of the equipment that maintains the controlled environment. The boards and power supplies within the cabinet also contribute to heat rise within the cabinets that can present an additional challenge to the reliable performance of the new design boards. This section describes the NRC staff's evaluation of the qualification testing and analysis to demonstrate the reliable performance of the new design boards to withstand the effects of such phenomena without a loss of the capability to perform their safety functions.

The GDC 22 provides criteria for "Protection System Independence"

> "The protection system shall 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 loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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."
>
> Those aspects of GDC 22 related to the effects of natural phenomena are described within this section. In addition, Section 3.9.2.6.3 describes the NRC staff's evaluation of testing to demonstrate the capability of the new design boards that ensure electrical independence between safety and non-safety signals that interface with the SSPS.

The regulations in 10 CFR 50.55a(h), "Protection and Safety Systems," incorporate the 1991 version of IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," for incorporation by reference, including the correction sheet dated January 30, 1995. Clause 5.4 of IEEE Std. 603 states safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting the performance requirements as specified in the design basis on a continuing basis.

Regulatory Guidance

RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," describes a method that is acceptable to the NRC staff for meeting the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants.

RG 1.152 conditionally endorses IEEE 7-4.3.2. IEEE 7-4.3.2, Clause 5.4, defines the equipment qualification requirements necessary to qualify digital computers for use in safety systems. These criteria, as expanded in sub-clauses 5.4.1 and 5.4.2, are in addition to those given in IEEE Std. 603-1991. Clause 5.4.1 specifies that the system qualification testing be

performed with all portions of the computer necessary to accomplish safety functions, or whose operation or failure could impair safety functions should be exercised during qualification testing with software and diagnostics that are representative of those used in actual operation. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs, outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Clause 5.4.2 defines the qualification of existing commercial computers for use in safety-related applications in nuclear power plants.

3.5.1 Environmental Qualification of System

Background

The original Solid State Protection System and Safeguards cabinets were environmentally qualified as part of a programmatic effort to address the guidance in RG 1.89, "Qualification of Class 1E Equipment for Nuclear Power Plants" (ADAMS Accession No. ML012880422), which endorses the procedures described in IEEE Standard 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," dated February 28, 1974. The TR states WCAP-8587 Revision 6-A (non-proprietary (NP)) (Reference 11) documents the Westinghouse methodology for performing equipment qualification programs to meet IEEE 323-1974. The NRC staff notes that the NRC has previously found that the equipment qualification methodology described within WCAP-8587 Revision 6 (NP), "Methodology for Qualifying Westinghouse WRD Supplied NSSS Safety Related Electrical Equipment," is acceptable for referencing in licensing applications to the extent specified and under the limitations described in its Safety Evaluation Report attached to its acceptance letter (Reference 11).

Analysis of Regulatory Guidance

Prior to March, 2007, the NRC staff based its regulatory evaluations of licensee conformance with the guidance on environmental qualification as described within RG 1.89, Revisions 0 and 1. RG 1.89, Revisions 0 and 1, state that the procedures for Class 1E equipment qualification described in the endorsed IEEE Std. 323-1974 are acceptable for satisfying the NRCs regulations pertaining to the qualification of electric equipment and provide, subject to conditions stated within the RG, an adequate basis for complying with the design verification requirements of Criterion III (Design Control) of Appendix B to 10 CFR Part 50 to verify the adequacy of the design under the most adverse design conditions. IEEE Standard 323-1974 describes basic procedures for qualifying Class IE equipment and interfaces that are to be used in nuclear power plants and components or equipment of any interface whose failure could adversely affect any Class 1E equipment. The 1974 version of the standard, as endorsed, delineated principles, procedures, and methods of qualification which, when satisfied, will confirm the adequacy of the equipment design for the performance of Class IE functions under normal, abnormal, design-basis-event, post-design-basis event, and containment-test conditions.

Although generally applicable to all locations of Class 1E electrical equipment relied upon to accomplish safety functions, the main focus of IEEE 323-1974 was to describe procedures and methodologies for qualifying electrical equipment that must accomplish safety functions to prevent or mitigate design-basis accidents associated with the Class 1E equipment exposure to

the harsher environments that arise due to the occurrence of steam line breaks, the use of containment sprays, etc., resulting in exposure of the Class 1E electrical equipment to elevated ambient temperature and pressure, humidity, chemical effects, radiation, aging, submergence, and other harsh environmental conditions.

In March, 2007, the NRC staff released its revised guidance pertaining specifically to computer-based I&C systems, which are primarily implemented in nuclear power plant locations that are characterized as “mild environments” that are not affected by the harsh conditions associated with design-basis accidents. In addition, because of ready accessibility for monitoring and maintenance in mild environments, the need to establish a qualified life does not apply. Nonetheless, the qualification criterion of 10 CFR 50.55a(h)(2) (for protection systems) does apply for safety-related computer-based I&C systems. Therefore, the NRC staff developed RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," to describe a method acceptable to the NRC staff for meeting the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants. RG 1.209 complements Revision 1 of RG 1.89, “Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants,” issued June 1984 (ADAMS Accession No. ML003740271), which addresses compliance with 10 CFR 50.49, “Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants,” for harsh environments that are subject to design-basis accidents.

RG 1.209 states the guidance described in IEEE Std. 323-2003, is appropriate for satisfying the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants, provided that the following enhancements and exceptions (hereinafter referred to as “conditions”) are met: (1) type testing is the preferred method for environmental qualification; (2) the qualification testing should be performed with the I&C system functioning, with software and diagnostics that are representative of those used in actual operation, while the system is subjected to the specified environmental service conditions, including abnormal operational occurrences; (3) the standards applicable to testing for EMI/RFI and surge are considered as environmental conditions, and that guidelines for conducting electromagnetic susceptibility testing of safety-related I&C systems appear in Revision 1 of RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” issued October 2003; (4) documentation of the evidence of qualification in a mild environment should be consistent with the guidance given in Section 7.2 of IEEE 323-2003 for harsh environments, based on the details of the actual environmental test conditions, test sequence, acceptance criteria, etc.; and (5) for safety-related computer-based I&C systems installed in a harsh environment, the regulatory positions of RG 1.209 supplement the harsh environment qualification practices endorsed in RG 1.89.

RG 1.209 also states for computer-based I&C systems, qualification is a validation of design to demonstrate that such systems are capable of performing their required safety functions under the specified environmental and operational stresses, rather than to establish a particular qualified life. Such qualification serves to provide additional assurance that the probability of common-cause failure attributable to environmental stressors is reduced to an acceptable level.

Clause 5.4.1 of IEEE 7-4.3.2 (endorsed by RG 1.152) mirrors the guidance at condition (2) of RG 1.209 by specifying that the system qualification testing should be performed with all portions of the computer necessary to accomplish safety functions, or whose operation or failure could impair safety functions, exercised during qualification testing with software and diagnostics that are representative of those used in actual operation. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs, outputs, display functions, diagnostics, associated components, communication paths, and interfaces.

Evaluation

To evaluate whether Westinghouse has adequately demonstrated that the new design boards are capable of performing their intended function(s) under the environmental conditions to which they will be subjected, the NRC staff evaluated the environmental qualification aspects of the TR and its supporting referenced reports against the criteria of RG 1.209 and RG 1.152 to evaluate whether it adequately addresses the capability of the boards to reliably withstand atmospheric effects (i.e., temperature and humidity), radiation effects, seismic effects, and electromagnetic and radio frequency interference.

The TR describes how various aspects of the qualification program for the new design boards were accomplished. Specifically, the technical bases for establishing the conditions under which the SSPS boards must function, and the methodology for demonstrating that the new SSPS boards can function reliably under those conditions originate within the early 1980s program for qualifying the SSPS cabinets and system. Westinghouse developed its program for qualifying the new design boards based on the conditions and procedures as described in its previously approved (Reference 11) equipment qualification program as described within WCAP-8587 Revision 6-A (NP), with enhancements to address appropriate newer criteria or supplemental testing. The NRC staff evaluated whether the appropriate conditions and procedures for such qualification have been applied to the environmental qualification of the new design boards. The NRC staff evaluation of the qualification program as applied to the design verification process for the new design boards for (1) atmospheric, (2) power supply fluctuations, (3) radiation, (4) seismic, and (5) electromagnetic/radiofrequency interference follows.

3.5.1.1 Atmospheric

As described above, GDC 2, "Design Bases for Protection against Natural Phenomena," requires that structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. One of the potential effects of such natural phenomena could be the loss of offsite power or other plant condition that results in the loss of HVAC systems that control the environment within the rooms housing the SSPS cabinets.

Also, as described above, GDC 4, "Environmental and Dynamic Effects Bases," requires that structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. Normal operation of the HVAC systems controlling the environment within the rooms housing

the SSPS cabinets encompasses a range of normal and off-normal conditions, including a temporary loss of cooling to the SSPS cabinets.

RG 1.209 states the guidance described in IEEE Standard 323-2003, is appropriate for satisfying the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants, provided that the following enhancements and exceptions (hereinafter referred to as "conditions") are met: (1) type testing is the preferred method for environmental qualification; (2) the qualification testing should be performed with the I&C system functioning, with software and diagnostics that are representative of those used in actual operation, while the system is subjected to the specified environmental service conditions, including abnormal operational occurrences; (3) the standards applicable to testing for EMI/RFI and surge are considered as environmental conditions, and that guidelines for conducting electromagnetic susceptibility testing of safety-related I&C systems appear in Revision 1 of RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," issued October 2003; (4) documentation of the evidence of qualification in a mild environment should be consistent with the guidance given in Section 7.2 of IEEE 323-2003 for harsh environments, based on the details of the actual environmental test conditions, test sequence, acceptance criteria, etc.; and (5) for safety-related computer-based I&C systems installed in a harsh environment, the regulatory positions of RG 1.209 supplement the harsh environment qualification practices endorsed in RG 1.89.

The NRC staff notes that the new design boards are mounted within electrical cabinets located within controlled environments within the plant. Variations can occur within the performance of HVAC, and the cabinets are subject to the limits of normal variations of heating and cooling and de-humidification, as well as the temporary failure of the equipment that maintains the controlled environment. The boards and power supplies within the cabinet also contribute to heat rise within the cabinets that can present an additional challenge to the reliable performance of the new design boards.

The NRC staff evaluated the description within the TR regarding the qualification testing and analysis to demonstrate reliable performance of the new design boards to withstand the effects of such phenomena without loss of capability to perform their safety functions. In addition, the NRC staff performed an audit of the referenced test plans and test reports referenced within the TR to verify that appropriate limits of testing and test performance criteria within RG 1.209 were being met.

The NRC staff found that the methodology outlined in the qualification testing program described in the NRC-approved Westinghouse report WCAP-8587 Revision 6-A (NP) (Reference 11) was followed for the qualification of the new design boards. Since these boards were designed and produced over a period of several years, multiple qualification tests had been performed to qualify the boards as the design was completed and to provide verification that the boards that were designed and qualified in the earlier tests would function appropriately when operational in conjunction with the boards that were designed and qualified during the later qualification tests.

The NRC staff noted that environmental qualification type testing for the new design boards was performed on several occasions during the board development and qualification effort. Some

boards had completed development prior to others; hence qualification testing was performed on the earlier developed boards on more than one occasion. The final testing included all the new design board specimens mounted into an open-frame card cage test rig that was placed into an air-circulating environmental chamber. The boards were powered and operational throughout the test sequence running with simulated inputs (i.e., system functioning), with software and diagnostics that are representative of those used in actual operation, while the system was subjected to the specified environmental service conditions, including the simulated abnormal operational occurrence tests as prescribed in the WCAP-8587(R6)-NP-A test methodology. The power supplies, input panel test tools, and output panel test tools were connected to the card cage with short cable runs, and staged at a location nearby the environmental chamber. The applied temperature and humidity was monitored and recorded through the duration of the test runs. During the testing, ambient temperature and humidity was varied in accordance with the approved test methodology to the extremes identified in the test plans. Figure 8-1 of the TR depicts the environmental test profile that was applied during the temperature and humidity cycling test. This profile was based on the test profile developed for the original SSPS cabinets as described in WCAP-8587(R6)-A (NP), and its daughter documents (Equipment Qualification Data Packages EQDP-ESE-16 and EQDP-ESE-17) specific to the SSPS cabinets. The original (1983) SSPS cabinet test profile was depicted as the humidity and temperature applied to the exterior of the cabinets of SSPS boards. This 1983 original profile included a maximum temperature for mild environments of 120 degrees Fahrenheit (°F) at 35 percent relative humidity, and a maximum 95 percent relative humidity at 82 °F. However, for the new design board testing, in order to account for the effects of Joulean (self) heating of the equipment, (temperature rise within the cabinets due to the heat from the power supplies and the complement of boards) the maximum temperature applied in the test profile for the new design boards was increased. To determine the appropriate magnitude to account for this temperature profile increase, a special test was performed on an operating SSPS system. The special test determined that an appropriate heat rise would be approximately 14 °F at a location just above the location of the uppermost SSPS board racks. To provide additional margin, the applied temperature test profile was raised to a maximum of 140 °F (rather than 134 °F) at the SSPS board location in the test chamber. Figure 8-1 of the TR indicates that the maximum applied test temperature profile was 140 °F. The test acceptance criteria was to ensure that each board type remained fully operable during functional testing performed during the environmental test exposure period, and that the output of the logic gates should not change state due to an unrequested condition. The test results revealed that all eight types of new design boards successfully completed environmental qualification testing.

The entire environmental qualification test, including the test plan, test procedure, test set-up, identification of the test equipment, functional test data, and test results evaluation, including a discussion of any anomalies and their analyses and resolutions was documented in a formal test report, complete with photographs of the test set-up, test specimens, and records of the input and output tracings, notes of the test technicians, and records of the measurement of the applied test conditions, consistent with the criteria described within RG 1.209.

The NRC staff finds that the temperature and humidity qualification tests were performed consistent with the approved test methodology as described in Reference 11, and were consistent with applicable portions of RG 1.209 and similar applicable portions of RG 1.152. Therefore this atmospheric (temperature and humidity) qualification is deemed acceptable.

Prior to the installation of the new design boards, however, licensees shall verify that the normal and abnormal temperature and humidity profile (Figure 8-1 of the TR) with a maximum temperature of 140 °F (including approximately 6 °F margin) under postulated faulted HVAC conditions envelopes the site-specific conditions expected inside the SSPS cabinets at the location immediately above the uppermost SSPS board racks. Alternatively, licensees shall confirm that the temperature profile of the original 1983 test (maximum of 120 °F under postulated faulted HVAC conditions) should envelope the site-specific expected fault temperature conditions just outside the SSPS cabinets. See Plant Specific Action Item No. 4.2.1 (Section 4.2.1).

3.5.1.2 Power Supply Fluctuations

As described above, GDC 4, "Environmental and Dynamic Effects Bases," requires that structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. Normal operation of the power supplies feeding the SSPS cabinets encompasses a range of power supply fluctuations representing both normal and off-normal conditions.

Also, as described above for environmental qualification, RG 1.209 states the guidance described in IEEE Std. 323-2003, is appropriate for satisfying the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants, provided that the qualification testing should be performed with the I&C system functioning, with software and diagnostics that are representative of those used in actual operation, while the system is subjected to the specified environmental service conditions, *including abnormal operational occurrences*.

Further, IEEE 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Section 4 states:

> A specific basis shall be established for the design of each safety system of the nuclear power generating station. The design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system, including design changes. The design basis shall be consistent with the requirements of ANSI/ANS [American Nuclear Society] 51.1-1983 or ANSI/ANS 52.1-1983 and shall document as a minimum:
>
> 4.7 The range of transient and steady-state conditions of both motive and control power and the environment (for example, voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform, and
>
> 4.8 The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions.

