B. H. Whitley
Director
Regulatory Affairs

Southern Nuclear
Operating Company, Inc.
42 Inverness Center Parkway
Birmingham, AL 35242

Tel 205.992.7079
Fax 205.992.5296

February 15, 2016

Docket Nos.: 52-025
52-026

ND-16-0083
10 CFR 50.90

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, DC 20555-0001

Southern Nuclear Operating Company
Vogtle Electric Generating Plant Units 3 and 4
Request for License Amendment:
Update of Common Qualified (Common Q) Platform
Software Program Manual and Topical Report (LAR-15-017)

Ladies and Gentlemen:

Pursuant to 10 CFR 52.98(c) and in accordance with 10 CFR 50.90, Southern Nuclear Operating Company (SNC), the licensee for Vogtle Electric Generating Plant (VEGP) Units 3 and 4, requests an amendment to Combined License (COL) Numbers NPF-91 and NPF-92, for VEGP Units 3 and 4, respectively. The requested amendment requires changes to the Updated Final Safety Analysis Report (UFSAR) in the form of departures from the incorporated plant-specific Design Control Document (PS-DCD) Tier 2 information and involves related changes to the associated plant-specific Tier 2* information.

The proposed departures consist of changes to 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," and WCAP-16097, "Common Qualified Platform Topical Report." The current licensing basis references WCAP-16096, Revision 01A and WCAP-16097, Revision 0, which have been superseded by later NRC-approved versions. 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. This license amendment request (LAR) requests approval of the new and revised Tier 2 and Tier 2* UFSAR text to support the following changes:

- Incorporate by reference the Nuclear Regulatory Commission (NRC)-approved versions of the Tier 2* WCAP-16096, Revision 4, "Software Program Manual for Common Q™ Systems" (also referred to as the Common Q SPM) and WCAP-16097, Revision 3, "Common Qualified Platform Topical Report" (also referred to as the Common Q Topical Report) 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 Software Program Manual (SPM) and Topical Report (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
- Incorporate by reference an updated version of Tier 2 APP-GW-GLR-017, "Resolution of Common Q NRC Items," which revises previous plant-specific action item responses that involve the update to WCAP-16097.
- 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 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 provides the description, technical evaluation, regulatory evaluation (including the Significant Hazards Consideration determination), and environmental considerations for the proposed changes in the License Amendment Request (LAR).

Enclosure 2 provides the disposition of the Plant-Specific Action Items and a Generic Open Item for WCAP-16096, Revision 4 and WCAP-16097, Revision 3.

Enclosure 3 provides the Common Q SPM and TR alternatives and the associated justifications for these alternatives.

Enclosure 4 identifies the requested changes and provides markups depicting the requested changes to the UFSAR text, tables, and figures.

Enclosure 5 provides APP-GW-GLR-017, "Resolution of Common Q NRC Items," Revision 2.

Enclosure 6 provides WCAP-15927, "Design Process for AP1000 Common Q Safety Systems," Revision 4.

This letter contains no regulatory commitments.

SNC requests staff approval of this license amendment by February 15, 2017, to support installation of the PMS cabinets. Delayed approval of this licensing request could result in delay of the associated construction activity and subsequent dependent construction activities. SNC expects to implement the proposed amendment (through incorporation into the licensing basis documents; e.g., the UFSAR) within 30 days of the approval of the requested changes.

In accordance with 10 CFR 50.91, SNC is notifying the State of Georgia of this LAR by transmitting a copy of this letter and enclosures to the designated State Official.

Should you have any questions, please contact Mr. Christopher L. Whitfield at (205) 992-5071.

Mr. Brian H. Whitley states that: he is the Regulatory Affairs Director of Southern Nuclear Operating Company; he is authorized to execute this oath on behalf of Southern Nuclear Operating Company; and to the best of his knowledge and belief, the facts set forth in this letter are true.

Respectfully submitted,

SOUTHERN NUCLEAR OPERATING COMPANY

Brian H. Whitley

BHW/CLW/ljs

Sworn to and subscribed before me this 15th *day of* February, 2016

Notary Public: Lisa Myrick Spears

My commission expires: June 18, 2019

Enclosures:
1) Request for License Amendment: Update of Common Q Platform Software Program Manual and Topical Report (LAR-15-017)
2) Plant-Specific Action Item and Generic Open Item Dispositions for WCAP-16096, Revision 4 and WCAP-16097, Revision 3 (LAR-15-017)
3) Common Q Software Program Manual (SPM) and Topical Report Alternatives and Justification (LAR-15-017)
4) Proposed Changes to the Licensing Basis Documents (LAR-15-017)
5) APP-GW-GLR-017, Revision 2, Resolution of Common Q NRC Items (LAR-15-017)
6) WCAP-15927, Revision 4, Design Process for AP1000 Common Q Safety Systems (LAR-15-017)

cc:
Southern Nuclear Operating Company / Georgia Power Company
Mr. S. E. Kuczynski (w/o enclosures)
Mr. M. D. Rauckhorst
Mr. D. G. Bost (w/o enclosures)
Mr. M. D. Meier (w/o enclosures)
Mr. J. T. Gasser (w/o enclosures)
Mr. D. H. Jones (w/o enclosures)
Ms. K. D. Fili (w/o enclosures)
Mr. D. L. McKinney (w/o enclosures)
Mr. T.W. Yelverton (w/o enclosures)
Mr. B. H. Whitley
Mr. C. R. Pierce
Mr. D. L. Fulton
Mr. M. J. Yox
Mr. J. C. Haswell
Mr. T. R. Takats
Mr. W. A. Sparkman
Mr. J. P. Redd
Ms. K. A. Roberts
Document Services RTYPE: VND.LI.L00
File AR.01.02.06

Nuclear Regulatory Commission
Ms. C. Haney (w/o enclosures)
Mr. M. Delligatti (w/o enclosures)
Mr. L. Burkhart (w/o enclosures)
Mr. J. McKirgan (w/o enclosures)
Mr. P. Kallan
Mr. C. Patel
Mr. W. C. Gleaves
Mr. B. M. Bavol
Ms. R. Reyes
Ms. M. A. Sutton
Mr. M. E. Ernstes
Mr. G. Khouri
Mr. L. M. Cain
Mr. J. D. Fuller
Mr. C. B. Abbott
Ms. S. Temple
Mr. I. A. Anchondo
Ms. J. Uhle

State of Georgia
Mr. J. H. Turner

Oglethorpe Power Corporation
Mr. M. W. Price
Mr. K. T. Haynes
Ms. A. Whaley

Municipal Electric Authority of Georgia
Mr. J. E. Fuller
Mr. S. M. Jackson

Dalton Utilities
Mr. T. Bundros

WECTEC
Ms. K. Stoner (w/o enclosures)
Mr. C. A. Castell

Westinghouse Electric Company, LLC
Mr. R. Easterling (w/o enclosures)
Mr. J. W. Crenshaw (w/o enclosures)
Mr. C. D. Churchman (w/o enclosures)
Mr. L. Woodcock
Mr. P. A. Russ
Mr. G. F. Couture
Mr. M. Y. Shaqqo

Other
Mr. J. E. Hesler, Bechtel Power Corporation
Ms. L. A. Matis, Tetra Tech NUS, Inc.
Dr. W. R. Jacobs, Jr., Ph.D., GDS Associates, Inc.
Mr. S. Roetger, Georgia Public Service Commission
Ms. S. W. Kernizan, Georgia Public Service Commission
Mr. K. C. Greene, Troutman Sanders
Mr. S. Blanton, Balch Bingham
Mr. R. Grumbir, APOG
Mr. J. R. Bouknight, South Carolina Electric & Gas Company
Mr. D. Kersey, South Carolina Electric & Gas Company
Mr. B. Kitchen, Duke Energy
Mr. S. Franzone, Florida Power & Light

Southern Nuclear Operating Company

ND-16-0083

Enclosure 1

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

Request for License Amendment:

Update of Common Q Platform Software Program Manual and Topical Report

(LAR-15-017)

(Enclosure 1 consists of 28 pages, including this cover page)

Table of Contents

1. SUMMARY DESCRIPTION
2. DETAILED DESCRIPTION AND TECHNICAL EVALUATION
3. TECHNICAL EVALUATION (Incorporated into Section 2)
4. REGULATORY EVALUATION
    - 4.1. Applicable Regulatory Requirements/Criteria
    - 4.2. Precedent
    - 4.3. Significant Hazards Consideration Determination
    - 4.4. Conclusions
5. ENVIRONMENTAL CONSIDERATIONS
6. REFERENCES

Pursuant to 10 CFR 52.98(c) and in accordance with 10 CFR 50.90, Southern Nuclear Operating Company (SNC, or the "Licensee") hereby requests an amendment to Combined License (COL) Nos. NPF-91 and NPF-92 for Vogtle Electric Generating Plant (VEGP) Units 3 and 4, respectively.

1. SUMMARY DESCRIPTION

The requested amendment involves changes to the Common Qualified (Common Q™) platform and the development processes for the AP1000 protection and safety monitoring system (PMS) hardware and software arising from the proposed incorporation of the following three incorporated by reference (IBR) Tier 2* documents into the Updated Final Safety Analysis Report (UFSAR).

- WCAP-16096, "Software Program Manual for Common Q™ Systems"
- WCAP-16097, "Common Qualified Platform Topical Report"
- WCAP-15927, "Design Process for AP1000 Common Q Safety Systems"

These three documents describe the hardware and software development process for the Common Q platform. They also discuss the process for system-level design, software design and implementation, and hardware design and implementation for the AP1000 PMS development. This license amendment request (LAR) requests approval of the following:

- Incorporate by reference the Nuclear Regulatory Commission (NRC)-approved versions of the Tier 2* WCAP-16096, Revision 4, "Software Program Manual for Common Q™ Systems," and WCAP-16097, Revision 3, "Common Qualified Platform Topical Report," 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 Software Program Manual (SPM) and Topical Report (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.
- Incorporate by reference an updated revision of Tier 2 APP-GW-GLR-017, "Resolution of Common Q NRC Items," which revises previous plant-specific action item and generic open item responses that involve the update to WCAP-16097. APP-GW-GLR-017, Revision 2, is provided as Enclosure 5 of this letter.
- Incorporate by reference an updated revision of Tier 2* WCAP-15927, "Design Process for AP1000 Common Q Safety Systems," into the UFSAR. WCAP-15927, Revision 4, is provided as Enclosure 6 of this letter.

- Remove Tier 2* WCAP-17201-P, "AC160 High Speed Link Communication Compliance to DI&C-ISG-04 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.

2. DETAILED DESCRIPTION AND TECHNICAL EVALUATION

Overview

The AP1000 PMS is based on the Common Q platform, as currently documented in the NRC-approved WCAP-16096, Revision 01A and WCAP-16097, Revision 0. Both WCAP-16096 and WCAP-16097 have been subsequently revised and approved by the NRC. This amendment request proposes to incorporate the newer versions of these WCAPs into the licensing basis.

The Common Q platform uses a set of qualified building blocks that can be used for various safety system applications. The building blocks include Advant Controller (AC160), flat panel display system, power supplies, and communication subsystems. The Common Q-based PMS is designed to provide protection from unsafe reactor operation during steady-state and transient power operations. The PMS also initiates selected protective functions to mitigate the consequences of design-basis events and accidents to safely shutdown the plant automatically or by manual actions.

The Detailed Description and Technical Evaluation are presented in the following LAR subsections:

- Subsection 2.1, "Impacted Documents"

  This subsection gives a description of WCAP-16096, WCAP-16097, WCAP-15927, WCAP-17201, and UFSAR Appendix 7A and the proposed impacts.

- Subsection 2.2, "Changes to Regulatory Guide Conformance"

  This subsection discusses the proposed changes to UFSAR Appendix 1A. The changes establish the Common Q SPM and/or TR as the licensing basis for the development of the Common Q portion of PMS in lieu of the applicable digital I&C Regulatory Guides.

- Subsection 2.3, “Disposition of Plant Specific Action Items (PSAIs) and a Generic Open Item (GOI)”

  This subsection provides a disposition for the new plant specific action items and generic open item listed in the Safety Evaluations (SEs) for WCAP-16096-P-A, Revision 4 and WCAP-16097-P-A, Revision 3.

- Subsection 2.4, “Common Q SPM and TR Alternatives”

  This subsection describes the alternatives used instead of select methods described in the Common Q SPM, pursuant to the provisions provided in the SE for WCAP-16096.

- Subsection 2.5, “Proposed Changes to the Licensing Basis”

  This subsection summarizes proposed licensing basis changes.

- Subsection 2.6, “Summary of Proposed Changes”

  This subsection summarizes the proposed changes.

2.1 Impacted Documents

The requested amendment provides updates to the following UFSAR Tier 2* reference documents:

- Change WCAP-16096-NP-A, "Software Program Manual for Common Q™ Systems,” from Revision 01A to Revision 4.

- Add WCAP-16096-P-A, “Software Program Manual for Common Q™ Systems,” Revision 4.

- Change WCAP-16097-P-A, “Common Qualified Platform Topical Report,” from Revision 0 to Revision 3.

- Change WCAP-16097-NP-A, “Common Qualified Platform Topical Report,” from Revision 0 to Revision 3.

- Change WCAP-15927, “Design Process for Common Q Safety Systems,” from Revision 2 to Revision 4.

2.1.1 WCAP-16096, “Software Program Manual for Common Q™ Systems,” and WCAP-16097, “Common Qualified Platform Topical Report”

WCAP-16096-P-A and WCAP-16096-NP-A, Revision 4 and WCAP-16097-P-A and WCAP-16097-NP-A, Revision 3 were approved by the NRC in SEs dated February 7, 2013 (see ADAMS Accession Nos.: ML13022A124 (Letter); ML13022A009 (16096 SE); ML13022A011 (16097 SE)). A summary of the NRC-approved changes is provided for information below.

WCAP-16096, "Software Program Manual for Common Q™ Systems"

Description of Change

The Licensee proposes to incorporate the proprietary and non-proprietary versions of WCAP-16096, Revision 4 into the licensing basis.

This WCAP was updated to reference more current NRC guidance and supporting industry standards to be used for the development of a safety-related system application, and to incorporate the updated Westinghouse processes. The key updates to the Common Q Software Program Manual include:

- The responsibility for the performance of system testing was changed from the design team to an independent team.

– The roles and responsibilities for producing the Requirements Traceability Matrix (RTM) were clarified.

– A Test Plan, Computer Security Plan, and Installation Plan were added.

Based on the NRC's approval of WCAP-16096, Revision 4, as described below, the Licensee proposes to incorporate portions of this WCAP revision into the licensing basis. The Licensee proposes to exclude WCAP-16096, Section 12, "Secure Development and Operational Environment Plan," from being incorporated by reference into the UFSAR. 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, 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.

UFSAR Chapter 7 is updated to clarify that only the Common Q portion of PMS is developed using the Common Q SPM. 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 (CIM).

Technical Evaluation

The NRC reviewed the Common Q software development process for application software and issued an SE for WCAP-16096. In the NRC's SE, the staff concluded that the Common Q application development procedures continue to provide a quality software lifecycle process and these plans continue to commit to documentation of life cycle activities permitting the NRC or others to evaluate the quality of the design features upon which the safety determination will be based. The NRC staff concluded that the SPM, as applied to the Common Q safety systems, continues to meet the guidance of Regulatory Guide (RG) 1.152 (which endorses IEEE 7-4.3.2) and special characteristics of computer systems are adequately addressed. The NRC staff review also concluded that the Common Q safety software development processes continue to be capable of producing software that is able to satisfy the design requirements of General Design Criteria (GDC) 1 and 21.

The AP1000 PMS Computer Security Plan is specific for AP1000. It 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 and is consistent with the Common Q SPM incorporated by reference information.

Developing the AP1000 PMS using the updated Common Q SPM aligns the AP1000 PMS design and development processes with the more current regulatory guides and industry standards.

WCAP-16097, "Common Qualified Platform Topical Report"

Description of Change

The Licensee proposes to incorporate 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. The key updates to the Common Q Topical Report include:

– A technical description of the Common Q modules (i.e., AI687/AI688) used in the AP1000 PMS. This aligns with descriptions already included in WCAP-16675, "AP1000 Protection and Safety Monitoring System Architecture Technical Report" (Tier 2, incorporated by reference).

– A technical description of the flash capabilities for processor module PM646A.

– The process for Commercial Dedication is updated to align with work performed on the AP1000 project.

– Added compliance section for Digital Instrumentation and Controls (DI&C) Interim Staff Guidance (ISG) guidance document, DI&C ISG-4.

Technical Evaluation

Per the NRC's SE for WCAP-16097 the staff concluded that, for the systems and components reviewed, the updated Common Q platform meets the requirements of 10 CFR Part 50, Appendix A, General Design Criteria 1, 2, 4, 12, 13, 19, 20, 21, 22, 23, 24, and 25, and the Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991 for the design of safety-related reactor protection systems, engineered safety features systems, and other plant systems, and the guidelines of Regulatory Guide 1.152 and supporting industry standards for the design of digital systems and, therefore, the Common Q platform is acceptable.

The AP1000 PMS is developed in accordance with the updated Common Q Topical Report; therefore the PMS continues to fulfill the safety functions described in UFSAR Chapter 7.

2.1.2. WCAP-15927, "Design Process for Common Q Safety Systems"

Description of Change

The Licensee proposes to update WCAP-15927 from Revision 2 to Revision 4 to address the following:

- Reference the NRC-approved WCAP-16096-P-A, Revision 4 and WCAP-16097-P-A, Revision 3
- Identify alternatives to the Common Q SPM and TR defined processes (see section 2.4 of this license amendment request for specific alternatives and justifications)
- Remove the reference to the specific tool (i.e., Document Index) used to document the technical baseline
- Incorporate editorial/administrative changes (i.e., updating trademarks, fixing typographical errors, and adding the AP1000 standard acronym document as a reference). See Section 2.5 for a summary of these editorial/administrative changes.

Technical Evaluation

The editorial/administrative changes have no impact on the process requirements of WCAP-15927 and do not reduce any licensing commitments.

Removal of the reference to the specific tool (i.e., Document Index) for documenting the technical baseline allows the AP1000 vendor the flexibility to change tools without impacting the licensing basis. This change does not impact any process requirements nor does it reduce any licensing commitments. The text continues to require the establishment of a documented technical baseline.

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

Description of Change

WCAP-17201-P, "AC160 High Speed Link Communication Compliance to DI&C-ISG-04 Staff Positions 9, 12, 13 and 15 Technical Report" is a Tier 2* IBR document in the UFSAR. The purpose of WCAP-17201-P was to augment the information in the WCAP-16097-P-A, Revision 0 to support the NRC staff's conclusion regarding the satisfaction of DI&C-ISG-04 Staff Positions 9, 12, 13, and 15. The Licensee proposes to delete this WCAP from the licensing basis.

Technical Evaluation

Because WCAP-16097-P-A, Revision 3 addresses Positions 9, 12, 13, and 15 from DI&C ISG-4, WCAP-17201-P is no longer required. Retaining both WCAPs would put duplicate information in the licensing basis.

2.1.4. UFSAR Appendix 7A, "Instrumentation and Controls Licensing Basis Document Changes"

Appendix 7A, "Instrumentation and Controls Licensing Basis Document Changes" was previously added to UFSAR Chapter 7 in a license amendment that modified information related to certain UFSAR incorporated by reference documents. This license amendment request proposes to revise Appendix 7A to modify information affected by adopting the latest NRC-approved versions of the Common Q SPM and TR. The following Tier 2 incorporated by reference documents are proposed to be revised in UFSAR Appendix 7A: WCAP-15775 (Revision 4), WCAP-17184 (Revision 2), WCAP-16438 (Revision 3), WCAP-15776 (Revision 0), WCAP-16592 (Revision 2), WCAP-16674 (Revision 4), and WCAP-16675 (Revision 5).

2.1.4.1. WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report"

Description of Change

WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," Section 3.3 discusses the design, verification, and validation process for I&C systems. This section is updated, as follows: [plant-specific] Design Control Document (DCD) [(i.e., UFSAR)] Section 7.1.2.14 is referenced as the location in which the design, verification, and validation process for the AP1000 instrumentation and control systems is described. This reference replaces WCAP-13383, "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report" and CE-CES-195,"Software Program Manual for Common Q Systems."

WCAP-15775, Section 4.2 discusses human diversity as it relates to instrumentation and control systems in the AP1000 plant. This section is updated to reference WCAP-16096-P-A and WCAP-15927 as the documents in which the design, verification, and validation programs for the Common Q portion of the PMS are described. These references replace WCAP-13383 and CE-CES-195.

The reference section of WCAP-15775 is updated by replacing WCAP-13383 and CE-CES-195 with WCAP-16096-P-A, Revision 4 and WCAP-15927, Revision 4.

Technical Evaluation

Referencing [plant-specific] DCD Section 7.1.2.14, WCAP-16096-P-A, Revision 4, and WCAP-15927, Revision 4 instead of CE-CES-195 and WCAP-13383 is consistent with the change and technical evaluation in Section 2.1.1 above. Both this UFSAR section and WCAP-16096-P-A, and WCAP-15927 describe the design, verification, and validation process for the AP1000 PMS and already include the appropriate references.

2.1.4.2. WCAP-17184, "AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report"

Description of Change

The Reference section of WCAP-17184 is updated to reference WCAP-15927, Revision 4.

Technical Evaluation

Referencing WCAP-15927, Revision 4 (alternate document number APP-GW-J1R-001) is consistent with the proposed change and technical evaluation in Section 2.1.2 above.

2.1.4.3. WCAP-16438, "FMEA of AP1000 Protection and Safety Monitoring System"

Description of Change

WCAP-16096 is moved from the Reference section to the Bibliography section of WCAP-16438. The proprietary version of WCAP-16438 is referenced instead of the non-proprietary version.

Technical Evaluation

Referencing the NRC-approved WCAP-16096-P-A is consistent with the change and technical evaluation in Section 2.1.1 above.

The Bibliography section of WCAP-16438 provides citation of additional sources that were considered in preparation of this document or incidentally cited in its text. The Reference section lists design inputs that were considered in preparation of the document. Moving WCAP-16096 to the Bibliography section of WCAP-16438 is consistent with this approach.

2.1.4.4. WCAP-15776, "Safety Criteria for the AP1000 Instrumentation and Control Systems"

Description of Change

The following changes are made to WCAP-15776:

- NRC-approved WCAP-16096-P-A, Revision 4 replaces WCAP-13383, "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report," and CE-CES-195,"Software Program Manual for Common Q Systems," in WCAP-15776 Sections 2.8, 3.4, and 7.
- The life cycle stages in WCAP-15776, Section 3.4 are updated to be consistent with WCAP-16096, Revision 4.
- WCAP-16097-P-A, Revision 3 replaces references to WCAP-13383 and CENPD-396-P in WCAP-15776 Sections 3.4 and 7.

Technical Evaluation

NRC-approved WCAP-16096-P-A, Revision 4 and WCAP-16097-P-A, Revision 3 supersede WCAP-13383, CE-CES-195, and CENPD-396-P. Referencing WCAP-16096-P-A, Revision 4 and WCAP-16097-P-A, Revision 3 instead of WCAP-13383, CE-CES-195, and CENPD-396-P and aligning the life cycle stages in WCAP-15776 with those in WCAP-16096 is consistent with the proposed change and technical evaluation in Section 2.1.1 above.

