SAFETY EVALUATION BY THE OFFICE OF NEW REACTORS

RELATED TO AMENDMENT NOS. 79 and 78

TO THE COMBINED LICENSE NOS. NPF-91 AND NPF-92, RESPECTIVELY

SOUTHERN NUCLEAR OPERATING COMPANY, INC.

GEORGIA POWER COMPANY

OGLETHORPE POWER COMPANY

MEAG POWER SPVM, LLC

MEAG POWER SPVJ, LLC

MEAG POWER SPVP, LLC

CITY OF DALTON, GEORGIA

VOGTLE ELECTRIC GENERATING PLANT UNITS 3 AND 4

DOCKET NOS. 52-025 AND 52-026

1.0 INTRODUCTION

By letter dated February 15, 2016, (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16046A009), Southern Nuclear Operating Company (SNC or the licensee) submitted license amendment request (LAR) 15-017 requesting U.S. Nuclear Regulatory Commission (NRC or the Commission) approval for amendments to the Vogtle Electric Generating Plant Units 3 and 4 (VEGP 3&4) combined licenses (COL) NPF-91 and NPF-92, respectively.

The LAR proposes to revise the Updated Final Safety Analysis Report (UFSAR) text and tables, and information incorporated by reference into the UFSAR related to updates to WCAP-16096, “Software Program Manual for Common Q™ Systems” (ADAMS Accession Nos. ML12205A053 and ML12205A052), WCAP-16097, “Common Qualified Platform Topical Report” (ADAMS Accession Nos. ML12207A512 and ML12207A510). The current licensing basis references WCAP-16096, Revision 01A and WCAP-16097, Revision 0, which are newer versions that have been approved by the staff.

The newer revisions of WCAP-16096 and WCAP-16097 are being adopted for the AP1000 Protection and Safety Monitoring System (PMS) by adding them to the AP1000 licensing basis.

The LAR proposes the following changes:

- Incorporate by reference the NRC-approved versions of the Tier 2* WCAP-16096, Revision 4, "Software Program Manual for Common Q™ Systems" (also referred to as the Common Qualified (Common Q) Software Program Manual (SPM)) and WCAP-16097, Revision 3, "Common Qualified Platform Topical Report" (also referred to as the Common Q Topical Report (TR)) into the UFSAR, including the use of alternative approaches in lieu of certain requirements in WCAP-16096, Revision 4 and WCAP-16097, Revision 3. The existing revisions of WCAP-16096 and WCAP-16097 will be removed from the UFSAR.

- Establish the Common Q SPM and TR as the licensing basis for the development of the Common Q portion of the PMS in lieu of the applicable digital instrumentation & control (I&C) regulatory guides (RG).

- Identify APP-GW-GLR-017, Revision 0, "Resolution of Common Q NRC Items," as the historical reference document that addressed the COL Information Item identified in UFSAR Subsection 7.1.6.2.

- Incorporate by reference an updated revision of Tier 2* WCAP-15927, "Design Process for AP1000 Common Q Safety Systems," into the UFSAR.

- Remove Tier 2* WCAP-17201-P, "AC160 High Speed Link Communication Compliance to DI&C-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc)," Staff Positions 9, 12, 13 and 15 Technical Report," as a UFSAR incorporated by reference document.

- Revise UFSAR Appendix 7A, "Instrumentation and Controls Licensing Basis Document Changes," to capture changes to the affected UFSAR incorporated by reference documents.

- Revise and add new Tier 2 and Tier 2* UFSAR text to support the changes described above.

Enclosure 1 of the February 15, 2016, letter provides the description, technical evaluation, regulatory evaluation (including the Significant Hazards Consideration determination), and environmental considerations for the proposed changes in the LAR. Enclosure 2 of the letter provides the disposition of the plant-specific action items (PSAIs) and generic open items (GOIs) for WCAP-16096, Revision 4 and WCAP-16097, Revision 3. Enclosure 3 of the letter provides the Common Q SPM and TR alternatives and the associated justifications for these alternatives. Enclosure 4 of the letter identifies the requested changes and provides markups depicting the requested changes to the UFSAR text, tables, and figures. Enclosure 5 of the letter provides APP-GW-GLR-017, Revision 2. Enclosure 6 of the letter provides WCAP-15927, Revision 4.

To support its safety evaluation (SE) of LAR 15-017, the staff conducted a regulatory audit from August 2 to 3, 2016, at the Westinghouse Electric Company (Westinghouse) offices located in Rockville, Maryland (ADAMS Accession No. ML16252A382). The purpose of this audit was to determine if the proposed design process changes and licensing documentation revisions continue to comply with the applicable regulatory criteria. The staff performed a confirmatory review of the design process and licensing documents that were listed in LAR 15-017 which were not submitted as part of the LAR.

By letter dated August 19, 2016 (ADAMS Accession No. ML16232A576), a supplement (LAR 15-017S1) to LAR 15-017 was submitted to the NRC which consisted of several enclosures. Enclosure 7 of the letter provides the responses to the staff's Request for Additional Information (RAI) Question No. 4 regarding Enclosure 2 of the LAR; RAI Question Nos. 2, 4 through 8 regarding Enclosure 3 of the LAR; and RAI Question No. 1 of Enclosure 5 of the LAR. Enclosure 8 of the letter provides propriety text excerpts that are redacted from the RAI response information contained in Enclosure 7.

By letter dated August 26, 2016 (ADAMS Accession No. ML16239A392), an additional supplement (LAR 15-017S2) to LAR 15-017 was submitted to the NRC. LAR 15-017S2 provides a revised schedule for the submittal of remaining RAIs not covered in supplement LAR 15-017S1.

By letter dated September 13, 2016 (ADAMS Accession No. ML16257A604), an additional supplement (LAR 15-017S3) to LAR 15-017 was submitted to the NRC which consisted of two enclosures. Enclosure 11 of the letter provides the response to RAI Question Nos. 1 through 3 regarding Enclosure 2 of the LAR, RAI Question No. 3 regarding Enclosure 3 of the LAR, and additional information requested by the staff during the audit of LAR 15-017 held on August 2 to 3, 2016. Enclosure 12 of the letter provides a copy of WCAP-15927, Revision 5.

By letter dated December 16, 2016 (ADAMS Accession No. ML16351A490), an additional supplement (LAR 15-017S4) to LAR 15-017 was submitted to the NRC which consisted of two enclosures. Enclosure 13 of the letter provides the responses to RAI Question Nos. 1 through 3 regarding Enclosures 7 and 8 of LAR 15-017S1, and RAI Question Nos. 4 through 6 of Enclosures 11 and 12 of LAR 15-017S3.

By letter dated March 17, 2017 (ADAMS Accession No. ML17076A410), an additional supplement (LAR 15-017S5) to LAR 15-017 was submitted to the NRC which consisted of three enclosures. Enclosure 14 provides the requested clarifications and additional updates and corrections to information provided in the original LAR and supplements. Enclosure 15 provides revised marked up UFSAR text to support these changes. Enclosure 16 provides a copy of WCAP-15927, Revision 6.

In the letters dated August 19, 2016, August 26, 2016, September 13, 2016, December 16, 2016, and March 17, 2017, the licensee provided additional information that supplemented the application. This information did not expand the scope of the application and did not change the NRC staff's original proposed no significant hazards consideration determination as published in the *Federal Register* on April 12, 2016 (81 FR 21602).

2.0 REGULATORY EVALUATION

Tier 2* Information is defined in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 52, Appendix D, Section II.F and is subject to the change process described in Section VIII.B.6. The proposed revisions in LAR 15-017 are required to meet the following requirements:

- 10 CFR Part 52, Appendix D, VIII.B.6 requires prior NRC approval for departure from Tier 2* information. The proposed changes are to WCAP-16096, WCAP-16097, and WCAP-15927, which are referenced in the UFSAR as Tier 2* documents. Therefore, a license amendment request is required as proposed in LAR 15-017.

- 10 CFR Part 52, Appendix D, Section VIII.B.5.a allows an applicant or licensee who references this appendix to depart from Tier 2 information, without prior NRC approval, unless the proposed departure involves a change to or departure from Tier 1 information, Tier 2* information, or the Technical Specifications, or requires a license amendment under paragraphs B.5.b or B.5.c of the section. The proposed activity makes changes to Tier 2 information that involve Tier 2* changes and, and thus requires prior NRC approval for the involved Tier 2 departures.

- 10 CFR 50.34(f)(2)(iii) requires a control room design that reflects state-of-the-art human factor principles.

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

- 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 1, "Quality standards and records," requires that 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.

- 10 CFR Part 50, Appendix A, GDC 2, "Design basis for protection against natural phenomena," requires that structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena without loss of capability to perform their safety functions.

- 10 CFR Part 50, Appendix A, GDC 4, “Environmental and dynamic effects design basis,” 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.

- 10 CFR Part 50, Appendix A, GDC 13, “Instrumentation and control,” requires that instrumentation shall be provided to monitor and control variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to ensure adequate safety.

- 10 CFR Part 50, Appendix A, GDC 19, “Control room,” requires that a control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions.

- 10 CFR Part 50, Appendix A, GDC 20, “Protection system functions,” requires that the protection system shall be designed to initiate automatically the operation of appropriate systems to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and to sense accident conditions and to initiate the operation of systems and components important to safety.

- 10 CFR Part 50, Appendix A, GDC 21, “Protection system reliability and testability,” requires 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 Part 50, Appendix A, GDC 22, “Protection system independence,” requires that 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.

- 10 CFR Part 50, Appendix A, GDC 23, “Protective system failure modes,” requires that the protection system shall 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, or postulated adverse environments are experienced.

- 10 CFR Part 50, Appendix A, GDC 24, “Separation of protection and control,” requires that the protection system shall 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 which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system.

- 10 CFR Part 50, Appendix A, GDC 25, "Protection system requirements for reactivity control malfunctions," requires that the protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems.

- 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants" 10 CFR Part 50, Appendix B Criteria I, II, III, V, VI, VII, XI, and XV.

Staff previously concluded that the SPM and Common Q TR satisfy the above regulatory requirements. However, staff's evaluation of the Common Q SPM and TR stated that plant specific application analyses must be performed to ensure the generic approval granted by the WCAP-16096 SE (ADAMS Accession Nos. ML13022A124 (Letter); ML13022A009 (SE)) and WCAP-16097 SE (ADAMS Accession Nos. ML13022A124 (Letter); ML13022A009 (SE)) remain valid for a specific system or plant application utilizing the Common Q platform. In this SE, staff reviews the disposition of the new PSAIs specified by the WCAP-16096 SE and the new PSAIs and GOIs specified by the WCAP-16097 SE (see Section 3.3 of this SE).

3.0 TECHNICAL EVALUATION

3.1 Evaluation of Impacted Documents

3.1.1 Evaluation of WCAP-16096, "Software Program Manual for Common Q™ Platform" and WCAP-16097, "Common Qualified Platform Topical Report."

Software Program Manual for Common Q™ Systems

The Common Q SPM specifies the development, documentation, utilization, and maintenance of software to be developed for use with the Common Q platform in nuclear safety applications. It also provides guidance for the maintenance, implementation, and use of commercial-grade hardware and previously developed software.

The LAR proposes to incorporate the proprietary and non-proprietary versions of WCAP-16096, Revision 4 into the licensing basis. This WCAP was updated to reference later NRC guidance and supporting industry standards to be used for the development of a safety-related system application. In addition, this WCAP updated the Common Q component descriptions and their configuration, as well as incorporating the updated Westinghouse processes.

Staff previously evaluated the Common Q SPM which was submitted by Westinghouse as WCAP-16096-NP-A and 16096-P-A, Revision 4. The results of this evaluation are documented in an SE. Staff's evaluation of the SPM concluded that the Common Q safety system software development processes when properly implemented are capable of producing software that will satisfy the requirements of 10 CFR Part 50, Appendix A, GDCs 1 and 21, and 10 CFR Part 50, Appendix B Criteria I, II, III, V, VI, VII, XI, and XV.

Staff's evaluation of the Common Q SPM stated that plant specific application analyses must be performed to ensure the generic approval granted by the WCAP-16096 SE remains valid for a specific system or plant application utilizing the Common Q platform. Staff reviewed the disposition of the new PSAIs specified by the WCAP-16096 SE and finds them acceptable (see Section 3.3 of this SE).

The LAR states that only the Common Q portion of PMS is developed using the Common Q SPM. In addition, the LAR proposes to update UFSAR Chapter 7 to clarify that only the Common Q portion of PMS is developed using the Common Q SPM. Staff reviewed the proposed changes and determined it was acceptable because neither Revision 01A nor Revision 4 of the Common Q SPM describes the development process for other portions of PMS, such as the Component Interface Module.

The LAR proposes to exclude Section 12, "Secure Development and Operational Environmental Plant," of WCAP-16096 from being incorporated by reference into the UFSAR. The LAR states that while Section 12 of WCAP-16096 provides an acceptable method to comply with computer security requirements, the licensee will instead continue to use the current incorporated by reference document APP-GW-J0R-012, "AP1000 Protection and Safety Monitoring System Computer Security Plan," for the AP1000 PMS. Staff's evaluation of the PMS computer security plan concluded that the AP1000 computer security plan satisfies the requirements of 10 CFR 50.55(a)(h), IEEE Std. 603-1991 Clauses 5.6.3 and 5.9, and GDC 21 (see Section 3.4 of this SE).

Common Q™ Platform Topical Report

The Common Q TR specifies the hardware and software associated with the Common Q platform in nuclear safety applications. It also specifies the design, qualification, reliability, and commercial grade dedication of the Common Q platform.

The LAR proposes to incorporate the proprietary and non-proprietary versions of WCAP-16097, Revision 3 into the licensing basis. This WCAP was updated to reference later NRC guidance and supporting industry standards to be used for the development of a safety-related system application. This activity also updates the Common Q component descriptions and their configuration, as well as incorporating the updated Westinghouse processes.

Staff previously evaluated the Common Q TR which was submitted by Westinghouse as document number WCAP-16097-NP-A and 16097-P-A, Revision 3. The results of this evaluation are documented in an SE. Staff's evaluation of the Common Q TR concluded that the design of the revised Common Q platform satisfies the requirements of 10 CFR Part 50, Appendix A, GDCs 1, 2, 4, 12, 13, 19, 20, 21, 22, 23, 24, and 25; and IEEE Std. 603-1991 for a generic system application and is acceptable for safety-related I&C applications in nuclear power plants.