The NRC staff notes that the applied power to the cabinets and to the power supplies associated with the use of the new design boards can have a range of steady state and

transient conditions, and such fluctuations in applied power can have the potential for functional degradation of safety system performance.

To evaluate how Westinghouse has addressed these IEEE 603-1991 criteria, the NRC staff evaluated the description within the TR regarding the qualification testing and analysis to demonstrate reliable performance of the new design boards to withstand the effects of such phenomena without loss of capability to perform their safety functions. In addition, the NRC staff performed an audit of the referenced test plans and test reports referenced within the TR to verify that appropriate limits of testing and performance test criteria within RG 1.209 and IEEE 603-1991 were being met.

The NRC staff found that the TR describes the analysis and testing performed to verify that postulated fluctuations in power supply do not have an adverse effect on the performance of the new design boards. The NRC staff notes that Westinghouse has identified that the system operating parameters and environmental parameters associated with the original SSPS system cabinets have not changed. Further, Westinghouse confirmed that an appropriate specification for anticipated voltage fluctuations accounting for anticipated dips and rises in the DC power supply output due to postulated changes in input power supply is plus or minus (+/-) 3 percent. Therefore, the environmental qualification testing included a cycling test to simulate power supply fluctuations for the new design boards of a maximum of 49.44 Volts direct current (Vdc) and minimum of 46.56 Vdc for the 48 volt power supply, and a maximum of 15.45 Vdc and minimum of 14.55 Vdc for the 15 Volt power supply. Figure 8-1 of the TR also depicts the magnitude and cycling durations for this power supply fluctuation test. All eight new design boards successfully passed the voltage variation testing portion of the environmental qualification testing. Similar to the temperature and humidity testing described above, the voltage variation qualification test, including the test plan, test procedure, test set-up, identification of the test equipment, functional test data, and test results evaluation, was documented in a formal test report, complete with photographs of the test set-up, test specimens, and records of the input and output tracings, notes of the test technicians, and records of the measurement of the applied test conditions, consistent with the criteria described within RG 1.209.

Westinghouse also performed an analysis of the impact of power supply ripple accompanying the 48-Volt and 15-Volt power supplies. The original specification for SSPS included a maximum allowed ripple specification of 340 millivolt (mV) and 150 mV rms for the 48 Vdc and 15 Vdc power supplies, respectively. In its evaluation of power supply noise associated with any remaining originally-supplied Basler SSPS Switching Power Supplies (Part 2374A07G01), Westinghouse noted that these dual-48/15 Vdc switching power supplies have a switching frequency fluctuation between 15 kilohertz (kHz) and 30 kHz that is dependent upon output load. The Westinghouse analysis demonstrates that the magnitude of ripple, after being filtered through voltage conversion and filtering circuits, will have a negligible impact on the operation of the new design boards.

The NRC staff finds that Westinghouse appropriately specified and conducted power supply fluctuation qualification tests, and performed an analysis of power quality that are consistent with the approved test methodology as described in the applicable Westinghouse topical reports (Reference 11), and consistent with applicable portions of RG 1.209 and similar applicable portions of RG 1.152. The NRC staff also finds that conditions having the potential for

functional degradation of safety system performance have been addressed as required in IEEE 603-1991, and that provisions have been incorporated in the design of the new design boards to retain the capability for performing the safety functions. Therefore, this power supply qualification testing and power quality analysis is deemed acceptable.

3.5.1.3 Radiation

As described above, GDC 4 "Environmental and Dynamic Effects Bases" requires that structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. The NRC staff notes that the new design boards are intended to be located within cabinets in auxiliary or control buildings that are separated by distance and shielding from areas of the containment building where it would be expected to have significant normal and off-normal radiological conditions. The rooms within the control or auxiliary buildings are generally expected to have normal and off-normal radiological conditions that would result in a total lifetime exposure of less than 1 X 10E+3 Rads. Further, the safety actions to be accomplished by the SSPS system to trip the reactor and actuate safeguards features are primarily designed to be accomplished before significant levels of radiation can leave the containment building.

Prior to March, 2007, the NRC staff based its regulatory evaluations of licensee conformance with the guidance on environmental qualification as described within RG 1.89, Revisions 0 and 1, which state that the procedures for Class 1E equipment qualification described in the endorsed IEEE Standard 323-1974 are acceptable for satisfying the NRCs regulations pertaining to the qualification of electric equipment.

In March, 2007, the NRC staff released its revised guidance pertaining specifically to computer-based I&C systems, which are primarily implemented in nuclear power plant locations that are characterized as “mild environments” that are not affected by the harsh conditions associated with design-basis accidents. In addition, because of ready accessibility for monitoring and maintenance in mild environments, the need to establish a qualified life does not apply. Nonetheless, the qualification criterion of 10 CFR 50.55a(h)(2) (for protection systems) does apply for safety-related computer-based I&C systems. Therefore, the NRC staff developed RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants" to describe a method acceptable to the NRC staff for meeting the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants. RG 1.209 complements Revision 1 of RG 1.89, “Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants,” issued June 1984 (ADAMS Accession No. ML003740271), which addresses compliance with 10 CFR 50.49, “Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants,” for harsh environments that are subject to design-basis accidents. RG 1.209 endorses, with exceptions and clarifications, IEEE Std. 323-2003. The IEEE Std., at Clause 6.3.1.9, “Radiation,” states in the type testing, “all materials or components, for which radiation causes significant aging, shall be irradiated to simulate the effects of the radiation exposure. If normal and accident radiation doses and dose rate are demonstrated to have no effect on the safety function(s) of the equipment, then radiation testing may be excluded, and the justification should be documented.”

The Discussion section (Section B) of RG 1.209 states advanced digital systems tend to use metal oxide semiconductor (MOS) technology, particularly complementary MOS (CMOS) technology. The radiation threshold for MOS devices is generally lower than those for bipolar (analog) devices. However, MOS technology is preferred for ICs because of its technical superiority in other areas (such as higher input impedance, fewer manufacturing processing steps, better temperature stability, and lower noise). Commercial MOS devices are very sensitive to ionizing doses, in contrast to their relative insensitivity to neutron fluence. Ionizing dose radiation hardness levels for MOS IC families range from about 10 gray (Gy) or 1 kilorad (krad) for commercial off-the-shelf (COTS) circuits to about 105 Gy (104 krad) for radiation-hardened circuits.

The NRC staff notes that the current version of NRC RG 1.89, Revision 1 (June 1984), states electric equipment that may be exposed to low-level radiation doses should not generally be considered exempt from radiation qualification testing, but that exceptions to this may be based on qualification by analysis supported by test data or operating experience that verifies that the dose and dose rates will not degrade the operability of the equipment below acceptable values.

To evaluate how Westinghouse has addressed RG 1.209 discussion regarding the analysis of materials used for the new design boards, the NRC staff evaluated the description within the TR, regarding the Westinghouse qualification analysis performed to demonstrate reliable performance of the new design boards in an environment where it is expected that normal and off-normal radiation exposure will be less than 1 X 10E+3 Rads. In addition, the NRC staff performed an evaluation of the TRs referenced within the TR to verify that an appropriate evaluation has been performed.

The TR states the basis for its analysis of radiation exposure is provided in WCAP-8587(R6)-A (NP). As described within Westinghouse TR WCAP-8587 Revision 6-A (NP), an analysis was performed to identify applicable test data and operating experience identifying the effects of the exposure of various radiation doses on materials used in safety-related electrical equipment furnished to licensees by Westinghouse. Appendix C of WCAP-8587(R6)-A (NP) concludes that radiation aging below 1 X 10E+4 rads (100 gray) gamma is not a significant factor in the ability of the equipment to perform its safety function(s) during the design basis event. However, since the SSPS new design boards contain CMOS technology, they are limited to a gamma radiation threshold of 1 X 10E+3 rads (10 gray), consistent with Section B, “Discussion,” of RG 1.209. SSPS new design board failures induced by normal background gamma radiation below 1 X 10 E+3 rads alone are considered to be random. Any electronic components exposed to a gamma radiation dose above 1 X 10 E+3 rads (10 gray) needs to be evaluated to determine the acceptability.

In Reference 11, the NRC staff previously concurred with the conclusions of WCAP-8587. Since 1983, there has been no significant operating experience indicating that safety-related components located in very low radiation dose zones are beginning to fail due to their continued exposure to very low radiation doses. Therefore, the NRC staff finds that the Westinghouse analysis in WCAP-8587(R6)-A (NP), Appendix C, “Effects of Gamma Radiation Doses Below 1 X 10E+4 rads on the Mechanical Properties of Materials,” still holds, and that the provisions of RG 1.209 regarding analysis of materials used in safety-related DI&C systems are met. Licensees shall confirm, however, that a site-specific analysis shows that the location in which the new design boards will be installed will not result in a lifetime total integrated dose exposure

of greater than 1 X 10 E+3 rads (10 gray). See Plant Specific Action Item No. 4.2.2 (Section 4.2.2).

3.5.1.4 Seismic Qualification

GDC 2 requires structures, systems, and components important to safety be designed to withstand the effects of natural phenomena such as earthquakes…without loss of capability to perform their safety functions. The design basis for these structures, systems, and components must reflect: (1) appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed.

Appendix S to 10 CFR Part 50 states the SSCs required to withstand the effects of the safe-shutdown earthquake (SSE) ground motion or surface deformation are those necessary to assure (1) the integrity of the reactor coolant pressure boundary; (2) the capability to shut down the reactor and maintain it in a safe-shutdown condition; or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guideline exposures of 10 CFR 50.34(a)(1). Section IV(a)(1)(ii) of Appendix S to 10 CFR Part 50 requires the nuclear power plant to be designed so that, if the SSE ground motion occurs, certain SSCs will remain functional and within applicable stress, strain, and deformation limits. In addition to seismic loads, the design of these safety-related SSCs must take into account applicable concurrent normal operating, functional, and accident-induced loads. Section IV(a)(1)(iii) of Appendix S to 10 CFR Part 50 requires the safety functions of SSCs to be assured during and after the vibratory ground motion associated with the SSE ground motion through design, testing, or qualification methods.

Section VI, “Application to Engineering Design,” of Appendix A, “Seismic and Geologic Siting Criteria for Nuclear Power Plants,” to 10 CFR Part 100, “Reactor Site Criteria” provides criteria for identifying appropriate Safe Shutdown Earthquake and Operating Basis Earthquake levels. This section states, “The nuclear power plant shall be designed so that, if the Safe Shutdown Earthquake occurs, certain structures, systems, and components will remain functional. These structures, systems, and components are those necessary to assure (i) the integrity of the reactor coolant pressure boundary, (ii) the capability to shut down the reactor and maintain it in a safe condition, or (iii) the capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the guideline exposures of this part.” It also states, “All structures, systems, and components of the nuclear power plant necessary for continued operation without undue risk to the health and safety of the public shall be designed to remain functional and within applicable stress and deformation limits when subjected to the effects of the vibratory motion of the Operating Basis Earthquake in combination with normal operating loads. The engineering method used to insure that these structures, systems, and components are capable of withstanding the effects of the Operating Basis Earthquake shall involve the use of either a suitable dynamic analysis or a suitable qualification test to demonstrate that the structures, systems and components can withstand the seismic and other concurrent loads, except where it can be demonstrated that the use of an equivalent static load method provides adequate conservatism.”

RG 1.100, Revision 3, "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants," describes a method acceptable to the NRC staff for complying with NRC's regulations with respect to seismic qualification of equipment. Revision 3 of this guide endorses, with several clarifications and exceptions, IEEE Std. 344-2004, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.” Revision 2 of RG 1.100 endorses, with few exceptions, the use of the methodologies described in IEEE Std. 344-1987.

IEEE 344-1987, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations,” was developed to expand and amplify guidance contained within ANSI/IEEE Std. 344-1975 for developing programs to seismically qualify Class 1E equipment for nuclear power generating stations. Section 4 of IEEE 244-1987 states Equipment being qualified must demonstrate that it can perform its safety function during and after an earthquake. The required safety function depends not only on the equipment itself but also on the system and plant in which it is to function. When the safety function of equipment requires a demonstration of operability during the earthquake, it shall be demonstrated during the strong motion portion of the qualification simulation.

IEEE Std. 344-2004, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations,” was developed to expand and clarify guidance for developing programs to seismically qualify Class 1E equipment for nuclear power generating stations. Specific areas of amplification included were based on experience gained since 1987. The revised recommended practice defines more fully the procedures by which Class 1E equipment can be seismically qualified. It presents practices and qualification methods that are deemed acceptable to the nuclear power generation industry, its equipment suppliers, and the industrial test and analysis facilities utilized by the industry, reflecting an effort to recommend state-of-the-art techniques at the time of its publication. The IEEE 344-2004 Recommended Practice acknowledges that strict adherence to it alone to obtain equipment seismic qualification will not suffice for assurance of public health and safety since it is the integrated performance of structures, fluid systems, instrumentation systems, electrical systems, and man/machine interface systems of a nuclear power generating station that establishes totally safe operating conditions.

To evaluate how Westinghouse has addressed these code and guidance criteria, the NRC staff evaluated the description within the TR regarding the qualification testing and analysis to demonstrate reliable performance of the new design boards to withstand the effects of such seismic phenomena without loss of capability to perform their safety functions. In addition, the NRC staff performed an audit of the referenced test plans and test reports referenced within the TR to verify that appropriate limits of testing and performance test criteria appropriate to the use of the new design boards as installed within cabinets at nuclear power plants in the United States have been implemented.

The NRC staff notes that IEEE 344-1987, as amplified by IEEE 344-2004, identifies that the ground motion (horizontal and vertical) may be filtered by intervening building structures to produce amplified or attenuated narrowband motions within the structure. (The major change from IEEE Std. 344-1987 to IEEE Std. 344-2004 is the update and expansion of Clause 10, “Experience,” which describes the use of experience data as a method for seismic qualification of Class 1E electrical equipment (including I&C components).) The dynamic response of

equipment on structures may be further amplified or attenuated to an acceleration level many times more or less than that of the maximum ground acceleration, depending upon the equipment damping and natural frequencies. The narrowband response spectra that typically describe a building floor motion indicate that single-frequency excitation of equipment subcomponents can predominate. For example, for components mounted away from rigid supports, the resultant motion may be predominantly single frequency in nature and centered near or at the resonant frequency of the system of support structures employed. Damping is the generic name ascribed to the numerous energy dissipation mechanisms in a system. In practice, damping depends on many parameters, such as the structural system, mode of vibration, strain, normal force, velocity, materials, etc. For equipment composed of an assembly of components, there is usually no single value of damping. Damping is associated with every part of the equipment ranging from bolted or welded construction to uniform material. The value of damping may vary from place to place, depending on numerous factors. In testing, the equipment may be qualified by subjecting it to a simulated seismic motion as defined by the RRS. The response spectrum defines the seismic motion by way of the peak response of an array of single-degree of-freedom damped oscillators. Since the oscillators are hypothetical, any practical value of damping, for example, 5 percent may be employed in the RRS for testing, and it need not correspond to the actual equipment damping.

The TR states the seismic qualification program for the new design boards was conducted over several years, and several tests. Earlier designed boards underwent earlier seismic performance tests, while later designed boards experienced tests of their own, culminating in a final test that included all eight new design boards. After the last testing was completed, several analyses were performed to verify that sufficient qualification test data exists to adequately demonstrate that the seismic response requirements for multiple plant-specific seismic performances exist. Testing was performed in accordance with the recommended practices and analyses as described in IEEE 344-1987. The boards were qualified by mounting them into card cages that were, in turn, mounted onto a rigid test rig that was mounted onto a triaxial seismic shake table, and subjected to a series of applied seismic motion tests. The card cages were installed in a manner that simulates their actual installation within SSPS cabinets, with the rear of the card cage unsecured. The applied seismic motion imparted to the test table was in the form of multi-frequency random excitation of at least 30 seconds duration, while being monitored with several accelerometers and recorded. In addition, the card cages holding the new design boards was monitored with accelerometers and recorded throughout the test. The card cages were subjected to a minimum of five OBEs and one SSE. During the tests, functional tests were performed. During the OBE tests, one input of each logic gate of the universal logic board (ULB) was set to logic “high.” Prior to the first OBE and after the fifth OBE, functional testing was performed to vary all inputs at each logic combination, and monitor the output states. Similar functional testing was performed for the SSE test. An additional SSE test was performed with a second input to each gate of the ULB manually changed to simulate a trip input condition.