2.1.4.5. WCAP-16592, "Software Hazard Analysis of AP1000™ Protection and Safety Monitoring System"

Description of Change

The Reference section and Section 1.2, "Scope," of WCAP-16592 are updated to replace the current Common Q SPM with NRC-approved WCAP-16096-P-A, Revision 4.

Technical Evaluation

Referencing NRC-approved WCAP-16096-P-A, Revision 4 is consistent with the proposed change and technical evaluation in Section 2.1.1 above.

2.1.4.6. WCAP-16674, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components"

Description of Change

The Reference section of WCAP-16674 is updated to reference NRC-approved WCAP-16096-P-A, Revision 4 and WCAP-16097-P-A, Revision 3.

Various sections are updated to change the reference of IEEE 7-4.3.2 from the 1993 version to the 2003 version.

Technical Evaluation

Referencing NRC-approved WCAP-16096-P-A, Revision 4 and WCAP-16097-P-A, Revision 3 and IEEE 7-4.3.2-2003 is consistent with the change and technical evaluation in Section 2.1.1 above. The AP1000 I&C design, as described in WCAP-16674, is consistent with IEEE 7-4.3.2-2003.

2.1.4.7. WCAP-16675, "AP1000™ Protection and Safety Monitoring System Architecture Technical Report"

Description of Change

The Reference section of WCAP-16675 is updated to reference NRC-approved WCAP-16096-P-A, Revision 4 and WCAP-16097-P-A, Revision 3. Various sections are updated to change the reference of IEEE 7-4.3.2 from the 1993 version to the 2003 version.

Technical Evaluation

Referencing NRC-approved WCAP-16096-P-A, Revision 4 and WCAP-16097-P-A, Revision 3 and IEEE 7-4.3.2-2003 is consistent with the change and technical evaluation in Section 2.1.1 above. The AP1000 I&C design, as described in WCAP-16675, is consistent with IEEE 7-4.3.2-2003.

2.2. Changes to Regulatory Guide Conformance

This subsection discusses the proposed changes to UFSAR Appendix 1A. The changes establish the Common Q SPM and/or TR as the licensing basis for the development of the Common Q portion of PMS in lieu of the applicable digital I&C Regulatory Guides.

Description of Change

An exception is taken to Regulatory Guides 1.152, 1.168, 1.169, 1.170, 1.172, and 1.173 as currently presented in UFSAR Appendix 1A. Updates are proposed to the Appendix 1A Clarification/Summary Description of Exception column to state that the Common Q portion of PMS was developed using the Common Q SPM, which was reviewed and approved by the NRC using the criteria of updated regulatory guides and industry standards.

Technical Evaluation

The Common Q portion of PMS meets the requirements of 10 CFR Part 50, Appendix A, General Design Criteria 1, 2, 4, 12, 13, 19, 20, 21, 22, 23, 24, and 25, and IEEE Standard 603-1991 for the design of safety-related reactor protection systems, engineered safety features systems, and other plant systems.

The Common Q application development process is a quality software life cycle process that requires documentation of life cycle activities. The Common Q safety software development processes are capable of producing software that is able to satisfy the design requirements of GDC 1 and 21. In addition, the Common Q SPM meets 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."

The NRC staff reviewed and approved the Common Q SPM and TR with the support of the updated regulatory guidance and determined that they are an acceptable approach to meet the underlying regulatory requirements described above.

Therefore, the Common Q SPM and TR are considered an acceptable approach to meet the applicable underlying regulatory requirements for the AP1000 PMS.

2.3. Disposition of Plant Specific Action Items (PSAIs) and a Generic Open Item (GOI)

Enclosure 2 discusses the new PSAIs and a Generic Open Item contained within 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 technical evaluation and proposed UFSAR changes, as applicable, due to select PSAIs are also provided in Enclosure 2.

2.4. Common Q SPM and TR Alternatives

Description of Change

The Common Q portion of PMS is developed in accordance with WCAP-16096, Revision 4 and WCAP-16097, Revision 3. PSAI 1 in the NRC 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. Accordingly, alternatives and justifications for the AP1000 PMS are documented in WNA-PD-00042-WAPP, "AP1000 Protection and Safety Monitoring System Software Development Plan." The Common Q SPM alternatives are also documented in the SPM companion document, WCAP-15927, to support their classification as Tier 2* material. In addition, an alternative to WCAP-16097, Revision 3 is documented in WCAP-15927.

Technical Evaluation

The alternatives and justifications are documented in Enclosure 3 of this license amendment request. The alternatives to the SPM-defined processes continue to meet the regulatory requirements as described in Section 2.2 above.

2.5. Proposed Changes to the Licensing Basis

The UFSAR text provided as the baseline for the markups described below and provided in Enclosure 4 includes changes that were recently incorporated into the VEGP Units 3 and 4 UFSAR based on a plant-specific departure from DCD Tier 2 information. The changes made by the internally generated departure were evaluated in accordance with the change process in 10 CFR Part 52, Appendix D, Section VIII, paragraph B.5.a, and determined not to require NRC approval prior to implementation.

Note that the complete summary of changes for WCAP-16096, Revision 4 and WCAP-16097, Revision 3 are included in the Revision History/Record of Changes in each document.

Proposed UFSAR Tier 2/Tier 2* Chapter 1, Table 1.6-1, "Material Referenced" Changes

1. The proprietary version of WCAP-16096 Revision 4 is added, and the revision number of the non-proprietary version of WCAP-16096 is updated from Revision 01A to Revision 4. A note is added to exclude Section 12 of WCAP-16096 from being incorporated by reference. A parenthetical is added to reference WCAP-15927 for SPM alternatives.

2. WCAP-16097 is updated from Revision 01 to Revision 3 and the title is corrected. (Note that Table 1.6-1 incorrectly refers to the May 2003 version of the Topical Report as Revision 01 instead of Revision 0.) A parenthetical is added to reference WCAP-15927 for Topical Report alternatives.

3. WCAP-15927 is updated from Revision 2 to Revision 4.

4. WCAP-17201 is deleted.

5. A note is added after the following document titles to identify that modifications are provided in UFSAR Appendix 7A: WCAP-16674, WCAP-16675, and WCAP-16592.

6. APP-GW-GLR-017 is updated to identify Revision 2 as the licensing basis revision.

Proposed UFSAR Tier 2/Tier 2* Section 1.9, "Compliance with Regulatory Criteria" Changes

1. The title of Regulatory Guide 1.152, Revision 1 is corrected, and the cross-references are changed to refer to Chapter 7, rather than the individual plant-specific DCD sections, in Table 1.9-1, "Regulatory Guide/Section Cross-Reference."

2. Regulatory Guide 1.152, Revision 3 is added to Table 1.9-1, with a cross-reference to Chapter 7.

Proposed UFSAR Appendix 1A, "Conformance with Regulatory Guides" Changes

1. The title of Regulatory Guide 1.152, Revision 1 is corrected, and Revision 2 is deleted from the revised title line for Revision 1.
2. An "exception" is identified for the Regulatory Guides 1.152, 1.168, 1.169, 1.170, 1.172, and 1.173. A statement is made in the "Clarification/Summary Description of Exceptions" column for each Regulatory Guide indicating that the Common Q portion of the protection and safety monitoring system is developed using the Common Q SPM and/or TR.

Proposed UFSAR Tier 2/Tier 2* Chapter 7 Changes (excluding changes due to plant-specific action items)

1. Section 7.1, “Introduction,” is revised to remove the reference to WCAP-17201 (i.e., Reference 2).

2. Section 7.1.2.14, “Verification and Validation,” is revised to:

   - Replace the original citation to the non-proprietary version of the SPM with a citation to the proprietary version of the SPM.

   - Clarify that WCAP-16096-P-A describes the V&V program for Common Q portion of the protection and safety monitoring system.

3. Section 7.1.2.14.1, “Design Process” is revised to:

   - Replace the original citation of the SPM with the proprietary version.

   - Clarify that the Common Q portion of PMS was developed in accordance with WCAP-16096-P-A.

   - Clarify that the Common Q SPM provides the design process used for the Common Q portion of the PMS for compliance to the specific regulatory guides.

4. Section 7.1.2.14.3, “Operational Process,” is added to describe the software operations plan and the administrative controls contained within it.

5. Section 7.1.7, “References” is revised to:

   - Delete (i.e., change to “Not used.”) WCAP-17201 (Reference 2).

   - Update the revision level of WCAP-16097 (Reference 8) from Revision 0 to Revision 3, add parenthetical referring to WCAP-15927 for alternatives to WCAP-16097, and correct the document title.

   - Add the proprietary version of WCAP-16096, Revision 4, update the revision level of WCAP-16096 (Reference 9) from Revision 01A to Revision 4, and add parenthetical referring to WCAP-15927 for alternatives to WCAP-16096.

   - Identify Revision 2 as the licensing basis revision of APP-GW-GLR-017 (Reference 18).

   - Add a note to WCAP-16675 (Reference 19) to identify that modifications are provided in UFSAR Appendix 7A.

   - Update revision level of WCAP-15927 (Reference 20) from Revision 2 to Revision 4.

- Add a note to WCAP-16674 (Reference 25) to identify that modifications are provided in UFSAR Appendix 7A.

6. UFSAR Figure 7.1-2 is updated to replace the original citation to the non-proprietary version of the SPM with a citation to the proprietary version of the SPM.

7. Section 7.2.4, "References" is revised to add a note to WCAP-16592 (Reference 4) to identify that modifications are provided in UFSAR Appendix 7A.

Proposed UFSAR Tier 2 Changes Due to WCAP-16096 and WCAP-16097 SE Plant-Specific Action Items and a Generic Open Item

1. WCAP-16097 PSAI 6.1 and GOI 7.1: APP-GW-GLR-017 (Tier 2, IBR), Table 3-1 is revised to reflect the S600 I/0 modules (AI687 and AI688) already existing in the certified design via WCAP-16675, "AP1000™ Protection and Safety Monitoring System Architecture Technical Report." The introduction section and GOI resolution are updated to align with the revised PSAI 6.1 response. Accordingly, UFSAR Table 1.6-1 and UFSAR Section 7.1.7 are updated to reflect the new revision of APP-GW-GLR-017.

2. WCAP-16097 PSAI 6.18: Tier 2 UFSAR Subsection 7.1.2.14.3, "Operational Process," is proposed to be added. This subsection requires that the PMS and its division room are in the appropriate configuration prior to making setpoint changes.

3. WCAP-16096 PSAI 4: Section 7.1.2.14.3, "Operational Process," is proposed to be added to the UFSAR as Tier 2 text. This section requires the development of a software operations plan.

Proposed UFSAR Appendix 7A Changes

1. Revise Section 7A.1 for WCAP-15775 to reference [plant-specific] DCD Subsection 7.1.2.14, WCAP-16096-P-A and WCAP-15927, and to delete the references to WCAP-13383 and CE-CES-195.

2. Revise Section 7A.3 for WCAP-17184 to reference APP-GW-J1R-001 (alternate document number for WCAP-15927), Revision 4.

3. Revise Section 7A.4 for WCAP-16438 to reference to WCAP-16096-P-A, Revision 4 and move this reference from the Reference section to the Bibliography section.

4. Revise Section 7A.5 for WCAP-15776 to reference WCAP-16096-P-A, Revision 4 and WCAP-16097-P-A, Revision 3, delete the references to WCAP-13383 and CE-CES-195, and to update the Common Q life cycle phases to be consistent with WCAP-16096, Revision 4.

5. Add new Section 7A.6 for WCAP-16592 to reference WCAP-16096-P-A, Revision 4.

6. Add new Section 7A.7 for WCAP-16674 to reference WCAP-16096-P-A, Revision 4, WCAP-16097-P-A, Revision 3, and IEEE 7-4.3.2-2003.

7. Add new Section 7A.8 for WCAP-16675 to reference WCAP-16096-P-A, Revision 4, WCAP-16097-P-A, Revision 3, and IEEE 7-4.3.2-2003.

Proposed UFSAR Table 19.59-18 Changes

1. The “Insight” column is revised to specify Revision 1 of Regulatory Guide 1.152 and account for the Common Q portion of PMS and its adherence to the SPM and TR.

2. The “Disposition” column is revised to clarify the pointer to the UFSAR Appendix 1A compliance statement.

Proposed WCAP-15927 Changes

1. Section 1, “Introduction and Scope” is changed to cite the latest NRC-approved proprietary version of the SPM and to make editorial changes to correct the trademarks for Common Q and AP1000.

2. Section 2, “Definitions” is changed to update the trademarks for Advant, AP1000, and Common Q. In addition, the definition for AMPL is corrected to “ABB Master Programming Language.”

3. Section 3, “AP1000-Specific Application Development,” is changed to cite the latest NRC-approved proprietary version of the SPM and to make an editorial change to correct the trademark for Common Q. Also in this same section, typographical errors for IEEE Standard 1074-1995 are corrected.

4. Section 3.1, “Conceptual Phase,” is changed to remove the term “Document Index” as the tool used to establish and document the technical baseline.

5. Section 3.9, “Alternative Methods to Processes Defined in WCAP-16096-P-A,” is added to capture Common Q SPM alternatives.

6. Section 3.10, “Alternative Methods to Processes Defined in WCAP-16097-P-A,” is added to capture Common Q TR alternatives.

7. Section 4.1, “Industry Standards and Codes,” is changed to correct the title for item numbers 4.1.1 and 4.1.2.

8. Section 4.2, “Westinghouse Documents,” is changed to update the first and second references (4.2.1 and 4.2.2) to the NRC-approved, proprietary version of WCAP-16096, Revision 4 and WCAP-16097, Revision 3.

2.6. Summary of Proposed Changes

In summary, this LAR requests approval of the following:

- Incorporate by reference the NRC-approved versions of the Tier 2* WCAP-16096, Revision 4, "Software Program Manual for Common Q™ Systems" and WCAP-16097, Revision 3, "Common Qualified Platform Topical Report" 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 Topical Report as the licensing basis for the development of the Common Q portion of the PMS in lieu of the applicable digital I&C Regulatory Guides.

- Incorporate by reference an updated revision of Tier 2 APP-GW-GLR-017, "Resolution of Common Q NRC Items" which revises previous plant-specific action item and generic open item responses that involve the update to WCAP-16097.

- 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 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.

These new revisions accurately reflect the process for system-level design, software design and implementation, and hardware design and implementation for the AP1000 PMS development. The proposed changes to adopt the updated WCAP-16096 and WCAP-16097, and to revise WCAP-15927, as described above, do not adversely affect plant design, any physical aspect of the plant, system function, or any equipment qualification previously performed. The changes would not adversely affect any safety-related equipment or function, radioactive material barrier, effluent types, or safety analysis.

3. TECHNICAL EVALUATION (Incorporated into Section 2)

4. REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements/Criteria

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

- 10 CFR 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, thus, requires prior NRC approval.

- 10 CFR 50.55a(a)(1), "Quality Standards for Systems Important to Safety," requires that "Structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed." The Common Q Topical Report was determined to be an acceptable approach to satisfying the regulatory requirements in 10 CFR 50.55a(a)(1) applicable to the Common Q portion of the protection and safety monitoring system. Therefore, it is concluded that the requirements of 10 CFR 50.55a(a)(1) are met.

- 10 CFR 50.55a(h), "Protection and safety systems," approves the 1991 version of 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. The Common Q portion of the protection and safety monitoring system described in WCAP-16096 (Revision 4), including the proposed alternatives in Enclosure 3, WCAP16097 (Revision 3), and WCAP-15927 (Revision 4) continues to meet the requirements in IEEE Standard 603-1991 and, therefore, satisfies 10 CFR 50.55a(h).

- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants"

The design of the Common Q-based safety systems continues to meet the relevant requirements of GDC 1, 2, 4, 13, and 19 through 25.

<u>General Design Criteria:</u>

- GDC 1, "Quality Standards and Records," states 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.

The Common Q topical report adequately identifies the regulatory guides and industry codes applicable to the Common Q. The Common Q Topical Report was determined to be an acceptable approach to satisfying the regulatory requirements in GDC 1. Therefore, the requirements of GDC 1 are met.

- GDC 2, "Design Basis for Protection Against Natural Phenomena," states 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.

  Westinghouse has identified those systems and components for the safety systems designed to survive the effects of earthquakes, abnormal environments and missiles, and other natural phenomena. These systems and components continue to be consistent with their design bases. Therefore, the requirements of GDC 2 are met.

- GDC 4, "Environmental and Dynamic Effects Design Basis," states 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.

  Equipment in the Common Q-based portion of the protection and safety monitoring system is qualified for a mild environment per the AP1000 Equipment Qualification Program. The appropriate Electromagnetic Interference (EMI)/ Radio Frequency Interference (RFI) testing, environmental testing, and seismic testing is performed to demonstrate that the equipment in the Common Q portion of the protection and safety monitoring system will function under prescribed mild environment conditions. Therefore, the requirements of GDC 4 are met.

- GDC 13, "Instrumentation and Control," states 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

  The Common Q portion of the protection and safety monitoring system appropriately supports actions to monitor and operate the nuclear power unit in a safe and reliable manner during normal operation, anticipated operational occurrences, and accident conditions. Therefore, the design of the Common Q portion of the protection and safety monitoring system satisfies the requirements of GDC 13.

- GDC 19, "Control Room," states 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.

The Common Q portion of the protection and safety monitoring system appropriately supports actions to monitor and operate the nuclear power unit from a control room in a safe and reliable manner during normal operation, anticipated operational occurrences, and accident conditions. Therefore, the design of the Common Q portion of the protection and safety monitoring system satisfies the requirements of GDC 19.

- GDC 20, "Protection System Functions," states 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.

  The Common Q portion of the protection and safety monitoring system conforms to the design bases requirements of IEEE Std 603-1991. It includes the provision to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown consistent with the accident analysis presented in UFSAR Chapter 15. Therefore, the Common Q portion of the protection and safety monitoring system satisfies the requirements of GDC 20.

- GDC 21, "Protection System Reliability and Testability," states that the protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.

  The Common Q portion of the protection and safety monitoring system facilitates conformity to the guidelines for periodic testing in Regulatory Guide 1.22 and Regulatory Guide 1.118. The Common Q portion of the protection and safety monitoring system facilitates conformity to Regulatory Guide 1.47 for bypassed and inoperable status indication. The Common Q portion of the protection and safety monitoring system facilitates the conformity to the guidelines on the application of the single-failure criterion in IEEE Std 379-2000 as supplemented by Regulatory Guide 1.53. The Common Q portion of the protection and safety monitoring system satisfies the requirements of IEEE Std 603-1991 with regard to system reliability and testability. Therefore, the Common Q portion of the protection and safety monitoring system satisfies the requirements of GDC 21.

- GDC 22, "Protective System Independence," states 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.

  The Common Q portion of the protection and safety monitoring system conforms to the guidelines in Regulatory Guide 1.75 for protection system independence. Implementing the Common Q platform as part of the protection and safety monitoring system will not adversely affect the plant's existing compliance with Regulatory Guide 1.75. The Common Q portion of the protection and safety monitoring system satisfies the requirement of IEEE Std 603-1991 with regard to

system independence. Therefore, the Common Q portion of the protection and safety monitoring system satisfies the requirements of GDC 22.

- GDC 23, "Protective System Failure Modes," states 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.

  The AP1000 failure modes and effects analysis adequately demonstrates how the protection and safety monitoring system will operate with a single failure under all postulated operating conditions. The proposed activity does not affect this analysis. Therefore, the proposed design approaches are consistent with the requirements of GDC 23.

- GDC 24, "Separation of Protection and Control," states 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.

  The Common Q portion of the protection and safety monitoring system and the plant operating control systems continue to satisfy the requirements of IEEE Std 603-1991 with regard to protection and control system interactions. Regulatory Guide 1.153 endorses IEEE Std 603-1991 as an acceptable method for satisfying the requirements of GDC 24. Therefore, the Common Q portion of the protection and safety monitoring system satisfies the requirements of GDC 24.

- GDC 25, "Protection System Requirements for Reactivity Control Malfunctions," states 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.

  The Common Q portion of the protection and safety monitoring system continues to satisfy protection system requirements for malfunctions of the reactivity control system such as accidental withdrawal of control rods. Therefore, the Common Q portion of the protection and safety monitoring system satisfies the requirements of GDC 25.

- 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 are applicable to WCAP-16096. WCAP-16096 specifies plans that will provide a quality software life cycle process, including documentation of life cycle activities. Therefore, these criteria are still met.

4.2 Precedent

No precedent is identified.

4.3 Significant Hazards Consideration Determination

The requested amendment would revise the Combined License (COL) in regard to the AP1000 at Vogtle Electric Generating Plant (VEGP) Units 3 and 4, by revising plant-specific Design Control Document (DCD) Tier 2* and associated Tier 2 material that covers the processes for system-level design, software design and implementation, and hardware design and implementation for the AP1000 PMS development. There is no design change to the plant.

This license amendment requests approval of the following:

- Incorporate by reference the NRC-approved versions of the Tier 2* WCAP-16096, Revision 4, "Software Program Manual for Common Q™ Systems" and WCAP-16097, Revision 3, "Common Qualified Platform Topical Report" 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 Topical Report as the licensing basis for the development of the Common Q portion of the PMS in lieu of the applicable digital I&C Regulatory Guides.

- Incorporate by reference an updated revison of Tier 2 APP-GW-GLR-017, "Resolution of Common Q NRC Items" which revises previous plant-specific action item and generic open item responses that involve the update to WCAP-16097.

- 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 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.

These Tier 2* and involved Tier 2 changes require NRC approval prior to implementation.

An evaluation to determine whether or not a significant hazards consideration is involved with the proposed amendment was completed by focusing on the three standards set forth in 10 CFR 50.92, "Issuance of amendment," as discussed below:

4.3.1 Does the proposed amendment involve a significant increase in the probability or consequences of an accident previously evaluated?

Response: No

WCAP-16096 (Common Q Software Program Manual) was updated to Revision 4 to reference later NRC endorsed regulatory guides and standards and update the requirements for the software design and development processes for the Common Q portion of the AP1000 Protection and Safety Monitoring System (PMS). WCAP-16097 (Common Q Topical Report) was updated to Revision 3 to describe new Common Q components and standards currently used for the AP1000 PMS implementation of the Common Q platform. These two WCAPs have been reviewed and approved by the NRC in Safety Evaluations dated February 7, 2013. WCAP-15927 was updated to reference the newest revisions of WCAP-16096 and WCAP-16097 and for editorial corrections. The proposed activity adopts the updated versions as incorporated by reference documents into the Updated Final Safety Analysis Report (UFSAR). Other proposed document changes support the implementation of the updated versions of WCAP-16096, WCAP-16097, and WCAP-15927.

The Common Q platform is an acceptable platform for nuclear safety-related applications. The Common Q system meets the requirements of 10 CFR Part 50, Appendix A, General Design Criteria (Criteria 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, and 25), the Institute of Electrical and Electronics Engineers (IEEE) Standard 603-1991 for the design of safety-related reactor protection systems, engineered safety features systems and other plant systems, and the guidelines of Regulatory Guide 1.152 and supporting industry standards for the design of digital systems.

Because the Common Q platform and the Protection and Safety Monitoring System (PMS) implementation of the Common Q platform meet the criteria in the applicable General Design Criteria, the revisions to these documents do not affect the prevention and mitigation of abnormal events, such as accidents, anticipated operational occurrences, earthquakes, floods and turbine missiles, or their safety or design analyses as described in the licensing basis. The incorporation of the updated documents does not adversely affect the interface with any structure, system, or component (SSC) accident initiator or initiating sequence of events. Thus, the probabilities of the accidents previously evaluated in the UFSAR are not affected.