Staff's evaluation of the Common Q topical report stated that plant specific application analyses must be performed to ensure the generic approval granted by the WCAP-16097 SE remains valid for a specific system or plant application utilizing the Common Q platform. Staff reviewed the disposition of the new PSAIs and GOIs specified by the WCAP-16097 SE and finds them acceptable (see Section 3.3 of this SE).

3.1.2 Evaluation of WCAP-15927, "Design Process for Common Q Safety Systems"

WCAP-15927 describes all the developmental phases and processes associated with the Common Q portion of the PMS. In addition, this document contains additional requirements on the design and testing teams developing the PMS.

The LAR proposes to reference an updated revision of Tier 2* WCAP-15927 (i.e., from Revision 2 to Revision 4) into the licensing basis. The updated revision of WCAP-15927 incorporates editorial/administrative changes (i.e., updating trademarks, fixing typographical errors, updating the revision number of WCAP-15927, and adding the AP1000 standard acronym document as a reference). By letter dated September 13, 2016, SNC submitted LAR 15-017S3, which is a supplement to LAR 15-017, to reference WCAP-15927 from Revision 4 to Revision 5. However, pages 3 to 21 were missing from Enclosure 12 to LAR 15-017S3[1]. In RAI Question No. 6 of Enclosure 12 of the LAR, the staff asked the licensee to provide the missing pages of Enclosure 12. In its response to RAI Question No. 6 of Enclosure 12 of the LAR, dated December 16, 2016, the licensee stated that LAR 15-017S3 was resubmitted on October 19, 2016 (ADAMS Accession No. ML16293A702). In addition, the revision number for WCAP-15927 was updated from Revision 5 to Revision 6 to account for the deleted Common Q SPM alternative to Section 4.3.2.6, "Site Installation and Checkout Phase." The staff reviewed the proposed mark-ups and revision updates provided in Enclosure 12 to LAR 15-017S3 and the response to RAI Question No. 6 of Enclosure 12 of the LAR and finds them acceptable because these proposed changes have no impact on the process requirements of WCAP-15927 nor does it reduce any licensing commitments. Therefore, RAI Question No. 6 of Enclosure 12 of the LAR is resolved and closed.

By letter dated March 17, 2017, SNC submitted LAR 15-017S5, which is a supplement to LAR 15-017, to provide updates to LAR 15-017 that were needed to address Revision 6 of WCAP-15927. These included changes to the text of the original LAR provided in ND-16-0083, Enclosure 1, and changes to the UFSAR markups provided in Letter ND-16-0083, Enclosure 4, "Proposed Changes to the Licensing Basis Documents." The licensee stated that these changes to the UFSAR markups were not provided in a format that is consistent with that commonly used in SNC's license amendment requests. Also, the licensee stated that the UFSAR markups in Letter ND-16-2548 inadvertently omitted changing the date of WCAP-15927

[1] LAR 15-017S3 included Enclosure 12, which provided WCAP-15927, Revision 5.

in UFSAR Table 1.6-1. Staff reviewed the proposed changes to the UFSAR presented in LAR 15-017S4 Enclosure 13 and finds them acceptable because these editorial/administrative changes have no impact on the process requirements of WCAP-15927, nor does it reduce any licensing commitments.

The LAR proposes alternatives to the Common Q SPM and TR defined processes. Staff reviewed the proposed alternatives and finds them acceptable (see Section 3.3 of this SE).

The LAR proposes to remove the reference to the specific tool (i.e., Document Index) used to document the technical baseline. Staff determined this was acceptable because the licensing basis still requires the technical baseline to be documented and this change does not impact any processes of WCAP-15927, nor does it reduce any licensing commitments.

3.1.3 Evaluation of WCAP-17201, "AC160 High Speed Link Communication Compliance to DI&C-ISG-04 Staff Positions 9, 12, 13 and 15 Technical Report"

The LAR proposes to delete WCAP-17201-P from the licensing basis. WCAP-17201-P is a Tier 2* incorporated by reference document in the UFSAR. The purpose of this document was to address how the High Speed Links (HSLs) communication described in the Common Q TR is compliant with DI&C-ISG-04 Staff Positions 9, 12, 13, and 15. Staff finds the removal of this document acceptable because WCAP-16097-P-A, Revision 3 addresses Positions 9, 12, 13, and 15 from DI&C-ISG-04. Thus, retaining both WCAPs would put duplicate information in the licensing basis.

3.1.4 Evaluation of Proposed Vogtle Units 3 and 4 UFSAR Appendix 7A Revisions

The LAR proposes to revise Appendix 7A to modify information affected by adopting the latest NRC-approved versions of the Common Q SPM and TR. To maintain consistency throughout the VEGP 3&4 UFSAR and the documents incorporated by reference in the VEGP 3&4 UFSAR, changes to add the licensing basis revision numbers for Common Q SPM and TR, along with the reference to the changes provided in VEGP 3&4 UFSAR Appendix 7A at each location in which these two WCAPs are referenced in the UFSAR including Appendix 7A. The following Tier 2 incorporated by reference documents were revised in UFSAR Appendix 7A:

- WCAP-15775 (Revision 4), "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report,"

- WCAP-17184 (Revision 2), "AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report,"

- WCAP-16438 (Revision 3), "FMEA of AP1000 Protection and Safety Monitoring System,"

- WCAP-15776 (Revision 0), "Safety Criteria for the AP1000 Instrumentation and Control Systems,"

- WCAP-16592 (Revision 2), "Software Hazard Analysis of AP1000™ Protection and Safety Monitoring System,"

- WCAP-16674 (Revision 4), "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," and

- WCAP-16675 (Revision 5), "AP1000™ Protection and Safety Monitoring System Architecture Technical Report."

Staff reviewed the proposed VEGP 3&4 UFSAR mark-ups and revision updates provided in Enclosure 4 to LAR 15-017 and determined that these changes are acceptable.

3.2 Evaluation of Changes to Regulatory Guidance Conformance

The LAR proposes changes to UFSAR Appendix 1A to establish the Common Q SPM and TR as the licensing basis for the development of the Common Q portion of PMS in lieu of the applicable digital I&C RGs. An exception was taken to RG 1.152, "Criteria for Use of Computers In Safety Systems of Nuclear Power Plants"; RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"; RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"; RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"; RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"; and RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," as currently presented in UFSAR Appendix 1A. The staff reviewed the exceptions in UFSAR Appendix 1A and found them acceptable because staff determined that the Common Q SPM and TR as applied to Common Q safety systems substantively conform to the guidance of RG 1.152, 1.168, 1.169, 1.170, 1.172, and 1.173, and that the special characteristics of computer systems have been adequately addressed.

Based on the original safety conclusions, staff determined that the Common Q safety system software development processes when properly implemented are capable of producing software that will satisfy the requirements of GDC 1 and 21. In addition, staff determined that the Common Q system meets the requirements of 10 CFR Part 50, Appendix A, GDCs 1, 2, 4, 12, 13, 19, 20, 21, 22, 23, 24, and 25, and IEEE Std. 603-1991 for the design of safety-related reactor protection systems, engineered safety features systems, and other plant systems, and the guidelines of RG 1.152, 1.168, 1.169, 1.170, 1.172, and 1.173, and supporting industry standards for the design of digital systems and is, therefore, acceptable.

3.3 Evaluation of Disposition of Plant-Specific Action Items and Generic Open Items

Enclosure 2 of the letter discusses the PSAIs and GOIs contained within the SEs for WCAP-16096-P-A and WCAP-16096-NP-A, Revision 4; and WCAP-16097-P-A and WCAP-16097-NP-A, Revision 3. The staff's assessment of the licensee's compliance with each of these items is as follows:

WCAP-16097: Common Q Topical Report – Plant-Specific Action Items

1. WCAP-16097 PSAI 6.1 – *Each licensee implementing a specific application based upon the Common Q platform must assess the suitability of the S600 I/O modules to be used in the design against its plant-specific input/output requirements*.

   The LAR states that the original disposition of WCAP-16097 PSAI 6.1 in APP-GW-GLR-017 is still valid to address the suitability of the AP1000 PMS. Staff agrees with the licensee's conclusion in the original disposition of WCAP-16097 PSAI 6.1 that it uses its Quality Assurance (QA) program (as described in Chapter 17 of the UFSAR) to determine the suitability of all input and output (I/O) devices.

   The LAR proposes to revise Table 3-1, "PMS Input/Output Signal" in APP-GW-GLR-017 to align it with the S600 I/O modules (i.e., AI688 and AI687) described in WCAP-16675, which was part of the certified design. Staff determined that these changes are acceptable because the S600 I/O Modules identified in Table 3-1 were approved for use in Table 1 of the NRC's SE for WCAP-16097, Revision 3.

   The LAR proposes changes to the introduction section and the GOI 7.1 resolution as described in Enclosure 5 to LAR 15-017, to clarify that the AI685 module is not used in the AP1000 design. Staff reviewed the proposed DCD mark-ups and revision updates provided in Enclosure 5 to LAR 15-017 and determined that these changes are acceptable because the AI685 module is not used in the AP1000 design.

   Based on the above discussion, staff finds PSAI 6.1 is met.

2. WCAP-16097 PSAI 6.4 – *Each licensee implementing a Common Q application must verify that its plant environmental data (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the Common Q equipment is to be installed are enveloped by the environment considered for the Common Q qualification testing, and that the specific equipment configuration to be installed is similar to that of the Common Q equipment used for the tests. The licensee must also ensure that the plant specific common Q system configuration does not exceed the configuration used during platform qualification testing. See Sections 4.2.2.1.1, 4.2.2.1.2, and 4.2.2.1.3. The Common Q test specimen was configured for seismic testing using dummy modules to fill all the used rack slots. As part of the verification of its plant-specific equipment configuration the licensee must check that it does not have any unfilled rack slots. See Section 4.2.2.1.2.*

The LAR states that the original disposition of WCAP-16097 PSAI 6.4 in APP-GW-GLR-017 is still valid. The original disposition states that the Common Q safety equipment is located in the Auxiliary Building in a mild (non-harsh) environment. Furthermore, the original disposition identified the following inspections, tests, analyses, and acceptance criteria (ITAAC) for the PMS:

- <u>Seismic Qualification</u>: The seismic qualification of the PMS seismic Category I equipment is covered by DCD Tier 1 (ITAAC) 2.5.2, Item 2 (ADAMS Accession No. ML11171A500).

- <u>Electromagnetic Compatibility (EMC) Qualification:</u> The PMS equipment will be tested or analyzed to confirm that it has electrical surge withstand capability, and can withstand the electromagnetic interference (EMI), radio frequency interference (RFI), and electrostatic discharge conditions that would exist before, during and following a design basis accident without loss of safety function for the time required to perform the safety function (DCD Tier 1 (ITAAC) 2.5.2, Item 3).

- <u>Temperature and Humidity Qualification</u>: The AP1000 temperature and humidity conditions for qualification of PMS equipment are presented in DCD Appendix 3D. Temperature and humidity qualification of the PMS equipment is covered by DCD Tier 1 (ITAAC) 2.5.2, Item 4.

- <u>Testing Reports</u>: The as tested AP1000 PMS Architecture Diagrams will be included in testing reports covered by DCD Tier 1 ITAAC 2.5.2.

The completion of the Common Q qualification testing activities will be confirmed by the referenced ITAACs.

Reference 21 in staff's SE for WCAP-16097-P-A, Revision 3, defines the system limitations imposed on the system designer to maintain the system design within the bounds of the equipment qualification (EQ) program. The licensee made a determination that the plant environmental data envelope bounds the requirements of the Common Q application within its installed environment. The licensee has verified that the plant specific common Q system configuration did not exceed the configuration used during platform qualification testing. During the audit conducted from August 2 to 3, 2016, the licensee provided additional test documentation, as well as environmental information for the areas into which the Common Q system will be installed at the plant to show that all of the Common Q equipment meets plant specific environmental requirements.

Lastly, the original disposition states that the Common Q hardware will include dummy modules in unused chassis slots. The dummy modules populating the unused chassis slots during seismic testing are essentially the outer cases and front faces of modules similar in size and appearance to the active modules, but lacking the internal electronics and associated hardware. During the audit conducted from August 2 to 3, 2016, staff confirmed the Common Q test specimen was configured for seismic testing using dummy modules to fill all the used rack slots.

Based on the above discussion, staff finds PSAI 6.4 is met.

3. <u>WCAP-16097 PSAI 6.15</u> – *During the software development process, the licensee must specify plant specific requirements for system automatic self-testing features that are needed to ensure proper functioning of the Common Q application during operation*.

   The LAR states that Section 6 of the software requirements specification (SRS) for the PMS defines the requirements for reporting the results of the inherent, automatic self-testing features of the Common Q platform during operation. Furthermore, the LAR states that these features are also described in WCAP-16675, "AP1000 Protection and Safety Monitoring System Architecture Technical Report" (Tier 2, Incorporated by Reference). During the audit conducted from August 2 to 3, 2016, staff reviewed Section 6 of the SRS and confirmed that it included a requirement for the automatic self-testing/diagnostic features during operation. Staff assessed the implementation of this requirement and found it acceptable. Therefore, staff finds PSAI 6.15 is met.

4. <u>WCAP-16097 PSAI 6.16</u> – *A licensee implementing a Common Q DPPS shall ensure that no more than four processor modules are installed within a single AC160 controller*.

   The LAR provides a commitment for the VEGP 3&4 AP1000 design to use no more than four processor modules within a single AC160 controller. The PM646A processor module was approved for use in Table 1[2], "Common Q Qualified Components," of the NRC's SE for WCAP-16097-P-A, Revision 3. Staff assessed the commitment and determined it was acceptable because this restriction is captured in Section 4.1 of WCAP-16097, Revision 3, which is incorporated by reference into the AP1000 licensing basis in this LAR. Therefore, staff finds PSAI 6.16 is met.

5. <u>WCAP-16097 PSAI 6.17</u> – *A licensee implementing a Common Q DPPS must ensure that all hardware components used for system development are approved for use in nuclear safety system Class 1E applications and are listed in Table 1*.

   The LAR proposes to use the DI621 module which was not listed in Table 1 of the WCAP-16097-P-A, Revision 3. The LAR states that although the DI621 module is not listed in Table 1, it was included in the AP1000 certified design as described in WCAP-16675. Furthermore, the LAR states that the DI621 module is qualified for use in the

[2] Table 1 of the NRC's SE for WCAP-16097-P-A, Revision 3 contains a complete listing of approved hardware modules of the updated Common Q system platform.