During and following the tests, the test specimens maintained their structural integrity, and the outputs of the test boards remained continuous at the required logic levels simulated. During the SSE tests, the output of the test specimens appropriately changed state upon demand during the test run. All test boards passed their required functional test after selected test runs, and passed the required baseline functional tests following completion of the required tests.

The Westinghouse seismic qualification program for the new design boards included an effort to identify the appropriate required response spectrum (RRS) that was needed to be applied as a test required response spectrum (TRRS) as input to the seismic response test table for any testing that was needed to demonstrate adequate seismic performance. As the basis for identification of a proper set of RRS curves, Westinghouse began with the information contained within the original SSPS qualification test reports from the original 1970s and 1980s series of tests of the SSPS cabinets. At that time, however, the accepted practice for demonstrating seismic performance of safety-related equipment was to apply single-axis shake-table testing, in combination with formal analysis of the equipment response, to demonstrate that the equipment could continue to function during and following simulated seismic motion. Some of the early test reports did not identify a specific RRS, but were conducted simply to understand the seismic performance of and qualify measurements of the highest levels of seismic motion that the equipment could sustain while still providing required safety functions.

The Westinghouse seismic qualification program for the new design boards included an effort to identify an appropriate set of Required Response Spectra that would envelope the conditions expected in the bulk of the Westinghouse-designed nuclear steam supply systems in the United States and International arena. The accelerometer data obtained from the early seismic test programs, along with seismic testing documented in WCAP-8694, “Seismic Qualification of Rotary Relay for Use in the Solid State Protection System,” January 1976 (Reference 12, pertaining to SSPS rotary relays, which were also mounted within the SSPS cabinets) were used to develop in-equipment response spectra (IERS) for the SSPS printed circuit boards at 5 percent critical damping. The SSPS in-equipment (TRRS) in the three principal orthogonal axes of the equipment was defined with frequency content over the range of 1 to 33 Hz. During previous seismic qualification testing of SSPS components, the seismic acceleration time-history inputs were developed with frequency content from a range of 1 to 100 Hz to ensure the in-equipment TRRS would be enveloped by the test response spectra in compliance with IEEE Std. 344-1987. These in-equipment response spectra were used as the basis for the establishment of the RRS used for the seismic testing of the new design boards. With regard to the Unites States plants, a concerted effort was made to ensure that the in-equipment response spectrum envelopes the RRS for all potential installations of the new design boards was enveloped by the TRRS used in the qualification testing. This analysis revealed that not all potential site installations were completely enveloped without performing additional analyses using site-specific seismic design data. It was initially found that a few plants had current design basis vertical direction RRS envelopes that slightly exceeded the IERS TRRS over a very narrow frequency range. To remedy this, Westinghouse performed additional evaluations of the frequency and amplitude of content of vertical and horizontal direction site-specific floor response spectra, structural dynamic modeling of the SSPS cabinets, and evaluations of other site-specific seismic qualification data to establish that the TRRS applied during the seismic tests actually envelope anticipated United States nuclear plant current design basis required response spectra. Also, Westinghouse performed an analysis of the impact of board mounting orientation to confirm that there are no seismically-sensitive components that were mounted in an orientation manner that would subject them to adverse seismic response. This analysis revealed that all seismically-sensitive components on the eight new design SSPS boards are designed to be mounted in a horizontal orientation for which the horizontal direction IERS TRRS bounded the current design basis for all US plant-specific horizontal envelopes, and for which no anomalies were noted during the seismic testing.

The NRC staff concludes that the seismic qualification for the new design boards has been performed in accordance with the recommended practices and analyses as described in IEEE 344-1987, and therefore is consistent with the guidance provided in RG 1.100, Revision 2. Since the changes to this RG that were made to address the changes in IEEE 344-2004 regarding the use of experience data do not impact the methodology used to qualify the new design boards, the NRC staff finds that compliance with RG 1.100, Revision 3, has also been demonstrated. Therefore, the requirements of GDC-2 and Appendix A to 10 CFR Part 100 have been appropriately addressed for seismic effects and that the new design SSPS board seismic test response spectrum envelopes the current design basis required response spectra for US nuclear plants which may implement the new design boards.

3.5.1.5 Electromagnetic Interference/Radio Frequency Interference

As described above, GDC 4, "Environmental and Dynamic Effects Bases," requires that structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. The environmental conditions include ambient electromagnetic and radiofrequency noise in the vicinity of the SSPS cabinets that could have a range of normal and off-normal conditions.

RG 1.180 , Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," describes a method acceptable to the NRC staff for design, installation, and testing practices to address the effects of EMI/RFI and power surges on safety-related I&C systems. The RG identifies recommended test methods and operating envelopes for emissions and susceptibility testing. These operating envelopes were found to be acceptable test criteria representative of locations within a nuclear power plant where safety-related I&C systems either are or are likely to be installed and include control rooms, remote shutdown panels, cable spreading rooms, equipment rooms, auxiliary instrument rooms, relay rooms, and other areas (e.g., the turbine deck) where safety-related I&C system installations are planned. The operating envelopes were deemed acceptable for analog, digital, and hybrid system installations. The technical basis for the operating envelopes begins with the MIL-STD envelopes corresponding to the electromagnetic environment for military ground facilities, which were judged to be comparable to that of nuclear power plants based on general layout and equipment type considerations. Plant emissions data were used to confirm the adequacy of the operating envelopes. From the MIL-STD starting point, susceptibility envelopes were adjusted to account for the plant emissions data reported in NUREG/CR-6436, “Survey of Ambient Electromagnetic and Radio-Frequency Interference Levels in Nuclear Power Plants” (November 1996) and EPRI TR-102323. When changes to the operating envelopes from the MIL-STD origin were motivated by technical considerations, consistency among the envelopes for comparable test criteria was promoted. As a result of these considerations, the operating envelopes presented in RG 1.180 are equivalent or less restrictive than the MIL-STD envelopes that served as their initial basis. Where applicable, conditions permitting exemption of specific test methods were described.

RG 1.209 states the guidance described in IEEE Std. 323-2003, is appropriate for satisfying the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants, provided that the following enhancements and exceptions (hereinafter referred to as “conditions”) are met: “(3) the standards applicable to

testing for EMI/RFI and surge are considered as environmental conditions, and that guidelines for conducting electromagnetic susceptibility testing of safety-related I&C systems appear in Revision 1 of RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” issued October 2003.”

To evaluate how Westinghouse has addressed the potential for electromagnetic interference or radio frequency interference to adversely impact the accomplishment of safety functions by the new design boards, the NRC staff evaluated the description within the TR regarding the qualification testing and analysis to demonstrate reliable performance of the new design boards to withstand the effects of such phenomena without loss of capability to perform their safety functions. In addition, the NRC staff performed an audit of the test plans and test reports referenced within the TR to verify that appropriate limits of testing and performance test criteria within RG 1.209 and RG 1.180, Revision 1, were being met.

The NRC staff notes that Section 8 of the TR describes a comprehensive test program that was completed in two phases to evaluate the susceptibility of the new design boards to radiated and conducted electromagnetic and radiofrequency interference and to identify whether conducted or radiated emissions from these boards could adversely impact nearby safety-related components. As part of its test plans, Westinghouse identified an appropriate set of tests that should be performed to test the equipment performance under simulated radiated and conducted EMI/RFI conditions, and to verify that emissions from this equipment are within values deemed to be considered allowable for nuclear power plant electrical equipment room environments. The tests performed address the criteria and guidance (with two exceptions-see below) contained in RG 1.180, Revision 1, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety Related Instrumentation and Control Systems.” The selection of the regulatory guidance within RG 1.180, Revision 1, as the means to specify how this equipment should be tested and how it should perform from an EMI/RFI perspective is deemed by the NRC staff to be appropriate for this application.

Some of the tests conducted reference the use of guidance within the International Electrotechnical Commission's (IEC) Standards (some of which are also referenced within RG 1.180, Revision 1) in order to demonstrate compliance to the European Community EMC CE mark. However, the Westinghouse test plans state that the test guidance and acceptance criteria of RG 1.180, Revision 1, take precedence over the CE mark requirements. The NRC staff recognizes that strict adherence to the RG represents one way to address the regulatory requirements. During the test planning, Westinghouse identified that not all the regulatory guidance within RG 1.180, Revision 1, are appropriate to the use of the new design boards. The new design boards have a specific, limited use, restricting their application to within the SSPS cabinets of existing plants. Westinghouse applied engineering analysis to ascertain that the new SSPS boards will not cause low frequency emissions on the power lines feeding the boards, since the new design boards receive highly-regulated DC power from existing SSPS cabinet DC power supplies that have rigid specifications for maximum distortion, and neither the power supplies nor the cabinet wiring are expected to be revised or replaced when installing the new design boards. Therefore Westinghouse elected to take exception to the conduct of the MIL-STD-461E Test Method CE101 (Conducted Emissions, Low Frequency 30 Hz to 10 kHz). Further, RG 1.180, Revision 1, states equipment not intended to be installed in areas with other equipment sensitive to magnetic fields could be exempt from the RE101 (Radiated Emissions, Magnetic Field 30 Hz to 100 kHz) test. Westinghouse test planners

elected to not complete MIL-STD-461E Test Method RE101 (Radiated Emissions, Magnetic Field 30 Hz to 100 kHz) since the (normally closed door) SSPS cabinets are located in the instrument rooms where they will not be near any magnetically sensitive equipment. The NRC staff agrees with this reasoning, and notes that Table V, "Requirements Matrix" of MIL-STD-461E indicates that this test is recommended for use with surface ships and aircraft, (typically where the packaging of electronics is limited to closely-confined spaces, such as cockpits), but is not required for ground installations such as military bases (where space permits installation of electronics into free-standing cabinets). The applicability of MIL-STD-461E tests for nuclear plants is normally compared against the EMC requirements for military ground bases. Also, Westinghouse did conduct IEC 61000-6-4 Test Methods for EMI/RFI Emissions CISPR-11 (Conducted emissions, high-frequency, 150 kHz to 30 MHz) and CISPR-11 (Radiated emissions, electric field, 30 MHz to 1 GHz). The emissions test acceptance criteria for these tests were based on the CISPR-11 Class A criteria.

The acceptance criteria specified in RG 1.180, Revision 1, consistently state in each test section: "Acceptable performance should be defined in the test plan by the end user or testing organization according to the applicable equipment, subsystem, or system specifications." In this instance, the "end user" will be the licensees, but the "testing organization" is Westinghouse Electric Company. As a "testing organization" Westinghouse has elected to apply the set of tests and acceptance criteria as described in the individual test reports for the new design boards it has developed. The NRC staff has evaluated the selection of tests that were performed, and finds that with the exception of the tests that were excluded for acceptable reasons, there is a general equivalency with the set of tests performed with those identified in RG 1.180, Revision 1. Where appropriate, IEC Standard tests were applied in lieu of the excluded MIL-STD tests. The NRC staff also notes that RG 1.180 was last updated in October 2003, and the NRC staff recognizes that advances in the industry regarding the bases for selection of appropriate EMI/RFI testing, methods, and threshold levels may have occurred since then.

The NRC staff notes that the TR identifies test acceptance criteria that were applied for the performance tests developed to demonstrate the new design board maximum emission levels and immunity to the conducted and radiated electromagnetic and radiofrequency noise environments. The performance standard for emissions tests were such that emissions levels should not exceed the limits specified in the test plan. The performance standard for susceptibility testing stated there should be no actuations of the ESF output functions or drive relay chatter longer than 2 milliseconds (ms). Chatter of the memory output indication may cause the status lights to blink on and off, as long as the status lights return to their expected state when the test signal is removed. For surge and electrical fast transient tests, the test specimens were required to demonstrate that they could recover to normal operation and accuracy after the application of the test transient signal, without permanent degradation that prevents safety functionality.

According to Section 8.3 of the TR, for the immunity tests, the acceptance criteria for the performance of the boards (Acceptance Criterion A, B, and C, as stated), were derived from British Standard BS EN 61000-6-2, February 2007. The NRC staff notes that this standard appears to have evolved from the performance criteria described in Section 4, "Performance criteria" of IEC Standard 61000-6-2, 2nd Edition, 01/2005, "Electromagnetic Compatibility – Part 6-2: Generic Standards—Immunity for Industrial Environments." The decision to apply this

set of acceptance criteria is largely left to the organizations specifying the intended use/purchase specifications of the equipment under test rather than prescribed within RG 1.180. The referenced IEC and BS standards documents were developed significantly after the issuance of RG 1.180, Revision 1, and therefore these acceptance criteria are not specifically described within the RG. Nonetheless, the NRC staff finds that the selection of the set of acceptance criteria utilized in the EMC testing are reasonable for use with this equipment because they are practical to apply, and they differentiate performance requirements on the basis of the impact of the test waveform upon the ability of the new design boards to remain functional during and after its application to enable the accomplishment of required safety functions.

The NRC staff performed an audit of several susceptibility and emissions test reports that were referenced within the TR. The NRC staff notes the applied susceptibility and emissions test methods were sufficiently rigorous and provided the coverage necessary to simulate a broad range of conducted and radiated noise waveforms as provided for in the guidance documents and IEC standards. Anomalies that occurred during the testing associated with the test set-up were appropriately addressed, and re-testing was performed when deemed necessary. With the exception of the tests that had a direct adverse impact on the power supplies feeding the card cages into which the test specimens were mounted, all boards met either the A or B Acceptance Criteria. The safety function output of the new design boards did not change state during the susceptibility tests, although some of the indication lights may have blinked on and off. The purpose of the susceptibility tests was not to test the SSPS power supplies, but to monitor the response of the new design boards to the test waveform applied. In the susceptibility tests where the power supplies were adversely affected by the test conditions, the loss of power to the boards affected their performance. However, this performance condition would be also expected if a random failure were to occur that affected a power supply in an SSPS cabinet.

The EMC compatibility qualification testing, including the test plans, test procedures, test set-ups, identification of the test equipment, functional test data, and test results evaluations, including a discussion of any anomalies and their analyses and resolutions, were documented in formal test reports, complete with photographs of the test set-ups, test specimens, and records of the input and output tracings, notes of the test technicians, and records of the measurement of the applied test conditions, consistent with the criteria described within RG 1.209.

Tables 8-1 and 8-3 of the TR identify the maximum emissions levels to which the SSPS boards were found to have been limited. Tables 8-2 and 8-4 of the TR identify the test waveform levels, frequency ranges, and results of the susceptibility testing. Although the emissions from the new design SSPS boards have been found to be sufficiently low to permit safe operation of these boards in the vicinity of other safety related equipment, licensees shall ensure that the ambient radiated EMI/RFI levels within the vicinity of their site-specific locations of SSPS cabinets will not exceed the susceptibility levels to which the boards have been tested, or to which RG 1.180, Revision 1, recommends for testing. See Plant Specific Action Item No. 4.2.3 (Section 4.2.3).

The NRC staff finds that the EMI/RFI qualification testing for the new design SSPS boards performed was consistent with the intent of RG 1.180 and RG 1.209. Therefore, the requirements of GDC-4 have been appropriately addressed for EMI/RFI effects.

3.5.2 Power Quality

See Section 3.5.1.2.