Therefore, the proposed amendment does not involve a significant increase in the probability or consequences of an accident previously evaluated.

4.3.2 Does the proposed amendment create the possibility of a new or different kind of accident from any accident previously evaluated?

Response: No

The proposed changes to adopt the updated WCAP-16096, WCAP-16097, and WCAP-15927 into the UFSAR do not adversely affect the design or operation of safety-related equipment or equipment whose failure could initiate an accident beyond what is already described in the licensing basis. These changes do not adversely affect fission product barriers. No safety analysis or design basis acceptance limit/criterion is challenged or exceeded by the requested change.

Therefore, the proposed amendment does not create the possibility of a new or different kind of accident from any accident previously evaluated.

4.3.3 Does the proposed amendment involve a significant reduction in a margin of safety?

Response: No

The proposed changes to adopt the updated WCAP-16096, WCAP-16097, and WCAP-15927 into the UFSAR do not adversely affect the design, construction, or operation of any plant SSCs, including any equipment whose failure could initiate an accident or a failure of a fission product barrier. No analysis is adversely affected by the proposed changes. Furthermore, no system function, design function, or equipment qualification will be adversely affected by the changes.

Therefore, the proposed amendment does not involve a significant reduction in a margin of safety.

Based on the above, it is concluded that the proposed amendment does not involve a significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and, accordingly, a finding of “no significant hazards consideration” is justified.

4.4 Conclusions

Based on the considerations discussed above, (1) there is reasonable assurance that 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 (3) the issuance of the amendment will not be inimical to the common defense and security or to the health and safety of the public. The above evaluations demonstrate that the requested changes can be accommodated without an increase in the probability or consequences of an accident previously evaluated, without creating the possibility of a new or different kind of accident from any accident previously evaluated, and without a significant reduction in a margin of safety. Having arrived at negative declarations with regard to the criteria of 10 CFR 50.92, this assessment determined that the requested change does not involve a Significant Hazards Consideration.

5. ENVIRONMENTAL CONSIDERATIONS

The requested amendment revises plant-specific Design Control Document (DCD) Tier 2* and associated Tier 2 material that is incorporated into the Updated Final Safety Analysis Report (UFSAR). The requested amendment involves changes to the design processes for the AP1000 PMS hardware and software arising from incorporation of revisions to the following three incorporated by reference (IBR) Tier 2* documents in the UFSAR.

- WCAP-16097, "Common Qualified Platform Topical Report"
- WCAP-16096, "Software Program Manual for Common Q™ Systems"
- WCAP-15927, "Design Process for Common Q Safety Systems"

These three documents describe the hardware and software development process for the Common Q Platform. They also discuss the process for system-level design, software design and implementation, and hardware design and implementation for the AP1000 Protection and Safety Monitoring System (PMS) development.

The requested amendment also adds, deletes, and provides clarifications and editorial corrections to Tier 2 and Tier 2* UFSAR text to support the changes described above.

Sections 2 and 3 of this license amendment request provide additional details of the proposed changes.

The Licensee has determined that the anticipated construction and operational effects of the proposed amendment meet the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9), in that:

(i) There is no significant hazards consideration.

An evaluation was completed to determine whether or not a significant hazards consideration is involved by focusing on the three standards set forth in 10 CFR 50.92, "Issuance of amendment." The updates to the UFSAR text and licensing documents, as described above, do not adversely affect the plant design or any physical aspect of the plant. The Significant Hazards Consideration determined that (1) the proposed amendment does not involve a significant increase in the probability or consequences of an accident previously evaluated; (2) the proposed amendment does not create the possibility of a new or different kind of accident from any accident previously evaluated; and (3) the proposed amendment does not involve a significant reduction in a margin of safety. Therefore, it is concluded that the proposed amendment does not involve a significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and accordingly, a finding of "no significant hazards consideration" is justified.

(ii) There is no significant change in the types or significant increase in the amounts of any effluents that may be released offsite.

The proposed changes adopt the approved updated Common Q Platform and its development processes for AP1000 by incorporating by reference newer revisions of the documents. These documents describe the design of the Common Q platform used in the protection and safety monitoring system and the processes used for its development.

The update to the Common Qualified Platform Topical Report, Software Program Manual for Common Q Systems, and the Design Process for Common Q Safety Systems is unrelated to any aspects of plant construction or operation that would introduce any changes to effluent types (e.g., effluents containing chemicals or biocides, sanitary system effluents, and other effluents) or affect any plant radiological or non-radiological effluent release quantities. Furthermore, these changes do not diminish the functionality of any design or operational features that are credited with controlling the release of effluents during plant operation.

Therefore, it is concluded that the proposed amendment does not involve a significant change in the types or a significant increase in the amounts of any effluents that may be released offsite.

(iii) There is no significant increase in individual or cumulative occupational radiation exposure.

The proposed changes to adopt the approved updated Common Q Platform and its development processes for AP1000 have no effect on individual or cumulative occupational radiation exposure during plant operation. The proposed changes are only related to the Common Q Platform design itself. There are no proposed changes that will negatively impact or change any system functions related to radiation exposure.

Therefore, the proposed amendment does not involve a significant increase in individual or cumulative occupational radiation exposure.

Based on the above review of the requested amendment, it has been determined that anticipated construction and operational effects of the proposed amendment do not involve (i) a significant hazards consideration, (ii) a significant change in the types or significant increase in the amounts of any effluents that may be released offsite, or (iii) a significant increase in the individual or cumulative occupational radiation exposure. Accordingly, the requested amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9). Therefore, pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the proposed amendment.

6. REFERENCES

- Safety Evaluation by the Office of Nuclear Reactor Regulation, Westinghouse Topical Report WCAP-16097-P, Revision 3, “Common Qualified Platform,” TAC. No. ME5157, February 7, 2013 (ADAMS Accession No. ML13022A011)

- Safety Evaluation for Westinghouse Topical Report WCAP-16096-P, Revision 4, “Software Program Manual for Common Q Systems,” TAC. No. ME5159, February 7, 2013 (ADAMS Accession No. ML13022A009)

Southern Nuclear Operating Company

ND-16-0083

Enclosure 2

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

Plant-Specific Action Item and Generic Open Item Dispositions for WCAP-16096, Revision 4 and WCAP-16097, Revision 3

(LAR-15-017)

(Enclosure 2 consists of 13 pages, including this cover page)

PLANT-SPECIFIC ACTION ITEM AND GENERIC OPEN ITEM DISPOSITIONS FOR WCAP-16096, REVISION 4 AND WCAP-16097, REVISION 3

This enclosure discusses the new plant-specific action items (PSAIs) and a generic open item (GOI) contained within the Safety Evaluations (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 and updates the disposition for WCAP-16097, Revision 0 PSAI 6.1 and GOI 7.1. A description of the required plant-specific action items changes, if any, along with the technical evaluation are provided.

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.

PSAI 6.1 Disposition

The process description for the response to PSAI 6.1 in APP-GW-GLR-017 (Non-Proprietary), "AP1000 Standard Combined License Technical Report – Resolution of Common Q NRC Items," is still valid to address the suitability of the AP1000 PMS. Table 3-1 in the disposition in APP-GW-GLR-017 is updated to show the following modules used for the AP1000 and to delete the AI685 module. This update requires changes to the introduction section and the GOI 7.1 resolution to correct statements that indicate the AI685 module is used in the AP1000.

Item	I/O Signal Type	S600 I/O Module
2	Current Input	AI688
3	Voltage Input	AI688
4	Resistance Temperature Detectors (RTD) Input	AI687
5	Millivolt (Thermocouple) Input	AI687

Proposed Licensing Basis Changes

UFSAR Tier 2 IBR document, APP-GW-GLR-017, Table 3-1 is revised to align it with the S600 I/O modules described in WCAP-16675, which was part of the certified design.

Technical Evaluation

This proposed change is consistent with the proposed change and technical evaluation in Section 2.1.1 of Enclosure 1 of this license amendment request.

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.

PSAI 6.4 Disposition

The original disposition in APP-GW-GLR-017 is still valid. The disposition for the additional statement (see underlined portion) is:

Westinghouse has an applications restrictions document that was submitted to the NRC (Reference 21 in the NRC SE for WCAP-16097-P-A, Revision 3, “Common Qualified Platform Topical Report”). This restrictions document defines system limitations imposed on the system designer to maintain the system design within the bounds of the Equipment Qualification Program. The PMS system design specification complies with the hardware restrictions specified in the restrictions document.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

WCAP-16097 PSAI 6.15

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.

PSAI 6.15 Disposition

Section 6 of the software requirements specification for the PMS defines the requirements for reporting the results of the inherent, automatic self-testing features of the Common Q platform during operation. These features are also described in WCAP-16675, “AP1000 Protection and Safety Monitoring System Architecture Technical Report” (Tier 2, Incorporated by Reference).

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

WCAP-16097 PSAI 6.16

A licensee implementing a Common Q DPPS shall ensure that no more than four processor modules are installed within a single AC160 controller.

PSAI 6.16 Disposition

A processor module in this context is defined as the PM646A. It has been confirmed that the Vogtle Electric Generating Plant, Units 3 &4 AP1000 design uses no more than four processor modules within a single AC160 controller. This restriction is captured in Section 4.1 of WCAP-16097, Revision 3, which is proposed to be incorporated into the AP1000 licensing basis in this license amendment request. Therefore, the AP1000 will be committed to the following:

> "Presently the Common Q™ Applications require an upper limit of four PM646As. Any applications of more than four PM646As will be evaluated for compliance with Section 7 requirements when needed." (WCAP-16097, Revision 3, Section 4.1)

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

WCAP-16097 PSAI 6.17

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.

PSAI 6.17 Disposition

The WCAP-16097 Safety Evaluation identifies the AC160 components that the NRC staff has approved for use in Class 1E applications in WCAP-16097, Revision 3 Safety Evaluation Table 1.

The PMS uses the approved components in Table 1 in WCAP-16097-P-A, Revision 3. Though the DI621 module is not listed in Table 1 of the SE, it is included in the AP1000 certified design as described in WCAP-16675. The DI621 module is qualified for use in the PMS as a Class 1E component by undergoing commercial dedication and equipment qualification using the same Commercial Dedication Instructions (CDIs) as the modules listed in Table 1. The commercial dedication of the DI621 module is covered by the ITAAC listed in Tier 1 Table 2.5.2-8, Item 13.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

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.

PSAI 6.18 Disposition

PMS setpoints for reactor trip and ESFAS actuation functions are changed using the safety-related Maintenance and Test Panel in the Maintenance Test Cabinet (MTC), as described in WCAP-16675. The SE states that "Placement of the function enable key switch in the enable position causes a system alarm but does not inhibit operation of the remaining Common Q system in any way." However, for the AP1000 PMS the MTP performs an interlock such that setpoint changes cannot be made unless the MTP function enable keyswitch is in the enable position. This interlock is part of the MTP safety-related software. As a result, it is sufficient to only bypass the channel associated with the setpoint change instead of the entire division. Bypassing an entire division would revert all reactor trip and ESFAS actuation functions to a 2-out-of-3 coincident logic. Bypassing the channel would only revert the safety function associated with the setpoint change to a 2-out-of-3 coincidence configuration, with the remaining safety functions maintaining a 2-out-of-4 coincidence configuration. This is preferable from a system reliability perspective. Bypassing a channel for setpoint changes is consistent with WCAP-16675, Section 2.2.6.1, "Setpoint and Calibration Constant Changes."

Since the PMS division will remain operational during setpoint changes for reactor trip and ESFAS actuation functions, as described above, the PMS division room environment needs to be considered when opening the MTC door to make setpoint changes. Therefore, administrative controls will be developed so that the division room environment does not interfere with PMS equipment when plant personnel are making setpoint changes to reactor trip and ESFAS actuation functions. The administrative controls will account for local emissions from nearby equipment and activities (e.g., welding) while the MTC door is open.

The permissive setpoints for blocks and resets (e.g., P-10) can also be changed. However, there is no associated maintenance bypass associated with these setpoints and they affect multiple safety functions in a division. Therefore, administrative controls will be developed to declare the affected division of the PMS inoperable prior to changing permissive setpoints.

Proposed Licensing Basis Changes

A change is proposed to add Tier 2 UFSAR Subsection 7.1.2.14.3, "Operational Process," to require that the PMS and its division room are in the appropriate configuration prior to making setpoint changes, as described above.

Technical Evaluation

The proposed text captures the licensing basis changes necessary to satisfy this PSAI and is consistent with WCAP-16097, Revision 3. In addition, in reviewing WCAP-16675, the NRC previously approved the use of the MTP as a dedicated display interface for each division and to bypass the channel before any setpoint alterations. The staff evaluated the access controls per IEEE 603-1991, Clause 5.9. See NUREG-1793, Supplement 2, "Final Safety Evaluation Report Related to Certification of the AP1000 Standard Plant Design, Docket Number 52-006."

WCAP-16097 PSAI 6.19

A licensee implementing a specific application based upon the Common Q platform 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.

PSAI 6.19 Disposition

Per 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. This requirement is currently included in the AP1000 licensing basis since WCAP-16675 is incorporated by reference into the UFSAR.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

WCAP-16097 PSAI 6.20

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.

PSAI 6.20 Disposition

For the AP1000, this issue was already included in the scope of the WCAP-16097 PSAI 6.4 disposition in APP-GW-GLR-017.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

WCAP-16097 PSAI 6.21

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.

PSAI 6.21 Disposition

AP1000 PMS specific equipment qualification testing beyond that described in Reference 11 of the SE was performed as documented in the AP1000 PMS equipment qualification summary report. The AP1000 PMS equipment qualification summary report documents the following:

1. The High Speed Links (HSLs) were included in the PMS cabinets for Electromagnetic Compatibility (EMC) testing.
2. The PMS cabinets were required to maintain functional operability during each EMC test to demonstrate qualification.
3. The results of EMC testing and the conclusion that the PMS cabinets passed the required EMC tests.

Therefore, the HSL radiated emissions do not impact any locally mounted equipment in the PMS cabinet. In addition, the installation limitations included in the PMS equipment qualification summary report prevent any impact of radiated emissions on locally mounted equipment within the PMS divisional rooms.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

WCAP-16097 PSAI 6.22

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.

PSAI 6.22 Disposition

The AP1000 PMS is not using the AI685 modules. See disposition for PSAI 6.1 in APP-GW-GLR-017.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

WCAP-16097 PSAI 6.23

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.

PSAI 6.23 Disposition

The Common Q Record of Changes reviewed by the NRC is listed in WCAP-16097-P, Appendix 5. The changes include both Common Q hardware and software. WCAP-16097-P, Appendix 5 has been updated with the list of changes to the Common Q Platform for the AP1000 since the issuance of the NRC's SE in 2013. This enclosure documents the analysis that confirms that the changes have not invalidated the original safety conclusion.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

WCAP-16097 PSAI 6.24

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 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 Disposition

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.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

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.

PSAI 6.25 Disposition

The architecture for the AP1000 PMS, as described in WCAP-16674, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," does not rely upon the use of Interface and Test Processors (ITPs) and AF100 busses to provide separation between safety and non-safety signals.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

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.

GOI 7.1 Disposition

The current resolution for GOI 7.1 in APP-GW-GLR-017 (Non-Proprietary), "AP1000 Standard Combined License Technical Report – Resolution of Common Q NRC Items," Revision 0 discusses the development and qualification of the AI685 module. The resolution concludes by stating that the GOI 7.1 resolution is applicable to the AP1000 design. However, as documented in the resolution to PSAI 6.1, the AI685 module is not part of the certified and approved AP1000 design. Therefore, the GOI 7.1 resolution is not applicable to the AP1000 design. The last sentence in the original GOI 7.1 resolution is corrected to state that the AI685 module is not used for the AP1000 design and the GOI resolution does not apply. This revision aligns APP-GW-GLR-017 with the S600 I/O modules described in WCAP-16675.

Proposed Licensing Basis Changes

UFSAR Tier 2 IBR document, APP-GW-GLR-017 is revised. The Introduction section and the last sentence in the GOI 7.1 resolution are corrected to state that the AI685 module is not used for the AP1000 design and the GOI resolution does not apply.

Technical Evaluation

This proposed change is consistent with the proposed change and technical evaluation in Section 2.1.1 of Enclosure 1 of this license amendment request.

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.

GOI 7.11 Disposition

Similar to the other Common Q components used for the AP1000 PMS, seismic and environmental qualification testing on the DI621 was performed as part of the AP1000 PMS equipment qualification program following the methodology in UFSAR Appendix 3D.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

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 Disposition

The Common Q portion of PMS is developed in accordance with WCAP-16096, Revision 4. However, in some instances, there are alternate methods used instead of the processes described in WCAP-16096, Revision 4.

Per the SPM, the PQP includes the Project Plan, which identifies the Software Development Plan (WNA-PD-00042-WAPP) as the location for the SPM alternatives and justifications. See Enclosure 3 for the SPM alternatives proposed in this license amendment request.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

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.

PSAI 2 Disposition

The software lifecycle design and implementation documents for the protection and safety monitoring system, as described in Branch Technical Position (BTP) 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” Sections B.2.2 and B.2.3, are:

- Safety analyses – protection and safety monitoring system Software Hazards Analysis and IV&V phase summary reports.
- Verification and validation analysis and test reports – protection and safety monitoring system IV&V phase summary reports and module, unit, integration, and system test reports.
- Configuration management reports – protection and safety monitoring system configuration management release reports.
- Testing activities - protection and safety monitoring system module, unit, integration, and system test reports.

These reports cover the following activities: requirements, implementation, integration, validation, installation, and operations and maintenance.

The software lifecycle design outputs for the AP1000 protection and safety monitoring system are:

- Software Requirements Specifications (SRS) - AP1000 protection and safety monitoring software requirements specification.
- Hardware/Software architecture descriptions (SADs) – AP1000 protection and safety monitoring system design specification and software requirements specification.
- Software design specifications (SDSs) – AP1000 protection and safety monitoring system software design documents.
- Code Listings - AP1000 protection and safety monitoring system software release records identify the source and location of the source code.
- Build Documents - The elements of System Build Documents (SBDs) are implemented in a collection of various PMS documents including the PMS Subsystem Design Specification (SSyDS), Software Design Descriptions (SDDs), Configuration Management Release Records (CMRRs), Verification & Validation (V&V) task reports, and ultimately the V&V Phase Summary Reports.

- Installation Configuration Tables – Database Release Record for the System Design Specification for the AP1000 protection and safety monitoring system.
- Operations Manuals – AP1000 protection and safety monitoring system technical manual.
- Maintenance Manuals - AP1000 protection and safety monitoring system technical manual.
- Training Manuals – AP1000 protection and safety monitoring system training material.

The SPM is implemented in accordance with the 10 CFR 50 Appendix B program. This ensures that the implementation documents are reviewed and approved.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

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.

PSAI 3 Disposition

The licensee Quality Assurance (QA) activities for the PMS are covered by the Quality Assurance program described in Chapter 17 of the UFSAR.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

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.

PSAI 4 Disposition

Westinghouse provides a PMS technical manual that meets BTP 7-14, Section B.3.1.8.4 for a software operations plan and will be issued prior to system turn-over.

Proposed Licensing Basis Changes

Section 7.1.2.14, “Operational Process” is proposed to be added to the UFSAR as Tier 2 text that requires the development of an operations plan.

Technical Evaluation

This proposed change meets the PSAI and is consistent with the change and technical evaluation in Section 2.1.1 of Enclosure 1 of this license amendment request.

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.

PSAI 5 Disposition

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.

Site acceptance testing and installation testing of the protection and safety monitoring system is covered by DCD Tier 1 ITAAC Table 2.5.2-8, Item 11.e (COL Appendix C, ITAAC No. 2.5.02.11.e).

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

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.

PSAI 6 Disposition

A review of the current AP1000 PMS Common Q Record of Changes document determined that there were no changes to the Common Q SPM. The change to WCAP-16096 from Revision 01A to Revision 4, including the alternatives, is addressed in this license amendment request.

Proposed Licensing Basis Changes

None

Technical Evaluation

N/A

Southern Nuclear Operating Company

ND-16-0083

Enclosure 3

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

Common Q Software Program Manual (SPM) and Topical Report Alternatives and Justification

(LAR-15-017)

(Enclosure 3 consists of 10 pages, including this cover page)

COMMON Q SOFTWARE PROGRAM MANUAL (SPM), REVISION 4 AND TOPICAL REPORT (TR), REVISION 3 ALTERNATIVES AND JUSTIFICATION

This enclosure documents the alternatives used instead of the processes described in WCAP-16096, "Software Program Manual for Common Q™ Systems," Revision 4.

Table A3-1, "Common Q Software Program Manual Alternatives"

SPM Section	SPM Text	Alternative/Justification
Glossary of Terms: Project Quality Plan (PQP) 4.3.2.1 Initiation (Concept) Phase	A document that specifies alternatives or supplements to the Westinghouse 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 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.	Alternative 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. Justification The Project Plan identifies the Software Development Plan as the location for the SPM alternatives and justifications. The Software Development Plan also identifies itself as the companion document to the Project Plan. Both of these documents are approved by the Quality Organization.

SPM Section	SPM Text	Alternative/Justification
4.3.1 Organization Exhibit 2-1 Design/IV&V Team Organization	The NA organization includes a Quality organization and an Engineering organization. The design team and the IV&V team are organized within the Engineering organization.	Alternative The NA organization includes a Quality organization and an Engineering organization. The design team and the Independent Verification & Validation (IV&V) team are in separate organizations at least to the Director level. See updated SPM Exhibit 2-1 Design/IV&V Team Organization following this table (Figure A3-1). Justification 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.
4.3.2.6 Site Installation and Checkout Phase	The preparation of the site test plan will be initiated during the requirements phase to support evaluation of requirement testability on-site.	Alternative 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. Justification 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.

SPM Section	SPM Text	Alternative/Justification
4.6.2.10 Post Mortem Review	Suggestions for improvement and/or best practices that are identified during the Post Mortem Review should be documented via EXHIBIT 11-2 CORRECTIVE ACTIONS PROCESS.	Alternative 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. Justification 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.
5.5.1 Management of IV&V	The resources for performing the IV&V shall be identified in the Project Quality Plan (Reference 4) that is prepared by the Project Manager during the conception phase of the software life cycle.	Alternative 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. Justification 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.