PMS as a Class 1E component by undergoing commercial dedication and equipment qualification using the same Commercial Dedication Instructions (CDI) as the modules listed in Table 1.

The commitment to perform the process to use commercial grade computer hardware and software items in the PMS appears in DCD Tier 1 (ITAAC) 2.5.2, Item 13. DCD Tier 1 (ITAAC) 2.5.2, Item 13 was completed by SNC on April 15, 2015 (ADAMS Accession No. ML15106A433). The NRC inspectors performed an inspection of construction activities associated with DCD Tier 1 (ITAAC) 2.5.2, Item 13, documented in an inspection report dated April 30, 2015 (ADAMS Accession No. ML15120A400), and found that the ITAAC acceptance criteria was met. Staff determined the use of DI621 acceptable because the DI621 module is following the same CDI process identified in DCD Tier 1 (ITAAC) 2.5.2, Item 13. Furthermore, staff determined that the equipment qualification for the DI621 module was acceptable because the DI621 module followed the NRC-approved methodology in UFSAR Appendix 3D. This was the same equipment qualification as the modules listed in Table 1 of the NRC's SE for WCAP-16097-P-A, Revision 3. Therefore, staff finds PSAI 6.17 is met.

6. WCAP-16097 PSAI 6.18 – *The licensee implementing Common Q applications must ensure that administrative controls are put into place to ensure that changes to setpoints are only performed while the system is not being relied upon to perform its safety functions. The affected division of the Common Q safety system must be declared inoperable prior to implementation of setpoint changes*.

The LAR states that PMS setpoints for reactor trip (RT) and engineered safety features actuation (ESFAS) functions are changed using the safety-related Maintenance and Test Panel in the Maintenance Test Cabinet (MTC), as described in WCAP-16675. To address WCAP-16097 PSAI 6.18, the LAR proposes to add a new Tier 2 Subsection 7.1.2.14.3, "Operational Process," to describe the software operations plan and the administrative controls within it. From the information contained in the disposition, it was not clear to staff how the administrative controls for implementing setpoint changes will affect the Technical Specifications. In addition, it was not clear to staff how the setpoint changes will be modified for both RT and ESFAS functions when one channel is in an operational bypass mode and at the same time another channel is tripped. For such reasons, staff asked the following RAI questions.

In RAI Question No. 1, Item (1) of Enclosure 2 of the LAR, staff requested the licensee to describe how the administrative controls for implementing setpoint changes will affect the Technical Specifications for the affected PMS division. In its response to RAI Question No. 1, Item (1) of Enclosure 2 of the LAR, dated September 13, 2016, the licensee stated that:

> The administrative controls for implementing setpoint changes will not impact the current Technical Specifications. When the plant is in a

condition where the associated function is required to be operable, the administrative controls will involve declaring the channel associated with the setpoint change inoperable and not relying on its function until declared operable again. The controls for an inoperable channel would then comply with the required actions described in the Technical Specifications for inoperable channels. In each case, the Technical Specification Required Action(s) provides the appropriate level of safety when a channel is declared inoperable for the setpoint change. Alternatively, setpoint changes can be made when the plant is in a condition where the associated channel is not required to be operable, in which case, no Technical Specification action would apply.

> When implementing a setpoint change, both sub-channels for the function within that division will be declared inoperable and will not be relied upon for any function. The appropriate Technical Specification actions for the affected channel will be entered, setpoint changes made, and channel operability reestablished prior to declaring the channel operable and exiting the Limiting Condition for Operation (LCO) actions. For example, the reactor trip (RT) and Engineered Safety Features Actuation System (ESFAS) functions in LCOs 3.3.1 and 3.3.8 require 4 operable channels; with one channel inoperable the Required Action is to place the channel in bypass or trip within 6 hours. If the setpoint change is implemented and the channel declared operable prior to expiration of the allowed Completion Time, completing the Required Action to bypass or trip the channel is not required to comply with the Technical Specification action.

Based on the staff's review of the licensee's response to RAI Question No. 1, Item (1) of Enclosure 2 of the LAR, staff finds the licensee's response acceptable because the administrative controls for implementing setpoint changes will not impact the current Technical Specifications. When implementing a setpoint change the appropriate Technical Specification actions for the affected channel will be entered, setpoint changes made, and channel operability reestablished prior to declaring the channel operable and exiting the Limiting Condition for Operation (LCO) actions. Staff also reviewed the markups of the PSAI 6.18 Disposition and Tier 2 UFSAR Subsection 7.1.2.14.3 provided with the response and found them acceptable. Therefore, RAI Question No. 1, Item (1) of Enclosure 2 of the LAR is resolved and closed.

In RAI Question No. 1, Item (2) of Enclosure 2 of the LAR, staff requested clarification whether setpoint changes for blocks and resets include permissive signals that permit manual bypass of associated functions. In its response to RAI Question No. 1, Item (2) of Enclosure 2 of the LAR, the licensee stated that:

> Yes, the proposed license amendment request (LAR) update below includes implementing setpoint changes for permissive signals that

> automatically bypass/enable or permit manual bypass of associated functions. When the plant is in a condition where the function associated with a permissive is required to be operable and a permissive setpoint is to be changed, the associated Technical Specification function's channel(s) are first declared inoperable and the required Technical Specification action is taken as described in response (1) above. The PMS division does not need to be declared inoperable prior to making setpoint changes for permissives, therefore the proposed LAR and UFSAR wording is corrected below.

Based on the staff's review of the licensee's response to RAI Question No. 1, Item (2) of Enclosure 2 of the LAR, staff found the licensee's response acceptable because it clarified that setpoint changes for blocks and resets include permissive signals that automatically bypass/enable or permit manual bypass of associated functions. Therefore, RAI Question No. 1, Item (2) of Enclosure 2 of the LAR is resolved and closed.

In RAI Question No. 1, Item (3) of Enclosure 2 of the LAR, staff requested the licensee to clarify what is meant by the term "operational," in the proposed markups for Tier 2 Subsection 7.1.2.14.3. In its response to RAI Question No. 1, Item (3) of Enclosure 2 of the LAR, the licensee stated that:

> When making setpoint changes during plant conditions that require the associated channel to be operable, only the channel for which the setpoint (or an associated permissive setpoint) is being changed is declared inoperable. The other channels within the PMS division will remain "operational" in that they are not declared inoperable and they are not bypassed or tripped (i.e., they will be operable - capable of performing their specified safety function).

Based on the staff's review of the licensee's response to RAI Question No. 1, Item (3) of Enclosure 2 of the LAR, staff finds the licensee's response acceptable because the term "operational" is consistent with staff's definition of Operable[3]. Therefore, RAI Question No. 1, Item (3) of Enclosure 2 of the LAR is resolved and closed.

In RAI Question No. 2, Item (1) of Enclosure 2 of the LAR, staff requested the licensee to describe how the voting logic in the other PMS divisions would be affected for all RT and ESFAS functions while implementing setpoint changes under all different operating

[3] A system, subsystem, train, component, or device is operable or has operability when it is capable of performing its specified functions and when all necessary attendant instrumentation, controls, electrical power, cooling or seal water, lubrication, or other auxiliary equipment that are required for the system, subsystem, train, component, or device to perform its functions are also capable of performing their related support functions [NRC Glossary].

conditions. In its response to RAI Question No. 2, Item (1) of Enclosure 2 of the LAR, the licensee stated that:

> When reactor trip (RT) or Engineered Safety Features (ESF) actuation setpoint changes are implemented, both sub-channels for the function within that division will be declared inoperable and will not be relied upon for any safety function. The safety function will be appropriately implemented by the remaining operable redundant channels, as limited by applicable Technical Specification actions. All automatic RT and most automatic ESF actuations have four redundant channels, one for each PMS division, that are inputs to two out-of-four (2/4) voting logic. A setpoint change (actuations and permissives) would impact one channel in one division leaving 3 operable channels. If the inoperable channel undergoing the setpoint change is bypassed, the logic would become 2/3 in all divisions for the given RT or ESF actuation. For all other voting logic configurations (1/2, 2/2, 2/3), the design prohibits both sub-channels from being simultaneously bypassed in order to remain single-failure tolerant. In all cases (1/2, 2/2, 2/3, and 2/4), whether or not the inoperable channel is bypassed or tripped (for the time allowed by Technical Specifications, as described in response to RAI 1) its capability is not relied upon (due to declaring it inoperable) even though it could function to trip at either the old or the new setpoint if process conditions reached that setpoint.
>
> Alternatively, setpoint changes can be made when the plant is in a condition where the associated channel is not required to be operable.

Based on the staff's review of the licensee's response to RAI Question No. 2, Item (1) of Enclosure 2 of the LAR, staff found the licensee's response acceptable because there are at least two channels available for a minimum 2-out-of-4 coincidence vote. In addition, the design prohibits both sub-channels[4] from being simultaneously bypassed in order to remain single-failure tolerant. Therefore, RAI Question No. 2, Item (1) of Enclosure 2 of the LAR is resolved and closed.

In RAI Question No. 2, Item (2) of Enclosure 2 of the LAR, staff requested the licensee to describe the licensee's actions to ensure that in the presence of a system designed for division-based maintenance that at least one sub-channel within the given division will remain operational. In its response to RAI Question No. 2, Item (2) of Enclosure 2 of the LAR, the licensee stated that:

> The Function Enable Keyswitch does not impact the capability of the safety system from performing its safety function, because it only

[4] Each of the four divisions of the PMS is made up of two sub-channels.

enables/disables the soft buttons used to perform maintenance activities and provides a hardwired interlock to allow Manual Partial Actuations (MPAs) or Manual Partial Bypasses (MPBs). When the Function Enable Keyswitch is in the DISABLED position, actions at the MTP (e.g., setpoint changes, MPBs, MPAs, Test Injections) are not permissible (i.e., the soft buttons that are used to perform the actions at the MTP are disabled). Upon turning the Function Enable Keyswitch to the ENABLED position, actions at the MTP are permitted by enabling the soft buttons that control these actions. Placing the Function Enable Keyswitch into the ENABLED position does not prohibit any safety system function. Additionally, for MPB and MPA functions, the Function Enable Keyswitch is used as a hardwired interlock in the Bistable Processing Logic (BPL) for permitting these functions.

As noted in the RAI, WCAP-16675 states "When the Function Enable keyswitch is disabled, all surveillance test conditions are removed and all external inputs to the safety system functions are restored." This statement means the following: When the Function Enable Keyswitch is DISABLED, all surveillance test conditions that were initiated at the MTP are removed and all external (e.g., sensor) inputs to the safety system that were replaced with surveillance test conditions initiated at the MTP are restored. MPBs and MPAs are not automatically reset when the Function Enable is placed in the DISABLED position. They remain in the last state entered by the maintenance (e.g., bypassed or unbypassed). The Function Enable Keyswitch does not cause any sub channels within the division to be non-operational. It only provides an interlock at the display level (BPL level for MPAs/MPBs) to allow maintenance activities. All channels can be operational when the Function Enable Keyswitch is in the ENABLED position. However, when making setpoint changes, both sub-channels would be declared inoperable and not relied on to be operational.

Based on the staff's review of the licensee's response to RAI Question No. 2, Item (2) of Enclosure 2 of the LAR, staff found the licensee's response acceptable because while the Function Enable switch is divisionally-based, it does not place the entire division in test by the key switch simply by placing the key switch in the "ENABLED" position. The staff understands that it is only after altering settings related to a given sub-channel that the given sub-channel, or a singular function within the sub-channel, is impacted. While it is possible to bypass both sub-channels within a given division with the Function Enable switch, the staff understands that doing so would be controlled administratively. Therefore, RAI Question No. 2, Item (2) of Enclosure 2 of the LAR is resolved and closed.

Based on the above discussion, staff finds PSAI 6.18 is met.

7. <u>WCAP-16097 PSAI 6.19</u> – *A licensee implementing a Common Q DPPS must ensure that the serial communications link between the Maintenance and Test Panel (MTP) and the Processor Module is disabled by means of a physical disconnection (i.e., cable is removed from the serial port at the front of the PM646A). Alternative means of disconnecting this serial communication link may be considered, however, any means of disabling this communication link which rely upon software logic would invalidate the DI&C-ISG-04 conformance safety conclusions in Section 4.1.3.4 Staff Position 1, Point 10 of this SE*.

   The LAR states that in WCAP-16675, "AP1000™ Protection and Safety Monitoring System Architecture Technical Report," Westinghouse requires that the serial cable used to program the PM646A is disabled by means of physical disconnection. Staff reviewed the commitment and found it acceptable because this requirement is captured in WCAP-16675, which is part of the AP1000 licensing basis. Therefore, staff finds PSAI 6.19 is met.

8. <u>WCAP-16097 PSAI 6.20</u> – *A licensee implementing an application based upon the Common Q platform that utilizes fiber optic cables to connect HSL's between safety divisions shall ensure that all plant specific environmental qualification requirements for this cabling are met*.

   The LAR states that the disposition of WCAP-16097 PSAI 6.20 was already included in the scope of the disposition to WCAP-16097 PSAI 6.4 in APP-GW-GLR-017. From the information contained in the disposition for WCAP-16097 PSAI 6.4 at APP-GW-GLR-017, it was not clear to staff how the plant specific EQ requirements for the fiber optic cables were met. Therefore, in RAI Question No. 3 of Enclosure 2 of the LAR, staff requested the licensee to demonstrate how WCAP-16097 PSAI 6.20 is met. In its response to RAI Question No. 3 of Enclosure 2 of the LAR, the licensee stated the AP1000 fiber optic cables used to connect HSLs between safety divisions were already included in the scope of the original PSAI (i.e., WCAP-16097, Revision 1, PSAI 6.4). In addition, the response further states that this PSAI takes credit for the EQ and seismic ITAAC of the PMS (i.e., plant-specific Tier 1 Table 2.5.2-8 Items 2 (i, ii, and iii), 3, and 4). Staff determined this response was acceptable because these ITAAC require the AP1000 PMS design (including HSLs) to meet EQ and seismic requirements. As such, the fiber optic cables used to connect HSLs between PMS safety divisions must receive plant-specific EQ and seismic tests before the associated ITAAC can be closed and fuel loaded into the plant. In addition, the functional monitoring equipment used to monitor PMS equipment during the environmental and seismic testing detects if a loss of HSL communication was experienced during the testing, which was an acceptance criteria used during each phase of testing. Therefore, RAI Question No. 3 of Enclosure 2 of the LAR is resolved and closed.

   Based on the above discussion, staff finds PSAI 6.20 is met.