3.5.3 Response Time Characteristics and Testing

GDC 18 “Inspection and Testing of Electric Power Systems," states:

> “The systems shall be designed with a capability to test periodically... (2) the operability of the systems as a whole and, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system, and the transfer of power among the nuclear power unit, the offsite power system, and the onsite power system.”

GDC 20 "Protection System Functions," states:

> “The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.”

The regulations in 10 CFR 50.55a(h), "Protection and Safety Systems," approves the 1991 version of IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," for incorporation by reference, including the correction sheet dated January 30, 1995. The criteria contained in this standard establish minimum functional and design requirements for the power, instrumentation, and control portions of safety systems for nuclear power generating stations.

Clause 4 of IEEE Std. 603-1991 requires, in part, that a specific design basis be established for the design of each safety system. Since this is an upgrade to certain circuit boards within the SSPS system, the design basis for the new design boards is the same as the existing boards. No changes to the design basis of the SSPS was identified or reviewed. Performance criteria, including system response times, system accuracies, ranges, and rates of change, should also be identified in the system design basis. Since the variables monitored have not changed, conformance with this cause is ensured if each new circuit board performs the same functions as its associated original design circuit board.

RG 1.118, “Periodic Testing of Electric Power and Protection Systems,” describes a method acceptable to the NRC staff for complying with the NRC's regulations with respect to the periodic testing of the electric power and protection systems. This RG endorses the use of IEEE Std. 338-1987, "Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems." The standard provides design and operational criteria for the performance of periodic testing as part of the surveillance program of nuclear power plant safety systems. The periodic testing consists of functional tests and checks, calibration verification, and time response measurements, as required, to verify that the safety system performs to meet its defined safety functions.

Clause 6.3.4 of IEEE 338-1987 states response time testing shall be required only on safety systems or subsystems to verify that the response times are within the limits given in the Safety Analysis Report including Technical Specifications. Response time testing of all safety-related equipment is not required if, in lieu of response time testing, the response time of safety system equipment is verified by functional testing calibration checks or other tests, or both. This is acceptable if it can be demonstrated that changes in response time beyond acceptable limits are accompanied by changes in performance characteristics that are detectable during routine periodic tests.

In TR WCAP-14036-P-A, Revision 1, "Elimination of Periodic Protection Channel Response Time Tests" (ADAMS Accession No. ML100050325), the Westinghouse Owners Group attempted to show that relaxing the requirements to perform periodic response time testing on all RTS and ESFAS protection functions in the analog or digital process racks is allowable under this provision of IEEE Std. 338. The systems for which relief from response time testing has been requested included the SSPS, inclusive of the ULB, the UVD Board, and the SGD Board. The results of Failure Modes and Effects Analyses (FMEA), as described in WCAP-14036-P-A, Revision 1, demonstrated that component degradation will not increase the response time beyond the bounding response time without that degradation being detectable by other periodic surveillance tests, such as channel checks and calibrations. In its SE for WCAP-14036-P, Revision 1, the NRC staff found that the FMEA performed were sufficiently rigorous to substantiate the conclusions reached in WCAP-14036-P regarding detection of response time degradation, and concurred that response time testing is redundant to other periodic surveillance tests and that appropriate surveillance testing alternatives to response time testing were in place per the existing requirements of plant specific technical specifications. The NRC staff also concluded that the determination of bounding response times using FMEA and as listed in Table 8-1 of WCAP-14036-P-A, Revision 1, is a valid method for determining the response time requirements of systems depended upon to mitigate accident and transient conditions.

To evaluate whether Westinghouse has adequately demonstrated that the performance of the new design boards have time responses that are within the bounding times allowed for in the time response testing elimination analysis in a manner that is consistent with the NRC staff's evaluation in its approved for use of WCAP-14036-P-A, Revision 1, the NRC staff reviewed the information presented in Sections 2 and 10 of the TR. The NRC staff performed an audit of the documents referenced within those sections.

In Section 2 of the TR, it is stated that the time responses of the new design ULB, SGD, and UVD board outputs is affected by the addition of an resistor capacitor filter between the output of the main CPLD and the output driver stage. The filters were added to reduce noise output and to prevent the self-test signals from propagating off the boards into the other circuits that may be connected to their outputs. These filters were designed as 20 microseconds (µSec) filters. A straight pass-through operation for the ULB now requires from 25 - 35 µSec to pass through, whereas the original ULB required from 6 - 12 µSec. Circuit board testing for time response shows this filter adds approximately 25 µSec to the SGD output signal for a straight pass-through actuation signal, and adds approximately 25 µSec to the UVD output signal for a straight pass-through actuation signal.

The TR states the new SSPS card designs must operate within the same bounding times and not exceed the times as described in WCAP-14036-P-A, Revision 1. The TR also states the bounding time for the solid state protection system reactor trip functions was determined to be 20 ms. The 20 ms is twice the expected time for an input relay to drop out. Section 4.8 of WCAP-14036-P-A defines the reactor trip functions expected delay for the ULB and UVD at 349 µSec. Since 349 µSec is insignificant compared to the expected input relay response time, there was no specific response time allocated to these cards and the bounding time for a reactor trip function is described as twice the response time for an input relay to drop out. The limiting components impacting the maximum credible failure times for the ULB and UVD are the self-test time and the output RC filter that limits test pulses from being sent off the board to the next device in the string. Using the same type of FMEA analysis as the original WCAP-14036-P-A provides a credible time response of 567 µSec for a reactor trip function, assuming that a new design ULB is being used in conjunction with a new design UVD board. The 567 µSec is still insignificant compared to the 20 ms bounding value. Therefore, the new cards used for trip functions are within the original bounding times for a reactor trip function, assuming that a single new design ULB is being used in conjunction with a single new design UVD board.

Similarly, the TR states for ESFAS initiating functions, the original bounding times per WCAP-14036-P-A were 26 ms for an ESF train of input relay picking up, the signal passing through the ULB and SGD, and its measurement at the output of the SGD board. An additional 26 ms was added to provide an allowance for master relay operation and 36 ms was added for each slave relay. The 26 ms is twice the expected time for an input relay to pick up. WCAP-14036-P-A stated that for the ESF functions, the expected delay for a ULB and SGD was 806 µSec. Since the 806 µSec is insignificant compared to the relay response time, there was no specific response time allocated to these cards and the bounding time for a ESF actuation was described as twice the response time for an input relay to pick up plus the additional times of the master and slave relays. Using the same type of FMEA analysis as the original WCAP-14036-P-A provides a credible time response of 567 µSec for an ESFAS actuation function, assuming that a new design ULB is being used in conjunction with a new design SGD board. The 567 µSec is still insignificant compared to the 26 ms bounding value. Therefore, the new cards used for ESFAS actuation functions are within the original bounding times for an ESFAS function assuming that a single new design ULB is being used in conjunction with a single new design SGD board.

In addition, the TR provides an analysis of the expected reactor trip or ESFAS initiation response time performance assuming that multiple stacked new design ULB, UVD, and SGD boards are being used. This analysis revealed that the worst-case (i.e., highest number of stacked circuits) safety function was the circuit used to initiate Safety Injection and Reactor Trip functions. This complex SSPS function was analyzed assuming key ULB and SGD board or UVD board failures to their worst-case time responses. The analysis revealed that the worst-case SSPS output time delay would be 2.059 ms for the ESF actuation function. Assuming that all logic cards for this function failed to their worst-case time response, the total worst-case SSPS output time delay would be approximately 2.6 ms, or approximately 10 percent of the allowed response time as described within WCAP-14036-P-A, Revision 1.

The NRC staff finds that there is sufficient information in the TR to adequately demonstrate that the performance of the new design boards have time responses that are within the bounding

times allowed for in the time response testing elimination analysis in a manner that is consistent with the NRC staff's evaluation in its approved for use of WCAP-14036-P-A, Revision 1, assuming that only new design boards are being used to accomplish reactor trip or ESFAS actuation functions. The NRC staff also notes that some licensees may elect to use an appropriate combination of new design ULB, UVD, and SGD boards in conjunction with original design SSPS boards. The new design boards have been found to require a few microseconds greater response time than their original design SSPS counterparts, and still be capable of functioning within the bounding response times described within WCAP-14036-P-A, Revision 1. The NRC staff finds the performance of the new design boards in conjunction with original design SSPS boards accomplishing the same reactor trip or ESFAS actuation function would also have time responses that are within the bounding times allowed for in the time response testing elimination analysis in a manner that is consistent with the NRC staff's evaluation in its approved for use of WCAP-14036-P-A, Revision 1.

3.6 Defense-in-Depth and Diversity

BTP 7-19, Revision 6, provides guidance to the NRC staff on performing an evaluation of the defense-in-depth and diversity of a DI&C system. Section 1.9, "Design Attributes to Eliminate Consideration of CCF [Common Cause Failure]," states testability can be used to eliminate consideration of CCF: "Testability – A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100 percent tested)."

For the purpose of minimizing the possibility of CCF from the new design boards, Westinghouse performed various analyses (See TR Sections 6, 7, and 9.4). Of the eight new design boards, three (i.e., ULB, SGD, and UVD) process the safety-related signals. These three boards each contain a main CPLD and a test CPLD (which is used to self-test the main CPLD). Each of the three main CPLDs was analyzed (See TR Section 6) to determine if there was a possibility of a design feature that could result in a CCF. In addition, each of the three test CPLDs was analyzed (see TR Section 7) for potential adverse impacts on the main CPLD. In addition, an FMEA (failure modes and effects analysis) was conducted on each board by an independent group within Westinghouse to determine the impact of component failures. The NRC does not endorse analysis as a method for eliminating consideration of CCF; however, the analyses conducted are consistent with good engineering practices and help reduce the possibility of CCF.

In addition, Westinghouse performed an analysis of all the circuits on the CPLD using the appropriate vendor supplied tool, with the intention of demonstrating that the testing that was already performed (See TR Section 5) met the "testability" criteria in BTP 7-19, Section 1.9(2), in order to eliminate consideration of CCF. This analysis demonstrated that not all possible sequences were tested, and also included additional analysis that the untested sequences did not need to be tested since they were functionally irrelevant.

The analyses and testing are sufficiently rigorous and complete to allow the NRC staff to eliminate consideration of CCF. No diverse system is required to address CCF of the CPLD-based SSPS boards.

3.7 Communications

IEEE Std. 603-1991, Clause 5.6, “Independence,” requires independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design basis events, and (3) safety systems and other systems. SRP Chapter 7, Appendix 7.1-C, Section 5.6, “Independence,” provides acceptance criteria for this requirement, and among other guidance, provides additional acceptance criteria for communications independence. Section 5.6 states where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portions, and that if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system should not be able to affect the functions of the safety system.

The IEEE Std. 7-4.3.2-2003, Clause 5.6, “Independence,” endorsed by RG 1.152, Revision 3, provided guidance on how IEEE Std. 603 requirements can be met by digital systems. This clause of IEEE Std. 7-4.3.2 specifies that, in addition to the requirements of IEEE Std. 603-1991, data communication between safety channels or between safety and non-safety systems do not inhibit the performance of the safety function. SRP Chapter 7, Appendix 7.1-D, Section 5.6, “Independence,” provides acceptance criteria for equipment qualifications. This section states 10 CFR Appendix A, GDC 24, “Separation of protection and control systems,” states “the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.”

BTP 7-11 provides guidance for the application and qualification of isolation devices. BTP 7-11 applies to the use of electrical isolation devices to allow connections between redundant portions of safety systems or between safety and non-safety systems. Therefore, this SE only considers applicability between safety and non-safety systems.

SRP Section 7.9, “Data Communications Systems,” also contains guidance for data communication systems.

Additional Guidance on interdivisional communications is contained in DI&C-ISG-04, Revision 1, “Highly-Integrated Control Rooms – Communication Issues” (ADAMS Accession No. ML083310185).

The diagrams in the TR were reviewed and it was determined that there is no digital communications between the redundant divisions of an SSPS system. Each independent division communicates to either the main control board or the plant computer. This communication is through a multiplexed line that is electrically isolated by the ISO board. In addition, the communication is one way out from the SSPS through and LED/Photo-diode circuit.

Since the new design boards do not change the SSPS design, which does not allow interdivisional communication, the design meets the Independence clause.

3.8 System, Hardware, Software and Methodology Modifications

The original SSPS was designed and documented in two topical reports (one Proprietary, one not), and was reviewed and approved by the NRC in March 1974. The designs of the logic boards were not described in these reports. The new design boards are intended to implement the same functions, and are not considered derivative designs but rather original designs in themselves. The other sections of this SE evaluate the new designs in their entirety; therefore, no evaluation of “modifications” to approved aspects was performed.

Any future revisions of this Topical Report that are required be submitted to the NRC for review and approval should follow a software development process that meets the current NRC endorsed standards and guidance.

3.9 Review of System and IEEE Std. 603 requirements

10 CFR 50.55a(h) , "Protection and Safety Systems," approves the 1991 version of IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," for incorporation by reference, including the correction sheet dated January 30, 1995.

The scope of IEEE Std. 603-1991 includes all I&C safety systems (i.e., those typically described in Sections 7.2 through 7.6 of a site-specific Updated Final Safety Analysis Report (UFSAR)). Except for the requirements for independence between control systems and safety systems, IEEE Std. 603-1991 does not apply directly to non-safety systems such as the control systems and diverse I&C systems (i.e., those typically described in Sections 7.7 and 7.8 of the UFSAR).

3.9.1 Clause 4, Design Basis

Clause 4 of IEEE Std. 603-1991 requires, in part, that a specific design basis be established for the design of each safety system. Since this is an upgrade to certain circuit boards within the SSPS system, the design basis for the new design boards is the same as the existing boards. No changes to the design basis of the SSPS was identified or reviewed.

Since the new design boards performed all of the function of the original design boards, under the same basis conditions (e.g., environmental), then the new design boards are consistent with the documented design basis (The new design boards perform all of functions of the original design boards, with some additional diagnostics and associated indications.).

3.9.1.1 Clause 4.1, Identification of the Design Basis Events

Clause 4.1 requires the identification of the design bases events applicable to each mode of operation. This information should be consistent with the analyses of UFSAR, Chapter 15, events. SRP BTP 7-4 provides specific guidance on the failures and malfunctions that should be considered in identification of design bases events for systems that initiate and control auxiliary feedwater systems. SRP BTP 7-5 provides specific guidance on the reactivity control malfunctions that should be considered in the identification of design basis events. The

malfunctions postulated should be consistent with the control system failure modes described in the UFSAR (typically Sections 7.6 and 7.7).

The plant design basis events are not being changed by the TR; therefore no evaluation against this clause was performed.

3.9.1.2 Clause 4.2, Identification of Safety Functions and Protective Actions

Clause 4.2 requires documentation of the safety functions and corresponding protective actions of the execute features for each design basis event. Since the safety functions and protective actions have not changed, conformance with this cause is ensured if each new circuit board performs the same functions as the associated original design circuit board.

The safety functions and associated protective actions are not being changed by the TR; therefore no evaluation against this clause was performed.

3.9.1.3 Clause 4.3, Permissive Conditions for Operating Bypasses

Clause 4.3 requires documentation of the permissive conditions for each operating bypass capability that is to be provided. Since the permissive conditions for each operating bypass have not changed, conformance with this cause is ensured if each new circuit board performs the same functions as the associated original design circuit board.

The permissive conditions for operating bypass are not being changed by the TR; therefore no evaluation against this clause was performed.

3.9.1.4 Clause 4.4, Identification of Variables Monitored

Clause 4.4 requires the identification of variables that are monitored in order to provide protective action. Performance criteria, including system response times, system accuracies, ranges, and rates of change, should also be identified in the system description. Since the variables monitored have not changed, conformance with this cause is ensured if each new circuit board performs the same functions as the associated original design circuit board.