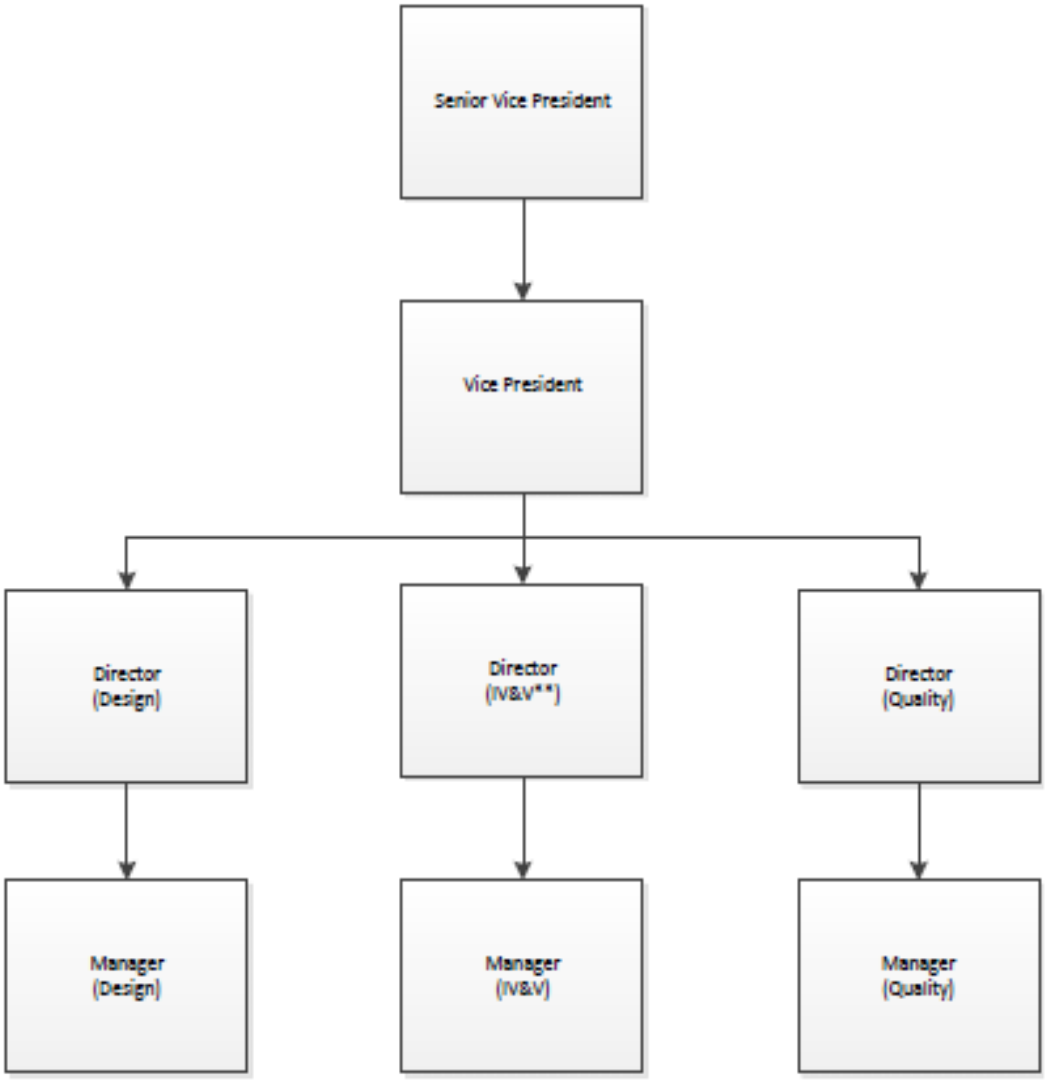
SPM Section	SPM Text	Alternative/Justification
6.3.2 Configuration Change Control	Software Change Request Procedure, Step 5: Revised System Baseline: The SCR forms will be used as the basis to track all system changes and to verify that changes have been properly implemented and that documentation has been updated.	Alternative 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. Justification 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.
6.3.4 Configuration Audits and Reviews	Configuration Audits and Reviews 3. External audits by customers or regulators shall be coordinated by the EPM [Engineering Project Manager] who will schedule personnel to be available if additional support is required.	Alternative 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. Justification 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 Westinghouse Level 2 process meets the intent of the commitment. There are designated resources used to ensure personnel are available to support external audits. There is no requirement in Regulatory Guide 1.169 or IEEE 828 to have an Engineering Project Manager coordinate audits.

SPM Section	SPM Text	Alternative/Justification
6.4 SCM Schedule	SCM milestones that shall be indicated on the project schedule include: • CCB establishment • Establishment of a configuration baseline, and • Implementation of change control procedures.	Alternative 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. Justification 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.
9.2.3 Control	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 this log.	Alternative 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. Justification 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.

SPM Section	SPM Text	Alternative/Justification
10.5.1 Software Verification and Validation Plan	The PQP shall also define the tracking and recording process for the hardware configuration pertinent to the software verification and validation process during all phases of the software life cycle.	Alternative 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. Justification 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.
10.10 Computer Code Certificate	The completion of the implementation 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).	Alternative 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). Justification This alternative corrects a typographical error in the SPM, since there is not an “implementation and checkout phase.”
11.4 Corrective Action	Corrective actions shall be documented on Exception Reports and Common Q™ Comment Records by the design team and shall be completed by the due date specified on the form…Once the independent reviewer is satisfied with the corrective action taken, the report form shall be signed.	Alternative 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. Justification 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.

SPM Section	SPM Text	Alternative/Justification
12 Secure Development and Operational Environment Plan	Secure Development and Operational Environment	Alternative 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." Justification 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.

Figure A3-1, "Exhibit 2-1 Design/IV&V Team Organization"



*This example organization chart shows the minimum level of separation required for the Design, IV&V, and Quality Teams

**System level validation testing is performed by another group, which meets the same level of independence as the IV&V group depicted in this organization chart

Table A3-2, "Common Q Topical Report Alternatives"

TR Section	TR Text	Alternative/Justification
References	References 27. WCAP-17266, Rev.0, "Common Q Platform Generic Change Process," Westinghouse Electric Company LLC.	Alternative 27. WCAP-17266, "Common Q Platform Generic Change Process," Westinghouse Electric Company LLC. Justification 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.

Southern Nuclear Operating Company

ND-16-0083

Enclosure 4

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

Proposed Changes to the Licensing Basis Documents

(LAR-15-017)

Note:
Added text is shown as **Blue Underline**
Deleted text is shown as ~~**Red Strikethrough**~~
Omitted text is shown as three asterisks (*** * ***)

(Enclosure 4 consists of 19 pages, including this cover page)

The UFSAR text provided as the baseline for these markups includes changes that were recently incorporated into the VEGP Units 3 and 4 UFSAR based on a plant-specific departure from DCD Tier 2 information. The changes made by the internally generated departure were evaluated in accordance with the change process in 10 CFR Part 52, Appendix D, Section VIII, paragraph B.5.a, and determined not to require NRC approval prior to implementation.

1. **UFSAR Section 1.6, Table 1.6-1, "Material Referenced":**

   Revise Tier 2 and Tier 2* text applicable to DCD Section 7.1 in UFSAR Table 1.6-1 to reflect changes to referenced WCAPs.

DCD Section Number	Westinghouse Topical Report Number	Title
* * *		
7.1	* * *	
	[*WCAP-16096-P-A* *WCAP-16096-NP-A*	*Software Program Manual for Common Q™ Systems, ~~Revision 01A, December 2004~~ Revision 4, February 2013 (1) (as modified by the SPM alternatives in WCAP-15927, Revision 4)*]*
	[*WCAP-16097-P-A* *WCAP-16097-NP-A*	*Common Qualified Platform Topical Report, Revision ~~01, May 2003~~ Revision 3, February 2013 (as modified by the Topical Report alternatives in WCAP-15927, Revision 4)*]*
	* * *	
	WCAP-16674-P WCAP-16674-NP	AP1000 I&C Data Communication and Manual Control of Safety Systems and Components, Revision 4 (as modified by changes provided in Appendix 7A)
	WCAP-16675-P WCAP-16675-NP	AP1000 Protection and Safety Monitoring System Architecture Technical Report, Revision 5 (as modified by changes provided in Appendix 7A)
	APP-GW-GLR-017	AP1000 Standard Combined License Technical Report, Resolution of Common Q NRC Items, Revision 2
	* * *	
	[*WCAP-15927 (NP)*	*Design Process for AP1000 Common Q Safety Systems, ~~Revision 2,November 2008~~ Revision 4, April 2015*]*
	* * *	
	~~[WCAP-17201-P~~	~~*AC160 High Speed Link Communication Compliance to DI&C-ISG-04 Staff Positions 9, 12, 13 and 15, Revision 0, February 2010*]*~~
	* * *	

Add the following Note 1 (applicable to WCAP-16096) following UFSAR Table 1.6-1:
Notes:

1. [*Section 12, "Secure Development and Operational Environment Plan," of WCAP-16096, "Software Program Manual for Common Q™ Systems," Revision 4, is not applicable to the AP1000.*]*

Revise Tier 2 text applicable to DCD Section 7.2 in UFSAR Table 1.6-1 to reflect changes to referenced WCAPs.

DCD Section Number	Westinghouse Topical Report Number	Title
7.2	* * *	
	WCAP-16592-P WCAP-16592-NP	Software Hazards Analysis of AP1000 Protection and Safety Monitoring System, Revision 2 (as modified by changes provided in Appendix 7A)
	* * *	

2. UFSAR Section 1.9, Table 1.9-1, "Regulatory Guide/Section Cross-References":

Division 1 Regulatory Guide		Chapter, Section or Subsection
* * *		
1.152	Criteria for ~~Programmable~~ Digital Computers ~~System Software~~ in Safety ~~Related~~ Systems of Nuclear Power Plants ~~(Task 1C 127-5)~~ (Rev. 1, January 1996)	7~~.1~~ ~~7.2~~ ~~7.3~~ ~~7.4~~ ~~7.5~~ ~~7.6~~
1.152	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants (Rev. 2, January 2006)	Not referenced; see Appendix 1A
1.152	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants (Rev. 3, July 2011)	7
* * *		

3. UFSAR Appendix 1A, "Conformance with Regulatory Guides":

Revise Tier 2 Regulatory Guide conformance positions and summary descriptions for Regulatory Guide (RG) 1.152, RG 1.168, RG 1.169, RG 1.170, RG 1.172, and RG 1.173, as follows:

Criteria Section	Referenced Criteria	AP1000/ FSAR Position	Clarification/Summary Description of Exceptions
		* * *	
Reg. Guide 1.152, ~~(Task 1C 127-5),~~ Rev. 1, 1/96 ~~and Rev. 2, 1/06~~ – Criteria for ~~Programmable~~ Digital Computers ~~System Software~~ in Safety ~~Related~~ Systems of Nuclear Power Plants **Regulatory Guide 1.152, Rev. 2, 1/06 – Criteria for Use of Computers in Safety Systems of Nuclear Power Plants** Conformance of the design aspects with Revision 1 of the Regulatory Guide is as stated below in the DCD.			
General	ANSI/ IEEE-ANS-7-4.3.2 -1993	Exception ~~Conforms~~	The Common Q portion of the protection and safety monitoring system is developed using the Common Q Software Program Manual (SPM) (as modified by the SPM alternatives in WCAP-15927, Revision 4) and Common Q Topical Report (as modified by the Topical Report alternatives in WCAP-15927, Revision 4). The Common Q SPM and Topical Report were reviewed and approved by the NRC. The Common Q SPM and Topical Report meet IEEE Std. 7-4.3.2-2003, as endorsed by Regulatory Guide 1.152, Revision 3.
Conformance with Revision 2 of this Regulatory Guide for programmatic and/or operational aspects is documented below.			
General		Exception	The Cyber Security Program is based on March 2009 revisions of the 10 CFR 73.54 regulations in lieu of Revision 2 of this Regulatory Guide.
		* * *	
Reg. Guide 1.168, Rev. 0, 9/97 and Rev. 1, 2/04 – Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants Conformance of the design aspects with Revision 0 of the Regulatory Guide is as stated below in the DCD.			
General		Exception ~~Conforms~~	See Chapter 7 for a discussion of the instrumentation and control software program related to Common Qualified Platform (Common Q). The Common Q portion of the protection and safety monitoring system is developed using the Common Q SPM (as modified by the SPM alternatives in WCAP-15927, Revision 4). The Common Q SPM was reviewed and approved by the NRC using the criteria of IEEE Std. 1012-1998 and IEEE Std. 1028-1997 as endorsed by Regulatory Guide 1.168, Revision 1.

Criteria Section	Referenced Criteria	AP1000/ FSAR Position	Clarification/Summary Description of Exceptions
Conformance of the design aspects with Revision 1 of the Regulatory Guide is as stated below.			
General		Exception	See Chapter 7 for a discussion of the instrumentation and control software program related to the Component Interface Module (CIM) subsystem. Exceptions to the standards endorsed by Regulatory Guide 1.168, Revision 1 (i.e., IEEE 1012-1998 and IEEE 1028-1997) related to the CIM subsystem are noted below.
General	IEEE 1012-1998	Exception	The CIM subsystem takes exception to the requirement in Section 7.6 that states each Independent Verification and Validation (IV&V) Anomaly Report shall contain "recommendations." The IV&V Anomaly Reports do not require recommendations so that the independence of IV&V is maintained.
General	IEEE 1028-1997	Exception	The CIM subsystem takes exception to the requirement in Section 4.5.4 that requires team members to review the relevant materials prior to the management review. The project manager is required to distribute review materials before the meeting, and the material is reviewed during the meeting. The CIM subsystem takes exception to Section 4.6, which requires a management review to be considered complete when specific criteria are met. There is no requirement to officially declare the management review complete. The management review is considered complete at the discretion of the program manager in conjunction with the management review team. However, the CIM subsystem management reviews adhere to the meeting goals and outputs as defined by IEEE 1028, Sections 4.6 and 4.7 (with the exceptions noted in this appendix). The CIM subsystem takes exception to the guidance in Section 4.7, which requires specific criteria for documenting and tracking action item statuses, anomalies, and review team member participation as management review outputs. Contrary to IEEE 1028: • Only significant action items are formally documented and tracked in management meeting minutes. • Anomalies are formally tracked using issue tracking databases. • Members of the review teams are not formally captured as a management review output. The CIM subsystem takes exception to the guidance in Section 8.5.5.1, which requires auditors to perform activities outside the scope of the audit plan, if the activities are required to define the full extent of an issue. Contrary to IEEE 1028, auditors are not directed to

Criteria Section	Referenced Criteria	AP1000/ FSAR Position	Clarification/Summary Description of Exceptions
			perform or document reviews outside of the assigned audit scope or to take actions beyond that required by the audit plan. Issues found during an audit are entered into a corrective action tracking system. The corrective action program formally evaluates the issues and determines if an "extent of condition" investigation is required.
Conformance with Revision 1 of this Regulatory Guide for programmatic and/or operational aspects is documented below.			
General		Conforms	
Reg. Guide 1.169, Rev. 0, 9/97 – Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants			
General		Exception	Westinghouse uses the Common Q SPM (as modified by the SPM alternatives in WCAP-15927, Revision 4) to develop and maintain the Common Q portion of the protection and safety monitoring system. The Common Q SPM was reviewed and approved by the NRC using the criteria of Regulatory Guide 1.169, Revision 0 and IEEE 828-2005.
General	IEEE 828-1990	Exception	The CIM subsystem takes exception to the requirement in Section 2.3.4 to perform a configuration audit on a configuration item prior to its release. Configuration audits occur after the release of a configuration item document instead of prior to its release. Configuration audits are complete prior to installation of the Configuration Item in the plant. See Chapter 7 for a discussion of the instrumentation and control software program.
Reg. Guide 1.170, Rev. 0, 9/97 – Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants			
General		Exception	The Common Q portion of the protection and safety monitoring system is developed using the Common Q SPM (as modified by the SPM alternatives in WCAP-15927, Revision 4). The Common Q SPM was reviewed and approved by the NRC using the criteria of Regulatory Guide 1.170, Revision 0 and IEEE 829-1998. The CIM subsystem complies with Regulatory Guide 1.170, Revision 0 with the exception(s) identified below.
General	IEEE 829-1983	Exception	The CIM subsystem takes exception to the requirement in Section 3 to specify the version/revision level of the test items within the test plan. The CIM Test Plan is authored to be independent of the specific versions/revisions of the test items to be tested and requires the latest approved test plan version to be used.

Criteria Section	Referenced Criteria	AP1000/ FSAR Position	Clarification/Summary Description of Exceptions
General	IEEE 829-1983	Exception	The CIM subsystem takes exception to the required structure/format specified for Test-Design Specification (Section 4), Test-Case Specification (Section 5), Test-Procedure Specification (Section 6), Test-Item Transmittal Report (Section 7), Test Log (Section 8), Test-Incident Report (Section 9), and Test-Summary Report (Section 10). The CIM subsystem documents corresponding to the documents referred to in Sections 4 through 10 contain the content required by IEEE 829.
General	IEEE 829-1983	Exception	The CIM subsystem takes exception to the requirements in Sections 7.2.2 and 7.2.4 to include a reference to the test plan and deviations from the test plan when transmitting test items. The version/revision of the test item is recorded in the test record. There will be no deviations from the identified software documentation at the time of the software release.
General	IEEE 829-1983	Exception	The CIM subsystem takes exception to the requirement in Section 8 to record the start and end times of a test event. The date of the event is recorded, not the specific start and end times.
General	IEEE 829-1983	Exception	The CIM subsystem takes exception to the requirement in Section 10 to summarize resource consumption data in the test report. Resource consumption data is addressed in project schedules and budget data. See Chapter 7 for a discussion of the instrumentation and control software program.
		* * *	
Reg. Guide 1.172, Rev. 0, 9/97 – Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants			
General		Exception ~~Conforms~~	The Common Q portion of the protection and safety monitoring system is developed using the Common Q SPM (as modified by the SPM alternatives in WCAP-15927, Revision 4). The Common Q SPM was reviewed and approved by the NRC using the criteria of Regulatory Guide 1.172, Revision 0 and IEEE 830-1998. See Chapter 7 for a discussion of the instrumentation and control software program.

Criteria Section	Referenced Criteria	AP1000/ FSAR Position	Clarification/Summary Description of Exceptions
Reg. Guide 1.173, Rev. 0, 9/97 – Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants			
General		Exception	Westinghouse uses the Common Q SPM (as modified by the SPM alternatives in WCAP-15927, Revision 4) to develop and maintain the Common Q portion of the protection and safety monitoring system. The Common Q SPM was reviewed and approved by the NRC using the criteria of IEEE 1074-1995 as endorsed by Regulatory Guide 1.173, Revision 0. The CIM subsystem complies with Regulatory Guide 1.173, Revision 0 with the exception(s) identified below.
General	IEEE 1074-1995	Exception	The CIM subsystem takes exception to the requirements in Sections 4.1.4, 4.1.5, and 4.1.7, respectively, to perform the "Formulate Potential Approaches" and "Constraints and Benefits" activity; the "Conduct Feasibility Study" activity; and the "Refine and Finalize Idea or Need" activity. Using information from previous projects, the basic CIM subsystem design approach was already formulated at the time the project was initiated.
General	IEEE 1074-1995	Exception	The CIM subsystem takes exception to the requirement in Section 7.4.3 to consider the software requirements as an input to the development of the training program. The training plan was written to be independent of the software requirements developed later in the project. See Chapter 7 for a discussion of the instrumentation and control software program.

4. UFSAR Section 7.1, "Introduction":

Revise Tier 2 text in the third paragraph to remove the reference to WCAP-17201 (Reference 2), as follows:

Chapter 7 for the AP1000 has been written to describe the protection system hardware utilizing the Common Qualified Platform (Common Q) described in Reference 8 (which includes the NRC SER)~~, and augmented by Reference 2~~. The I&C functional requirements of the AP600, which has received Design Certification, have been retained to the maximum extent compatible with the Common Q hardware and software.

5. UFSAR Section 7.1, Subsection 7.1.2.14, "Verification and Validation":

Revise Tier 2* and Tier 2 text, as follows:

[*Adequacy of the hardware and software is demonstrated for the protection and safety monitoring system through a verification and validation (V&V) program. Details on the verification and validation program for the Common Q portion of the protection and safety monitoring system are provided in WCAP-16096-~~N~~P-A (Reference 9.*]* WCAP-16096-~~N~~P-A defines a software development process consistent with appropriate industry standards.

6. UFSAR Section 7.1, Subsection 7.1.2.14.1, "Design Process":

Revise Tier 2* and Tier 2 text, as follows:

[*WCAP-16096-~~N~~P-A (Reference 9) provides a planned design process for Common Q software development during life cycle stages:*

*** * ***

WCAP-16096-~~N~~P-A (Reference 9), WCAP-15927 (Reference 20), and NRC-approved Westinghouse Quality Management System (Reference 21) describe design processes that will be used for the Common Q portion of the AP1000 protection and safety monitoring system.]*

*** * ***

Document 5: WCAP-16096-~~N~~P-A, "Software Program Manual for Common Q™ Systems"

*** * ***

7. UFSAR Section 7.1, New Subsection 7.1.2.14.3, "Operational Process":

Add a new Tier 2 subsection 7.1.2.14.3, as follows:

7.1.2.14.3 Operational Process

A software operations plan includes administrative controls to require that the PMS and its division room are in the appropriate configuration prior to making setpoint changes. This includes requiring a channel to be bypassed prior to making setpoint changes for reactor trip or ESFAS functions. In addition, the PMS division is declared inoperable prior to making setpoint changes for blocks and resets. The administrative controls prevent the protection and safety monitoring system division room environment from interfering with protection and safety monitoring system equipment when plant personnel are making setpoint changes. The administrative controls account for local emissions from nearby equipment and activities (e.g., welding) while the maintenance test cabinet (MTC) door is open.

8. UFSAR Section 7.1, Subsection 7.1.7, "References":

Revise Tier 2* and Tier 2 references, as follows:

* * *

2. Not used. ~~[*WCAP-17201-P, Revision 0, "AC160 High Speed Link Communication Compliance to DI&C-ISG-04 Staff Positions 9, 12, 13 and 15," February 2010.]**~~

* * *

8. [*WCAP-16097-P-A (Proprietary) and WCAP-16097-NP-A (Non-Proprietary), Revision 3 ~~0~~, "Common Qualified Platform Topical Report," February 2013 ~~May 2003~~ (as modified by the Topical Report alternatives in WCAP-15927, Revision 4).*]*

9. [*WCAP-16096-P-A (Proprietary) and WCAP-16096-NP-A (Non-Proprietray), Revision 4 ~~01A~~, "Software Program Manual for Common Q™ Systems," ~~December 2004~~ February 2013 (as modified by the Software Program Manual alternatives in WCAP-15927, Revision 4).*]*

* * *

18. APP-GW-GLR-017, AP1000 Standard Combined License Technical Report, "Resolution of Common Q NRC Items," Revision 2, Westinghouse Electric Company LLC.

19. WCAP-16675-P (Proprietary) and WCAP-16675-NP (Non-Proprietary), "AP1000 Protection and Safety Monitoring System Architecture Technical Report," Revision 5. (as modified by changes provided in Appendix 7A)

20. [*WCAP-15927, Revision 4 ~~2~~ (Non-proprietary), "Design Process for AP1000 Common Q Safety Systems," April 2015 ~~November 2008~~.*]*

* * *

25. WCAP-16674-P (Proprietary) and WCAP-16674-NP (Non-Proprietary), "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," Revision 4. (as modified by changes provided in Appendix 7A)

9. UFSAR Section 7.1, Figure 7.1-2, "Common Q Standard Process and AP1000 Project-Specific Documents":

Revise the uppermost block of the Common Q Standard Process Documents in this depiction of planning documents, as shown below:

WCAP-16096-~~N~~P-A Document 5

10. UFSAR Section 7.2, "Reactor Trip," Subsection 7.2.4, "References":

Revise Tier 2 Reference 4, as shown below:

4. WCAP-16592-P (Proprietary), WCAP-16592-NP (Non-Proprietary), "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System," Revision 2 (as modified by changes provided in Appendix 7A).

11. UFSAR Appendix 7A, "INSTRUMENTATION AND CONTROLS LICENSING BASIS DOCUMENT CHANGES":

[Note: For clarity, entirely new text that is being added to UFSAR Appendix 7A is depicted in blue font in these markups; new markups to add or delete text to the existing Appendix 7A text are identified with blue underlined font or red strike-out font, respectively; and existing markups in Appendix 7A that are unchanged by this LAR are depicted with black font (underlined or strike-out) as per the current UFSAR Appendix 7A.]