9. <u>WCAP-16097 PSAI 6.21</u> – *A licensee implementing an application based upon the Common Q platform that includes implementation of HSL must perform a site specific analysis to quantify the impact of higher electromagnetic emissions on operation of locally mounted equipment*.

   The LAR states that the AP1000 PMS specific EQ testing beyond that described in Reference 11 of the original SE was performed as documented in the AP1000 PMS equipment qualification summary report. Furthermore, the LAR states that the HSLs were included in the PMS cabinets for EMC testing which required the PMS cabinets to maintain functional operability during each EMC test to demonstrate qualification. The EQ report concluded that the PMS cabinets passed the required EMC tests. During the audit conducted from August 2 to 3, 2016, staff examined the HSLs test results in the EQ Summary Report. Staff confirmed that the PMS cabinets (including the HSLs) passed the required EMC tests. In addition, staff confirmed that the HSL radiated emissions do not impact any locally mounted equipment in the PMS cabinet. Therefore, staff finds PSAI 6.21 is met.

10. <u>WCAP-16097 PSAI 6.22</u> – *A licensee implementing an application based upon the Common Q platform that uses AI685 modules configured for either RTD or Thermocouple input must ensure that the installation includes a metallic barrier in front of the module*.

    The LAR states that the AP1000 PMS is not using the AI685 modules. Staff reviewed the disposition and determined it was acceptable because the AI685 module is not used for the AP1000 design. Therefore, staff finds PSAI 6.22 is not applicable to the AP1000 PMS. This is consistent with the disposition of WCAP-16097 PSAI 6.4.

11. <u>WCAP-16097 PSAI 6.23</u> – *A licensee implementing an application based upon the Common Q platform should perform a review of the current Common Q Record of Changes document to assess the validity of previously derived safety conclusions if changes have been made to the Common Q platform hardware, software, or processes defined in the Common Q TR*.

    The LAR states that Appendix 5, "Common Q Record of Changes," of WCAP-16097-P contains the list of changes to the Common Q Platform for the AP1000. Furthermore, the LAR states that since the issuance of the NRC's SE in 2013, Appendix 5 has been updated. The LAR concluded that that the Common Q hardware and software changes have not invalidated the original safety conclusion. During the audit conducted from August 2 to 3, 2016, staff examined the list of changes including both Common Q hardware and software processes, as well as editorial changes. Staff performed a sample review of the changes and confirmed that the changes have not invalidated the previously derived safety conclusion. Therefore, staff finds PSAI 6.23 is met.

12. <u>WCAP-16097 PSAI 6.24</u> – *A licensee implementing an application based upon the Common Q platform that relies on the [Flat Panel Display System (FPDS)] to perform safety critical functions shall perform an evaluation to address the added reliance on the FPDS to accomplish the required safety functions. The affects of not having the necessary information available on the FPDS during the design basis event should be considered and addressed in this evaluation*.

PSAI 6.24 addresses the FPDS, which provides the human-machine interface functions for the Common Q implementations. Section 2.1, "Common Q System," of the NRC's SE for WCAP-16097, Revision 3 states, in part, that:

> The FPDS can be used to support performance of safety critical actions by operators such as post-accident monitoring or control of safety related components.

Section 4.1.2, "Flat-Panel Display System" of the NRC's SE for WCAP-16097, Revision 3 provides additional considerations for cases where the FPDS is used to support performance of safety critical actions by operators, and it states that:

> For instances where the FPDS is performing safety critical functions or where it is credited to initiate or control protective actions, an additional safety significance evaluation shall be performed to address the added reliance on the FPDS to accomplish the required safety functions. Such an application may require re-classification of the FPDS as Safety Critical. For example, if the [Operator Module (OM)] is providing the only indication of a RG 1.97 Type A variable and thus being relied upon by the plant operator to initiate a required safety function, then the safety significance of the OM is elevated and the impacts of not having the necessary information available during the design basis event should be considered and addressed in this safety significance evaluation. This is PSAI 6.24.

Accordingly, PSAI 6.24 states that:

> A licensee implementing an application based upon the Common Q platform that relies on the FPDS to perform safety critical functions shall perform an evaluation to address the added reliance on the FPDS to accomplish the required safety functions. The affects [sic] of not having the necessary information available on the FPDS during the design basis event should be considered and addressed in this evaluation.

WCAP-16675-P, Revision 5, "AP1000 Protection and Safety Monitoring System Architecture Technical Report," is a proprietary document that describes the Common Q implementation of the AP1000 PMS (ADAMS Accession No. ML103370213). WCAP-

16675 describes that the FPDS, which is the generic term used in WCAP-16097 for the human-machine interface of the Common Q, is referred to as the “safety display” when mounted in the AP1000 main control room (MCR). In the AP1000 MCR, the safety displays are located on the Primary Dedicated Safety Panel (PDSP) and receive information for display from the Qualified Data Processing System. In Enclosure 2 of the letter dated February 15, 2016, SNC addressed PSAI 6.24 and stated:

> There are no Regulatory Guide 1.97 Type A variables used in the AP1000 I&C safety system. An evaluation was performed to address the reliance on the safety displays to accomplish required safety functions and the effects of not having the necessary information available on the safety displays during the design basis event. The evaluation concluded that the only safety critical functions based on the Common Q platform that rely on the Flat Panel Display System (FPDS) are those design basis events (DBE) that require operator action. The DBE are for Anticipated Operational Occurrences. No DBEs are limiting Design Basis Accidents. For these three DBEs, the information necessary for the operator to take action is captured on the FPDS and on alternate, non-safety related sources. No adverse safety consequences are expected if the safety system FPDS is not available.

In RAI Question No. 4 of Enclosure 2 of the LAR, staff requested the licensee to demonstrate how WCAP-16097 PSAI 6.24 is met. SNC responded to RAI Question No. 4 of Enclosure 2 of the LAR, in Enclosures 7 and 8 of the letter dated August 15, 2016. In Enclosure 7, SNC stated that:

> After reviewing the DBEs analyzed in Chapter 15, Chapter 6 (Section 6.2), and Appendix 19E for the AP1000 plant design, three DBEs were identified to require operator action. The DBEs are for Anticipated Operational Occurrences. No DBEs are limiting Design Basis Accidents. For these three DBEs, the information necessary for the operator to take action is captured on the FPDS and on alternate, non-safety related sources. For two of the events, procedures provide the guidance to use the alternate information on the Diverse Actuation System (DAS) so that the operators can reliably execute their emergency operating procedures. For the third event, there is an automatically initiated actuation in PMS that provides a backup to the operator action that relies on the safety displays. There is also a procedure for manual actuation using alternate information provided by the DAS or the normal operator workstations. Therefore, the required action can still occur for all three events even if the required information is not available on the FPDS-based safety displays. No adverse safety consequences are expected if the safety system FPDS is not available.

In Enclosure 8, which is proprietary, SNC identified each of the events that require or credit operator action, the required action operators perform during those events, the information provided by the safety displays, and the alternate information for each of the events. The staff reviewed Enclosures 7 and 8 and performed the following two actions:

(1) Although the licensee stated in Enclosure 7 of the letter dated August 15, 2016, that three DBE were identified to require operator action, the staff observed that four distinct events were evaluated in Enclosure 8. Specifically, the staff observed two of the DBE from Chapter 15 were combined and treated as one event for the evaluation. The staff provided SNC a draft RAI on January 13, 2017 (ADAMS Accession No. ML17014A000), to request the licensee clarify the number of DBEs that were evaluated. The staff and licensee and discussed the draft RAI at a public meeting on January 19, 2017 (ADAMS Accession No. ML17046A428).

SNC provided a response in Enclosure 14 of the letter dated March 17, 2017, and stated that two of the Chapter 15 events were treated as one event because the required operator action, the information required from the safety displays, the alternate sources of information, and the effects of not having that information available for the DBE are the same for both events. The staff finds the combined evaluation of the two events from Chapter 15 is acceptable because (1) the events are both categorized as events that result in an increase in mass in the reactor coolant system, and therefore the plant response to the events is similar, and (2) the operator actions and information provided by the safety displays are the same in both events.

(2) The staff reviewed VEGP 3&4 UFSAR, Revision 4, Chapter 15, "Accident Analyses" (ADAMS Accession No. ML15194A470), Chapter 6, "Engineered Safety Features" (ADAMS Accession No. ML15194A462), and Chapter 19, "Probabilistic Risk Assessment" (ADAMS Accession No. ML15194A474) as part of the evaluation of the RAI response. The results are documented below.

<u>UFSAR, Chapter 6 and Chapter 15</u>

The staff did not find that any operator actions were credited for any DBE described in Chapter 6 or Chapter 15. If no operator actions were needed to perform safety functions during any DBE, then operators would not need any information from the safety displays to accomplish any safety functions during the DBE, and no additional safety significance evaluation would need to be performed. Therefore, at a public meeting on September 19, 2015, the staff asked SNC to describe the difference between the UFSAR, Revision 4 and the information contained in the letter dated August 15, 2016 (ADAMS Accession No. ML16287A480).

During the public meeting, SNC explained that the UFSAR was being revised to incorporate changes resulting from License Amendment No. 52 (ADAMS Accession No. ML16201A435). License Amendment No. 52 authorized changes to the UFSAR to incorporate information in WCAP-17524, Revision 1, “AP1000 Core Reference Report” (ADAMS Accession No. ML15180A187), which was approved by the NRC on February 19, 2015. WCAP-17524, Revision 1 identified the changes that need to be incorporated into the UFSAR. In Section 4.6, “Non-LOCA Analyses,” of the SE for WCAP-17524, Revision 1 (ADAMS Accession No. ML16201A440), the staff identified the following changes to the UFSAR for three DBEs in Chapter 15:

> These changes incorporate required operator action to open the reactor vessel head vents (RVHVs) in order to prevent the pressurizer from overfilling with water during several design basis events (15.2.7 loss of normal feedwater flow, 15.5.1 inadvertent operation of the core makeup tanks at power, and 15.5.2 chemical and volume control system malfunction that increases reactor coolant system inventory).

The revisions to Sections 15.2.7, 15.5.1, and 15.5.2 of the VEGP 3&4 UFSAR authorized by License Amendment No. 52 also indicate that the operators will rely on the indication of pressurizer level to determine when to open the RVHVs. As shown in Table 7.5-1, “Post-Accident Monitoring System” Sheet 1/12 of the UFSAR (ADAMS Accession No. ML15194A463), pressurizer level is one of the post-accident monitoring variables provided on the safety display. As described in Section 7.7.1.11, “Diverse Actuation System,” indication of pressurizer level is also available on the DAS panel in the MCR. The DAS is a non-safety system that provides a diverse backup to the PMS when the PMS is not available during a DBE. Therefore, the operators will have a redundant and diverse indication of pressurizer level on the DAS panel if the indication is not available on the safety display during the DBE, and this will provide the information operators need to know to open the RVHVs.

WCAP-16675-P, Revision 5 indicates that the safety displays may also contain controls for the RVHVs. The staff provided SNC a draft RAI to request SNC address whether the controls for the RVHVs would still be available if the FPDS was not available during these DBEs (ADAMS Accession No. ML17081A477). In a letter dated December 16, 2016, SNC documented the questions in the draft RAI and provided responses to the questions. SNC described that the FPDS does not include the controls operators would use; rather, the controls are hardwired switches located on the PDSP and Secondary Dedicated Display Panel (SDSP). Hard-wired switches located on the PDSP and SDPS connect the controls directly to the components they operate, and thus, the RVHV controls will not be affected if the safety displays are not available. Therefore, the operators will still be able to operate the RVHVs if the FPDS is not available.

As shown in Table 7.5-1, “Post-Accident Monitoring System” Sheet 10/12 of the UFSAR, the safety displays provide indication of the position of the RVHVs. Position indication provides confirmation to the operator that the valve has changed position after he or she operators the valves’ controls. Therefore, the staff requested SNC consider the impact of not having RVHV position indication on the safety displays during the DBE. On January 13, 2017, the staff sent SNC a draft RAI to review. The staff and licensee discussed the draft RAI at a public meeting on January 19, 2017. SNC provided a response in Enclosure 14 of the letter dated March 17, 2017, and stated that the Ovation workstations would provide a redundant indication of the valve position. The Ovation workstations are the non safety operator workstations that operators normally use to monitor the plant, and they are not part of the FPDS as described in WCAP-16675. Therefore, the operators will have an alternate source of position indication available for RVHVs if the FPDS is not available.

Accordingly, the staff concludes that the required actions for these three DBE identified in Chapter 15 of the UFSAR can still occur even if the required information is not available on the safety displays, and therefore no adverse safety consequences are expected if the safety displays are not available.

UFSAR, Chapter 19

In Enclosure 8, SNC also evaluated an event described in Chapter 19, Appendix 19E, Section 19E.4.8.3, “Loss of Normal Residual Heat Removal System Cooling in Mode 5 with Reactor Coolant System Open.” The analysis of this event assumes that operators will manually perform the required actions using procedures and the information available on the safety displays. In Enclosure 7, SNC stated that if the safety displays do not provide the indication, then the operator can use alternate indications available on the DAS panel to perform the actions or indications on the operator workstations. Procedures provide direction to the operators to use alternate indications to perform the required actions if the safety displays are not available. The controls the operators need to perform these actions are hard-wired hand switches on the PDSP and SDSP, and redundant and diverse controls are also available on the DAS panel. Therefore, if the safety displays are not providing information, the operators will have an alternative indication to use to determine whether to perform the required action during this event.

Accordingly, the staff concludes that the required actions for the event identified in Chapter 19 of the UFSAR can still occur even if the required information is not available on the safety displays, and therefore no adverse safety consequences are expected if the safety displays are not available.

Human Factors Considerations

NRC regulations in 10 CFR Parts 50 and 52 require a variety of control and displays to be used by operators. Also, 10 CFR 50.34(f)(2)(iii) requires a control room design that reflects state-of-the-art human factor principles. NUREG-0711, "Human Factors Engineering Program Review Model," provides detailed guidance for NRC staff to use in verifying that these requirements are met. Section 18.2.1.2, "Assumptions and Constraints," of VEGP 3&4 UFSAR (ADAMS Accession No. ML15194A443) states:

> The human factors engineering process is designed to meet the human factors engineering design process requirements specified in NUREG-0711 (Reference 1).