The variables monitored are not being changed by the TR; therefore no evaluation against this clause was performed.

3.9.1.5 Clause 4.5, Minimum Criteria for Manual Protective Actions

Clause 4.5 requires the documentation of the minimum criteria under which manual initiation and control of protective actions may be allowed, including the points in time and the plant conditions during which manual control is allowed, the justification for permitting initiation or control subsequent to initiation solely by manual means, the range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations are to be performed, and that the variables in Clause 4.4 be displayed for use in taking manual action.

Since the new design boards are not involved in the implementation of the manual protective actions, no evaluation against this clause was performed.

3.9.1.6 Clause 4.6, Identification of the Minimum Number and Location of Sensors

Clause 4.6 requires the identification of the minimum number and location of sensors for those variables in Clause 4.4 that have spatial dependence (i.e., where the variable varies as a function of position in a particular region). The analysis should demonstrate that the number and location of sensors are adequate. Since the number and location of sensors have not changed, conformance with this cause is ensured if each new circuit board performs the same functions as the associated original design circuit board.

Since the new design boards are not involved in the implementation of the number and locations of sensors, no evaluation against this clause was performed.

3.9.1.7 Clause 4.7, Range of Transient and Steady-State Conditions

Clause 4.7 requires, in part, that the range of transient and steady-state conditions be identified for both the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform. Since the range of transient and steady-state conditions of sensors have not changed, conformance with this cause is ensured if each new circuit board performs the same functions (under the same conditions) as the associated original design circuit board.

The GDC 4 stipulates structures, systems, and components important to safety be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents.

The evaluation that each new board performs the same functions (under the same conditions) as the original design board is documented in Section 3.9.2.4.

The conditions qualified to are described in Section 3.5.

3.9.1.8 Clause 4.8, Conditions Causing Functional Degradation

Clause 4.8 requires the identification of conditions having the potential for causing functional degradation of safety system performance, and for which provisions must be incorporated to retain necessary protective action. This information should feed into additional evaluations, including Clause 5.5, “Integrity.”

The GDC 4 stipulates structures, systems, and components must be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit.

The physical conditions that must be protected against and the associated provision to protect against those conditions remain unchanged by the design change to the logic boards, with the one exception of virtual conditions, which are addressed in Section 3.12.

3.9.1.9 Clause 4.9, Methods used to Determine Reliability

Clause 4.9 requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design, and the identification of the methods used to verify that reliability goals imposed on the system design have been met.

During the April 2014 audit (ADAMS Accession No. ML14183B483), the NRC staff examined the MTBF calculations for ULB. The 80 percent duty cycle number in Table 9-1 of the TR was confirmed to match the value in the Westinghouse MTBF report. The NRC staff confirmed the calculated MTBF for the new design board is an improvement over the original board design.

These MTBF calculations identified the methods used to determine the reliability of the individual boards; therefore, the NRC staff determined that the applicant has met this criterion.

3.9.1.10 Clause 4.10, Control after Protective Actions

Clause 4.10 requires that the minimum design basis documentation include the critical points in time or plant conditions, after the onset of a design basis event. The documentation of critical points in time for the initiation of protective actions is used to derive certain performance criteria (e.g., response time); the ability of the digital safety system to meet certain performance criteria is evaluated under Clause 5.4.

Clause 4.10.3 requires the documentation of information that will be used in Clause 6.1.

The information documented under this clause should also be used in assessing conformance with Clause 6.2.3.

Section 10, of the TR addresses how the new design boards meet the existing response time criteria. To that end, Section 10 identifies the response time requirements for both Reactor Trip and ESF actuation. Therefore the response time requirements are documented. That is, the TR meets the criteria of Clause 4.10.

3.9.1.11 Clause 4.11, Equipment Protective Provisions

Clause 4.11 requires the documentation of the equipment protective provisions that prevent a safety system from accomplishing their safety function.

Since there are no equipment protective provisions that prevent a safety system from accomplishing their safety function within the new design boards, no evaluation against this criterion was performed.

3.9.1.12 Clause 4.12, Special Design Bases

Clause 4.12 requires the documentation of any other special design basis.
There are two Special Design Bases associated with software (SW): (1) common cause failure (CCF) and (2) Secure Development and Operational Environment (SDOE). The consideration of SW-CCF is addressed in Section 3.6. The consideration of SDOE is addressed in Section 3.12.

3.9.2 Clause 5, System

Clause 5 of IEEE Std. 603-1991 requires that the safety systems will, with precision and reliability, maintain plant parameters within acceptable limits established by design basis events. This criterion is addressed by insuring that the functional and performance criteria for the safety systems have been used in analyses to demonstrate that they maintain plant parameters within acceptable limits established by design basis.

Since the functional and performance requirements on the SSPS circuit boards have not been changed (except for response time), no evaluation against this criterion was performed (except for Response time which is addressed in Section 3.10.1.2.3 below).

Clause 5 of IEEE Std. 603-1991 also requires that power, instrumentation , and control portions of the safety systems be comprised of more than one safety group of which any one safety group can accomplish the safety function.

Since the safety grouping of the SSPS circuit boards have not been changed, no evaluation against this criterion was performed.

3.9.2.1 Clause 5.1, Single-Failure

Clause 5.1 requires that any single failure within the safety system shall not prevent proper protective action at the system level when needed. Guidance in the application of the single-failure criterion is provided in RG 1.53, Revision 2, “Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems,” which endorses IEEE Std. 379-2000, “Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.”

The SSPS system consists of two independent trains, the complete failure of either one will not prevent the SSPS from accomplishing its safety functions. The independence between these two trains of protective functions is maintained by the ISO boards; therefore the evaluation against these features is addressed in Section 3.9.2.6.1. In addition, periodic testing as required by the technical specifications ensures that each SSPS train is capable of performing its stipulated safety functions and that there are no failures in the system that would inhibit the safety functions.

During the April 2014 audit (ADAMS Accession No. ML14183B483), the FMEAs of the new design boards were examined to ensure there were no undetectable failures within the new design boards and certain concerns were raise in the audit report. The PWROG addressed these concerns by revising the FMEAs. Of the three FMEAs revised, the NRC selected the

FMEA for the ULB for docketing and confirmation of appropriate revision (ADAMS Accession No. ML14213A100).

The FMEAs document the analysis that there are no undetectable failures that could adversely impact the safety function of the SSPS boards. The NRC staff reviewed a sample (i.e., the ULB FMEA) of the FMEAs and determined that they were sufficiently comprehensive and complete. Therefore, the two independent trains of the SSPS continue to meet the single failure criterion.

Section 3.6, "Defense-in-Depth and Diversity," document the NRC staff evaluation of the testing and analysis to eliminate consideration of CCF.

3.9.2.1.1 Failure Modes and Effects Analysis

An FMEA can be used to address two regulatory requirements, GDC 23 and IEEE 603-1991, Clause 5.1. These two requirements mean that each system must be evaluated to understand the potential failures and the effects of those failures.

GDC 23, "Protection system failure modes," stipulates that the protection system be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

IEEE 603-1991, Clause 5.1, "Single-Failure Criterion," stipulates that the safety systems perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures and (2) all failures caused by the single failure. An FMEA is a method of analysis of potential failure modes within a system for determination of their effects. This information can then be used to assess the potential for an undetectable failure; therefore, an FMEA is a method for documenting a single failure analysis which can be conducted in accordance with IEEE Std. 379-2000 as endorsed by RG 1.53 (i.e., see Section 3.9.2.1, "Clause 5.1, Single-Failure," above).

Section 9.4, "FMEA Studies," of the TR summarizes describes three analysis performed on each board. The FMEAs for the ULB, UVD, and SGD boards were examined as part of the audit conducted in April of 2014 (ADAMS Accession No. ML14183B483). The FMEAs of the other boards were not examined during the audit because they were deemed to be less safety significant. That is, the safety functions of the SSPS are performed by only these three boards. The FMEA studies resulted in two conclusions (as documented in the TR):

1. There are no non-detectable failures that when paired with a detectable failure would cause a loss of safety function. (Addressing IEEE 603-1991, Clause 5.1)

2. The new design boards do not produce a different failure mode than has been previously analyzed. (Addressing GDC 23)

The NRC selected the FMEA for the ULB for docketing and review. A sample of the possible failures (e.g., failure of LEDS) that was analyzed in the FMEA was read and it was concluded that these analyses followed generally accepted industry practices and is acceptable.

A regulatory function (see Clause 5.1) of the FMEA with respect to the single failure criteria is to demonstrate that here are no undetectable failures that could inhibit the safety function. The entire ULB FMEA was skimmed to confirm that there were no such failures identified. The NRC staff did not find any identified failures in the ULB FMEA, therefore the FMEA studies document that the single failure criterion was met.

In addition, another regulatory function (See GDC 23) of an FMEA is to ensure that the protection system is designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis. Since the new design boards do not introduce any new or different failure mode, the SSPS continues to meet GDC 23.

3.9.2.2 Clause 5.2, Completion of Protective Action

Clause 5.2 requires that the safety systems be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features continues until completion, and that deliberate action is necessary to return the safety systems to normal. Appendix 7.1-C, Section 5.2, of the SRP provides acceptance criteria for this requirement.

Since this criterion is met by features outside the new design boards, no evaluation against this criterion was performed.

3.9.2.3 Clause 5.3, Quality

Clause 5.3 contains two requirements (one for “Product – (1)” quality and one for “Process - (2)” quality): (1) components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates, and (2) safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

The GDC 1 also contains “Product – (1)” and “Process – (2)” related quality requirements: (1) “structures, systems, and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed, and where generally recognized codes and standards are used, they must be identified and evaluated to determine their applicability, adequacy, and sufficiency and must be supplemented or modified as necessary to assure a quality product in keeping with the required safety function” and (2) “a quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.”

The technical evaluation of the new design boards focused on the product quality criteria since Westinghouse has an approved QA program that is evaluated separately. Certain product

quality criteria are achieved through technical aspects of the product as it is designed, manufactured, inspected, installed, tested, operated, and maintained; the evaluation of the development process of the new design boards against the related quality criteria is documented in Section 3.4.

In addition, the requirements for the new design boards include certain enhancements to improve the reliability or maintainability. The enhancements to each of the new design boards are described in Section 2 of the TR. The NRC staff reviewed these enhancements and agrees they improve the reliability and maintainability of the new designs; therefore this aspect of Clause 5.3 has been met.

3.9.2.4 Clause 5.4, Equipment Qualification

The IEEE Std. 603, Clause 5.4, states safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it should be capable of meeting the performance criteria as specified in the design basis (e.g., IEEE Std. 603, Clause 4.10), while being exposed to specified environmental conditions (e.g., IEEE Std. 603, Clause 4.7). Appendix 7.1-C, Section 5.4, of the SRP provides acceptance criteria for Clause 5.4.

The conditions under which each new board should be able to perform the same functions as the original design boards are documented in Section 3.9.1.7.

Environmental equipment qualification is addressed in Section 3.5.

Sections 2.1.2.2 and 10 of the TR address response time of the new design boards and of the SSPS system after the new design boards are installed. The new design boards and resulting SSPS were evaluated and tested against bounding response time criteria described in WCAP-14036-P-A, Revision 1, “Elimination of Periodic Protection Channel Response Time Tests” (ADAMS Accession No. ML100050325). The analysis demonstrated that the SSPS response time is dominated by relay actuation times and not by individual circuit board response times. Since the SSPS response time is ensured to be twice the relay response times, the small changes in the response times of the individual circuit boards is insignificant. This is further evaluated in Section 3.5.3 above.

Based on the response time analysis provided in the TR (see TR Section 10), the NRC staff concludes the new design circuit boards meet the response time criteria and therefore meet Clause 5.4 in this respect.

3.9.2.5 Clause 5.5, System Integrity

Clause 5.5 requires that the safety systems be designed such that the system can accomplish its safety functions under the conditions having the potential for causing functional degradation of safety system performance, and for which provisions must be incorporated to retain necessary protective action. SRP Chapter 7, Appendix 7.1-C, Section 5.5, “System Integrity,” provides acceptance criteria for system integrity. This acceptance criteria states the NRC staff may assess whether tests have been conducted on safety system equipment components and the system racks and panels as a whole to demonstrate the safety system performance is

adequate to ensure completion of protective actions despite conditions having the potential for causing functional degradation of safety system performance. The test or analysis should show that if the system does fail, it fails in a safe state, and that failures detected by self-diagnostics should also place a protective function into a safe state.

The physical conditions that must be protected against and the associated provision to protect against those conditions remain unchanged by the design change to the logic boards, with the one exception of virtual conditions, which are addressed in Section 3.12.

3.9.2.6 Clause 5.6, Independence

Clause 5.6 requires independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design bases events, and (3) safety systems and other systems.

Guidance for evaluation of physical and electrical independence is provided in RG 1.75, Revision 3, "Criteria for independence of Electrical Safety Systems," which endorses IEEE Std. 384-1992, "IEEE Standard Criteria for independence of Class 1E Equipment and Circuits." The safety system design should not have components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features that could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence is attained by physical separation and physical barriers. Electrical independence should include the use of separate power sources. Transmission of signals between independent channels should be through isolation devices.

SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence," provides additional acceptance criteria for communications independence. Section 5.6 states where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety function of the redundant portions. Further, if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system must not be able to affect the functions of the safety system. Section D.7 and DI&C-ISG-04 provide additional information on this topic.

3.9.2.6.1 Clause 5.6.1, Between Redundant Portions

Clause 5.6.1 states the safety systems shall be designed so that there is sufficient independence between redundant portions of a safety system such that the redundant portions are independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. Section D.7 and DI&C-ISG-04 describes the criteria for demonstration of this independence.

One of the ISO board's functions in the system is to provide a 1E barrier between the redundant SSPS divisions. Section 3.1.8 contains a brief description of this board. The new design board is designed to meet the same criteria as the original design board.

The BTP 7-11 identifies that RG 1.75, Revision 3, “Criteria for Independence of Electrical Safety Systems,” endorses IEEE Std. 384-1992, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,” which identifies specific electrical isolation criteria for isolation devices used in instrumentation and control circuits. IEEE 384, Section 7.2.2, “Isolation Devices,” contains specific criteria. Essentially, isolation devices must be designed and tested to withstand the maximum credible transient applied to one side of the device and not degrade the operation of the circuit connected to the other side below an acceptable level.

Section 8.5, of the TR describes how the maximum credible transient (for testing purposes) was determined, and it references a test report as documenting that the ISO board met this criteria. Section 8.5 contains sufficient detail to allow the NRC staff to conclude that the ISO board conforms to the criteria in Clause 5.6.1.

3.9.2.6.2 Clause 5.6.2, Effects of Design Basis Event

Clause 5.6.2 states the safety systems necessary to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of IEEE Std. 603. Clause 5.6.2 further states equipment qualification in accordance with Clause 5.4 is one method that can be used to meet this requirement. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that the degree of independence is sufficient.

Environmental equipment qualification is addressed in Section 3.5.

3.9.2.6.3 Clause 5.6.3, Other Systems

Clause 5.6.3 states the safety systems shall be designed such that credible failures in and consequential actions by other systems do not prevent the safety systems from meeting the requirements of IEEE Std. 603. Clause 5.6.3 is subdivided into sub-clauses for interconnected equipment, equipment in proximity, and the effects of a single random failure. Each of the sub-clauses should be addressed in the following paragraphs.

Clause 5.6.3.1 of IEEE Std. 603, “Interconnected Equipment,” states equipment that is used for both safety and non-safety functions, as well as the isolation devices used to affect a safety system boundary, shall be classified as part of the safety systems. This clause further states no credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance criteria during and following any design basis event needing that safety function and that a failure in an isolation device will be evaluated in the same manner as a failure of other equipment in a safety system. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that the degree of independence is sufficient.