- **Revise Section 7A.1, " WCAP-15775, AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," by adding an entirely new bullet for changes to Section 3.3 and revising the existing bullet for changes to Sections 4.2 and 6, as follows:**

  - **Revise Section 3.3, "Overall Instrumentation and Control Fault Tolerant Design Features," as follows:**

    The Design, Verification, and Validation Process - The design of the instrumentation and control systems hardware and software elements are controlled by a design, verification, and validation process that is described in ~~either WCAP-13383 (Reference 3) or CE-CES-195 (Reference 4)~~ [plant-specific] DCD Subsection 7.1.2.14. ~~WCAP-13383 provides details on the AP600 verification and validation plan. CE-CES-195 provides details on the Common Q verification and validation plan. Depending on the PMS system hardware used for AP1000, one of these programs will apply.~~ These processes are formal, rigorous means to detect and correct design errors before they can result in common-mode errors in the plant.

  - **Revise Section 4.2, Determining Diversity – Guideline 2, under diversity aspect number 4, Human Diversity, as follows:**

    The design, verification, and validation programs for instrumentation and control systems, as described in ~~described in~~ WCAP-16096-P-A (Reference 10) and WCAP-15927 (Reference 11) ~~WCAP-13383 (Reference 3) and CE-CES-195 (Reference 4)~~, require and specify the use of independent review. ~~It is a requirement of the DAS that different people will be responsible for its design and fabrication, including verification and validation.~~ At the system level, different design and IV&V teams are used on the DAS and PMS systems.

  - **Revise Section 6, References~~, by adding Reference 9~~, as follows:**

    3. ~~WCAP-13383, Revision 1, "AP600 Instrumentation and Control Hardware and Software Design Verification, and Validation Process Report," June 1996.~~ Deleted
    4. ~~CE-CES-195, Rev. 01, "Software Program Manual for Common Q Systems," May 26, 2000.~~ Deleted
    9. WCAP-17179, Revision 2 (as modified by changes provided in Appendix 7A), "AP1000 Component Interface Module Technical Report"
    10. WCAP-16096-P-A, Rev.4, "Software Program Manual for Common Q™ Systems," Westinghouse Electric Company LLC.
    11. WCAP-15927, Rev. 4, "Design Process for AP1000 Common Q Safety Systems," Westinghouse Electric Company LLC.

- **Revise Section 7A.3, "WCAP-17184-P, AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report," by adding a new set of changes for Reference 13 to the existing markups in the References section, as follows:**
  - **Revise the "REFERENCES" section as follows:**

    13. APP-GW-J1R-001 (Proprietary), Rev. 4 ~~2~~ "Design Process for AP1000 Common Q Safety System," Westinghouse Electric Company LLC.

    20. APP-GW-GLR-143 (Proprietary), Revision ~~0~~ 2 (as modified by changes provided in UFSAR Appendix 7A), "AP1000 Component Interface Module Technical Report," Westinghouse Electric Company LLC.

- **Revise Section 7A.4, "WCAP-16438-P and WCAP-16438-NP, FMEA of AP1000™ Protection and Safety Monitoring System," as follows:**
  - **Revise the REFERENCES section as follows:**

    6. WCAP-15775, Revision 4 (as modified by changes provided in UFSAR Appendix 7A), "AP1000™ Instrumentation and Control Defense-In-Depth and Diversity Report," Westinghouse Electric Company LLC.

    9. ~~WCAP-16096-NP-A, Rev. 1A, "Software Program Manual for Common Q Systems," Westinghouse Electric Company LLC.~~ Deleted

  - **Revise the BIBLIOGRAPHY section, as follows:**

    2. WCAP-16096-P-A, Rev.4, "Software Program Manual for Common Q™ Systems," Westinghouse Electric Company LLC.

- **Revise Section 7A.5, "WCAP-15776-NP, Safety Criteria for the AP1000 Instrumentation and Control Systems, April 2002," as follows:**

7A.5 WCAP-15776-NP, Safety Criteria for the AP1000 Instrumentation and Control Systems, April 2002

The UFSAR incorporates by reference Tier 2 document WCAP-15776-NP, Safety Criteria for the AP1000 Instrumentation and Control Systems, April 2002 See Table 1.6-1. WCAP-15776, Revision 0 (April 2002) includes the following revisions and additions as indicated by strikethroughs and underlines:

- **Revise Section 2.8, Design Basis: Reliability Methods (Paragraph 4.9 of IEEE 603-1991), as follows:**

  ~~WCAP-13383 (Reference 3), CE-CES-195~~ WCAP-16096-P-A (Reference 4), and NABU-DP-00014-GEN (Reference 5) describe planned design processes for the PMS hardware and software. A verification and validation (V&V) program demonstrates the adequacy of the hardware and software. ~~WCAP-13383 provides details on the AP600 verification and validation program. CE-CES-195~~ WCAP-16096-P-A provides details on the Common Q verification and validation program. ~~Depending on the protection and safety~~

~~monitoring system hardware used for AP1000, one of these programs will apply to AP1000.~~

- **Revise Section 3.4, Conformance to the Requirements for Quality Components and Modules (Paragraph 5.3 of IEEE 603-1991)**

  The quality of components and modules is consistent with use in a nuclear generating station safety system. The AP1000 quality assurance program conforms to GDC-1.

  Verification and Validation

  A V & V program demonstrates the adequacy of the hardware and software for the PMS. ~~Either WCAP-13383 (Reference 3) or CE-CES-195~~ WCAP-16096-P-A (Reference 4) provides details on the verification and validation program. ~~WCAP-13383 is an AP600 reference. CE-CES-195~~ WCAP-16096-P-A is a Common Q document. The software development process is consistent with the ~~following standards:~~ Regulatory Guides, as identified in DCD Appendix 1A, "Conformance with Regulatory Guides."

  * * *

  Design Process

  ~~WCAP-13383~~ WCAP-16096-P-A provides a planned design process for hardware and software development during the following life cycle stages:

  - ~~Design requirements phase~~ Concept
  - ~~System definition phase~~ Requirements Analysis
  - ~~Hardware and software development phase~~ Design
  - ~~System test phase~~ Implementation or Coding
  - ~~Installation phase~~ Test
  - Installation and Checkout
  - Operation and Maintenance
  - Retirement

  * * *

  ~~Depending on the protection and safety monitoring hardware used for AP1000, either WCAP-13383 or NABU-DP-00014-GEN describe design processes that will be used for AP1000.~~

  Commercial Dedication

  ~~WCAP-13383 (Reference 3) and CENPD-396-P~~ WCAP-16097-P-A (Reference 7) provides for the use of commercial off-the-shelf hardware and software through a commercial dedication process. Control of the hardware and software during the operational and maintenance phase is the responsibility of the Combined License applicant.

- **Section 7, References**
  - **Revise the REFERENCES section as follows:**

3. ~~WCAP-13383, Revision 1 (NP), "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report," June 1996.~~ Not Used.
4. ~~CE-CES-195~~ WCAP-16096-P-A, Rev. ~~01~~ 4, "Software Program Manual for Common Q™ Systems," ~~May 26, 2000~~ February 2013.
7. ~~CENPD-396-P~~ WCAP-16097-P-A, Rev. ~~01~~ 3, "Common Qualified Platform Topical Report," ~~May 2000~~ February 2013.

- **Add new Section 7A.6, "WCAP-16592-P and WCAP-16592-NP, Software Hazards Analysis of AP1000 Protection and Safety Monitoring System," as follows:**

7A.6 WCAP-16592-P and WCAP-16592-NP, "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System"

The UFSAR incorporates by reference Tier 2 document WCAP-16592-P, Software Hazards Analysis of AP1000 Protection and Safety Monitoring System. See Table 1.6-1. WCAP-16592, Revision 2, includes the following revisions and additions as indicated by strikethroughs and underlines.

- **Revise the Reference section, as follows:**

5. WCAP-16096-~~N~~P-A, Rev. 4 ~~1A~~, "Software Program Manual for Common Q™ Systems," Westinghouse Electric Company LLC.

- **Revise the Section 1.2, Scope, as follows:**

This report is based on the detail design of the PMS as shown in the AP1000 PMS Architecture Division Diagrams (Reference 7), the analysis of the "FMEA of AP1000 Protection and Safety Monitoring System" (Reference 3), and the software design, implementation, validation, and verification activities performed in accordance with WCAP-16096-~~N~~P-A, "Software Program Manual for Common Q™ Systems" (SPM) (Reference 5).

- **Add new Section 7A.7, " WCAP-16674-P and WCAP-16674-NP, AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," as follows:**

7A.7 WCAP-16674-P and WCAP-16674-NP, AP1000 I&C Data Communication and Manual Control of Safety Systems and Components

The UFSAR incorporates by reference Tier 2 documents WCAP-16674-P and WCAP-16674-NP, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components." See Table 1.6-1. WCAP-16674, Revision 4, includes the following revisions and additions as indicated by strikethroughs and underlines.

- **Revise the Reference section, as follows:**

1. WCAP-16097-P-A, Rev. ~~0~~ 3 (Proprietary), "Common Qualified Platform Topical Report," Westinghouse Electric Company LLC. ~~(This document is also referred to as CENPD-396-P-A, Revision 2.)~~

* * *

9. IEEE Standard 7-4.3.2-2003 ~~1993~~, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc., 2003 ~~1993~~.
10. WCAP-16096-~~N~~P-A (Proprietary), Rev. 4 ~~1A~~, "Software Program Manual for Common Q™ Systems," Westinghouse Electric Company LLC.

- **Revise Section 5.1.2, Case C – Unidirectional Network Datalink section, as follows:**

The flow of information between the two gateway subsystems is strictly from the safety subsystem to the non-safety subsystem. The unidirectional nature of the gateway is assured by the use of a single unidirectional fiber to connect the two gateway subsystems. Within the safety system, the fiber is connected to an optical transmitter. Within the non-safety system, the fiber is connected to a fiber-optic receiver. This arrangement provides electrical isolation between the systems (as required by IEEE 603-1991 {Reference 8}) and prevents all data flow (data, protocols, and handshaking) from the non-safety system to the safety system (providing the communication isolation envisioned by IEEE Standard 7-4.3.2-2003~~1993~~, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations {Reference 9}, Annex E ~~G~~).

* * *

The second part of the AOI gateway software was developed by Westinghouse. This software followed the process specified for "Important to Safety" software in WCAP-16096-~~N~~P-A, Software Program Manual for Common Q™ Systems (Reference 10) (the SPM), for safety software.

* * *

For SOE signals such as partial trip signals, reactor trip signals, and ESF actuation signals, each division provides the signals to the SOE system/interface via a unidirectional fiber-optic link. The flow of information is strictly from the safety subsystem to the non-safety SOE system/interface. The unidirectional nature of the link is assured by the use of a single unidirectional fiber. The safety end of the fiber is connected to an optical transmitter. The non-safety end of the fiber is connected to a fiber-optic receiver. This arrangement provides electrical isolation between the safety and non-safety portions of the system (as required by IEEE 603-1991 {Reference 8}) and prevents all data flow (data, protocols, and handshaking) from non-safety to safety (providing the communication isolation envisioned by IEEE 7-4.3.2-2003 ~~1993~~ {Reference 9}, Annex E ~~G~~).

- **Revise Section 5.2.1, Case D – Non-Safety Manual Control of System-Level Safety Functions and Non-Safety Interlock of PMS Test Functions section, as follows:**

  Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 8}) and prevent all but the required data flow from the non-safety system to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2-2003 ~~1993~~{Reference 9}, Annex E ~~C~~). (Note: this paragraph is repeated twice in WCAP-16674, Section 5.2.1)

- **Revise Section 5.2.2, Case E – Non-Safety Control of Safety Components section, as follows:**

  As mentioned above, the remote I/O bus that is used to connect the non-safety system to the Associated Class 1E remote node is fiber-optic. This arrangement provides electrical isolation between the safety system and the non-safety system as required by IEEE 603-1991 (Reference 8). The RNC and the communication function within the CIM implement the communications, and only the resulting discrete digital signals interface with the Class 1E priority logic in the CIM. The simple discrete signal interface from the communication function within the CIM to the Class 1E priority logic within the CIM provides the communication isolation envisioned by IEEE 7-4.3.2-2003 ~~1993~~ (Reference 9), Annex E ~~C~~.

- **Revise Section 8, Conclusions section, as follows:**

  Information is included on the data flows between the safety systems and the non-safety systems. The implementations are shown to meet the requirements of IEEE-603-1991 (Reference 8) and IEEE 7-4.3.2-2003 ~~1993~~ (Reference 9).

  Information is included on the CIM that is used to implement non-safety control of safety components. The module is shown to meet the requirements of IEEE-603-1991 and IEEE 7-4.3.2-2003 ~~1993~~.

  Information is included on the mechanisms the AP1000 I&C system provides for the manual control of the system-level safety functions and component-level functions. The mechanisms are shown to meet the requirements of IEEE-603-1991 and IEEE 7-4.3.2-2003 ~~1993~~.

- **Add new Section 7A.8, "WCAP-16675-P and WCAP-16675-NP, AP1000 Protection and Safety Monitoring System Architecture Technical Report," as follows:**

7A.8 WCAP-16675-P and WCAP-16675-NP, AP1000 Protection and Safety Monitoring System Architecture Technical Report

The UFSAR incorporates by reference Tier 2 documents WCAP-16675-P and WCAP-16675-NP, AP1000 Protection and Safety Monitoring System Architecture Technical Report. See Table 1.6-1. WCAP-16675, Revision 5, includes the following revisions and additions as indicated by strikethroughs and underlines.

- **Revise the Reference section, as follows:**

  2. WCAP-16097-~~N~~P-A (Non-Proprietary), Rev. 3 ~~0~~, Common Qualified Platform Topical Report, Westinghouse Electric Company LLC. ~~(This document is also referred to as CENPD-396-P-A, Revision 2.)~~

  23. IEEE Standard 7-4.3.2-2003 ~~1993~~, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Inc., 2003 ~~1993~~.

  31. WCAP-16096-~~N~~P-A (Non-Proprietary), Rev. 4 ~~1A~~, Software Program Manual for Common Q™ Systems, Westinghouse Electric Company LLC.

- **Revise the Forward section, as follows:**

  This document describes the Common Q implementation of the AP1000 PMS. The Common Q Platform is described in WCAP-16097-~~N~~P-A, Common Qualified Platform Topical Report (Reference 2), and WCAP-16097-P Appendix 4, Common Qualified Platform Integrated Solution (Reference 3).

- **Revise Section 3.2.2 Bistable Processor Logic to Local Coincidence Logic Communication section, as follows:**

  The PMS uses Common Q HSLs to transfer the partial trips, partial actuations, and related status information calculated in the BPL controllers to the LCL controllers. These links are used both locally within a division and externally across divisions. The links going across divisions use fiber-optic media converters and fiber-optic cable to provide the electrical isolation required by IEEE 603 (Reference 7). The links are true point-to-point links and provide the communication isolation envisioned in IEEE 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, (Reference 23), Annex E ~~G~~.

- **Revise Section 3.2.4 Integrated Communication Processor to Integrated Communication Processor Communication section, as follows:**

  The PMS uses Common Q HSLs to transfer data to support the QDPS function and data to support cross-division diagnostics between divisions. These links are only used externally across divisions. The links going across divisions use fiber-optic media converters and fiber-optic cable to provide the electrical isolation required by IEEE 603 (Reference 7). The links are true point-to-point links and provide the communication isolation envisioned in IEEE 7-4.3.2 (Reference 23), Annex E ~~G~~.

- **Revise Section 3.3.3 Isolated Unidirectional Datalink Signals to Non-Safety (Case C) section, as follows:**

  The flow of information between the two gateway subsystems is strictly from the safety subsystem to the non-safety subsystem. The unidirectional nature of the gateway is assured by the use of a single unidirectional fiber to connect the two gateway subsystems. Within the safety system, the fiber is connected to an optical transmitter. Within the non-safety system, the fiber is connected to a fiber-optic receiver. This arrangement provides electrical isolation

between the systems (as required by IEEE 603 {Reference 7}) and prevents all data flow (data, protocols, and handshaking) from the non-safety system to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2 {Reference 23}, Annex E ~~G~~).

* * *

The second part of the AOI gateway software was developed by Westinghouse. This software followed the process specified for "Important to Safety" software in WCAP-16096-~~N~~P-A, Software Program Manual for Common Q™ Systems (Reference 31) (the SPM), for safety software.

* * *

For SOE signals such as partial trip signals, reactor trip signals, and engineered safety feature (ESF) actuation signals, each division provides the signals to the SOE system/interface via a unidirectional fiber-optic link. The flow of information is strictly from the safety subsystem to the non-safety SOE system/interface. The unidirectional nature of the link is assured by the use of a single unidirectional fiber. The safety end of the fiber is connected to an optical transmitter. The non-safety end of the fiber is connected to a fiber-optic receiver. This arrangement provides electrical isolation between the safety and non-safety portions of the system (as required by IEEE 603-1991 {Reference 7}) and prevents all data flow (data, protocols, and handshaking) from non-safety to safety (providing the communication isolation envisioned by IEEE 7-4.3.2-~~1993~~ {Reference 23}, Annex E ~~G~~). It also provides functional isolation by preventing the non-safety equipment from adversely affecting the safety function. This type of interface is a variation of Case C in Figure 3-1.

- **Revise Section 3.3.4 System-Level Safety Functions from RSR Fixed-Position Switches and Non-Safety Interlock of PMS Test Functions (Case D), as follows:**

  Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 7}) and prevent all but the required data flow from the non-safety equipment to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2-~~1993~~ {Reference 23}, Annex E ~~G~~).

- **Revise Section 3.3.5 Non-Safety Control of Safety Components (Case E), as follows:**

  As mentioned above, the remote I/O bus that is used to connect the non-safety system to the associated Class 1E remote node is fiber-optic. This arrangement provides electrical isolation between the safety system and the non-safety system as required by IEEE 603 (Reference 7). The remote I/O node controller and the communication function within the CIM implement the communications, and only the resulting discrete digital signals interface with the Class 1E priority logic in the CIM. The simple discrete signal interface within the CIM provides the communication isolation envisioned by IEEE 7-4.3.2 (Reference 23), Annex E ~~G~~.

12. UFSAR Section 19.59, "PRA Results and Insights," Table 19.59-18, "AP1000 PRA-BASED INSIGHTS":

Revise …

Insight	Disposition
1. The protection and safety monitoring system (PMS) provides a safety-related means of performing the following functions: * * * The PMS software is designed, tested, and maintained to be reliable under a controlled verification and validation program written in accordance with IEEE 7-4.3.2 (1993) that has been endorsed by Regulatory Guide 1.152, Revision 1. For the Common Q portion of the PMS, this is performed in accordance with the Common Q Software Program Manual and Topical Report. Elements that contribute to a reliable software design include: * * *	Tier 1 Information * * * See App 1A for Compliance Statement for ~~(Compliance with~~ Reg. Guide 1.152~~)~~ * * *

Southern Nuclear Operating Company

ND-16-0083

Enclosure 5

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

APP-GW-GLR-017, Revision 2

Resolution of Common Q NRC Items

(LAR-15-017)

(Enclosure 5 consists of 31 pages, including this cover page)

APP-GW-GLR-017
Revision 2

February 2016

AP1000 Standard Combined License Technical Report

Resolution of Common Q NRC Items

Revision 2

Westinghouse Electric Company LLC
1000 Westinghouse Drive
Cranberry Township, PA 16066

©2016 Westinghouse Electric Company LLC
All Rights Reserved

REVISION HISTORY

RECORD OF CHANGES

Revision	Author	Description	Completed
0	Mark J. Stofko	Initial Issue	05/2006
1	Matthew A. Shakun	The following changes were made to address APP-GW-GEE-4380 and CAPAL 100320452: • Revised to make PSAI 6.1 consistent with WCAP-16097-P-A, Rev. 3, "Common Qualified Platform Topical Report" (Reference 9) • The DCD markups were also updated to reference Revision 1 of APP-GW-GLR-017	09/2015
2	Matthew A. Shakun	The following changes were made to address APP-GW-GEE-4380 and CAPAL 100355930: • Revised Introduction to clarify that GOI 7.1 is not applicable to the AP1000 design • Revised GOI 7.1 to clarify that the AI685 is not used in the AP1000 design • The DCD markups were also updated to reference Revision 2 of APP-GW-GLR-017	See EDMS

DOCUMENT TRACEABILITY & COMPLIANCE

Created to Support the Following Document(s)	Document Number	Revision
N/A		

OPEN ITEMS

Item	Description	Status
None.		

INTRODUCTION

This report summarizes the resolution of the 10 Generic Open Items (GOIs) and 14 Plant Specific Action Items (PSAIs) associated with NRC review of the Westinghouse Common Qualified (Common Q) Platform for the AP1000 plant specific design. The resolution of generic open items and plant-specific action items resulting from NRC review of the I&C platform is identified in AP1000 Design Control Document (DCD, Reference 1) Subsection 7.1.6. The resolution for generic open items and plant-specific action items is identified as COL Information Item 7.1-2 (FSER {Reference 2} Action Items 7.1.7-1 and 7.2.3-1) in DCD Subsection 7.1.6. GOI item 7.9 also provide information that was requested by ITAAC 2.5.2-8. Reference to this item will be will be made in future NRC ITAAC closure process. At this time, the ITAAC closure process is being developed by NRC and Industry.

COL Information item 7.1-2 is as follows:

> Combined License applicants referencing the AP1000 certified design will provide resolution for generic open items and plant-specific action items resulting from NRC review of the I&C platform. This will include definition of a methodology for overall response time testing.

For the GOIs, resolution was provided as part of the Common Q , NRC review process. The NRC has issued an SER that generically closed all of the GOIs, with the exception of GOI item 7.8. Westinghouse will be submitting a generic Common Q report to close GOI 7.8. For GOIs, 7.2 thru 7.7, the generic resolutions that was provided to NRC and reviewed and approved (References 4,6,7) are applicable to the AP1000 design. For items GOI 7.1, 7.8, 7.9, and 7.10, additional AP1000 specific information is provided in this report to supplement to Common Q generic design. A discussion of each GOI is provided in the report. The generic information provided in the NRC review of Common Q and the additional information provided in this report provides closure of all of the GOI items for AP1000.

As part of the review process, the NRC also issued Plant Specific Action Items 6.1 thru 6.13. These action items were provided by the NRC as a check list for any utility that would be implementing a Common Q I&C system(s) up-grade. The PSAIs were written for an operating plant implementing a Common Q upgrade, therefore some of the language, may not directly be applicable to a new plant. This report provides a discussion on how each of the PSAIs either have been addressed or will be addressed for the AP1000 design. In each case where a PSAI has not been addressed in the existing design, reference to an ITAAC that will provide the requested information for the plant action item. This report provides a discussion of how each PSAI is addressed.

TECHNICAL BACKGROUND AND CONCLUSIONS

Background

By letter dated June 5, 2000, Westinghouse (formerly CE Nuclear Power) submitted Reference 3 to the NRC for review, describing the design of the Common Qualified (Common Q) platform for safety-related instrumentation and control (I&C) applications in nuclear power plants.