Reference 1 to the UFSAR is NUREG-0711, Revision 2. NUREG-0711, Section 7.4, "Review Criteria," states, "*risk-important human actions should be identified from the PRA/HRA and used as input to the HFE design effort*." Additionally, APP-GW-GL-011, "AP1000 Identification of Critical Human Actions and Risk Important Tasks" (ADAMS Accession No. ML061030102), contains criteria for critical human actions specific to the AP1000 design and also identifies the AP1000 critical human actions and risk-important human actions. APP-OCS-GEH-320, "Human Factors Engineering Integrated System Validation Plan," Revision 6, Section 5.1.1, "Events," describes the incorporation of critical human actions and risk-important human actions in the HFE design process.

In RAI Question No. 3 of Enclosure 8 of the LAR, the staff requested the licensee to describe whether the required operator actions identified in Enclosure 8 of Letter ND-16-1391 meet the criteria to be classified as risk-important human actions and/or critical human actions. In its response to RAI Question No. 3 of Enclosure 8 of the LAR, dated December 16, 2016, the licensee stated the action to open the RVHVs identified in three of the DBEs analyzed in the UFSAR, Chapter 15 does not meet the criteria to be classified as risk-important human actions (RIHAs) or critical human actions.

To confirm the response, the staff reviewed the VEGP 3&4 UFSAR, Section 15.0.1.2, "Condition II: Faults of Moderate Frequency." This section of the UFSAR shows that the three DBEs from Chapter 15 are Condition II events, which are defined as faults of moderate frequency that at worst result in a reactor trip with the plant being capable of returning to operation. By definition, these events (or faults) do not propagate to cause a more serious events (i.e., Condition III or IV events), and thus, these events are classified as anticipated operational occurrences (AOOs), which are a type of DBE. Operator actions performed during AOOs do not meet the criteria to be classified as RIHAs because RIHAs are identified in beyond-design basis events. AOOs also do not meet the criteria to be classified as critical human actions, which APP-GW-GL-011 defines as actions performed during design basis accidents. Therefore, the actions performed during these AOOs do not meet the criteria in the VEGP 3&4 UFSAR to be included in the HFE program.

However, in its response to RAI Question No. 3 of Enclosure 8 of the LAR, SNC described that the actions to operate the RVHVs were included in the scenarios used to conduct the integrated systems validation (ISV), which a performance-based test of the human factors engineering design of the main control room. The staff reviewed APP-OCS-GEH-321, "AP1000 Human Factors Engineering Integrated System Validation Scenario Information," Revision 1, which is proprietary, and found that these actions were performed during ISV scenarios, and the ISV scenarios were more challenging than the scenarios described in the UFSAR, Chapter 15, for the three events. Therefore, the staff found that the licensee had evaluated the HFE design of controls and indications that operators may need to use during these events.

For the event identified in Enclosure 8 that is described in the VEGP 3&4 UFSAR, Chapter 19, the licensee stated that the actions performed by operators during this event are RIHAs, and these RIHAs were included in the HFE design program. The staff reviewed APP-OCS-GEH-321 and determined that these actions were included in the scenarios used to conduct the ISV. Therefore, the staff concludes that these actions have been incorporated into the HFE design program to demonstrate the feasibility and reliability of these actions, and RAI Question No. 3 of Enclosure 8 of the LAR is resolved and closed.

Conclusion

The staff concludes that the licensee has sufficiently evaluated the effects of not having information available on the safety display (i.e., FPDS) during the events where operators rely on the information to perform actions. The staff finds that the results of the licensee's evaluation provide reasonable assurance that no adverse safety consequences will result if the safety displays do not provide information during these events because alternate, redundant indications are available in the control room and procedures direct operators to use the alternate indications if the information is not available on the safety displays. Further, the staff finds that the licensee has satisfactorily addressed human factors considerations for the credited actions in Chapters 15 and 19. Therefore, the staff concludes SNC has satisfactorily addressed PSAI 6.24 and the requirements of 10 CFR 50.34(f)(2)(iii).

13. WCAP-16097 PSAI 6.25 – *A licensee implementing an application based upon the Common Q platform that relies upon the use of ITPs and the AF100 busses to provide separation between safety and non-safety signals must evaluate the plant-specific design against the independence criteria of IEEE 7-4.3.2-2003, Section 5.6.*

Staff reviewed the disposition to WCAP-16097 PSAI 6.25 and determined it was acceptable because the architecture for the AP1000 PMS does not rely upon the use of ITPs and AF100 busses to provide separation between safety and non-safety signals. Therefore, staff finds PSAI 6.25 is not applicable to the AP1000 design.

14. WCAP-16097 GOI 7.1 – *Westinghouse (formerly CENP) has committed to develop a new I/O module or re-design some of those already considered for use in the Common Q platform in order to meet the performance requirements of EPRI TR-107330.*

The LAR proposes to revise the introduction section and the GOI 7.1 resolution to correct statements that indicate the AI685 module is not used in the AP1000 design. Staff reviewed the changes in Enclosure 5 to LAR 15-017 and determined that these changes are acceptable because AI685 module is not used for the AP1000 design. Therefore, staff finds the GOI 7.1 resolution is not applicable to the AP1000 design.

15. WCAP-16097 GOI 7.11 – *Westinghouse has not yet conducted seismic and environmental qualification testing on the DI621 Digital Input module. The NRC staff's review of the I/O modules is discussed in Section 4.1.1.1.2.*

The LAR proposes to use DI621 module which was not listed in Table 1 of the WCAP-16097-P-A, Revision 3 (see WCAP-16097, PSAI 6.17). Staff reviewed the GOI disposition and determined it was acceptable because the seismic and EQ testing for DI621 module were performed in accordance with staff's approved UFSAR Appendix 3D methodology. In addition, the environmental qualification and seismic ITAAC for the PMS (i.e., plant-specific Tier 1 Table 2.5.2-8 Items 2 (i, ii, and iii), 3, and 4) require the AP1000 PMS design (including the DI621 module) to meet EQ and seismic requirements. As such, the DI621 module must receive plant-specific EQ and seismic tests before the associated ITAAC can be closed and fuel loaded into the plant. Therefore, staff finds GOI 7.11 is met.

WCAP-16096: Common Q Software Program Manual – Plant-Specific Action Items

1. WCAP-16096 PSAI 1 – *As noted in Sections 3.2.1 and 3.2.3, Westinghouse may choose to use alternatives to the SPM defined processes when performing Initiation phase activities for individual projects. These alternatives are required to be documented in the Project Quality Plan (PQP). This PQP should be reviewed to determine if alternatives to the SPM are being used for development of project specific software. When such alternatives are being used, the PQP should be evaluated to determine if the justifications for the use of alternatives to the SPM processes are acceptable.*

PSAI 1 in the NRC's SE for WCAP-16096, Revision 4 allows alternatives (along with justifications) to the SPM defined processes and requires them to be documented in the Project Quality Plan. The LAR proposes to use the SDP as the location for the SPM alternatives to the SPM processes or additional project specific information for the

Software Quality Assurance Plan (SQAP), Software Verification and Validation Plan (SVVP), Software Configuration Management Plan (SCMP), or the Software Operation and Maintenance Plan (SOMP). However, the proposed amendment was not clear in the relationship of the Project Plan and the SDP. Therefore, in RAI Question No. 1, Item (1) of Enclosure 3 of the LAR, staff requested the licensee to describe the relationship of the Project Plan and the SDP, and to demonstrate why it is acceptable to use the SDP instead of the Project Plan as the location for the SPM alternatives. In its response to RAI Question No. 1, Item (1) of Enclosure 3 of the LAR, dated August 19, 2016, the licensee stated that the Project Plan and the SDP are the same hierarchy level. The SDP identifies itself as the companion document to the Project Plan, and an extension, of the PMS Project Plan. Furthermore, the response stated that the software development activities are described in Part 5 of the Project Plan. This part of the Project Plan also provides details of the software project management and reviews performed on the AP1000 PMS software. Based on the staff's review of the licensee's response to RAI Question No. 1, Item (1) of Enclosure 3 of the LAR, staff finds the licensee's response acceptable because the Project Plan accounts for the SPM alternatives by referencing the SDP in Section 8.1. Furthermore, the SDP is a companion document, and an extension of the PMS Project Plan. Therefore, Question No. 1, Item (1) of Enclosure 3 is resolved and closed.

In RAI Question No. 1, Item (2) of Enclosure 3 of the LAR, staff requested the licensee to demonstrate why it is acceptable to use the Software Development Plan instead of the Project Plan as the location for the SPM alternatives to the SPM processes and/or additional project specific information. In its response to RAI Question No. 1, Item (2) of Enclosure 3 of the LAR, dated August 19, 2016, the licensee stated that the Project Plan accounts for the SPM alternatives by referencing the SDP in Section 8.1:

> The WCAP-16096-P-A (Reference 17) alternatives and justifications are documented in WNA-PD-00042-WAPP (Reference 15). See Section 16.0 for additional details.

The response further stated that both the Project Plan and the Software Development Plan are approved by the Project and Engineering Management, and by the Quality organization. The software engineers are required to train on both the Project Plan and the SDP so they will be cognizant of any alternatives to the Common Q SPM. Based on the staff's review of the licensee's response to RAI Question No. 1, Item (2) of Enclosure 3 of the LAR, staff finds the licensee's response acceptable. Therefore, RAI Question No. 1, Item (2) of Enclosure 3 of the LAR is resolved and closed.

For the reasons stated above, staff finds the proposed alternative to use the SDP as the location to capture alternative approaches used in the development of the PMS software is acceptable. Therefore, staff finds PSAI 1 is met.

2. WCAP-16096 PSAI 2 – *The Common Q SPM only includes the Software Life Cycle Process Planning Documentation as outlined in SRP BTP 7-14, Section B.2.1. As such, the plant-specific documentation outlined in SRP BTP 7-14, Sections B.2.2, "Software Life Cycle Process Implementation," and B.2.3, "Software Life Cycle Process Design Outputs," is to be evaluated separately for any application that references the Common Q SPM.*

   The LAR identifies the plant-specific documentation for the Software Life Cycle Process Implementation and Design Outputs. Staff reviewed the disposition and determined it was acceptable because it meets the acceptance criteria in BTP 7-14, Sections B.2.2, "Software Life Cycle Process Implementation," and B.2.3, "Software Life Cycle Process Design Outputs." Therefore, staff finds PSAI 2 is met.

3. WCAP-16096 PSAI 3 – *The Common Q SPM only addresses the vendor software planning processes for a Common Q-based system. For all activities in which the applicant or licensee assumes responsibility within a given project (including vendor oversight) for QA, additional evaluations, audits, or inspections must be performed to ensure that these licensee responsibilities are fulfilled.*

   To address WCAP-16096 PSAI 3, the LAR states that the QA activities for the PMS are covered by the QA program described in Chapter 17 of the UFSAR. Chapter 17 of the UFSAR describes the licensee's vendor oversight responsibilities.

   Section 17.1, "Quality Assurance During the Design and Construction Phases," of the UFSAR states in part that SNC is responsible for the establishment and execution of QA program requirements during the design, construction and operations phases of VEGP 3&4. SNC may delegate elements associated with the establishment and execution of the quality program, but retains responsibility for the quality assurance program. Oversight is provided through review and approval of vendor QA plans, by conducting QA audits and surveillances, and by direct participation in and oversight of the COL application development activities.

   Section 17.3, "Quality Assurance During Design, Procurement, Fabrication, Inspection, and/or Testing of Nuclear Power Plant Items," of the UFSAR states in part that activities affecting quality items and services for the AP1000 during design, procurement, fabrication, inspection, and/or testing will be performed as described in the "Westinghouse Electric Company Quality Management System (QMS)." While Westinghouse retains the overall responsibility for the AP1000 design, portions of the design are developed by external organizations. Each organization maintains a QA program that meets the NQA-1 criteria that apply to its work scope. In accordance with the QMS, Westinghouse performs an initial evaluation of these programs and monitors their continued effective implementation through audits, surveillance, and evaluation of the performance of external organizations.

For the reasons stated above, the staff determined the QA program described in Chapter 17 of the UFSAR provides the vendor oversight responsibilities for the PMS, and is therefore, acceptable. Therefore, staff finds PSAI 3 is met.

4. WCAP-16096 PSAI 4 – *Because the Common Q SPM does not address the criteria of BTP 7-14, Section B.3.1.8.4, "Software Operations Plan," an evaluation of compliance must be performed at the time of system development when the operational aspects of the system have been defined.*

   The LAR proposes to add a new Tier 2 Subsection 7.1.2.14.3, "Operational Process," which requires the development of an operations plan.

   > The protection and safety monitoring system has a software operations plan or procedure. The software operations plan addresses the secure operating environment of the protection and safety monitoring system. This includes precluding unauthorized changes to hardware, software, and system parameters. The software operations plan requires monitoring to detect penetration, or attempted penetration, of the system. There are also provisions on how to respond to unauthorized access.

   Staff reviewed the disposition and determined it was acceptable because it meets the acceptance criteria in BTP 7-14, Section B.3.1.8.4, "Software Operations Plan." Therefore, staff finds PSAI 4 is met.

5. WCAP-16096 PSAI 5 – *Site acceptance testing and installation testing are not covered under the Common Q Software Test Plan because they are considered to be licensee actions that are to be addressed during the development of a Common Q based application. As such, a project specific test plan should be developed and used to address these aspects of software test planning. Because the Common Q SPM does not address all aspects of the BTP 7-14 Section B.3.2.4 criteria, an evaluation of compliance must be performed at the time of system development when the site and installation testing activities have been defined.*

   The licensing basis requires the vendor to include site acceptance and installation testing of the PMS prior to turn over to the licensee. WCAP-16096, Revision 4 Section 4.3.2.2 provides requirements for test plans, including the site acceptance and installation test plan, consistent with the criteria in BTP 7-14. The site acceptance and installation test plan is developed by the vendor in accordance with WCAP-16096, Revision 4 Section 4.3.2.2. The commitment for the site acceptance testing and installation testing of the protection and safety monitoring system appears in DCD Tier 1 ITAAC Table 2.5.2-8, Item 11.e (COL Appendix C, ITAAC No. 2.5.02.11.e). The completion of this activity will be confirmed by the referenced ITAAC. Therefore, the staff finds PSAI 5 is met.

6. WCAP-16096 PSAI 6 – *A licensee implementing an application based upon the Common Q platform should perform a review of the current Common Q ROCs document to assess the validity of previously derived safety conclusions if changes have been made to the Common Q SPM.*

The LAR states that a review of the AP1000 PMS Common Q Record of Changes was performed and determined that there were no changes to the Common Q SPM. The staff examined the changes from Revision 01A to Revision 4 of the AP1000 PMS Common Q Record of Changes, including the alternatives addressed in this LAR (see Section 3.4 of this SE), and confirmed that the changes have not invalidated the previously derived safety conclusion. Therefore, staff finds PSAI 6 is met.