SRP BTP 7-11, “Guidance on Application and Qualification of Isolation Devices,” provides guidance for the application and qualification of isolation devices. BTP 7-11 applies to the use of electrical isolation devices to allow connections between redundant portions of safety systems or between safety and non-safety systems. This evaluation section only considers the independence between safety and non-safety systems.

Clause 5.6.3.2 of IEEE Std. 603, “Equipment in Proximity,” states equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, will be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment, and that physical separation may be achieved by physical barriers or acceptable separation distance.

This clause further states the physical barriers used to form a safety system boundary shall meet the requirements of Clause 5.3, Clause 5.4, and Clause 5.5 for the applicable conditions specified in Clause 4.7 and Clause 4.8 of the design basis. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that the degree of independence is sufficient.

Clause 5.6.3.3 of IEEE Std. 603, “Effects of a Single Random Failure,” requires that where a single random failure in a non-safety system can (1) result in a design basis event and (2) also prevent proper action of a portion of the safety system designed to protect against that event. The remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. IEEE Std. 379 provides additional guidance for the application of this requirement.

One of the ISO board’s functions in the system is to provide a Class 1E barrier between the safety-related logic and actuation signals and the non-safety indication signals used by the main control board and the plant computer. Section 3.1.8 contains a brief description of this board.

BTP 7-11 identifies that RG 1.75, Revision 3, “Criteria for Independence of Electrical Safety Systems,” endorses IEEE Std. 384-1992, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,” which identifies specific electrical isolation criteria for isolation devices used in instrumentation and control circuits. IEEE 384, Section 7.2.2, “Isolation Devices,” contains specific criteria. Essentially, isolation devices must be designed and tested to withstand the maximum credible transient applied to the device’s non-Class 1E side and not degrade the operation of the circuit connected to the Class 1E device below an acceptable level.

Section 8.5, of the TR describes how the maximum credible transient (for testing purposes) was determined, and it references a test report as documenting that the ISO board met this criteria. Section 8.5 contains sufficient detail to allow the NRC staff to conclude that the ISO board conforms to the criteria in Clause 5.6.3.

3.9.2.7 Clause 5.7, Capability for Test and Calibration

Clause 5.7 requires the capability for testing and calibration of the safety system equipment be provided while retaining the capability of the safety systems to accomplish their safety functions during power operations. It is expected that safety systems should be periodically tested; however, there are no features on the new design boards that are adjustable for calibration purposes. In addition, SRP BTP 7-17, “Guidance on Self-Test and Surveillance Test Provisions,” provides guidelines for reviewing the design of the self-test and surveillance test provisions. BTP 7-17 states (in part): “Surveillance test and self-test features for digital

computer-based protection systems should conform to the guidance of RG 1.22 and RG 1.118. Bypasses necessary to enable testing should conform to the guidance of RG 1.47."

The new design boards are described in Section 2, "Board Descriptions," of the TR, and Appendix A, "SSPS New Design Boards Theory of Operation," describes how the boards perform their required functions. These sections describe the Test CPLD on the ULB, SGD, and UVD boards and the associated status indications (i.e., board edge LEDs). In addition these sections describe the SAT and CCB boards and their associated operations. The ISO board is involved in testing to the extent that the ISO board outputs to the main control board Demultiplexer and to the plant computer Demultiplexer (if applicable) are inhibited during testing. In addition the DEC board has manual test switches to assist in trouble shooting multiplexing problems in the SSPS train without needing to remove the train from service.

The new design boards can be tested while in the SSPS cabinets, in the same manner as the original design boards, that is, the same functional test procedures (and associated required frequencies) that are currently being used for surveillance testing will not need to be changed to accommodate testing of the new design boards; therefore, no change to the manner of testing the SSPS is being proposed by the TR. Individual tests of the SSPS logic boards can be accomplished through specific switches in the SSPS that are not being changed as part of the TR. Sequences of tests are also automated and implemented on the SAT and CCB boards. In addition to these original capabilities to test the SSPS, the three of the new design boards (i.e., ULB, SGD, and UVD) include self-test features and additional diagnostic indications that enhance the ability for early identification of questionable board status; however, none of these new features are being credited for meeting regulatory requirements.

Based on the fact that the new design boards implement the same self-test functionality as the original design boards, these new boards meet the regulatory requirement for capability to test the SSPS system.

3.9.2.8 Clause 5.8, Information Displays

Clause 5.8 contains no requirements, but has four sub-clauses that do contain requirements.

3.9.2.8.1 Clause 5.8.1, "Display for Manually Controlled Actions"

Clause 5.8.1 requires that display instrumentation provided for manually controlled actions for which no automatic control is provided and that are necessary for the safety systems to accomplish their safety functions will be part of the safety systems. The design should minimize the possibility of ambiguous indications.

The circuit boards on the SSPS do not process signals for display or indication of process variables; therefore, this regulatory requirement is not applicable to the TR.

3.9.2.8.2 Clause 5.8.2, "System Status Indication"

Clause 5.8.2 requires that display instrumentation provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features.

Further, the design should minimize the possibility of ambiguous indications. The review of information displays for manually controlled actions should include assessment whether the displays will be functional (e.g., power will be available and sensors are appropriately qualified) during plant conditions under which manual actions may be necessary.

The new design boards process the same signals for display/indication of actuation status; therefore, no review against these criteria was performed.

3.9.2.8.3 Clause 5.8.3, “Indication of Bypasses”

Clause 5.8.3 requires that protective actions that have been bypassed or deliberately rendered inoperative for any other purpose be continuously indicated in the control room; this display instrumentation does not need to be considered a part of the safety system. The indication must be automatically actuated if the bypass or otherwise inoperative condition is expected to occur more frequently than once per year and is expected to occur when the affected system is specified to be operable. Safety system bypass and inoperable status indication should conform to the guidance of RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems.”

The new design boards process the same signals for display/indication of bypassed status as the original design boards; therefore, no specific review against these criteria was performed. This criterion was addressed generically by the evaluation that the new design boards perform the same functions as the original design boards, see Sections 3.1.1 through 3.1.8.

3.9.2.9 Clause 5.9, Control of Access

Clause 5.9 requires that the safety system be designed to permit administrative control of access to the equipment. Administrative access limited to qualified plant personnel is acceptable if done with the permission of the control room operator. The system should be designed with alarms and locks to preclude inappropriate access. Additionally, electronic access to the system (e.g., via a network connection) should be sufficiently restricted.

The TR only changed the logic boards with the SSPS cabinets; therefore, no physical control of access provisions is being changed. In addition, no electronic (i.e., digital or virtual) provisions are introduced since there are no digital communications added while the system is in operation.

The provisions for SDOE address, in part, control of access. The provisions to address SDOE are evaluated in Section 3.12.

3.9.2.10 Clause 5.10, Repair

Clause 5.10 requires that the safety system be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

The new design boards provide the same signals for recognition, location, replacement, and repair (the SSPS boards are not designed to be adjustable) of malfunctioning equipment; however, the new design boards also contain additional indications in the form of board edge

LEDs that are visible when the cabinet doors are opened. The LED indications include actuation status and certain fault identifications that are the result of the self-testing CPLD interrogating the main CPLD. Therefore, with respect to this criterion, the new design boards are superior to the existing boards, and are acceptable.

3.9.2.11 Clause 5.11, Identification

Clause 5.11 requires that the safety system equipment and documentation be distinctly identified for each redundant portion of a safety system; however, components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.

The new design boards are mounted in equipment that is clearly identified as being in a single redundant portion of a safety system (e.g., SSPS Train A); therefore the identification criteria is met by the individual new design boards. The boards are clearly marked for configuration management purposes.

3.9.2.12 Clause 5.12, Auxiliary Features

Clause 5.12 requires that auxiliary supporting features meet all requirements of IEEE Std. 603 and that auxiliary features meet those criteria necessary to ensure that they do not degrade the safety system below an acceptable level.

During the April 2014 audit (ADAMS Accession No. ML14183B483), the NRC staff examined the design of the auxiliary features on the ULB, SGD and UVD boards to evaluate conformance with IEEE 603-1991, Clause 5.12. The NRC staff found that auxiliary features will not impede the safety function in accordance with IEEE Std. 603-1991, Clause 5.12. Further, the NRC staff also identified that new design boards eliminate a significant number of single point vulnerabilities that existed in the original design board designs. New design boards also offer broad fault detection capability that will improve debug times both on and off the boards, a known issue with the original design boards. The NRC staff was not able to identify any failures that would impede the safety function that are not detectable. Finally, the NRC staff examined the MTBF calculations and confirmed the reliability of the new design boards is improved over the original design.

3.9.2.13 Clause 5.13, Multi-Unit Stations

Clause 5.13 requires that any shared structures, systems, or components between multi-unit generating stations be capable of simultaneously performing all necessary safety functions in any or all units. Guidance on the sharing of electrical power systems between units is contained in RG 1.32, Revision 3, “Criteria for Power Systems for Nuclear Power Plants,” which endorses IEEE Std. 308-2001. Guidance on application of the single-failure criterion to shared systems is contained in RG 1.53, Revision 3, which endorses IEEE 379-2000.

The logic boards in the SSPS cabinets only support one unit at a time and therefore this criterion is not applicable.

3.9.2.14 Clause 5.14, Human Factors Considerations

Clause 5.14 requires that human factors be considered at the initial stages and throughout the development process to assure that the functions allocated in whole or in part to the users and maintainers can be successfully accomplished to meet the safety system design goals.

Section 9.5, “Human Factors Considerations,” of the TR contains a summary of the design consideration relating to the new LEDs.

The new design boards provide the same signals for recognition, location, replacement, and repair of malfunctioning equipment; however, the new design boards also contain additional indications in the form of board edge LEDs that are visible when the cabinet doors are opened. The LED indications include certain fault identifications that are the result of the self-testing CPLD interrogating the main CPLD. Therefore, with respect to the “maintainers” aspect of this criterion, the new design boards are superior to the existing boards, and are acceptable. With respect to the “users” aspect of this criterion, the new design boards are the same as the existing boards, and are acceptable.

3.9.2.15 Clause 5.15, Reliability

Clause 5.15 requires that for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved.

Section 9, “Reliability, Failure Modes and Effects, and Human Interface Analyses,” of the TR contains a description of the analyses to support the reliability assessment of the new design boards:

- CPLD Reliability
- Mean Time Between Failure Calculations
- Single Point Vulnerability Studies
- Failure Modes and Effects analyses

This reliability assessment demonstrates that the reliability of the new design boards is at least as good as the reliability of the original design boards; therefore the reliability of the new design boards is acceptable.

3.9.3 Clauses 6, Sense and Command Features

Clause 6 of IEEE Std. 603-1991 provides the requirements for sensors and command features. The new design boards are only part of the Sense and Command Features; therefore, some of the sub-clauses of IEEE Std. 603-1991, Clause 6 are not applicable, as indicated below.

3.9.3.1 Clause 6.1, Automatic Control

Clause 6.1 requires that for each design basis event, all protective actions should automatically initiate, with the exception of those justified in Clause 4.5.

The TR does not propose any changes to the automatic controls that are, in part, implemented by the new design boards; therefore, no evaluation against this criterion was performed.

3.9.3.2 Clause 6.2, Manual Control

Clause 6.2 requires that means be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions, that the means will minimize the number of discrete manipulations, and will depend on the operation of a minimum of equipment consistent with the constraints of Clause 5.6.1 of IEEE Std. 603. RG 1.62 provides further guidance on this topic.

Clause 6.2 also requires implementation of manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 5.2 of IEEE Std. 603, with the information provided to the operators, the actions needed of these operators, and the quantity and location of associated displays and controls be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators, in an environment suitable for the operator, and suitably arranged for operator surveillance and action.

The implementation of the manual controls is outside of the new design boards; therefore, no evaluation against this criterion was performed.

3.9.3.3 Clause 6.3, Interaction with Other Systems

Clause 6.3 requires that if a single credible event can both cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designed to provide principal protection against the condition, either alternate channel or alternate equipment not subject to this failure be provided, or equipment not subject to failure caused by the same single credible event be provided. If the event of concern is a single failure of a sensing channel shared between control and protection functions, isolating the safety system from the sensing channel failure by providing additional redundancy or isolating the control system from the sensing channel failure by using data validation techniques to select a valid control input is acceptable.

The SSPS receives binary inputs from the PPS. The interaction with other systems is accounted for in the design of the PPS. The TR does not propose any changes to these interactions; therefore no evaluation against this criterion was performed.

3.9.3.4 Clause 6.4, Derivation of System Inputs

Clause 6.4 requires that, to the extent feasible and practical, sense and command feature inputs be derived from signals that are direct measures of the desired variables as specified in the design basis. If indirect parameters are used, the indirect parameter must be shown to be a

valid representation of the desired direct parameter for all events. Further, for both direct and indirect parameters, the characteristics of the instruments that produce the safety system inputs, such as range, accuracy, resolution, response time, and sample rate should be described.

The SSPS receives binary inputs from the PPS. That is, the ULB function in the SSPS is to provide voter logic to generate reactor trip and ESFAS actuation signals based on process protection system inputs and field contact inputs. The derivation of system inputs are accounted for in the design of the PPS. The TR does not propose any changes to these inputs; therefore no evaluation against this criterion was performed.

3.9.3.5 Clause 6.5, Capability for Testing and Calibration

Clause 6.5 requires that it must be possible to check, with a high degree of confidence, the operational availability of each sensor needed for a safety function during reactor operation, including the availability of those sensors that are needed during the post-accident period. SRP Chapter 7, Appendix 7.1-C, Section 6.5, “Capability for Testing and Calibration,” provides acceptance criteria for Clause 6.5.

The SSPS boards receive binary inputs from the PPS; they do not contain sensors or receive indications directly from sensors. The features used to check the operational availability of each input sensor needed for a safety function resides outside of the SSPS logic boards; therefore no evaluation against this criterion was performed.

3.9.3.6 Clauses 6.6, Operating Bypasses

Clause 6.6 requires that if the applicable permissive conditions are not met, a safety system must automatically prevent the activation of an operating bypass or initiate the appropriate safety function. Further, if plant conditions change such that an activated bypass is no longer permissible, the safety system must either remove the appropriate active operating bypass, restore plant conditions to the permissive conditions, or initiate the appropriate safety functions. The requirement for automatic removal of operational bypasses means that the reactor operator may not have a role in such removal; however, the operator may take action to prevent the unnecessary initiation of a protective action.

The operating bypass features of the SSPS are not implemented in the new design boards; they are implemented outside of these boards; therefore, no evaluation against this criterion was performed.

3.9.3.7 Clauses 6.7, Maintenance Bypass

Clause 6.7 requires that the safety system be designed such that while sense and command features equipment is in maintenance bypass, the capability of a safety system to accomplish its safety function must be retained, and during such operation, the sense and command features must continue to meet the Clauses 5.1 and 6.3. Additionally, provisions for a bypass must be consistent with the Technical Specification action statements.

The maintenance bypass features of the SSPS are not implemented in the new design boards; they are implemented outside of these boards; therefore no evaluation against this criterion was performed.

3.9.3.8 Clause 6.8, Setpoints

Clause 6.8 requires that the allowance for uncertainties between the process analytical limit documented in Clause 4.4 and the device setpoint must be determined using a documented methodology. Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design must provide a positive means of ensuring that the most restrictive setpoint is used.

The SSPS receives binary inputs from the PPS. The allowance for uncertainties between the process analytical limit documented in Clause 4.4 and the device setpoint are accounted for in the setpoint methodology of the PPS. The TR does not propose any changes to the setpoint methodology; therefore no evaluation against these setpoint criteria was performed.

3.9.4 Clause 7, Execute Features

Clause 7 provides the requirements for actuators and other executable features.