Reference 4 is the NRC safety evaluation (SE) report regarding the Reference 3 topical report. The SE provided the results of the NRC staff's review of the topical report, the accompanying appendices, and other supporting documents. Based on the information provided and the review conducted, the staff concluded that the design of the Common Q platform meets the relevant NRC regulatory requirements and is acceptable for safety-related instrumentation and control (I&C) applications in nuclear power

plants, subject to the satisfactory resolution of the generic open items (GOI) listed in Section 7.0 of the SE, and the plant specific action items (PSAI) listed in Section 6.0 of the SE.

The Common Q platform is a computer system consisting of a set of commercial-grade hardware and previously developed software components dedicated and qualified for use in nuclear power plants. The Common Q platform was developed by CENP from the standard AC160 computer system developed by ABB Automation Products, GmbH (ABB Products) of Europe. The Common Q platform is loaded with plant-specific application software to implement various nuclear plant safety system applications. The hardware components of the platform are:

- Advant Controller 160 (AC160) with PM646A processor module
- S600 input and output (S600 I/O) modules
- Bus communication interface (CI631) modules
- Power supply modules
- Communication systems
- Flat-panel display system (FPDS)
- Component Interface Module (CIM)
- Watchdog timer
- AF100 Interface (C1631)

The AC160 software, residing on flash PROM in the processor module, consists of a real-time operating system, task scheduler, diagnostic functions, communication interfaces and plant specific application programs. The application program is created using the Asea Brown Boveri (ABB) Master Programming Language (AMPL) Configuration Control (ACC) software development environment that includes a function block library for creating specific logic for the application.

The safety-related I&C systems based on the application of Common Q platforms provide protection against unsafe reactor operation during steady state and transient power operations. They also initiate selected protective functions to mitigate the consequences of design basis events and accidents, and to safely shut down the plant by either automatic means or manual actions.

To ensure that the digital I&C systems are implemented properly, the staff considered regulatory requirements, technical positions, guides, and standards in the Standard Review Plan (SRP), (NUREG-0800) Chapter 7, Revision 4, June 1997, in the review of the Common Q platform design.

Conclusions

This report addresses the resolution of generic open items (GOI) and plant specific action items (PSAI) as requested by Combined License Information Item 7.1-2 of the AP1000 Design Control Document (DCD), Table 1.8-2. These items were identified during the NRC's review of the Westinghouse Topical Report WCAP 16097-P-A (Common Q Platform). The GOIs and PSAIs apply to the AP1000 Protection and Safety Monitoring System (PMS) as described in this report.

Included, as part of the GOI 7.9 resolution, is a description of communications between AP1000 safety and non-safety systems, resulting in the following additional conclusions:

The PMS provides process signals to the Plant Control System (PLS) through the Advant to Ovation Interface (AOI). This is implemented with a physically unidirectional fiber optic data link that serves as an isolation device that prevents credible faults from propagating into the PMS from the PLS. (DCD Tier 1 (ITAAC) 2.5.2-8, Item 7.a)

The PMS provides process signals to the Data Display and Processing System (DDS) through the Advant to Ovation Interface (AOI). This is implemented with a physically unidirectional fiber optic data link that serves as an isolation device that prevents credible faults from propagating into the PMS from the DDS. (DCD Tier 1 (ITAAC) 2.5.2-8, Item 7.b)

The data communication between the safety system and non-safety systems does not inhibit the performance of the safety function. (DCD Tier 1 (ITAAC) 2.5.2-8, Item 7.c)

The priority logic in the Component Interface Module ensures that the automatic safety functions and Class 1E manual controls both have priority over the non-Class 1E soft controls. (DCD Tier 1 (ITAAC) 2.5.2-8, Item 7.d)

GENERIC OPEN ITEMS

The NRC staff identified 10 generic open items (GOIs) in Section 7 of the Reference 4 safety evaluation of the Common Q platform. Each GOI and its resolution are presented below.

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.

GOI 7.1 Resolution

A new analog input (AI) module, the AI685, has been developed and qualified. The previous S600 resistance-temperature detector (RTD) and thermocouple (T/C) modules did not have adequate sampling time for inputs required for protection. The AI685 can be configured for use as a voltage, RTD, or T/C analog input and has been qualified for environmental, seismic and EMC conditions. The AI685 design and qualification are documented in (Reference 5). This report was submitted to the NRC in August 2002.

On February 24, 2003 the NRC issued Reference 6. This report states that the AI685 analog input module is acceptable for use in safety systems in nuclear power plants. Also, the staff reviewed the changes that incorporate the AI685 into Revision 2 of the main body of the topical report and concluded that these changes are appropriate and acceptable.

Item GOI 7.1 was previously closed by the NRC by the Common Q review process. This resolution is not applicable since the AI685 is not used in the AP1000 design. See PSAI 6.1 for which S600 modules are used in the AP1000 design.

GOI 7.2

Westinghouse (formerly CENP) has not yet finalized the selection of the Common Q power supplies.

GOI 7.2 Resolution

The Common Q Power Supply System has been developed and qualified for environmental, seismic and EMC conditions. This is documented in Reference 5. This report was submitted to the NRC in August 2002.

On February 24, 2003 the NRC issued Reference 6. This report states that the staff has audited the development of the supplemental Common Q hardware and finds that Westinghouse has continued to follow its prescribed procedures. The staff concluded on that basis that the Common Q power supplies, as well as the other supplemental Common Q hardware components included in the Summary Qualification Report, are manufactured and/or dedicated in accordance with the applicable regulatory 10CFR Part 50, Appendix B, quality assurance requirements.

Item GOI 7.2 was previously closed by the NRC by the Common Q review process. This resolution is applicable to the AP1000 design.

GOI 7.3

Westinghouse (formerly CENP) has not submitted information on the design or dedication of the hardware watchdog timer and it has not yet been subjected to testing for environmental qualification.

GOI 7.3 Resolution

The internal PM646A watchdog timer meets the requirements for this on-line monitoring tool for Common Q system applications. Environmental qualification testing of the PM646A has been completed. This is documented in Reference 5. This report was submitted to the NRC in August 2002. A revision to the Common Q topical report was also submitted that describes the use of the internal PM646A watchdog timer.

On February 24, 2003 the NRC issued Reference 6. This report states that the staff has concluded that the internal PM646A watchdog timer has been qualified to meet the EMC, environmental, and seismic requirements for digital I&C safety systems in nuclear power plants to stated conditions. Westinghouse has acceptably addressed the staff's concerns regarding the qualification of the Common Q components. Also, the staff has reviewed the substitution of the built-in hardware watchdog timer function for the previously planned separate hardware watchdog timer module and concluded that the substitution of the built-in watchdog timer function in the design continues to meet the applicable regulatory requirements. The staff concluded, therefore, that these changes to the text in the topical report and appendices are appropriate and acceptable.

Item GOI 7.3 was previously closed by the NRC by the Common Q review process. This resolution is applicable to the AP1000 design.

GOI 7.4

Westinghouse (formerly CENP) has committed to arrange a value-added reseller agreement with QSSL that is similar to BA AUT-99-ADVANT-00, the value-added reseller agreement it has with ABB products. A value-added reseller agreement is needed to satisfy the configuration control and incoming inspection requirements of EPRI TR-106439.

GOI 7.4 Resolution

On June 22, 2001 the NRC issued Reference 7. This report states that the staff has reviewed the value-added reseller agreement with QNX Software Systems Limited (QSSL), the vendor for the flat panel display system (FPDS) operating system and display system, and concludes that it satisfies the configuration control and incoming inspection guidance of EPRI TR-106439. The reseller agreement is, therefore, acceptable.

Item GOI 7.4 was previously closed by the NRC by the Common Q review process. This resolution is applicable to the AP1000 design.

GOI 7.5

Westinghouse (formerly CENP) will perform additional EMC tests and measurements on the PM646.

GOI 7.5 Resolution

The PM646 processor module has been modified to the PM646A. This modification involved the removal of an internal terminating resistor for the High-Speed Data Links (HSLs). The link termination resistor is now external to the module, permitting high-speed data link output to multiple processors using a multi-drop configuration. Additional EMC tests and measurements were performed using the PM646A. These tests are documented in Reference 5. This report was submitted to the NRC in August 2002. A revision to the Common Q topical report was also submitted that describes the modification of the PM646 to the PM646A.

On February 24, 2003 the NRC issued Reference 6. This report states that the staff concluded that the internal PM646A processor module has been qualified to meet the EMC, environmental, and seismic requirements for digital I&C safety systems in nuclear power plants to stated conditions. Westinghouse has acceptably addressed the staff's concerns regarding the qualification of the Common Q components. Also, the staff has reviewed the change in resistor in the processor module and concurred that the resistor change is inconsequential and is, therefore, acceptable. The staff concluded that the PM646 and PM646A processor modules may be used interchangeably to suit the configuration requirements of the specific application.

Item GOI 7.5 was previously closed by the NRC by the Common Q review process. This resolution is applicable to the AP1000 design.

GOI 7.6

Westinghouse (formerly CENP) has not yet conducted seismic and environmental qualification testing on the non-AC160 hardware components. Items not yet tested include the FPDS, watchdog timer, and power supply modules.

GOI 7.6 Resolution

Seismic and environmental qualification testing on the non-AC160 hardware components has been completed. These components include the FPDS and the power supply modules. The external watchdog timer is no longer required. The internal PM646A watchdog timer meets the requirements for this on-line monitoring tool for Common Q system applications (refer to resolution of GOI 7.3 above). The seismic and environmental testing is documented in Reference 5. This report was submitted to the NRC in

August 2002. A revision to the Common Q topical report was also submitted that describes the use of the internal PM646A watchdog timer.

On February 24, 2003 the NRC issued Reference 6. This report states that the staff has audited the development of the supplemental Common Q hardware and finds that Westinghouse has continued to follow its prescribed procedures. The staff concluded on that basis that the supplemental Common Q hardware components included in the Summary Qualification Report are manufactured and/or dedicated in accordance with the applicable regulatory 10CFR Part 50, Appendix B, quality assurance requirements. The staff concluded that Westinghouse has acceptably addressed the staff's concerns regarding the qualification of the Common Q components, both AC160 and non-AC160.

Item GOI 7.6 was previously closed by the NRC by the Common Q review process. This resolution is applicable to the AP1000 design.

GOI 7.7

The staff has reviewed the information in the SVVP about software module testing and finds that the information provided is not sufficient for the staff to arrive at a conclusion about the adequacy of the scope of the tests for validating a software module.

GOI 7.7 Resolution

On June 22, 2001 the NRC issued Reference 7. This report states that Westinghouse submitted additional information indicating in which sections of CE-CES-195, Rev. 01, "Software Program Manual for Common Q Systems", and topical report CENPD-396-P, Rev. 1, "Common Qualified Platform," the staff would find the Westinghouse procedures for performing software module testing. The staff has reviewed the indicated sections and concludes that the procedures specified therein satisfy the software verification and validation program (SVVP) requirements of IEEE Std 7-4.3.2-1993 with regard to testing of software modules and are, therefore, acceptable.

Item GOI 7.7 was previously closed by the NRC by the Common Q review process. This resolution is applicable to the AP1000 design.

GOI 7.8

Westinghouse (formerly CENP) needs to provide in future submittals the design information for the loop controllers to support their diversity from the Common Q components.

GOI 7.8 Resolution

This GOI relates to the "level 3 loop controllers" referenced in the Common Q topical report integrated solution (Appendix 4). The level 3 loop controllers (LCs) provide component control based on signals from the ESFAS. Westinghouse is submitting a Common Q revision(June 2006) to address this issue.

In the AP1000 application, the CIM is used to combine signals from the PLS non-safety system soft controls and from the redundant ILCs in the PMS. Demand signals from the DAS automatic functions and the DAS manual switches bypass the CIM and interface to redundant component actuators. The CIM is configured to operate in state-based priority for the AP1000 application. This allows the preferred failure mode of the component to have the highest priority. The AP1000 application is shown in Figure 1.

With the generic submittal to the NRC on the CIM and the information presented above, this issue can be closed for AP1000.

GOI 7.9

The staff has reviewed the approach for the integrated solution of using the ITPs and the AF100 buses to provide separation of safety and non-safety signals and finds that there is not sufficient detail to permit an evaluation against the independence requirements set forth in IEEE Std 7-4.3.2 (Reference 8). This must be the subject of a future {Westinghouse (formerly CENP)} submittal.

GOI 7.9 Resolution

On June 22, 2001 the NRC issued a Safety Evaluation Report, Reference 7. This report states that Westinghouse has revised Appendix 4, "Common Qualified Platform Integrated Solution," to provide additional information on the use of the interface and test processors (ITPs) and the AF100 buses to provide separation of safety and non-safety signals. The staff has reviewed the revised information in Appendix 4, Rev. 2 on the use of the ITPs and the AF100 buses to provide separation of safety and non-safety signals and finds that the conceptual approach as presented therein is consistent with the independence requirements set forth in IEEE Std 7-4.3.2. The staff, therefore, concludes that this conceptual approach may be used for guidance for the anticipated application-specific and plant-specific designs involving the integration of multiple Common Q digital instrumentation and control (I&C) upgrades. This closes GOI 7.9 as far as the conceptual approach is concerned, but the evaluation of each forthcoming design remains a plant-specific action item because the staff finds that the forthcoming details of the actual designs may require an evaluation against the independence requirements for safety systems in specific nuclear power plants.

The following plant-specific design information is provided for AP1000 communication functions to close GOI 7.9. Although conceptually the same, the AP1000 I&C system differs in some details from the integrated solution described in Appendix 4, "Common Qualified Platform Integrated Solution." These differences, as they apply to GOI 7.9, are described below.

The AP1000 I&C system implements safety to non-safety communications and non-safety to safety communications in different ways.

Safety to Non-Safety Communication

The safety to non-safety communication is implemented with the Advant to Ovation Interface (AOI). The function of this interface is to provide dataflow from the AF100 bus of the Common Q safety system to the data highway of the Ovation non-safety system. The physical medium used is a dedicated physically unidirectional fiber optic Fast Ethernet data link. One node of the Fast Ethernet data link is the Maintenance and Test Panel (MTP) flat panel display system in the PMS. The other node of the Fast Ethernet data link is a non-safety workstation within DDS, that is a drop on the non-safety real-time data network. This arrangement is shown in Figure 2.

As mentioned above, the dedicated Fast Ethernet link used to connect the safety system to the non-safety system is fiber optic and is physically unidirectional. This arrangement provides electrical isolation between the systems and prevents all dataflow (data, protocols and handshaking) from the non-safety system to the safety system. Thus:

1. The PMS provides process signals to the DDS through isolation devices. The unidirectional fiber optic datalink serves as the an isolation device that prevents credible faults from propagating into the PMS from the DDS. (DCD Tier 1 (ITAAC) 2.5.2-8, Item 7.b)

2. Since the PLS utilizes the DDS network, the PMS also provides process signals to the PLS through DDS. Again, the unidirectional fiber optic datalink serves as an isolation device that prevents credible faults from propagating into the PMS from the DDS. (DCD Tier 1 (ITAAC) 2.5.2-8, Item 7.a)

3. Since the physical unidirectional nature of the connection prevents all dataflow from non-safety system to safety system, the data communication between the safety system and the non-safety systems does not inhibit the performance of the safety function. (DCD Tier 1 (ITAAC) 2.5.2-8, Item 7.c)

Non-Safety to Safety Communication

The non-safety to safety dataflow is not implemented using communication links; rather it is implemented using discrete digital signals. These signals are used to implement non-safety manual ESF system level actuations, manual blocks and resets, manual reactor trip, and manual component level controls.

The non-safety manual ESF system level actuations, manual blocks and resets, manual reactor trip originate from dedicate switches in the RSW.

The manual component controls originate in the PLS. To reduce the number of signals (cables) that must be run from the non-safety system to the safety system, the non-safety system's remote I/O capability will be used to deliver the signals to the safety system. Specifically, a remote I/O node from the non-safety system will be physically located within each division of the safety system. The remote I/O node will be electrically isolated from the non-safety system by the fiber optic remote I/O bus. The node controller will be powered by the safety system and will be qualified as Associated Class 1E equipment.

The remote I/O node will include one or more Class 1E component interface modules (CIM). Internally these modules contain the equivalent of a digital output module. The resulting signals, corresponding to the desired functions, are made available to non-processor based priority logic also contained in the module. The priority logic within the CIM combines the actuation requests with Class 1E automatic action signals and the Class 1E manual action requests from the PMS ESFAS subsystem. If conflicting demands are present, the safe state of the component takes priority.

As mentioned above, the remote I/O bus that is used to connect the non-safety system to the Associated Class 1E remote node controller is fiber optic. This arrangement provides electrical isolation between the safety system and the non-safety system as required by IEEE 603-1991 (Reference 1). The remote I/O node implements the communication function and only the resulting digital signals are available to the Class 1E priority logic in the CIM. The simple discrete signal interface within the CIM provides the communication isolation envisioned by IEEE 7-4.3.2-1993, Annex G (Reference 15). The priority logic within the CIM provides functional isolation by only implementing the functionality defined in the PMS functional design. Thus:

1. The data communication between the non-safety system and the safety systems does not inhibit the performance of the safety function. (DCD Tier 1 (ITAAC) 2.5.2-8, Item 7.c)

2. The Class 1E automatic safety functions and the Class 1E manual controls both have priority over the non-Class 1E demands. (DCD Tier 1 (ITAAC) 2.5.2-8, Item 7.d)

The generic closure of this item provided in reference 3 and the AP1000 implementation described above allows item GOI 7.9. to be closed for the AP1000 design.

GOI 7.10

The evaluation of the design for the multi-channel operator station control for the integrated solution requires detail beyond the scope of the present submittals.

GOI 7.10 Resolution

Common Q multi-channel operator stations are not used in the AP1000 design.

In AP1000, non-safety Ovation Workstations provide for component control of safety components. Non-safety control workstations are interfaced to the CIMs in PMS via Ovation Controllers. There are four Ovation Controllers, one per division. Separation between the safety and non-safety systems is provided by qualified 1E isolators. The CIMs arbitrate between inputs from the redundant ILCs and input from the non-safety Ovation Workstations. This is described in more detail in the resolution to GOI 7.8 above.

This closes GOI 7.10 for AP1000.

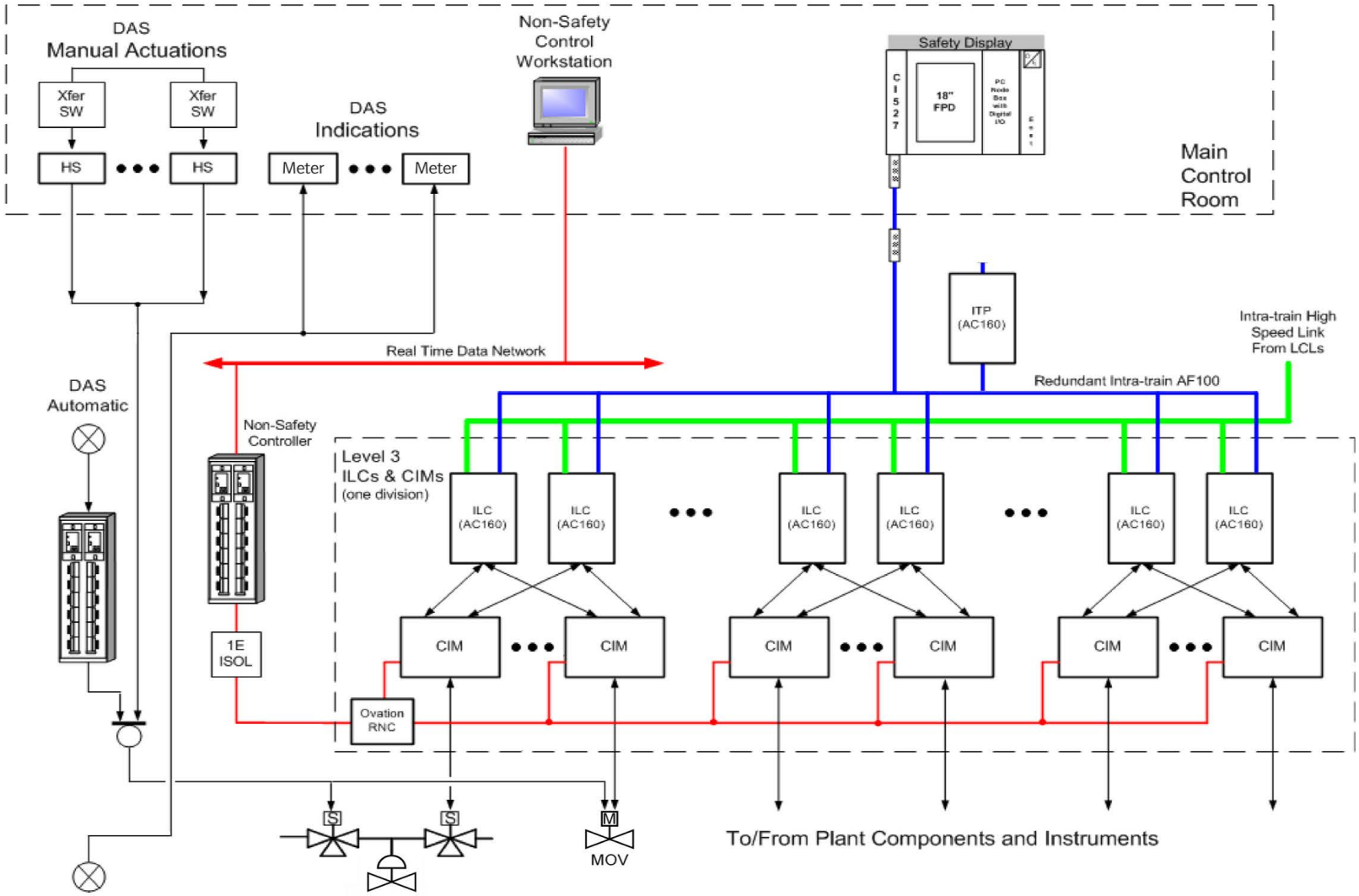


Figure 1. Component Logic System – AP1000 Application

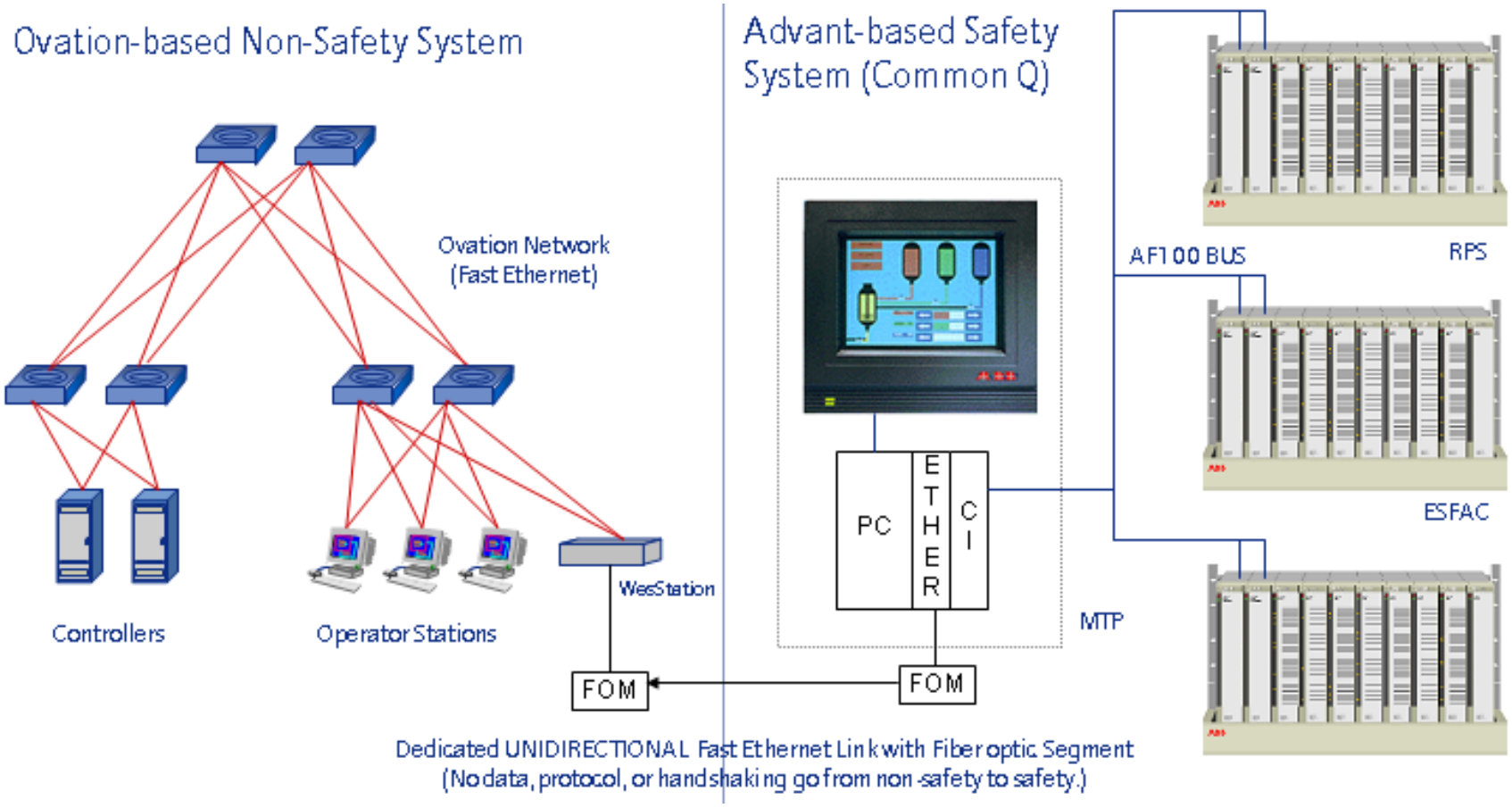


Figure 2. Safety to Non-Safety Communication

PLANT SPECIFIC ACTION ITEMS

The NRC staff identified 14 plant specific action items (PSAIs) in Section 6 of the Reference 4 safety evaluation of the Common Q platform. Each PSAI and its resolution are presented below.