3.4 Evaluation of Common Q SPM and TR Alternatives

WCAP-16096: Common Q Software Program Manual Alternatives

1. SPM Section 4.3.2.1, "Initiation (Concept) Phase – Glossary of Terms: Project Quality Plan (PQP)

The LAR proposes an alternative to Common Q SPM Sections, "Glossary of Terms: Project Quality Plan," and 4.3.2.1, "Initiation (Concept) Phase." The LAR proposes to use the SDP as the location for the SPM alternatives to the SPM processes or additional project specific information for the SQAP, SVVP, SCMP or SOMP. In addition, the LAR states that the SDP also identifies itself as the companion document to the Project Plan. However, the proposed amendment was not clear in relationship of the Project Plan and the SDP. Therefore, in RAI Question No. 1, Item (2) of Enclosure 3 of the LAR, staff requested the licensee to demonstrate why it is acceptable to use SDP instead of the Project Plan as the location for the SPM alternatives to the SPM processes and/or additional project specific information. In its response to RAI Question No. 1, Item (2) of Enclosure 3 of the LAR, dated August 19, 2016, the licensee stated that the Project Plan (i.e., WNA-PD-00283-WAPP) and the SDP are the same hierarchy level. The justification for the alternative was updated to add a missing text, as follows (underlined text represents new text):

> A document that specifies alternatives or supplements to the Westinghouse Quality Management System (QMS), Level 2, or Level 3 procedures as required to meet contractual requirements or quality standards other than those specified in the Westinghouse QMS. When the SPM refers to a PQP, it includes the Project Quality Plan and Project Plan (including the Software Development Plan) defined in the Westinghouse Quality Procedures. Any alternatives to the SPM processes or additional project specific information for the SQAP, SVVP, SCMP or SOMP shall be documented and justified in the PQP.

Based on the staff's review of the licensee's response to RAI Question No. 1, Item (2) of Enclosure 3 of the LAR, staff finds the licensee's response acceptable because the Project Plan accounts for the SPM alternatives by referencing the SDP in Section 8.1. Furthermore, the SDP is a companion document, and an extension of the PMS Project Plan. Therefore, RAI Question No. 1, Item (2) of Enclosure 3 of the LAR is resolved and closed.

Based on the above discussion, staff finds the alternative to Common Q SPM Sections, "Glossary of Terms: Project Quality Plan," and 4.3.2.1 is acceptable.

2. <u>SPM Section 4.3.1, "Organization," – Exhibit 2-1 Design/IV&V Team Organization</u>

The LAR proposes an alternative to Common Q SPM Section 4.3.1, "Organization." The alternative proposes to update Exhibit 2-1 – Design/IV&V Team Organization to show that design team and the Independent Verification & Validation (IV&V) team are in separate organizations at least to the Director level. The justification of the alternative states:

> The IV&V team and the design team are not under the same organization to maintain independence. This level of independence exceeds the criteria in the SPM.

In RAI Question No. 2 of Enclosure 3 of the LAR, staff requested the licensee to describe how the proposed alternative to Exhibit 2-1 "exceeds the criteria in [Section 4.3.1 of] the SPM," actually meets the site-specific requirements in the WCAP-16096. In its response to RAI Question No. 2 of Enclosure 3 of the LAR, dated August 19, 2016, the licensee stated that after the NRC-approved Common Q SPM was issued, the Westinghouse Safety System development organization structure changed. The response provided an organization chart (Figure A3-1) as an example to reflect the minimum level of independence required by the SPM. The new organization chart shows the same level of separation for the Design Team and IV&V Team as the current Exhibit 2-1, namely they are independent at the Director level. The response also revised the organization chart to show the Quality Team being independent of the Design and IV&V Teams at the Vice President level instead of the Director level. The staff determined this was acceptable because these changes are consistent with how Exhibit 2-1 is referred to in Section 2 of the SPM. The new organization chart (Figure A3-1) shows the same level of separation for the Design Team and IV&V Team as the current Exhibit 2-1, namely they are independent at the Director level. Based on staff's review of the licensee's response to RAI Question No. 2 of Enclosure 3 of the LAR, staff finds the licensee's response acceptable. Therefore, RAI Question No. 2 of Enclosure 3 of the LAR is resolved and closed.

Based on the above discussion, staff finds the alternative to Common Q SPM Section 4.3.1 is acceptable.

3. SPM Section 4.3.2.6, “Site Installation and Checkout Phase”

The LAR proposes an alternative to Common Q SPM Section 4.3.2.6, “Site Installation and Checkout Phase.” The alternative states:

> A site test plan is developed in accordance with the overall digital I&C test strategy to support installation testing and the Initial Test Program.

The justification of the alternative states:

> A separate schedule is developed that governs the overall scheduling of AP1000 site testing. Site test planning is initiated during PMS development, but independent of any particular PMS development phase. This is an appropriate approach for a new build project.

In RAI Question No. 3 of Enclosure 3 of the LAR, staff requested the licensee to demonstrate why the site test planning is independent of any particular PMS development phase. In its response to RAI Question No. 3 of Enclosure 3 of the LAR, the licensee stated, in part, that:

> A schedule is developed that governs the overall planning of AP1000 new build site testing. The planning for AP1000 site testing started early and included the development of testing methodology documents for instrumentation and controls (I&C), including the PMS. The methodology document describes different levels of testing starting with lower level testing at the component level, to site installation, and acceptance of the system. The site test team uses the outputs of the Requirements (i.e., Definition) phase and the Design and Implementation (i.e., Development) phase for actual development of the site testing specifications and procedures. Requirements traceability also provides assurance that the PMS requirements are tested prior to and post-installation, as appropriate that the planning for AP1000 site testing started early and included the development of testing methodology documents for instrumentation and controls (I&C), including the PMS.

During the audit conducted from August 2 to 3, 2016, staff reviewed the overall digital I&C test strategy and the draft site test plan for the PMS. Staff was not clear how this alternative would fall within the acceptance criteria of IEEE Std. 1012-1998, “IEEE Standard for System and Software Verification and Validation,” and the commitments in the Common Q SPM for the requirements phase, and potentially subsequent system development phases. Staff’s position continues to be that allowing the initiation of the Site Specific Acceptance Testing Plan to occur at any time during the PMS development phases rather than during the requirements phase relaxes the Common Q SPM requirement in a non-conservative manner. As such, this alternative would fall within the acceptance criteria of IEEE Std. 1012-1998 and the commitments in the Common Q SPM for the requirements phase, and potentially subsequent system development phases. In RAI Question No. 5, Item (a) of Enclosure 11 of the LAR, the staff requested the licensee to clarify what is meant by "The planning for AP1000 site testing started early." In its response to RAI Question No. 5, Item (a) of Enclosure 11 of the LAR, dated December 16, 2016, the licensee stated that:

> The PMS site test plan was initiated prior to, and maintained during and after, the PMS Requirements Phase. The SPM alternative was originally taken because Revision A of some site test planning documents were not archived during the Requirements Phase. Upon closer review, it was determined that other site planning documentation was created and archived early in the project. This satisfies the Common Q SPM requirement of initiating the site test plan during the requirement phase.
>
> The Common Q SPM alternative is proposed to be removed from the license amendment request…

Based on the staff's review of the licensee's response to RAI Question No. 3 of Enclosure 3 of the LAR and RAI Question No. 5, Item (a) of Enclosure 11 of the LAR, staff finds the licensee's responses unresolved because the LAR no longer includes this alternative. Therefore, RAI Question No. 3 of Enclosure 3 of the LAR and RAI Question No. 5, Item (a) of Enclosure 11 of the LAR are unresolved and closed.

In RAI Question No. 5, Item (b) of Enclosure 11 of the LAR, staff requested the licensee to describe how the proposed alternative will meet the processes of IEEE 1012-1998, (e.g., V&V Tasks 5.4.2, 5.4.3, and 5.4.4). In its response to RAI Question No. 5, Item (b) of Enclosure 11 of the LAR, the licensee stated that this question is no longer applicable since the LAR no longer includes this alternative. Based on the staff's review of the licensee's response to RAI Question No. 5, Item (b) of Enclosure 11 of the LAR, staff finds the licensee's response unresolved because the LAR no longer includes this alternative. Therefore, RAI Question No. 5, Item (b) of Enclosure 11 of the LAR is unresolved and closed.

The staff concludes this alternative is no longer applicable because the licensee withdrew this alternative from the LAR.

4. <u>SPM Section 4.6.2.10, "Post Mortem Review"</u>

The LAR proposes to use the Corrective Action, Prevention and Learning (CAPAL) system instead of Westinghouse Corrective Actions Process (CAP). The alternative states:

> Suggestions for improvement and/or best practices that are identified during the Post Mortem Review should be documented via the Corrective Action, Prevention and Learning (CAPAL) system.
>
> EXHIBIT 11-2 contains a screenshot of the Corrective Action Process (CAP) system. The CAP system has since been migrated to the Corrective Action, Prevention and Learning (CAPAL) system per Westinghouse Level 2 procedures.

The justification of the alternative to Section 4.6.2.10, “Post Mortem Review,” states:

> Suggestions for improvement and best practices are captured in the CAPAL system. Therefore, the required content is still captured and intent of this commitment is still met.

In RAI Question No. 4 of Enclosure 3 of the LAR, staff requested the licensee to describe how the CAPAL system meets the processes in the CAP system. In its response to RAI Question No. 4 of Enclosure 3 of the LAR, dated August 19, 2016, the licensee stated that the CAPAL system replaced the CAP system at a company-wide level in April 2014. The CAPAL system is the company-wide tool used by Westinghouse for corrective action. The Westinghouse corrective action program is governed by 10 CFR Part 50 Appendix B, Criterion XVI Corrective Action and the Westinghouse Quality Management System, which is incorporated by reference into the AP1000 licensing basis and approved by the NRC. The justification for the alternative to Section 4.6.2.10 was updated for clarification purposes, as follows (underlined text represents new text):

> Suggestions for improvement and best practices are captured in the CAPAL system. <u>The Westinghouse corrective action program is governed by 10 CFR Part 50 Appendix B, Criterion XVI Corrective Action and the Westinghouse Quality Management System (QMS), which is incorporated by reference into the AP1000 licensing basis and approved by the NRC. The Westinghouse corrective action program continues to meet the requirements within these documents.</u> Therefore, the required content is still captured and the intent of this commitment is still met.

Staff determined this was acceptable because the CAPAL system continues to meet the requirements in the CAP system. Based on the staff’s review of the licensee’s response to RAI Question No. 4 of Enclosure 3 of the LAR, staff finds the licensee’s response acceptable. Therefore, RAI Question No. 4 of Enclosure 3 of the LAR is resolved and closed.

Based on the above discussion, staff finds the alternative to Common Q SPM Section 4.6.2.10 is acceptable.

5. <u>SPM Section 5.5.1, “Management of IV&V”</u>

The LAR proposes an alternative to Common Q SPM Section 5.5.1, “Management of IV&V.” The alternative states:

> The resources for performing the IV&V shall be identified in the AP1000 PMS Software Verification and Validation Plan (SVVP) that is prepared by the IV&V team during the conception phase of the software life cycle.

The justification of the alternative to Section 5.5.1, “Management of IV&V,” states:

> The resources for performing IV&V are identified in a planning document prepared by the IV&V team during the Concept Phase and reviewed by the PMS Project Manager. Documenting the resource plan in the SVVP is consistent with IEEE 1012.

The management of IV&V spans all life-cycle phases. Staff reviewed the disposition and determined this was acceptable because documenting the resource plan in the SVVP is consistent with IEEE Std. 1012-1998. During the audit conducted from August 2 to 3, 2016, staff confirmed that the resources for performing the IV&V have been identified in the AP1000 PMS SVVP. Based on the above discussion, staff finds the alternative to Common Q SPM Section 5.5.1 is acceptable.

6. <u>SPM Section 6.3.2, “Configuration Change Control”</u>

The LAR proposes to use Westinghouse Design Change Proposals (DCPs), Engineering & Design Coordination Reports (E&DCRs), the Westinghouse Level 3 Request for Engineering Change (REC) process, and the Westinghouse Level 3 Configuration Management (CM) procedure instead of the Software Change Request (SCR) form. The alternative states:

> Design Change Proposals (DCPs), Engineering & Design Coordination Reports (E&DCRs), the Westinghouse Level 3 Request for Engineering Change (REC) process, and the Westinghouse Level 3 Configuration Management (CM) procedure are used as the basis to track all system changes, to verify that changes have been properly implemented, and to ensure that documentation has been updated.

The justification of the alternative states:

> The Software Change Request (SCR) form is inadequate for tracking changes for a complex system. The use of Westinghouse DCP, E&DCR, REC, and CM processes is an appropriate, comprehensive approach to

capturing plant-wide I&C system baseline changes. Westinghouse processes exceed this requirement by using an enhanced process.

In RAI Question No. 5 of Enclosure 3 of the LAR, staff requested the licensee to describe how the use of Westinghouse DCP, E&DCR, REC, and CM processes documentation for tracking changes meets to the tracking documentation in the SCR form. In its response to RAI Question No. 5 of Enclosure 3 of the LAR, dated August 19, 2016, the licensee stated that the proposed alternative was not consistent with the scope of Section 6.3, “Software Configuration Management Activities” or the subsection where this step resides, because this section is discussing the process for software changes, not system changes. The licensee further stated that the current statement in WCAP-16096, Revision 4 Section 6.3.2 refers to “system” changes instead of “software” changes is a typographical error. Thus, the licensee plans to continue to use the SCR form for software changes. The alternative and justification were updated, as follows (underlined text represents new text and strikethrough text represents deleted text):

<u>Alternative</u>:

~~Design Change Proposals (DCPs), Engineering & Design Coordination Reports (E&DCRs), the Westinghouse Level 3 Request for Engineering Change (REC) process, and the Westinghouse Level 3 Configuration Management (CM) procedure are used as the basis to track all system changes, to verify that changes have been properly implemented, and to ensure that documentation has been updated~~.

<u>Software Change Request Procedure, Step 5: Revised System Baseline: The SCR forms will be used as the basis to track all software changes and to verify that changes have been properly implemented and that documentation has been updated</u>.