The IEEE 603-1991 describes the three general elements of a safety system to be: (1) Sense and Command Features, (2) Execute Features, and (3) Power Sources. The new design boards are part of the sense and command features of the SSPS system, not part of the Execute Features; therefore these criteria do not apply and no evaluation against this criterion was performed.

3.9.5 Clause 8, Power Source

Clause 8 provides the requirements for the power sources supporting the DI&C system. Clause 8 requires that those portions of the Class 1E power system that are needed to provide the power to the many facets of the safety system are governed by the criteria of IEEE Std. 603-1991 and are considered a portion of the safety systems.

The IEEE 603-1991 describes the three general elements of a safety system to be: (1) Sense and Command Features, (2) Execute Features, and (3) Power Sources. The new design boards are part of the sense and command features of the SSPS system, not part of the Power Source features; therefore this criterion does not apply and no evaluation against this criterion was performed.

3.10 Review IEEE Std. 7-4.3.2

10 CFR 50.55a(h) , "Protection and Safety Systems," approves the 1991 version of IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," for incorporation by reference, including the correction sheet dated January 30, 1995.

The IEEE Std. 603-1991 does not directly discuss digital systems, but states guidance on the application of its criteria for safety systems using digital programmable computers (e.g., Field

Programmable Gate Arrays (FPGAs) and CLDs) is provided in IEEE Std. 7-4.3.2. IEEE Std. 7-4.3.2-2003 is endorsed by RG 1.152, Revision 3. IEEE Std. 7-4.3.2-2003 serves to amplify the criteria in IEEE Std. 603-1991. Within the context of IEEE Std. 7-4.3.2-2003, the term computer is a system that includes FPGAs, CPLDs, computer hardware, software, firmware, and interfaces.

3.10.1 Clause 5, System

Clause 5 contains no additional criteria beyond those in IEEE Std. 603-1991; however, some of the sub-clauses contain additional criteria. The sub-clauses are described in 5.1 through 5.15.

3.10.1.1 Clause 5.3, Quality

Clause 5.3 describes the typical digital system development life cycle. The licensee should describe the development life cycle actually used for the development of the system being proposed, and compare this to the typical life cycle. Any difference in the life cycle should be explained and justified.

Clause 5.3 contains two normative Criteria:

(1) "Computer development activities shall include the development of computer hardware and software."

(2) "The integration of the computer hardware and software and the integration of the computer with the safety system shall be addressed in the development process."

Clause 5.3 also contains 6 sub-parts that are addressed in detail below.

3.10.1.1.1 Clause 5.3.1, Software Development

Clause 5.3.1 requires an approved QA plan for all software that is resident at run time. In addition, the NRC staff considers this to include software, that while not itself resident at run time, is used to program the system (e.g., software used to generate hardware based logic). QA is the planned and systematic activities implemented within the quality system, and demonstrated as needed, to provide adequate confidence that an entity will fulfil requirements for quality. Westinghouse has an approved Quality Management System; an NRC approved 10 CFR 50 Appendix B quality assurance program that was evaluated separately. Project specific planned and systematic activities are evaluated in Section 3.4.2, "Planning Documentation." Therefore the planning and implementation activities for a quality assurance plan have been reviewed by the NRC staff and are sufficient for demonstrating that Clause 5.3.1 is met.

3.10.1.1.2 Clause 5.3.2, Software Tools

Clause 5.3.2 specifies that software tools used to support software development processes and V&V processes be controlled under the configuration management plan. The tools are further specified to be either developed to a similar standard as the safety-related software or the tools

be used in a manner such that defects not detected by the tools should be detected by V&V activities.

Configuration control of tools of the CPLD development tools was maintained under configuration control by Westinghouse as described in TR Section 4.5.1, “Configuration Control of Software.” Westinghouse evaluated the CPLD and associated development tools in order to minimize the possibility of these aspects for introducing problems. However, the output of the CPLD development tools (i.e., the circuit boards) was comprehensively tested (as described in TR Section 5); therefore, the CPLD development tools did not require qualification.

Westinghouse has a well-established configuration control system, the details of which were not evaluated during this review effort; the Westinghouse configuration management system has been evaluated elsewhere. The NRC staff reviewed the extensive testing and determined that it was adequate for not requiring that the CPLD development tools be demonstrated to have been developed in a high quality manner. Therefore the configuration management and testing are sufficient for demonstrating that Clause 5.3.2 is met.

3.10.1.1.3 Clause 5.3.3, Verification and Validation

Clause 5.3.3 states a V&V program should exist throughout the system lifecycle and that the software V&V effort should be performed in accordance with IEEE Std. 1012, as endorsed by RG 1.168, the criteria for the highest level of integrity (level 4) should be applied.

As identified in Section 3.4.1, “NRC staff Review Approach to the Development Process,” qualitative review of the development process for consistency with DI&C guidance documents, such as RG 1.168 and IEEE Std. 1012, would have limited results given the circumstances.

The (software) V&V analysis and reports is addressed in Section 3.4.3.1.

3.10.1.1.4 Clause 5.3.4, Independent V&V (IV&V)

Clause 5.3.4 defines the levels of independence necessary for the V&V effort in terms of technical, managerial, and financial independence.

The NRC staff conducted the second audit on July 15-17, 2014, at the Westinghouse Twinbrook facility in Rockville, Maryland. Of particular importance related to V&V reviews was the NRC staff observation that there was inconsistent independence of the verifiers performing V&V activity, as required by 10 CFR 50 Appendix B, involved in both design and testing activities. The PWROG took an action item to more thoroughly describe the testing, emphasizing the independence of the testing activities from the development activities.

The continuation of independent V&V discussion is provided in Section 3.4.3.1, “V&V Analysis and Reports,” of this SE.

3.10.1.1.5 Clause 5.3.5, Software Configuration Management

The files for the project lend themselves to configuration by procedures, assembly drawings and bills of materials (BOM) normally established and maintained as hardware components and systems.

The configuration management of the CPLD is controlled by the assembly drawing, artwork drawings, artwork Gerber files, configuration file and the chip manufacturer software tool, all of which are archived in EDMS. The files in EDMS are accessible but not changeable. Any change to the documents archived in EDMS would have to be a new revision and would not over write the existing archived revision.

The assembly drawing (e.g., ULB Assembly 6D30225) contains the assembly and manufacturing notes, BOM and assembly figure. In addition, the assembly drawing references (within the BOM) the artwork drawing, manufacturing test procedure, applicable configuration procedure, commercial dedication instruction, and schematic drawings. In the notes of the assembly drawing the specific allowable CPLD configuration files (located in EDMS) and the acceptable artwork revision are identified. The chip manufacturer software tool is included in the CPLD configuration file in EDMS. The artwork drawing (e.g., ULB artwork 3D91483) identify the required Gerber file for the board. The artwork revision (e.g., A02) must match the artwork revision identified in the assembly drawing.

The configuration management is also addressed in Section 3.4.2, “Planning Documentation.”

Westinghouse evaluated these configuration methods for the suitability for intended for the circuit boards developed as hardware devices and the commercially dedicated CPLDs (as described in TR Section 4.7) and found them acceptable.

3.10.1.1.6 Clause 5.3.6, Software Project Risk Management

Clause 5.3.6 defines the risk management activities for a software project. Project risk management is a tool for problem prevention: identifying potential problems, assessing their impact, and determining which potential problems must be addressed to assure that quality goals are achieved.

The NRC staff considers the use of commercial software and hardware to be attractive due to cost, schedule and availability, but there is some risk that a commercial grade dedication process will reveal a lack of the quality necessary for use in safety-related systems in nuclear power plants.

The project risk issues for this project are discussed in Section 4 of the TR and are acceptable to the NRC staff.

In Section 3.4.2, “Planning Documentation,” the NRC staff identified some inconsistencies existing in the planning documentation and with regards to the supporting documentation for the selection of the commercial design vendor and the applicability of the industry guidance to be used in the manufacturing process that may be related to risk.

The validity of risk is difficult to evaluate and particularly difficult to quantify after the process is completed without flaws related to the process identified to date. However, the NRC staff considers the maximum use of industry and NRC staff guidance as well as thorough documentation of the basis for engineering judgment, particularly when commercial grade dedication is involved, as described by the NRC staff SE on EPRI TR-106439, to adequately address this topic.

3.10.1.2 Clause 5.4, Equipment Qualification

Clause 5.4 defines the equipment qualification for a software project. These criteria, as expanded in sub-clauses 5.4.1 and 5.4.2, are in addition to those given in IEEE Std. 603-1991. The evaluation against these criteria is documented in Section 3.5, “System Qualifications.”

3.10.1.2.1 Clause 5.4.1, Computer System Testing

Clause 5.4.1 specifies that the system qualification testing be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs, outputs, display functions, diagnostics, associated components, communication paths, and interfaces. The evaluation against these criteria is documented in Section 3.5, “System Qualifications.”

3.10.1.2.2 Clause 5.4.2, Qualification of Existing Commercial Computers

Clause 5.4.2 defines the qualification of existing commercial computers for use in safety-related applications in nuclear power plants.

Existing computer components (i.e., CPLDs) were used in some of the new design boards; however, this criterion applies to computers as a whole and not to computer components. Each normative criterion under Clause 5.4.2 was examined for applicability to CPLDs; none were determined to be applicable.

Westinghouse evaluated the CPLD development tools for suitability for intended use (as described in TR Sections 4.3, 4.4, and 4.5 and evaluated in Section 3.10.1.1.2) and commercially dedicated the CPLDs (as described in TR Section 4.7).

3.10.1.2.3 Performance – Response Time

The IEEE 603-1991, Clause 4.10, requires that the design basis documentation contain the critical points in time after the onset of a design basis event for which the protective actions shall be initiated. IEEE 603-1991, Clause 5, requires that the safety system, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. IEEE 7-4.3.2-2003, Clause 5.4.1 (endorsed by RG 1.152, Revision 3), established that computer system qualification (e.g., response time performance) be performed with the computer functioning with diagnostics running (if the diagnostics are expected to be running during operation).

Section 10 of the TR describes the analyses and testing to justify the acceptability of the response times of the new design boards. This summary of the testing and analysis indicate that acceptable engineering practices were followed; therefore there is reasonable assurance that the boards meet the response time criteria. The NRC staff's evaluation of response time is discussed in Section 3.5.3 above.

3.10.1.3 Clause 5.5, System Integrity

Clause 5.5 specifies that in addition to the system integrity criteria provided by IEEE Std. 603-1991, the digital system should be designed for computer integrity, test and calibration, and fault detection and self-diagnostic activities. Sub-clauses 5.5.1 through 5.5.3 provide further criteria.

3.10.1.3.1 Clause 5.5.1, Design for Computer Integrity

Clause 5.5.1 specifies that the computer be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function (e.g., as required to be documented under IEEE 603-199 Clauses 4.7 and 4.8).

Digital equipment may be more sensitive to EMI/RFI than some analog equipment; therefore, sensitivity to EMI/RFI is addressed during equipment qualification, see Section 3.5. Other natural phenomena and environmental effects are also addressed in Section 3.5.

For input signals the new design boards are designed to operate at the same voltage levels as the original design boards (see TR Section 2).

Power supply fluctuation was covered in Section 8 of the TR. As part of the equipment qualification testing, power supply voltages for the 48 Vdc and 15 Vdc were varied by +/- 10 percent as specified in the requirements of WCAP 8587. The test was administered on a chassis of boards powered by a variable DC voltage source, and monitored for changes of output state while inputs were held at steady state. The evaluation of this testing is done in Section 3.5 of this SE.

3.10.1.3.2 Clause 5.5.2, Design for Test and Calibration

Clause 5.5.2 specifies that test functions not adversely affect the ability of the system to perform its safety function and that V&V, configuration management and QA are necessary for test functions that are inherent to the computer that is part of the safety system.

There are two categories of test features in the new design boards: (1) the self-test CPLDs (only on ULB, SGD, and UVD), and (2) the SAT board. The new implementation of the SAT board performs the same tests as the original design boards; the PWROG's intent was not to change this feature.

There is no difference in the configuration management or QA for self-test functions in the test CPLDs or the SAT board. The self-test functions were shown (see TR Section 7) and audited to not adversely affect the safety function (see April 2014 audit, ADAMS Accession No. ML14183B483). The self-test functions were not as rigorously tested (e.g., through fault

injections testing) as the functions associated with the protective actions; however, the functional testing and system testing were conducted with the test CPLDs running their self-diagnostics.

Based on a review of TR Section 7 and an examination of the new and original circuit schematics during the April 2014 audit, the NRC staff concludes that there is reasonable assurance that the self-test CPLDs will not impair the safety function of the ULB, SGD, and UVD boards.

3.10.1.3.3 Clause 5.5.3, Fault Detection and Self-Diagnostics

Clause 5.5.3 specifies that if reliability criteria warrant self-diagnostics, then the software should contain functions to detect and report computer system faults and failures in a timely manner, and that these self-diagnostic functions not adversely affect the ability of the system to perform its safety function nor cause spurious actuations of the safety function.

One of the considerations in the new design effort was to eliminate some known “single point vulnerabilities” and thereby increase the reliability of the new design boards above and beyond the requirements that apply to the existing boards. In addition implementing all of the self-test features that existed in the original design (i.e., the SAT board), self-diagnostics were added by using self-test CPLDs on the three boards that processed the safety signal (i.e., ULB, SGD, and UVD). The main function of the self-test CPLDs is the early detection failures (i.e., as soon as the failure occurred vs. during periodic surveillance testing) in the main CPLDs of these three boards. However, the inclusion of self-test CPLDs necessitated the addition of circuitry, which could itself fail. Section 7 of the TR includes a summary of the analysis of potential failure associated with the self-test circuitry; this analysis concludes that most of the failures are detectable or self-revealing, but some are only detected by the existing surveillance tests.

This identification of failures as early as possible is preferred because the identification of failures through self-testing increases the overall system reliability and availability. The CPLDs do not have a startup phase; the self-testing is periodic during the entire period of operation and includes test failure reporting through board edge LEDs. Based on these features, the new design boards meet the criteria of this clause.

3.10.1.4 Clause 5.6, Independence

Clause 5.6 specifies that in addition to the requirements of IEEE Std. 603-1991, data communication between safety channels or between safety and non-safety systems not inhibit the performance of the safety function. DI&C-ISG-04 discussed communications independence.

The evaluation of the communications against the applicable regulatory criteria is addressed in Section 3.7, “Communications.”

3.10.1.5 Clause 5.11, Identification

Clause 5.11 specifies that:

1. Firmware and software identification be used to assure the correct software is installed in the correct hardware component.

2. Means should be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.

3. Physical identification of hardware is implemented in accordance with IEEE Std. 603-1991.

SRP Appendix 7.1-D, Section 5.11, adds:

> The identification should be clear and unambiguous, include revision level, and should be traceable to configuration control documentation.

The evaluation of Westinghouse's configuration management plans against Appendix 7.1-D, Section 5.11 is addressed in Section 3.10.1.1.5 above.

The evaluation of the physical identification of hardware against IEEE Std. 603-1991, Clause 5.11, is addressed in Section 3.9.2.11 above.

As described in the TR, Westinghouse maintains configuration control of the software to be loaded onto each CPLD in its document management system. The specific version of the software to be loaded on each CPLD is provided by Westinghouse along with all of the other manufacturing information. Subsequently each board is tested according to manufacturing test instructions (a subset of design verification tests). The manufacturing instructions include direction to load identified version onto the CPLD and then to read and record the version of software loaded onto each board.

The NRC staff has read the descriptions as summarized above and agrees that they are adequate for addressing Clause 5.11.

3.10.1.6 Clause 5.15, Reliability

Clause 5.15 specifies that, in addition to the requirements of IEEE Std. 603-1991, when reliability goals are identified, the proof of meeting the goals should include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Software error recording and trending may be used in combination with analysis, field experience, or testing.