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.

PSAI 6.1 Resolution

The suitability of all new components is assessed to meet applicable requirements in accordance with the Quality Assurance Program. Performance requirements for these components are assured, for example, by specifying them in purchase contracts, observing vendor testing and analysis, reviewing vendor documentation, performing design reviews by the engineering department, and by performing validation tests after installation. The Quality Assurance Program is described in DCD Chapter 17 (Reference 1).

The PMS input/output categories and the S600 input/output module used to provide the interface are provided in Table 3-1 below.

Table 3-1. PMS Input/Output Signals

Item	I/O Signal Type	S600 I/O Module
1	Pulse input	DP620
2	Current input	AI688(1)
3	Voltage input	AI688(1)
4	Resistance Temperature Detectors (RTD) input	AI687(1)
5	Mili-volt input (thermocouple inputs)	AI687(1)
6	Contact input	DI621
7	Digital input	DI621
8	Voltage output	AO650
9	Contact output to Air Operated Valve	DO620
10	Contact output to Hydraulic Operated Valve	DO620
11	Contact output to Motor Operated Valve	DO620
12	Contact output to Solenoid Operated Valve	DO620
13	Contact output to Squib Valve	DO620
14	Contact output to Circuit Breaker	DO620

Note:
1. These Common Q modules are consistent with WCAP-16097-P-A, “Common Qualified Platform Topical Report” (Reference 9).

The S600 input and output modules comply with EPRI –TR-107330. The electrical characteristics of the input / output modules satisfy the interface requirements of the external components.

The S600 Input/Output modules are designed to fully meet the functional and signal interface requirements for the safety system input sensors and output loads. The S600 Input/Output modules are demonstrated to be capable of performing their design function by successful completion of testing, culminating in a Factory Acceptance Test (FAT) performed by the vendor. Acceptance criteria is based on the system requirements specification.

This addresses PSAI 6.1 for AP1000.

PSAI 6.2

A hardware user interface that replicates existing plant capabilities for an application may be chosen by a licensee as an alternative to the FPDS. The review of the implementation of such a hardware user interface would be a plant-specific action item.

PSAI 6.2 Resolution

AP1000 safety systems utilize the Flat Panel Display System (FPDS) as developed by Westinghouse for Common Q safety systems. An alternative hardware interface is not used. Therefore, PSAI 6.2 is not applicable to AP1000.

This addresses PSAI 6.2 for AP1000.

PSAI 6.3

If a licensee installs a Common Q application that encompasses the implementation of FPDS, the licensee must verify that the FPDS is limited to performing display and maintenance functions only, and it is not to be used such that it is required to be operational when the Common Q system is called upon to initiate automatic safety functions. The use of the FPDS must be treated in the plant specific FMEAs.

PSAI 6.3 Resolution

On June 22, 2001, the NRC issued Reference 7. This report states that this action item has been resolved and is considered closed. Therefore, no further evaluation is required.

This addresses PSAI 6.3 for AP1000.

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.

Westinghouse configured the Common Q test specimen 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.

PSAI 6.4 Resolution

The Common Q safety equipment is located in the Auxiliary Building in a mild (non-harsh) environment. Therefore, age related degradation is expected to be insignificant for temperature and humidity.

The AP1000 temperature and humidity conditions for qualification of protection and safety monitoring system equipment are presented in DCD Appendix 3D (Reference 1). Temperature and humidity qualification of the protection and safety monitoring system equipment is covered by DCD Tier 1 (ITAAC) 2.5.2, Item 4 (Reference 1).

The protection and safety monitoring system seismic Category I equipment will be tested or analyzed to confirm that it can withstand seismic design basis loads without loss of safety function. The seismic qualification of the protection and safety monitoring system seismic Category I equipment is covered by DCD Tier 1 (ITAAC) 2.5.2, Item 2 (Reference 1).

The protection and safety monitoring system equipment will be tested or analyzed to confirm that it has electrical surge withstand capability (SWC), and can withstand the electromagnetic interference (EMI), radio frequency interference (RFI), and electrostatic discharge (ESD) 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) (Reference 1).

The as tested AP1000 PMS Architecture Diagrams will be included in testing reports covered by DCD Tier 1 ITAAC 2.5.2 (Reference 1). 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.

The completion of these activities shall be confirmed by the referenced ITAACs. This addresses PSAI 6.4 for AP1000.

PSAI 6.5

On the basis of its review of the Westinghouse software development process for application software, the staff concludes that the SPM specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the staff or others to evaluate the quality of design features upon which the safety determination will be based. The staff will review the implementation of the life cycle process and the software life cycle process design outputs for specific applications on a plant specific basis.

PSAI 6.5 Resolution

In accordance with the Quality Assurance Program, administrative control procedures are used to establish software quality assurance and configuration management for process computer software, firmware and associated software development, computer systems, and associated documentation. They ensure that the integrity of a process software product is known and preserved throughout its life cycle from development to retirement. These controls also apply to the development tools and systems used to develop and test process software. The Quality Assurance Program is described in DCD Chapter 17 (Reference 1). The software life cycle process is covered by DCD Tier 1 (ITAAC) 2.5.2, Item 11 (Reference 1).

The completion of this activity shall be confirmed by the referenced ITAAC. This addresses PSAI 6.5 for AP1000.

PSAI 6.6

When implementing a Common Q safety system (i.e. PAMS, CPCS, or DPPS), the licensee must review Westinghouse's timing analysis and validation tests for that Common Q system in order to verify that it satisfies its plant specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the safety analysis report.

PSAI 6.6 Resolution

The accuracy and response time of the AP1000 safety systems is commensurate with the Chapter 15 Safety Analysis. The setpoint analysis and response time are covered by DCD Tier 1 (ITAAC) 2.5.2, Item 10 (Reference 1).

The completion these of activities shall be confirmed by the referenced ITAACs. This addresses PSAI 6.6 for AP1000.

PSAI 6.7

The OM and the MTP provide the human machine interface for the Common Q platform. Both the OM and MTP will include display and diagnostic capabilities unavailable in the existing analog safety systems. The Common Q design provides means for access control to software and hardware such as key switch control, control to software media, and door key locks. The human factors considerations for specific applications of the Common Q platform will be evaluated on a plant-specific basis.

PSAI 6.7 Resolution

The human factors engineering program for AP1000 is described in DCD Chapter 18 (Reference 1). PSAI 6.7 will be addressed by DCD Tier 1 (ITAAC) 3.2 (Reference 1). Completion of this item will address PSAI 6.7.

PSAI 6.8

If the licensee installs a Common Q PAMS, CPCS or DPPS, the licensee must verify on a plant-specific basis that the new system provides the same functionality as the system that is being replaced, and meets the functionality requirement applicable to those systems.

PSAI 6.8 Resolution

The AP1000 is a new plant safety system installation; therefore, PSAI 6.8 is not applicable to AP1000.

PSAI 6.9

Modifications to plant procedures and/or TS due to the installation of a Common Q safety system will be reviewed by the staff on a plant-specific basis. Each licensee installing a Common Q safety system shall submit its plant-specific request for license amendment with attendant justification.

PSAI 6.9 Resolution

The COL application will includes Technical Specification changes that are written specifically for the I&C platform implemented on the plant to address COL item 16.1-1. Plant procedures are addressed in COL item 13.5-1. Completion of these COL commitments addresses PSAI 6.9.

PSAI 6.10

A licensee implementing any Common Q applications (i.e., PAMS, CPCS, or DPPS) must prepare its plant specific model for the design to be implemented and perform the FMEA for that application.

PSAI 6.10 Resolution

A FMEA (APP-GW-GLR-018) has been prepared and is being transmitted separately in response to COL item 7.2-1, as discussed in the DCD Section 7.2.3.

This addresses PSAI 6.10 for the AP1000.

PSAI 6.11

If a licensee installs Common Q PAMS, CPCS, DPPS or Integrated Solution, the licensee shall demonstrate that the plant-specific Common Q application complies with the criteria for defense against common-mode failure in digital instrumentation and control system and meets the requirements of HICB BTP-19.

PSAI 6.11 Resolution

The AP1000 evaluation of Defense-in-Depth and Diversity is described in DCD Sections 7.1 and 7.7 and approved in NRC NUREG 1793 (Reference 2).

This addresses PSAI 6.11 for AP1000.

PSAI 6.12

A licensee implementing a Common Q DPPS shall define a formal methodology for overall response time testing.

PSAI 6.12 Resolution

The formal methodology for overall response time testing is based on the following:

The AP1000 Protection and Safety Monitoring System is designed to automatically initiate a protective action whenever a condition monitored by the system reaches a preset level. The protective action may consist of a reactor trip and/or an ESF actuation. In either case, the response time of the protective function shall be fast enough to limit the consequences of an event to acceptable levels, as verified by the accident analyses in DCD, Chapters 6 and 15.

A reactor trip signal acts to open the reactor trip circuit breakers, which feed power to the Control Rod Drive Mechanisms (CRDMs). The loss of power to the CRDMs causes the mechanisms to release the Rod Control Cluster Assemblies (RCCAs), which then fall by gravity into the core. There are various instrumentation delays associated with each trip function, including delays in signal generation, in opening the trip breakers, and in the release of the rods by the mechanisms.

For ESF actuation signals, the response time does not include the time required for the final actuated devices to change state (e.g., opening or closing of a valve). The accident analysis models assume time delays between the time that a process limit is reached and the necessary responsive action occurs.

The response time numbers used in the safety analysis models are chosen to be greater than the expected equipment response times. For example, the modeled delay times correspond to the time the trip condition is reached to the time the control rods are free and begin to fall.

During system integration testing (SIT) at the factory, response time is measured for all trip paths. This testing is performed according to a written procedure. The data is recorded and compared to allowable values. The allowable values are determined by performing a worst case timing analysis of all processors in the trip path.

After the equipment is installed in the plant, the overall response time of the trip channel must be verified to assure that the actual response time is less than the response time assumed in the accident analysis. In practice, this is difficult to measure because of the widespread location of all the components. Typically, more than one test is required to measure all components in the trip path, and the results from the individual tests are summed to obtain the overall response time. Response time testing is included in the preoperational testing of the Protection and Safety Monitoring System as described in DCD Section 14.2.9.1.12.

This testing will form the basis for the report that will be used to meet DCD Tier 1 (ITAAC) 2.5.2, Item 10 (Reference 1)

The completion of these activities shall be confirmed by the referenced ITAACs. This addresses PSAI 6.12 for AP1000.

PSAI 6.13

The analysis of the capacity of the shared resources to accommodate the load increase due to sharing.

PSAI 6.13 Resolution

The shared resource issue relates to multiple Common Q based systems using the same resources such as the AF100 bus or a Safety Display. An analysis will be performed to ensure that the capacity of shared resources for AP1000 safety systems is commensurate with anticipated loads. This issue will be addressed as part of the design process that is covered by DCD Tier 1 (ITAAC) 2.5.2, Item 11 (Reference 1).

The completion of these activities shall be confirmed by the referenced ITAACs. This will address PSAI 6.13 for AP1000.

PSAI 6.14

The licensee must ascertain that the implementation of the Common Q does not render invalid any of the previously accomplished TMI action items.

PSAI 6.14 Resolution

The AP1000 is a new plant without any “previous accomplished TMI action items. The AP1000 TMI features as discussed in Section 1.9 of the DCD are fully compatible with Common Q implementation. This addresses PSAI 6.14.

REGULATORY IMPACT

The use of the Common Q platform is discussed in the FSER (Reference 2) Subsection 7.1.3. The generic open items are discussed in FSER Subsections 7.1.7 and 7.2.3. The information included in this report

will close open items identified in the FSER and impact those write-ups. The information presented in this report is consistent with the conclusions presented in the NRC Final Safety Evaluation Report for the AP1000.

The changes to the DCD presented in this report do not represent an adverse change to the design function of the protection system or to how design functions are performed or controlled. The changes to the DCD do not involve revising or replacing a DCD – described evaluation methodology nor involve a test or experiment not described in the DCD. The DCD change does not require a license amendment per criteria of VIII. B.5.b of Appendix D to 10 CFR Part 52.

The closure of the generic and plant specific open items and associated DCD changes do not impact features that mitigate severe accidents. The capability of the protection system to automatically and manually actuate systems and components that mitigate severe accidents is not adversely impacted. Therefore, closure of the generic and plant specific open items and associated DCD changes does not affect resolution of severe accident issues and does not require a licensing amendment based on the criteria of VIII.B.5.c of Appendix D to 10 CFR Part 52.

DCD MARKUP

Revise the Second paragraph of 7.1.2.3 as follows:

> The ESF coincidence logic performs the appropriate voting operation on the bistable signals and generates the system-level ESF logic commands including the system-level manual commands. This includes both the manual system level actuations from the dedicated Class 1E switches in the MCR and those from the non-safety controls in the RSW. The~~se~~ ESF actuation subsystems decode the system commands and actuate the final equipment through the interlocking logic specific to each component. Component-level actuation signals are sent from the main control room to the ESF actuation subsystems over redundant data highways. Component status is transmitted from the ESF actuation subsystems to the main control room over the same redundant data highways. Those components used for safe shutdown can also be controlled from the remote shutdown workstation.
>
> In the absence of a safety system demand, the non-safety system is able to control the safety components. This function is arbitrated by the Class 1E Component Interface Modules (CIMs).

Revise Subsection 7.1.2.8 as follows:

7.1.2.8 Communication Functions

> The communication functions provide information from the plant protection subsystem, the ESF coincidence logic, the ESF actuation subsystems, and the QDPS subsystems to external systems. This includes outputs to the plant control system and the data display and processing system. Isolation devices provide electrical isolation between the protection and safety monitoring system and the external systems. The communication functions also provide soft control information from the nonsafety system to the safety system for operator-initiated actuation and component control.
>
> The communication functions are accomplished via channelized gateways and individual analog and digital signals as shown in Figure 7.1-1.

Safety to Non-Safety Communications

The PMS Gateway interfaces the safety PMS to the nonsafety real-time data network, which supports the remainder of the instrumentation and control system. The Gateway has two subsystems. One is the safety subsystem that interfaces to the Plant Protection Subsystem, the Engineered Safety Features Coincidence Logic, and the Qualified Data Processing Subsystem. The other is the nonsafety subsystem that interfaces to the real-time data network. The two subsystems are connected by a fiber-optic link that provides electrical isolation.

The ~~primary~~ flow of information between the two Gateway subsystems is strictly from the safety subsystem to the nonsafety subsystem. The unidirectional nature of the gateway is assured by the use of a single unidirectional fiber to connect the two gateway subsystems. This arrangement provides electrical isolation between the systems (as required by IEEE 603-1991 [Reference 1]) and prevents all dataflow (data, protocols and handshaking) from the non-safety system to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2-1993, Annex G [Reference 15]). Thus:

1. The PMS provides process signals to the DDS through isolation devices. The unidirectional fiber serves as an isolation device that prevents credible faults from propagating into the PMS from the DDS.

2. Since the PLS utilizes the DDS network, the PMS also provides process signals to the PLS through DDS. Again, the unidirectional fiber serves as an isolation device that prevents credible faults from propagating into the PMS from the DDS.

3. Since the physical unidirectional nature of the connection prevents all dataflow from non-safety system to safety system, the data communication between the safety system and the non-safety systems does not inhibit the performance of the safety function.

~~This information is a combination of plant process parameter values and equipment status information. The information that flows from the nonsafety subsystem to the safety subsystem is limited to the following:~~

~~The safety and nonsafety subsystems exchange periodic low-level interface signals that the communication controllers at each end of the link use to ensure that the link is functioning properly. These signals are used only by the communication controllers and are not propagated to the rest of the safety system. There is no application function in the safety system that uses this information.~~

~~The main control room and the remote shutdown workstation operator consoles are nonsafety.~~

~~The soft control inputs to the PMS from these locations are provided from the nonsafety subsystem to the safety subsystem of the Gateway.~~

~~The gateway provides both electrical and communication isolation between the nonsafety systems and the PMS. Other than the isolation function, the gateway is not required for any PMS safety function. There is no potential signal from the nonsafety system than will prevent the PMS from performing its safety functions.~~

~~Specifically, the Gateway will provide the following isolation features:~~

~~Electrical isolation between the Class 1E and non-Class 1E ports of the Gateway, as required by IEEE 603-1991 (Reference 1).~~

~~Communication isolation between the Class 1E and non-Class 1E ports of the Gateway, as envisioned by IEEE 7-4.3.2-1993, Annex G (Reference 15). This includes:~~

~~Class 1E communications buffering circuits to process the low-level interface signals.~~

~~Use of only simple connectionless protocols between the Class 1E and non-Class 1E ports of the Gateway. (Connectionless protocols do not use connection establishment/management/termination nor do they use acknowledgements/ negative-acknowledgements/retransmission.)~~

~~Software within the Class 1E portion of the gateway will filter the incoming message stream and accept only valid soft control commands from a predefined list of valid commands. All other messages will be discarded.~~

~~Application software running in the safety system will ensure the functional independence of the Class 1E functions from the soft control demands received from the nonsafety systems.~~

~~Specifically, the application software will provide the following features:~~

~~In cases where a component is controlled by an automatic safety function, the PMS application software will ensure that the automatic safety function and the Class 1E soft controls both have priority over the non-Class 1E soft controls.~~

~~In cases where a Class 1E component is not controlled by an automatic safety function, the PMS application software will ensure that the Class 1E controls have priority over the non-Class 1E soft controls.~~

Analog inputs required for both control and protection functions are processed independently with separate input circuitry. The input signal is classified as safety-related and is, therefore, isolated in the protection and safety monitoring system cabinet before being sent to the control system.

The plant protection and safety monitoring system also provides data to the plant control system pertaining to signals calculated in the subsystems, and to the data display and processing system.

Non-process signals are also provided to external systems. The non-process outputs inform the external systems of cabinet entry status, cabinet temperature, dc power supply voltages, and subsystem diagnostic status. Cabinet temperature sensing does not affect the safety-related function. The information is gathered for the sole purpose of analysis by external systems.

Non-safety to Safety Communication

The non-safety to safety dataflow is not implemented using communication links; rather it is implemented using discrete digital signals. These signals are used to implement manual ESF system level actuations, manual blocks and resets, manual reactor trip, and manual component level controls.

The manual component controls originate in the PLS. To reduce the number of signals (cables) that must be run from the non-safety system to the safety system, the non-safety system's remote I/O capability will be used to deliver the signals to the safety system. Specifically, a remote I/O node from the non-safety system will be physically located within each division of the safety system. The remote I/O node will be electrically isolated from the non-safety system by the fiber optic remote I/O bus. The node will be powered by the safety system and will be qualified as Associated Class 1E equipment.

The remote I/O node will include one or more Class 1E component interface modules (CIM). Internally these modules contain the equivalent of a digital output module. The resulting signals, corresponding to the desired functions, are made available to non-processor based priority logic also contained in the module. The priority logic within the CIM combines the actuation requests with Class 1E automatic action signals and the Class 1E manual action requests from the PMS ESFAS subsystem. If conflicting demands are present, the safe state of the component takes priority.

As mentioned above, the remote I/O bus that is used to connect the non-safety system to the Associated Class 1E remote node is fiber optic. This arrangement provides electrical isolation between the safety system and the non-safety system as required by IEEE 603-1991 (Reference 1). The remote I/O node implements the communication function and only the resulting digital signals are available to the Class 1E priority logic in the CIM. The simple discrete signal interface within the CIM provides the communication isolation envisioned by IEEE 7-4.3.2-1993, Annex G (Reference 15). The priority logic within the CIM provides functional isolation by only implementing the functionality defined in the PMS functional design. Thus:

1. The data communication between the safety system and the non-safety systems does not inhibit the performance of the safety function.

2. The Class 1E automatic safety functions and the Class 1E manual controls both have priority over the non-Class 1E demands.

Revise the second paragraph of 7.1.6 as follows:

7.1.6 Combined License Information

Completed. ~~Combined License applicants referencing the AP1000 certified design will provide~~ The resolution for generic open items and plant-specific action items resulting from NRC review of the I&C platform has been completed in reference 18.

Revise Reference section for Section 7.1 to include

18. APP_GW-GLR-017, AP1000 Standard Combined License Technical Report, "Resolution of Common Q NRC items", Revision 2

Revise Figures 7.1-1, 7.1-2, 7.1-3B. 7.1-9B, and 7.1-10 as attached.

Revise the Safe Shutdown Evaluation portion of 9A.3.1.2.5.2 as follows:

Safe Shutdown Evaluation

Table 9A-2 lists the safe shutdown components located in this fire area. The remote shutdown room contains circuits from the four Class 1E electrical divisions. Electrical separation to and inside the remote shutdown room is maintained per industry standards. The remote shutdown room is an alternate to the main control room. The transfer of operations to the remote shutdown workstation is controlled by a transfer switch set located in the remote shutdown workstation area. In the unlikely event that the fire damages the transfer switch set, causing transfer of control from the main control room to the remote shutdown workstation, the operator restores control to the main control room by de-energizing fire area 1202 AF 05 (stair S05) ~~the remote shutdown multiplexer cabinets in the instrumentation and control rooms~~. Safe shutdown is achieved using the safe shutdown components listed in Table 9A-2.