<u>Justification</u>:

~~The Software Change Request (SCR) form is inadequate for tracking changes for a complex system. The use of Westinghouse DCP, E&DCR, REC, and CM processes is an appropriate, comprehensive approach to capturing plant-wide I&C system baseline changes. Westinghouse processes exceed this requirement by using an enhanced process.~~
<u>Section 6.3, “Software Configuration Management Activities” and the subsection “Software Change Request Procedure” are discussing the process for software changes, not system changes. The alternative corrects the typographical error which incorrectly refers to system changes instead of software changes.</u>

Based on the staff's review of the licensee's response to RAI Question No. 5 of Enclosure 3 of the LAR, staff finds the licensee's response acceptable because the proposed alternative corrects the typographical error which incorrectly refers to system changes instead of software changes. In addition, the licensee will continue to use the SCR form to track all software changes and to verify that changes have been properly implemented. Therefore, RAI Question No. 5 of Enclosure 3 of the LAR is resolved and closed.

Based on the above discussion, staff finds the alternative to Common Q SPM Section 6.3.2 is acceptable.

7. <u>SPM Section 6.3.4, "Configuration Audits and Reviews"</u>

The LAR proposes an alternative to Common Q SPM Section 6.3.4, "Configuration Audits and Reviews." The alternative states:

> External audits by customers or regulators shall be coordinated by QA or Licensing who will schedule personnel to be available if additional support is required.

The justification of the alternative states, in part, that:

> Westinghouse's Quality Assurance Program Level 2 External Audits and Regulatory Inspections process governs external audits. External audits are coordinated via QA and regulatory audits are coordinated via Licensing (and QA). The Technical Lead, Licensing Lead, Quality Lead, and Responsible Management of the Audited Organization support the audit by ensuring the appropriate resources are available.

The alternative proposes to coordinate external audits by customers or regulators via QA or Licensing. Staff determined this was acceptable because the Westinghouse Level 2 process meets the intent of the commitment to designate resources to ensure personnel are available to support external audits. Based on the above discussion, staff finds the alternative to Common Q SPM Section 6.3.4 is acceptable.

8. <u>SPM Section 6.4, "SCM Schedule"</u>

The LAR proposes an alternative to Common Q SPM Section 6.4, "SCM Schedule." The alternative states:

> SCM milestones that shall be indicated in the project schedule include:
>
> - Establishment of a configuration baseline, and
> - Implementation of change control procedures.

> Establishment of the Configuration Control Board (CCB) is captured in the AP1000 I&C program plan.

The justification of the alternative states:

> Establishment of the CCB has already been completed and, therefore, there is no need to capture it in the project schedule. A description of the CCB process is provided in the AP1000 I&C program plan.

The alternative proposes to remove the establishment of a configuration baseline milestone from the project schedule. Staff determined this alternative was acceptable because the milestone to establish the CCB was completed. Staff agrees that the CCB milestone does not need to be captured in the schedule. During the audit conducted from August 2 to 3, 2016, staff reviewed the AP1000 I&C Program Plan. This document added a description of the CCB process due to the proposed alternative to SPM Section 6.4, "SCM Schedule." Staff confirmed that the CCB process described in AP1000 I&C Program Plan does not contradict the CBB process in the Common Q SPM. Although the staff agrees that carrying the CCB Meetings on the formal schedule is not required, it does not relieve the licensee from creating and actively implementing the use of the CCB at regular intervals. Therefore, staff finds the alternative to Common Q SPM Section 6.4 is acceptable.

9. <u>SPM Section 9.2.3, "Control"</u>

The LAR proposes an alternative to Common Q SPM Section 9.2.3, "Control." The alternative states:

> Per the Common Q Automation Issue Tracking System (RITS) Work Instruction, the RITS system maintains the SCR log.
>
> The Software Lead shall confirm that the approved SCR is entered into this log.

The justification of the alternative, states:

> The Platform Lead does not follow AP1000 PMS software changes. The intent of this commitment is still met by designating an appropriate person to confirm the approved SCR is entered into this log. The Common Q RITS Work Instruction designates the Software Lead for this responsibility.

In the alternative to Common Q SPM Section 9.2.3, "Control," the licensee proposed to designate the Software Lead to confirm the AP1000 PMS software changes. Section

5.4.3.1.5, “Engineering Project Manager,” of the SPM states that EPMs and Platform Leads may delegate the performance of necessary tasks to other persons but remain responsible for their execution. In RAI Question No. 6 of Enclosure 3 of the LAR, staff requested the licensee to describe how the Platform Lead would remain responsible for the execution of the AP1000 PMS software changes. In addition, the staff requested the licensee to describe how the use of Westinghouse processes will be used to track changes instead of the SCR form. In its response to RAI Question No. 6 of Enclosure 3 of the LAR, dated August 19, 2016, the licensee stated that the Platform Lead is not responsible for project-specific software changes and is only responsible for generic Platform software changes. To clarify the Platform Lead and Software Lead responsibilities, the alternative for SPM section 9.2.3 in the amendment request, the licensee changed to the following (underlined text represents new text and strikethrough text represents deleted text):

> ~~RITS system maintains the SCR log. The Software Lead shall confirm that the approved SCR is entered into this log.~~
>
> <u>An SCR log shall be maintained for the specific Common Q™ system implementation. The Platform Lead shall confirm that the approved SCR is entered into the SCR log for any internal generic software changes. The Lead Software Engineer shall confirm that the approved SCR is entered into the SCR log for any PMS-specific software changes.</u>

In their response, the licensee further stated that the proposed alternative is not consistent with the scope of SPM Section 6.3, “Software Configuration Management Activities” or the subsection where this step resides. This subsection gives the “Software Change Request Procedure.” As such, this section is discussing the process for software changes, not system changes. The current statement in WCAP-16096, Revision 4 Section 6.3.2 that refers to “system” changes instead of “software” changes is a typographical error. Staff found this response acceptable because the SCR form is the applicable tool for software changes. In addition, the alternative corrects the typographical error in which Section 6.3, “Software Configuration Management Activities” and the subsection “Software Change Request Procedure” incorrectly refers to system changes instead of software changes. Based on the staff’s review of the licensee’s response to RAI Question No. 6 of Enclosure 3 of the LAR, staff finds the licensee’s response acceptable. Therefore, RAI Question No. 6 of Enclosure 3 of the LAR is resolved and closed.

Based on the above discussion, staff finds the alternative to Common Q SPM Section 9.2.3 is acceptable.

10. <u>SPM Section 10.5.1, “Software Verification and Validation Plan”</u>

The LAR proposes an alternative to Common Q SPM Section 10.5.1, "Software Verification and Validation Plan." The alternative states:

> The AP1000 PMS SVVP shall define the tracking and recording process for the hardware configuration (i.e., test configuration records) pertinent to the software verification and validation process during all phases of the software life cycle.

The justification of the alternative states:

> The intent of this requirement is to ensure documentation of project specific V&V activities. This intent is met since there is a project specific SVVP (i.e., AP1000 PMS SVVP) that defines the tracking and recording process for the hardware configuration.

The alternative proposes to use the AP1000 PMS SVVP to define the tracking and recording process for the hardware configuration (i.e., test configuration records) pertinent to the software verification and validation process during all phases of the software life cycle. Staff determined this was acceptable because the intent of this requirement is to ensure documentation of project specific V&V activities. This intent is met since there is a project specific SVVP (i.e., AP1000 PMS SVVP) that defines the tracking and recording process for the hardware configuration. Therefore, staff finds the alternative to Common Q SPM Section 10.5.1 is acceptable.

11. <u>SPM Section 10.10, "Computer Code Certificate"</u>

The LAR proposes an alternative to Common Q SPM Section 10.10, "Computer Code Certificate." The alternative states:

> The completion of the installation and checkout phase Software Verification and Validation report is the basis for the issuance of a Computer Code Certificate (see EXHIBIT 10-1 COMPUTER CODE CERTIFICATE for content requirements).

The justification of the alternative states:

> This alternative corrects a typographical error in the SPM, since there is not an "implementation and checkout phase."

The alternative proposes to correct a typographical error in the SPM. Staff found this acceptable because this typographical error has no impact on the process requirements of the SPM and does not reduce any licensing commitments. Therefore, staff finds the alternative to Common Q SPM Section 10.10 is acceptable.

12. SPM Section 11.4, "Corrective Action"

The LAR proposes an alternative to Common Q SPM Section 11.4, "Corrective Action." The alternative states:

> Corrective actions shall be documented in RITS by the design team and shall be completed by the due date specified on the form…Once the RITS independent reviewer is satisfied with the corrective action taken, the report form shall be closed.

The justification of the alternative states:

> The RITS form contains the same information as the SPM Exception Report and Common Q Comment Record.
>
> Though a signature is not required, RITS requires login credentials for the independent reviewer to close out the report. Login credentials satisfy the function of a signature.

The LAR proposes to document the corrective actions in the Repair, Replacement and Automation Services Issue Tracking System (RITS), and for the independent RITS reviewer to close out the report. In RAI Question No. 7 of Enclosure 3 of the LAR, staff requested the licensee to provide a complete listing of the reporting relationships established to demonstrate that an adequate level of separation exists between the design team and the independent RITS reviewer. In its response to RAI Question No. 7 of Enclosure 3 of the LAR, dated August 19, 2016, the licensee stated that the requested amendment does not propose any changes to the licensing basis related to the independent review of corrective actions. The justification for the WCAP-16096 alternative to SPM Section 11.4 is updated for clarification purposes, as follows (underlined text represents new text):

> The RITS form contains the same information as the SPM Exception Report and Common Q Comment Record.
>
> Though a signature is not required, RITS requires login credentials for the independent reviewer to close out the report. Login credentials satisfy the function of a signature.
>
> <u>The requirements for reviewer independence have not changed. The independent reviewer of the corrective action continues to meet the requirements of 10 CFR Part 50 Appendix B, Criterion III Design Control. The independent reviewer is an individual or group other than those who performed the original design, but who may be from the same organization.</u>

Staff reviewed the disposition and determined it was acceptable because WCAP-16096, Revision 4, still requires an independent review of the corrective actions. Criterion III of Appendix B to 10 CFR Part 50 requires the independent reviewer to be an individual or group other than those who performed the original design, but who may be from the same organization. This alternative does not violate the independence of checkers and verifiers of Criterion III of Appendix B to 10 CFR Part 50. Based on staff's review of the licensee's response to RAI Question No. 7 of Enclosure 3 of the LAR, staff finds the licensee's response acceptable. Therefore, RAI Question No. 7 of Enclosure 3 of the LAR is resolved and closed.

Based on the above discussion, staff finds the alternative to Common Q SPM Section 11.4 is acceptable.

13. SPM Section 12, "Secure Development and Operational Environment Plan"

The LAR proposes an alternative to Common Q SPM Section 12, "Secure Development and Operational Environment Plan." The alternative states:

> The SPM, Section 12, details a Secure Development and Operational Environment Plan for Common Q systems. While this plan provides an acceptable method to comply with computer security requirements, AP1000 PMS will instead continue to use the Incorporated by Reference document APP-GW-J0R-012, "AP1000 Protection and Safety Monitoring System Computer Security Plan."

The justification of the alternative states:

> The AP1000 PMS Computer Security Plan is specific for AP1000 and has been determined to be an acceptable method used to demonstrate how computer security is incorporated into the design and development of AP1000 safety systems. The AP1000 PMS Computer Security Plan is consistent with the Common Q SPM incorporated by reference information and, therefore, should be used in place of any Section 12 references made within the Common Q SPM.

In RAI Question No. 8 of Enclosure 3 of the LAR, staff requested the licensee to describe how the AP1000 PMS computer security plan meets or exceeds the criteria in Section 12 of WCAP-16096. In its response to RAI Question No. 8 of Enclosure 3 of the LAR, dated August 19, 2016, the licensee stated that the PMS computer security plan describes the process followed for the development of the PMS to maintain a secure development and operational environment. Furthermore, the response stated that unlike WCAP-16096 Revision 4, the WCAP-16096 incorporated by reference into the current licensing basis (i.e., WCAP-16096, Revision 01A) does not outline a computer security plan. WCAP-16096, Revision 4, which is proposed to be added in this amendment request, contains a generic computer security plan for Common Q systems. Staff found the licensee's response acceptable because the PMS computer security plan was reviewed and approved by the staff in NUREG-1793 Supplement 2 (ADAMS Accession No. ML12271A045). In addition, the staff's evaluation of the PMS computer security plan concluded that the AP1000 computer security plan satisfy the requirements of 10 CFR 50.55(a)(h), IEEE Std. 603-1991 Clauses 5.6.3 and 5.9, and GDC 21. Therefore, RAI Question No. 8 of Enclosure 3 of the LAR is resolved and closed.

Based on the above discussion, staff finds the alternative to Common Q SPM Section 12 is acceptable.

WCAP-16097: Common Q Topical Report Alternatives

1. Common Q TR Section, "References" – Table A3-2, "Common Q Topical Report Alternatives"

The LAR proposes to remove the revision number for the WCAP-17266 reference from the TR Section, "Reference." The justification of the alternative states:

> Removing the revision number for the WCAP-17266 reference is consistent with how the Common Q SPM references this document. WCAP-17266 is not an input into WCAP-16097, but a lower-level process document. Therefore, identifying a revision number is unnecessary. This document will continue to meet the commitment in WCAP-16097, Revision 3, Section 12 which requires it to describe the screening and evaluation process for determining what Common Q platform changes are available for audit, and which changes require re-submission to the NRC.

In RAI Question No. 1 of Enclosure 3 of the LAR, related to WCAP-16097, staff requested the licensee to describe the configuration controls for WCAP-17266 to ensure errors are properly identified, captured, tracked, resolved and placed into a records management system to ensure the issue is available for historical reference. In its response to RAI Question No. 1 of Enclosure 3 of the LAR, dated August 19, 2016, the licensee stated that even though the revision number is removed from the reference section in WCAP-16097, WCAP-17266 itself will still be subject to the document control procedure under the Westinghouse Quality Procedure program. The licensee updated the justification as follows (underlined text represents new text):

> Removing the revision number for the WCAP-17266 reference is consistent with how the Common Q SPM references this document. WCAP-17266 is not an input into WCAP-16097, but a lower-level process document. Therefore, identifying a revision number is unnecessary. This document will continue to meet the commitment in WCAP-16097,

Revision 3, Section 12 which requires it to describe the screening and evaluation process for determining what Common Q platform changes are available for audit, and which changes require re-submission to the NRC.