As stated in RG 1.152 and SRP Appendix 7.1-D, the NRC does not endorse the concept of quantitative reliability goals as the sole means of meeting the NRC's regulations for reliability in digital computers for safety-related applications. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the system.

The SRP Appendix 7.1-C, Section 5.15, “Reliability,” states:

> “SRP BTP 7-14 provides guidance for software development processes that are expected to produce reliable software. Software that complies with the quality criteria of subsection 5.3 above [i.e., 7.1-C Section 5.3 and IEEE 7-4.3.2-2003 Clause 5.3] and that is used in safety systems that provide measures for defense against common-cause failures as described in subsection 5.1 above [i.e., 7.1-C Section 5.1 and IEEE 7-4.3.2-2003 Clause 5.1] are considered by the NRC staff to comply with the fundamental reliability requirements of GDC 21, IEEE Std. 279-1971, and IEEE Std. 603-1991.”

The evaluation of the software reliability is addressed through the evaluation of the quality of the software development process in Section 3.4, “Software Development Process,” above.

3.11 Technical Specification changes

There are no changes to the Technical Specifications required to implement the new design boards, therefore no changes to the Technical Specifications are proposed by this TR; therefore, no evaluation was performed against the 10 CFR 50.36 criteria.

3.12 Secure Development and Operational Environment

GDC 21, “Protection system reliability and testability”, requires in part that “the protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.”

10 CFR 50.55a(h) requires that protection systems for nuclear power plants meet the requirements of IEEE Std. 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations,” and the correction sheet dated January 30, 1995. With respect to the use of computers in safety systems, IEEE Std. 7-4.3.2-2003 specifies computer-specific requirements to supplement the criteria and requirements of IEEE Std. 603 and is endorsed by RG 1.152.

IEEE Std. 603-1991, Clause 4.8, requires that the design basis documentation include: “The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).” Furthermore, IEEE Std. 603-1991, Clause 5.5, “System Integrity,” states, “the safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.”

IEEE Std. 603-1991, Clause 5.6.3.1(2), “Interconnected Equipment,” states, “No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.”

IEEE Std. 603-1991, Clause 5.9, “Control of Access,” states, “The design shall permit the administrative control of access to safety system equipment. These administrative controls

shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof."

RG 1.152, Regulatory Position C.2, "Secure Development and Operational Environment for the Protection of Digital Safety Systems," supersedes the guidance in DI&C-ISG-06, Section D.12, "Secure Development and Operational Environment." RG 1.152 describes a method that the NRC staff deems acceptable for complying with the NRC's regulations (i.e., GDC 21, and IEEE 603) for promoting high functional reliability, design quality, and a SDOE for the use of digital computers in the safety systems of nuclear power plants.

3.12.1 Development Environment

RG 1.152, Regulatory Positions 2.1 - 2.5, describe digital safety system guidance for the establishment of a secure environment during the design and development phases of the life cycle. The guidance is specifically intended to ensure reliable operation of digital safety systems.

There are two aspects to ensuring that no unwanted code is included during the development of an application: (1) preventing the introduction of unwanted code, and (2) screening for and eliminating any unwanted code that could have been introduced. For large and complex systems, there is not a high degree of confidence that all unwanted code can be detected (after it has been introduced; therefore, for large and complex system, both (1) and (2) are necessary.

The new design boards are relatively simple, so much so that it is possible to completely analyze and test the safety functions of these boards to detect any unwanted logic configurations. Through the analysis of the final design CPLD logic configuration using the vendor supplied chip viewer tool, and through comprehensive testing by the PWROG, the applicant has ensured that there is no unwanted logic configuration in the final controlled version of the new design boards that perform the safety functions.

3.12.2 Operational Environment

Some of the CPLD-based SSPS boards contain Joint Test Action Group (JTAG) interfaces; however, the boards contain jumpers to enable this interface and the boards are shipped without these jumpers installed. In addition, the boards must be removed from the SSPS cabinet in order to allow access to the JTAG interfaces. Therefore, there is no new (e.g., virtual) access capability that must be controlled. There have been no proposed changes to the existing control of access provisions; therefore no evaluation of these provisions has been performed.

Since there are no digital communications to the new design boards while they are installed in the SSPS cabinets, there are no electronic integrity threats (while the boards are operational) that must be addressed; therefore no evaluation of virtual integrity threats and provisions has been performed.

4.0 CONCLUSION

The continued operation of the Westinghouse SSPS is dependent on the availability of new design printed circuit boards. The original SSPS circuit boards have been redesigned using programmable logic devices (i.e., a CPLD). Based on the evaluations, audits, and technical reviews summarized in this Safety Evaluation, the NRC staff concludes that the new design SSPS boards can be used to replace the original design boards. The following provides a summary of the NRC staff's conclusions regarding this TR.

The validation testing identified no issues that would preclude the new design boards from meeting the requirements and operating conditions of the original design circuit boards.

A comprehensive set of functional and system operational tests were conducted on the prototypes from the design vendor to ensure that the design of the new design boards met the requirements to be used as circuit board replacements in the SSPS. The design cannot be changed without affecting the revision level of the controlled file, and the CPLD configuration files are controlled by design processes. The results of the manufacturing tests provide reasonable assurance that the manufacturing process has not introduced an error or deficiency that could ultimately affect the safety function of the new circuit board.

The required functionality of the SSPS new design circuit boards has been tested to demonstrate that their performance is identical to the original design circuit boards' functional requirements. The design specification included the system requirements from the original SSPS system description, system standard, and the circuit board schematic drawings. The system testing was consistent with the current safety system design description and the new design boards were verified to operate within the same system parameters as the original design boards. The NRC staff has reasonable assurance that the functionality of the new design circuit boards has been evaluated and tested to meet the system requirements.

The calculated MTBF for the new design circuit boards is greater than the MTBF for the original design circuit boards.

The NRC staff evaluation of the qualification program included: (1) atmospheric, (2) power supply fluctuations, (3) radiation, (4) seismic, and (5) electromagnetic/radiofrequency interference. The temperature and humidity qualification tests were performed consistent with the approved test methodology. The power supply qualification testing and power quality analysis was determined to be acceptable. The SSPS cabinets are located in very low radiation dose zones and the WCAP-8587(R6)-A (NP) analysis continues to be applicable. The seismic qualification was performed to envelope current design basis nuclear plant required response spectra in accordance with the recommended practices and the requirements of GDC-2 and Appendix A to 10 CFR Part 100 have been appropriately addressed. The EMI/RFI qualification testing was performed consistent with the intent of RG 1.180 and RG 1.209, and the requirements of GDC-4 have been appropriately addressed for EMI/RFI effects. Therefore, the appropriate conditions and procedures for qualification have been appropriately applied to the environmental qualification of the new design boards.

The performance of the new design boards have time responses that are within the bounding times allowed for in the time response testing elimination analysis in a manner that is consistent

with the NRC staff's SE for WCAP-14036-P-A, Revision 1. This conclusion applies to as-built configurations using only new design boards or combinations of new and original design boards to provide reactor trip or ESF actuation functions.

The new design ULB, SGD, and UVD boards process the SSPS safety-related signals. These three boards each contain a main CPLD and a test CPLD. Each of the three test CPLDs was analyzed for potential adverse impacts on the main CPLD. In addition, a failure modes and effects analysis was performed for each board by an independent group to determine the impact of component failures. In addition, Westinghouse performed an analysis of all the circuits on the main CPLDs using the appropriate vendor supplied tool, with the intention of demonstrating that the testing performed met the "testability" criteria in BTP 7-19, Section 1.9(2), in order to eliminate the consideration of a CCF. This analysis demonstrated that not all possible sequences were tested, and included an additional analysis that the untested sequences did not need to be tested, since they were functionally irrelevant. These analyses and testing are sufficiently rigorous and complete to allow the NRC staff to eliminate the consideration of a CCF.

There are no digital communications between the redundant trains (divisions) of the SSPS. Each independent train communicates to the main control board and (if applicable) the plant computer Demultiplexers. This communication is through multiplexed data lines that are electrically isolated by ISO boards. In addition, the communication is one way out from the SSPS through an LED/Photo-diode circuit. Since the new design boards do not change the SSPS design, which does not allow interdivisional communication, the new design boards meet the independence criterion.

The Westinghouse FMEA studies demonstrated that there are no non-detectable failures that when considered with a detectable failure, would cause a loss of safety function, and that the new design boards do not produce a different failure mode than previously analyzed. The FMEAs demonstrated that there are no undetectable failures that could inhibit the safety function, and therefore demonstrate that the single failure criterion is met. The FMEAs also demonstrate that the SSPS, with the new design boards installed, will fail in the specified fail-safe state or into a state demonstrated to be acceptable on some other defined basis. Since the FMEAs show there are no undetectable failures that could adversely impact the safety functions of the new design SSPS boards, the two independent trains of the SSPS continue to meet the single failure criterion.

The reliability assessment demonstrates that the reliability of the new design boards is at least as good as the reliability of the original design boards; therefore, the reliability of the new design boards is acceptable.

The new design boards are relatively simple, such that it is possible to completely analyze and test the safety functions of these boards to detect any unwanted logic configuration. Through the analysis of the final design CPLD logic configuration using the vendor supplied chip viewer tool, and through almost complete testing by Westinghouse, as well as independent Beta testing that was performed by PWROG, the applicant has ensured that there is no unwanted logic configuration in the final controlled version of the new design boards that perform the safety functions.

Since there are no digital communications to the new CPLD-based design SSPS boards while they are installed in the SSPS cabinets, there are no electronic integrity threats (when the SSPS is required to be operable) that must be addressed.

The SSPS consists of two independent trains; the complete failure of either one will not prevent the SSPS from accomplishing its safety functions. The independence between these two trains of protective functions is maintained by the ISO board. In addition, periodic testing ensures that the SSPS is capable of performing its safety functions, and that there are no failures in the system that would inhibit the safety functions from being performed. Based on this review, the NRC staff has reasonable assurance that the new design SSPS printed circuit boards are a more reliable upgrade to the original design circuit boards, and include the necessary functional characteristics for the safety system to perform its safety function.

Based on the evaluations and technical reviews discussed herein, the NRC staff finds the new design SSPS boards can be used to replace the original design boards. However, the NRC staff finds that because each plant's configuration and operating conditions are unique, a licensee must confirm (before installing the new design boards) that the tested qualification levels envelope the extreme conditions expected at its plant. The NRC staff also finds that the unique configuration of each plant makes it important that each licensee analyze whether the new design boards can be installed under 10 CFR 50.59 without prior NRC approval. Therefore, this SE addresses only the generic issues associated with installing the new design boards. Licensees may reference this SE, as applicable, when performing a 10 CFR 50.59 Evaluation. The plant-specific action items identified in Section 4.2 do not obviate an applicant's or licensee's responsibility to adequately address new or changed design basis or regulations that apply, in addition to those considered in this SE.

4.1 Summary of Regulatory Compliance

The NRC has concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by in installation of the new design boards in the proposed manner, and (2) there is reasonable assurance that such activities will be conducted in compliance with the NRC's regulations.

4.2 Plant Specific Action Items

The following plant specific action items shall be addressed by licensees installing a new design SSPS board, in support of the evaluations required to be performed during the 10 CFR 50.59 Evaluation or license amendment request processes.

4.2.1 Atmospheric

Prior to the installation of the new design boards, licensees shall ensure that the normal and abnormal temperature and humidity profile (Figure 8-1 of the TR) with a maximum temperature of 140 °F (including approximately 6 °F margin) under postulated faulted HVAC conditions envelopes the site-specific conditions expected inside the SSPS cabinets at the location immediately above the uppermost SSPS board racks. Alternatively, licensees shall confirm that the temperature profile of the original 1983 test (maximum of 120 °F under postulated faulted

HVAC conditions) should envelope the site-specific expected fault temperature conditions just outside the SSPS cabinets. See Section 3.5.1.1, “Atmospheric.”

4.2.2 Assumed Lifetime Total Integrated Dose

Licensees shall confirm that a site-specific analysis shows that the location in which the new design boards will be installed will not result in a lifetime total integrated dose exposure of greater than 1 X 10 E+3 rads (10 gray). See Section 3.5.1.3, “Radiation.”

4.2.3 EMI/RFI Levels

Tables 8-1 and 8-3 of the TR identify the maximum emissions levels to which the SSPS boards were found to have been limited. Tables 8-2 and 8-4 of the TR identify the test waveform levels, frequency ranges, and results of the susceptibility testing. Although the emissions from the new design SSPS boards have been found to be sufficiently low to permit safe operation of these boards in the vicinity of other safety related equipment, licensees should ensure that the ambient radiated EMI/RFI levels within the vicinity of their site-specific locations of SSPS cabinets will not exceed the susceptibility levels to which the boards have been tested, or to which RG 1.180, Revision 1, recommends for testing. See Section 3.5.1.5, “Electromagnetic Interference/Radio Frequency Interference.”

4.2.4 Technical Specification Actuation Logic Test Surveillance

Installation of one or more new design ULB, UVD, SGD and/or SAT printed circuit boards in either SSPS train requires licensees to perform an Actuation Logic Test Surveillance, or equivalent logic test, to demonstrate operability of the SSPS, if not already required by the plant Technical Specifications. The performance of an Actuation Logic Test, or an equivalent logic test, supports the NRC staff’s reasonable assurance finding with regards to the independent verification and equivalency testing of the manufactured circuit boards with the original design verification testing. See Section 3.4.3.1, “V&V Analysis and Reports” and Section 3.4.3.2, “Testing Activities.”

5.0 REFERENCES

The following is a list of references used throughout this document.

1. Westinghouse Document 418A49, Revision 4, "Westinghouse Design Specification Universal Logic Board Replacement."

2. Westinghouse Document TDH121803001, Revision 2, "Project Plan, SSPS Circuit Boards Re-Design," July 17, 2006.

3. Westinghouse Document ULTPTDH001, Revision 2, "Universal Logic Board Test Plan."

4. Westinghouse Document 1TS2870, Revision 1, "Universal Logic Board 6D30225G01/G02/G03/G04 Functional Test."

5. Westinghouse Document 1TS2868, Revision 0, "Universal Logic Board 6D30225 Test Decomposition."

6. Westinghouse Document 1TS2871_COMP4, Revision 0, "Universal Logic Board 6D30225G01/G02 System.

7. Westinghouse Document 1TS2887, Revision 0, “Safeguards Driver Board Test Plan.”

8. Westinghouse Document CDI-3015, Revision 3, “Commercial Dedication Instruction for the Universal Logic Board 6D30225.”

9. Westinghouse Document 1TS2958, Revision 3, “Universal Logic Board 6D30225G01/G02/G03/G04 Configuration Procedure for Manufacturing and Repair.”

10. Westinghouse Document 1TS2963, Revision 4, “Universal Logic Board 6D30225G01/G02/G03/G04 Functional Test Procedure for Manufacturing and Repair.”

11. NRC Letter, dated November 10, 1983 from Mr. Cecil O. Thomas, USNRC, to Mr. E. P. Rahe, Jr., Westinghouse Electric Corporation, “Acceptance for Referencing of Licensing Topical Reports WCAP-8587, Revision 6 (NP), “Methodology for Qualifying Westinghouse WRD Supplied NSSS Safety Related Electrical Equipment,” and WCAP-9714()/9750 (N), “Methodology for the Seismic Qualification of Westinghouse WRD Supplied Equipment.” (ADAMS Accession Number 8312020062—Microform Address 21389:348-21389:362,21389:348-21390:083)

12. Westinghouse Document WCAP-8694, Revision 0, “Seismic Qualification of Rotary Relay for Use in the Solid State Protection System,” January 1976.

13. Westinghouse Document WCAP-14036-P-A, Revision 1, “Elimination of Periodic Protection Channel Response Time Tests” (ADAMS Accession No. ML100050325).