Even though the revision number is removed from the reference section in WCAP- 16097, WCAP-17266 itself will still be subject to the document control procedure under the Westinghouse Quality Procedure program. If an error is identified in WCAP-17266, then a corrective action issue would be identified and documented in accordance with Westinghouse Corrective Action Program. The Corrective Action Program is the means to capture, track, and resolve errors to ensure the issue is available for historical reference. The corrective action program is also the means to ensure a new revision of WCAP-17266 is placed into the Westinghouse Quality Records System.

Staff agrees that Westinghouse Quality Records System in accordance with Westinghouse Quality Procedure W2-6.1-100, "Document Control" provides revision control for WCAP-17266. However, the response to the RAI was not clear for why not having the revision number of WCAP-17266 in WCAP-16097 is acceptable. Therefore, in RAI Question No. 1 of Enclosure 7 of the LAR, staff asked the licensee to describe how a change in WCAP-17266 will be captured, tracked, and resolved in WCAP-16097, if the revision number of WCAP-17266 is not referenced. In its response to RAI Question No. 1 of Enclosure 7 of the LAR, dated December 16, 2016, the licensee stated that WCAP-17266 is controlled by the I&C standard safety system platform configuration control process. This process requires any changes to WCAP-17266 to be screened for impacts against the NRC-approved Common Q SPM and TR. If the TRs are impacted, an updated version would be submitted for generic NRC-approval, or the change would be processed in a license change package for a specific project. Based on staff's review of the licensee's response to RAI Question No. 1 of Enclosure 3 of the LAR and RAI Question No. 1 of Enclosure 7 of the LAR, staff finds the licensee's responses acceptable. Therefore, RAI Question No. 1 of Enclosure 3 of the LAR and RAI Question No. 1 of Enclosure 7 of the LAR are resolved and closed.

Based on the above discussion, staff finds the alternative to Common Q TR is acceptable.

3.5 Evaluation of Proposed Changes to the Licensing Basis

To maintain consistency throughout the VEGP 3&4 UFSAR and the documents incorporated by reference in the VEGP 3&4 UFSAR, changes to add the licensing basis revision numbers for Common Q SPM and TR, along with the reference to the changes provided in VEGP 3&4 UFSAR Appendix 7A at each location in which these two WCAPs are referenced in the UFSAR including Appendix 7A. The licensee provided the proposed UFSAR mark-ups in Enclosure 4 to

LAR 15-017 for VEGP 3&4 UFSAR Chapter 7, Sections 7.1, 7.2, Figure 7.1-2, and Appendix 7A. Staff reviewed the proposed VEGP 3&4 UFSAR mark-ups and revision updates provided in Enclosure 4 to LAR 15-017 and concludes that these changes are acceptable.

3.6 Other Safety Evaluation Notes

Updates Regarding APP-GW-GLR-017

By letter dated March 17, 2017, SNC submitted LAR 15-017S5, to address clarifications requested by the staff to support review of LAR 15-017. In this letter, the licensee provided updates and corrected the classification of APP-GW-GLR-017, "AP1000 Standard Combined License Technical Report, Resolution of Common Q NRC Items." The licensee stated that this document was improperly referenced as an incorporated by reference (IBR) document in the original submittal of LAR 15-017. The licensee further stated that in response to new GOIs/PSAIs associated with the upgraded Common Q platform, APP-GW-GLR-017 was revised to Revision 2 and this revision was included as part of the proposed changes described in the original submittal of LAR 15-017. The licensee concluded that the changes to incorporate APP-GW-GLR-017, Revision 2, in the UFSAR were unnecessary and inappropriate because: (1) Revision 0 was the version of this document that closed a Combined License Information Item (COLII) and should have been retained as a historical reference to the statement in UFSAR subsection 7.1.6.2; and (2) APP-GW-GLR-017 is not incorporated by reference into the UFSAR, so changes to this document do not require incorporation into the UFSAR. To resolve this discrepancy, the licensee proposed changes to the original LAR 15-017 text to properly identify Revision 0 as the historical reference document that requested closure of the COLII in UFSAR Subsection 7.1.6.2 and 7.1.7. Additionally, the reference to Revision 0 was restored in UFSAR Table 1.6-1, Material Referenced. Finally, the LAR text that requested approval of Revision 2 as IBR information was revised to identify it as the location of information provided to support the review of the LAR. The new text in APP-GW-GLR-017, Revision 2, that captures the updated PSAIs and GOIs information is not incorporated by reference into the UFSAR.

Enclosure 5, "Resolution of Common Q NRC Items," of LAR 15-017

In the Record of Changes for Revision 2 of APP-GW-GLR-017, the licensee states that DCD markups were updated to reference Revisions 1 and 2 of APP-GW-GLR-017. However, staff discovered changes to Sections 7.1.2.3, 7.1.2.8, "Communication Functions," 7.1.6, "Combined License Information," 9A3.1.2.5.2, "Safe Shutdown Evaluation," and the newly added Subsection 9A.3.1.2.8.4, "Safe Shutdown Evaluation." These DCD markups were not discussed in Enclosure 1 of the letter. In RAI Question No. 1 of Enclosure 5 of the LAR, staff requested the licensee to describe the nature of the DCD markups. In its response to RAI Question No. 1 of Enclosure 5 of the LAR, dated August 19, 2016, the licensee stated the DCD markups in APP-GW-GLR-017 were provided during the design certification to facilitate NRC review prior to submittal of an amendment. This included the reference to APP-GWGLR-017 itself, listed in DCD Section 7.1.6. The DCD changes referenced above were part of the original design certification approval process and included in the approved AP1000 design. Lastly, the proposed amendment only revises APP-GW-GLR-017 to update PSAI 1, Table 3-1 and GOI 7.1, as described in the license amendment request. Because the revision number changed on APP-GW-GLR-017, the DCD markups within APP-GW-GLR-017 were also updated to change the revision number of APP-GW-GLR-017 itself. Based on staff's review of the licensee's response to RAI Question No. 1 of Enclosure 5 of the LAR, staff finds the licensee's response acceptable. Therefore, RAI Question No. 1 of Enclosure 5 of the LAR is resolved and closed.

4.0 STATE CONSULTATION

In accordance with the Commission's regulations 10 CFR 50.91(b)(2), the Georgia State official was notified of the proposed issuance of the amendment. The State official had no comments.

5.0 ENVIRONMENTAL CONSIDERATION

The amendment changes a requirement with respect to installation or use of a facility component located within the restricted area as defined in 10 CFR Part 20, "*Standards for Protection Against Radiation*." Staff has determined that the amendment involves no significant increase in the amounts, and no significant change in the types, of any effluents that may be released offsite, and that there is no significant increase in individual or cumulative occupational radiation exposure. The Commission has previously issued a proposed finding that the amendment involves no significant hazards consideration, and there has been no public comment on such finding (*Federal Register*, 81 FR 21602, dated April 12, 2016). Accordingly, the amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with issuing the amendment.

6.0 CONCLUSION

Staff has concluded, based on the considerations discussed above, that there is reasonable assurance that (1) the health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with the Commission's regulations, and the new PSAIs and GOIs specified by the WCAP-16096 SE and WCAP-16097 SE, and (3) the issuance of the amendment will not be inimical the common defense and security or the health and safety of the public. Therefore, staff concludes that the Tier 2*, and associated Tier 2 changes proposed in LAR 15-017, as supplemented, are acceptable.

7.0 REFERENCES

1. Vogtle Electric Generating Plant (VEGP) Updated Final Safety Analysis Report (UFSAR), Revision 4 and Tier 1, Revision 3, dated July 21, 2015 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML15194A443).

2. AP1000 Design Control Document, Revision 19, dated June 13, 2011 (ADAMS Accession No. ML11171A500).

3. U.S. Nuclear Regulatory Commission, “Final Safety Evaluation Report Related to the Combined Licenses for Vogtle Electric Generating Plant, Units 3 and 4,” Volume 1, NUREG-2124, dated September 30, 2012 (ADAMS Accession No. ML12271A045).

4. Letter from Brian H. Whitley, Southern Nuclear Operating Company to U.S. Nuclear Regulatory Commission, “Software Program Manual and Topical Report (LAR 15-017),” dated February 15, 2016 (ADAMS Accession No. ML16046A009).

5. WCAP-16096-P and 16096-NP, Revision 4, “Software Program Manual for Common Q Systems,” dated February 2013 (ADAMS Accession Nos. ML12205A053 and ML12205A052).

6. WCAP-16097-P and WCAP-16097-NP, Revision 3, “Common Qualified Platform Topical Report,” dated February 2013 (ADAMS Accession Nos. ML12207A512 and ML12207A510).

7. U.S. Nuclear Regulatory Commission, “Safety Evaluation for Westinghouse Topical Report WCAP-166096-P, Revision-4, Software Program Manual For Common Q Systems” TAC No. ME5159,” dated February 7, 2013 (ADAMS Accession Nos. ML13022A124 (Letter); ML13022A009 (SE)).

8. U.S. Nuclear Regulatory Commission, “Safety Evaluation by the Office of Nuclear Reactor Regulation Westinghouse Topical Report WCAP-16097-P, Revision 3, “Common Qualified Platform” TAC No. ME5159,” dated February 7, 2013 (ADAMS Accession Nos. ML13022A124 (Letter); ML13022A009 (SE)).

9. U.S. Nuclear Regulatory Commission, “Request for Additional Information on License Amendment Request: Update of Common Qualified Platform Software Program Manual and Topical Report,” dated July 13, 2016 (ADAMS Accession No. ML16190A263).

10. U.S. Nuclear Regulatory Commission, “Audit Report: Update of Common Qualified Platform Software Program Manual and Topical Report,” dated September 12, 2016 (ADAMS Accession No. ML16252A382).

11. Letter from Brian H. Whitley, Southern Nuclear Operating Company to U.S. Nuclear Regulatory Commission, "Supplement to Request For License Amendment: Update of Common Qualified (Common Q) Platform Software Program Manual and Topical Report (LAR 15-017S1)," dated August 19, 2016 (ADAMS Accession No. ML16232A576).

12. Letter from Brian H. Whitley, Southern Nuclear Operating Company to U.S. Nuclear Regulatory Commission, "Supplement to Request For License Amendment: Update of Common Qualified (Common Q) Platform Software Program Manual and Topical Report (LAR 15-017S2)," dated August 26, 2016 (ADAMS Accession No. ML16239A392).

13. Letter from Brian H. Whitley, Southern Nuclear Operating Company to U.S. Nuclear Regulatory Commission, "Supplement to Request For License Amendment: Update of Common Qualified (Common Q) Platform Software Program Manual and Topical Report (LAR 15-017S3)," dated September 13, 2016 (ADAMS Accession No. ML16257A604).

14. U.S. Nuclear Regulatory Commission, "Request for Additional Information on WEC-81, 'Common Q Platform Upgrade – PMS System'," dated October 11, 2016 (ADAMS Accession No. ML17081A477).

15. Letter from Brian H. Whitley, Southern Nuclear Operating Company to U.S. Nuclear Regulatory Commission, "Supplement to Request For License Amendment: Update of Common Qualified (Common Q) Platform Software Program Manual and Topical Report (LAR 15-017S4)," dated December 16, 2016 (ADAMS Accession No. ML16351A490).

16. Letter from Brian H. Whitley, Southern Nuclear Operating Company to U.S. Nuclear Regulatory Commission, "Supplement to Request For License Amendment: Update of Common Qualified (Common Q) Platform Software Program Manual and Topical Report (LAR 15-017S5)," dated March 17, 2017 (ADAMS Accession No. ML17076A410).

17. Letter from Michael J. Yox, Southern Nuclear Operating Company to U.S. Nuclear Regulatory Commission, "Completion of ITAAC 2.5.02.13 [Index Number 552]," dated April 15, 2016 (ADAMS Accession No. ML15106A433).

18. U.S. Nuclear Regulatory Commission, "Virgil C. Summer Nuclear Station, Units 2 and 3 – NRC Integrated Inspection Reports 05200027/2015001, 05200028/2015001," dated April 30, 2016 (ADAMS Accession No. ML15120A400).

19. WCAP-16675-P and 16675-NP, Revision 5, "AP1000™ Protection and Safety Monitoring System Architecture Technical Report," dated November 30, 2010 (ADAMS Accession No. ML103370213).

20. U.S. Nuclear Regulatory Commission, “FINAL REVISION Proposed (2) Clarifications for LAR 15-017 & LAR 13-35 (WEC52) for Vogtle 3&4 and Summer 2&3,” dated January 13, 2017 (ADAMS Accession No. ML17014A000).

21. U.S. Nuclear Regulatory Commission, “Summary of January 19, 2017, Public Meeting With Southern Nuclear Operating Company and South Carolina Electric and Gas,” dated March 22, 2017 (ADAMS Accession No. ML17046A428).

22. VEGP UFSAR, Revision 4, Chapter 15, “Accident Analyses,” dated July 21, 2015 (ADAMS Accession No. ML15194A470).

23. VEGP UFSAR, Revision 4, Chapter 6, “Engineered Safety Features,” dated July 21, 2015 (ADAMS Accession No. ML15194A462).

24. VEGP UFSAR, Revision 4, Chapter 19, “Probabilistic Risk Assessment,” dated July 21, 2015 (ADAMS Accession No. ML15194A474).

25. U.S. Nuclear Regulatory Commission, “Summary of September 15, 2016, Public Meeting With Southern Nuclear Operating Company and South Carolina Electric and Gas,” dated October 24, 2016 (ADAMS Accession No. ML16287A480).

26. U.S. Nuclear Regulatory Commission, “License Amendment No. 52 For Vogtle Units 3 and 4, Core Reference Report (LAR 16-001),” dated August 19, 2016 (ADAMS Accession No. ML16201A435).

27. WCAP-17524-P and WCAP-17524-NP, Revision 1, “Westinghouse Electric Co. - Transmittal of WCAP-17524-P-A, Revision 1 and WCAP-17524-NP-A, Revision 1, "AP1000 Core Reference Report," (Proprietary/Non-Proprietary), dated July 8, 2015 (ADAMS Accession No. ML15180A187).

28. U.S. Nuclear Regulatory Commission, “Safety Evaluation That Supports License Amendment No. 52 For Vogtle Units 3 and 4, Core Reference Report (LAR 16-001),” dated August 19, 2016 (ADAMS Accession No. ML16201A440).

29. VEGP UFSAR, Revision 4, Chapter 17, “Instrumentation and Controls,” dated July 21, 2015 (ADAMS Accession No. ML15194A463).

30. APP-GW-GL-011, “AP1000 Identification of Critical Human Actions and Risk Important Tasks,” dated April 21, 2006 (ADAMS Accession No. ML061030102).