Most remote shutdown workstation controls use soft-controls which communicate over multiplexed data channels. Fire-induced spurious actuation from these multiplexed soft controls is not assumed. Fire-induced actuations from the dedicated switches in this area are prevented during normal operation by the transfer switch logic, which only enables operation from the remote shutdown workstation dedicated switches when control is transferred to the remote shutdown workstation.

Neither a fire nor fire suppression activities in this fire area affect the safe shutdown capability of components located in adjacent fire areas.

Add a Safe Shutdown Evaluation to Subsection 9A.3.1.2.8.4 as follows:

Safe Shutdown Evaluation

Table 9A-2 lists the safe shutdown components located in this fire area. The stairwell contains circuits for the transfer switch set which is used to transfer control from the control room to the remote shutdown workstation in the event of a control room evacuation. Electrical separation to and inside the stairwell is maintained per industry standards. In the unlikely event that the fire damages the transfer switch set, causing transfer of control from the main control room to the remote shutdown workstation, the operator restores control to the main control room by using controls located in the instrumentation and control rooms. Safe shutdown is achieved using the safe shutdown components listed in Table 9A-2.

Neither a fire nor fire suppression activities in this fire area affect the safe shutdown capability of components located in adjacent fire areas.

Revise Table 9A-2 (Sheet 13 of 14) as follows:

REFERENCES

1. APP-GW-GL-700, "AP1000 Design Control Document, Revision 15."

2. NUREG 1793, NRC " Final Safety Evaluation Report for AP1000 Design", September 2004

3. WCAP-16097-P-A (CENPD-396-P, Rev. 01), "Common Qualified Platform," May 2003, including Appendices 1, 2, 3, 4 (Rev. 01) and CE-CES-195, Rev. 01, Software Program Manual for Common Q Systems.

4. NRC Safety Evaluation Report, "Acceptance for Referencing of Topical Report CENPD-396-P, Rev. 01, 'Common Qualified Platform' and Appendices 1, 2, 3 and 4, Rev. 01 (TAC No. MA1677)," August 11, 2000.

5. Westinghouse Report 00000-ICE-37764, Revision 02, "Summary Qualification Report of Hardware Testing for Common Q Applications," August 2002.

6. NRC Safety Evaluation Report, "Safety Evaluation by the Office of Nuclear Reactor Regulation Related to the Westinghouse Common Q Platform Closeout of Generic Open Items and Approve Changes to Topical Report CENPD-396-P, Rev. 01, Common Qualified Platform", February 24, 2003.

7. NRC Safety Evaluation Report, "Safety Evaluation for the Closeout of Several of the Common Qualified Platform Category 1 Open Items Related to Reports CENPD-396-P, Revision 1 and CE-CES-195, Revision 1 (TAC No. MB0780)," June 22, 2001.

8. IEEE 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

9. WCAP-16097-P-A (Proprietary), Rev. 3, "Common Qualified Platform Topical Report," Westinghouse Electric Company LLC.

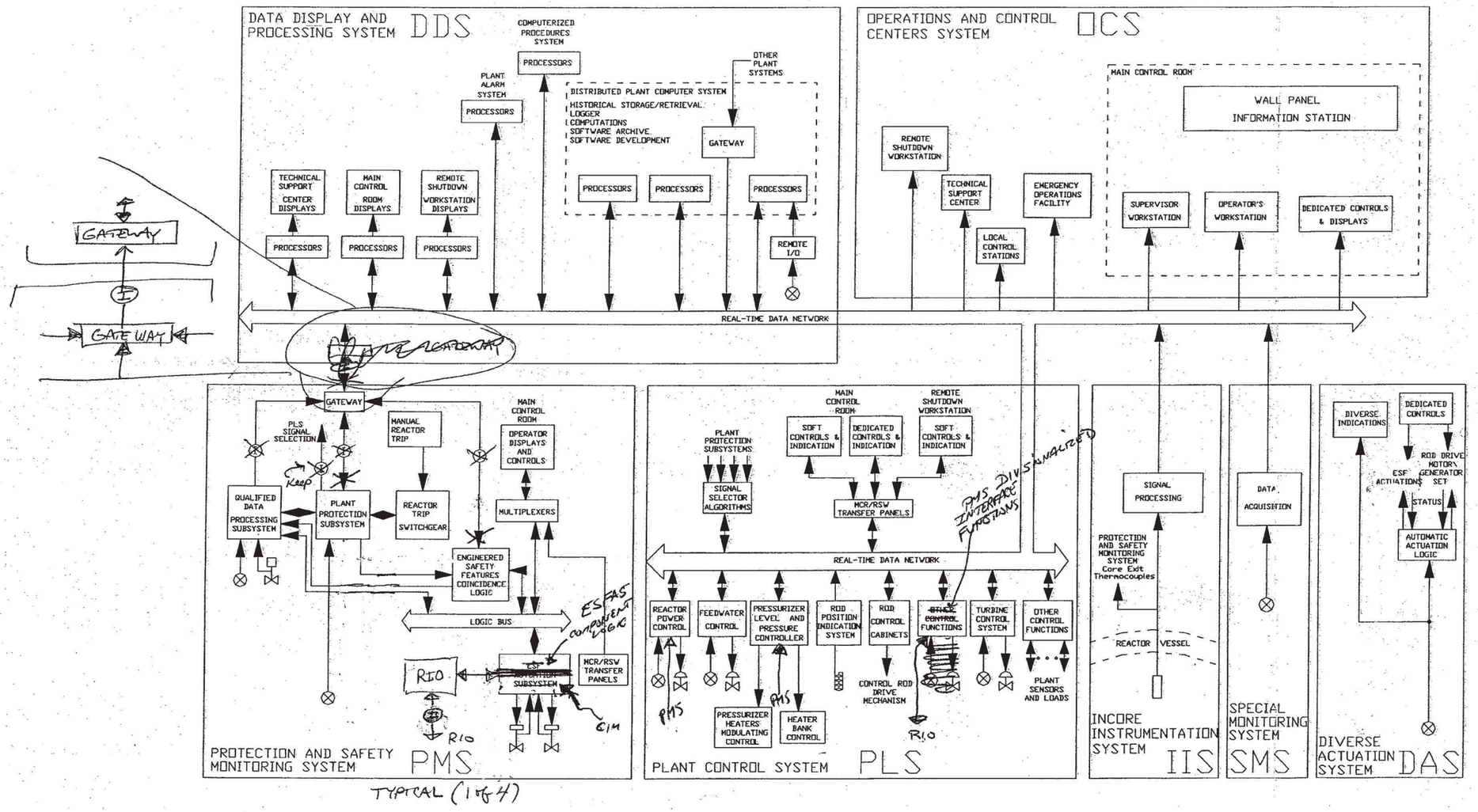


Figure 7.1-1

Instrumentation and Control Architecture

ATTACHMENT TO APP-GW-GLR-017

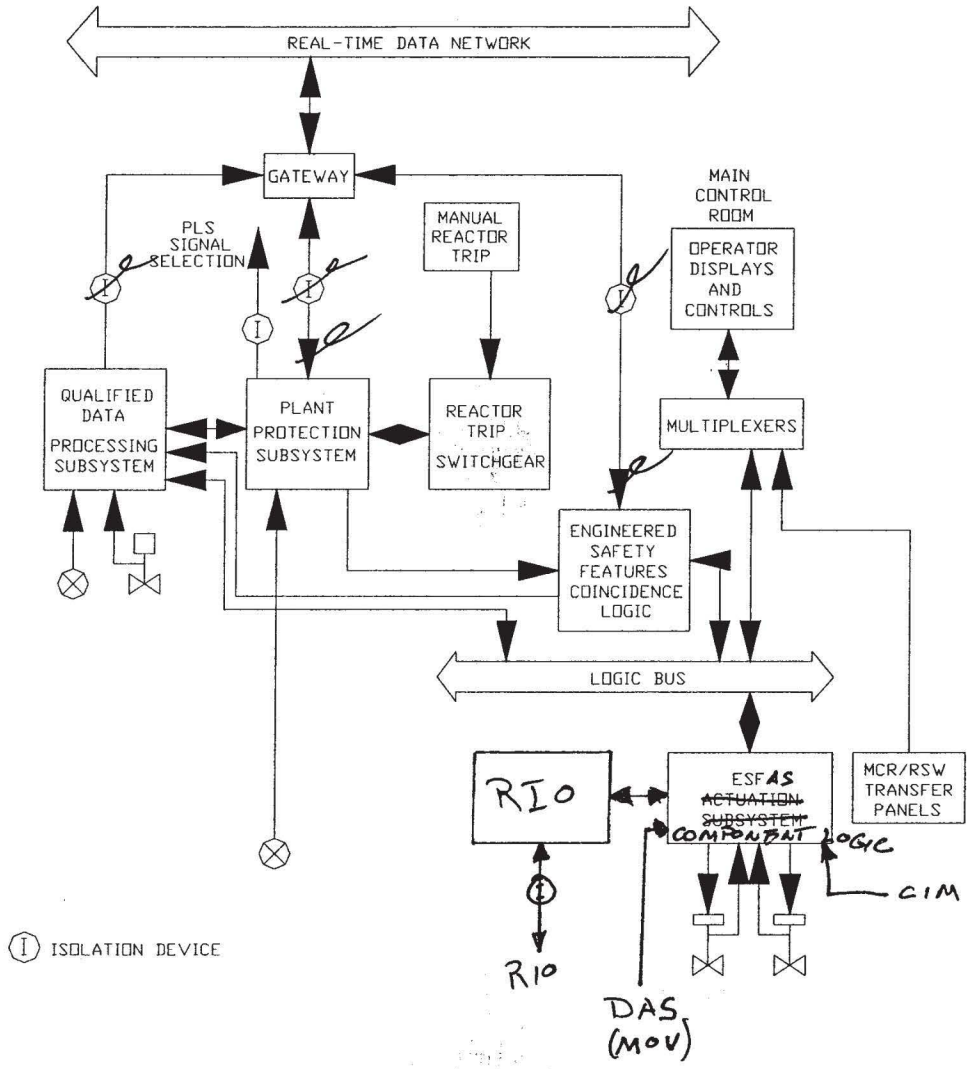


Figure 7.1-2

Protection and Safety Monitoring System

ATTACHMENT TO APP-GW-GLR-017

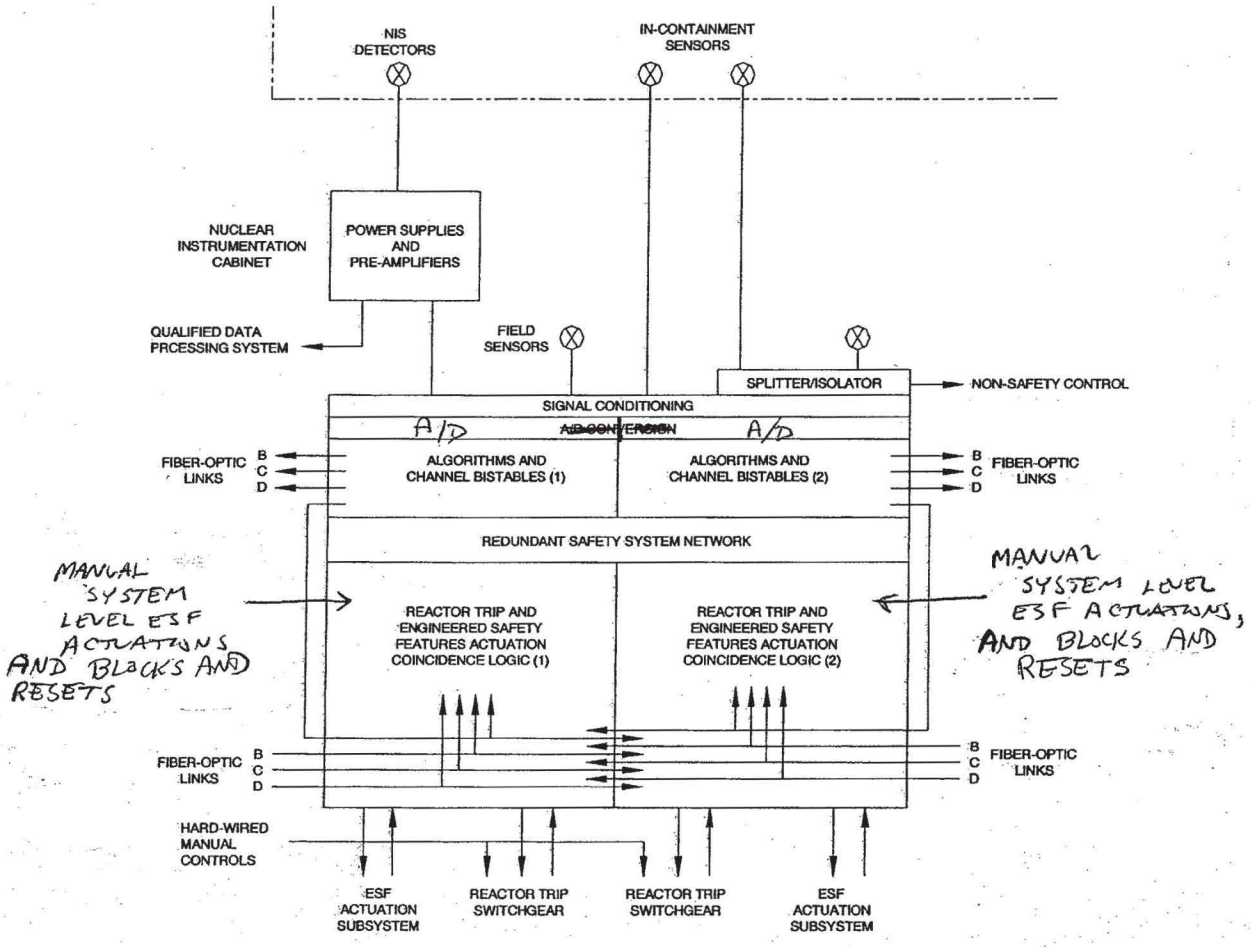


Figure 7.1-3B

Plant Protection Subsystem and Engineered Safety Features Coincidence Logic (Common Q Platform)

ATTACHMENT TO
APP-GW-GLR-017

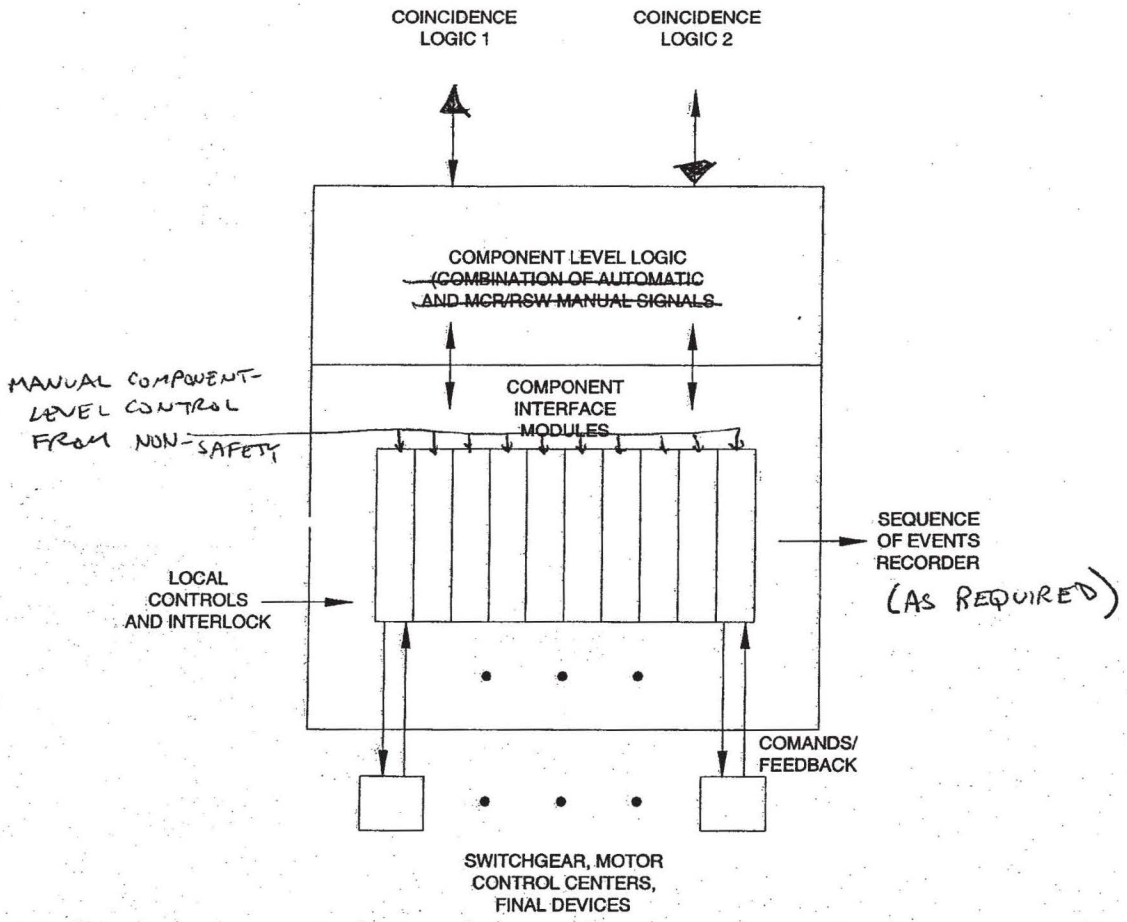


Figure 7.1-9B

Engineered Safety Features Actuation Subsystem (Common Q Platform)

ATTACHMENT TO APP-GW-GLR-017

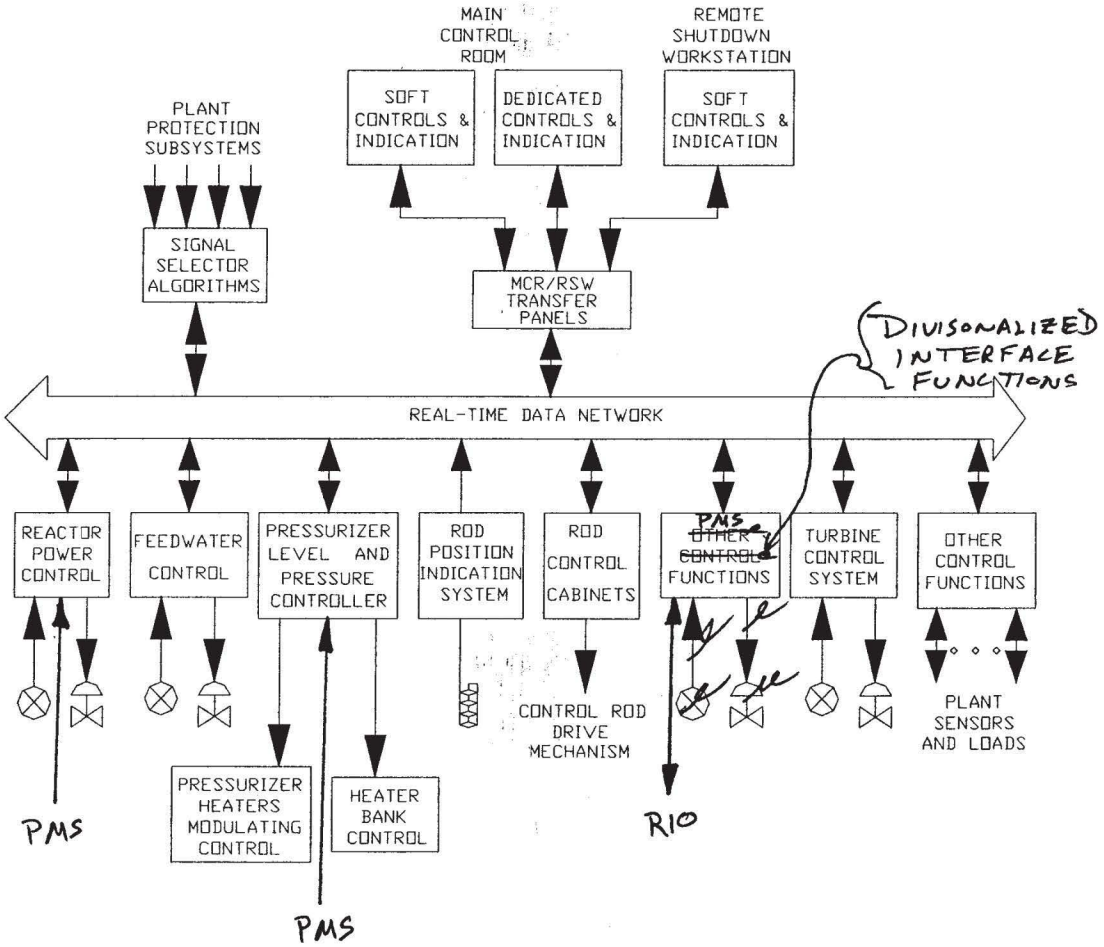


Figure 7.1-10

Plant Control System

Southern Nuclear Operating Company

ND-16-0083

Enclosure 6

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

WCAP-15927, Revision 4

Design Process for AP1000 Common Q Safety Systems

(LAR-15-017)

(Enclosure 6 consists of 30 pages, including this cover page)

WCAP-15927
APP-GW-J1R-001
Revision 4

September 2015

Design Process for AP1000 Common Q Safety Systems

WCAP-15927
APP-GW-J1R-001
Revision 4

Design Process for AP1000 Common Q Safety Systems

Matthew A. Shakun*
Product and Plant Licensing

September 2015

Verifier: Jason E. Zielinski*, Principal Engineer
AP1000 Safety Systems Software Engineering

Reviewer: Richard M. Paese*, Senior Licensing Engineer
U.S. Licensing

Reviewer: John S. Wiesemann*, Project Manager
AP1000 PMS

Approved: Mark J. Stofko*, Manager
Product and Plant Licensing

*Electronically approved records are authenticated in the electronic document management system.

Westinghouse Electric Company LLC
1000 Westinghouse Drive
Cranberry Township, PA 16066, USA

© 2015 Westinghouse Electric Company LLC
All Rights Reserved

TABLE OF CONTENTS

LIST OF TABLES iii

LIST OF FIGURES iii

REVISION HISTORY iv

1 INTRODUCTION AND SCOPE 1-1

2 DEFINITIONS 2-1
2.1 ACRONYMS 2-1
2.2 TERMS 2-2

3 AP1000-SPECIFIC APPLICATION DEVELOPMENT 3-1
3.1 CONCEPTUAL PHASE 3-2
3.2 SYSTEM DEFINITION PHASE 3-2
3.2.1 Platform Requirement Analysis 3-2
3.2.2 System Requirements Analysis/Functional Design 3-3
3.2.3 System Architectural Design 3-5
3.2.4 Software Requirements Analysis 3-6
3.2.5 System Hardware Requirements 3-8
3.3 SOFTWARE DESIGN PHASE 3-8
3.4 HARDWARE DESIGN PHASE 3-9
3.5 SOFTWARE IMPLEMENTATION PHASE 3-10
3.5.1 Final RSED 3-10
3.5.2 Final Software Definition Document 3-10
3.6 HARDWARE IMPLEMENTATION (ASSEMBLY) PHASE 3-11
3.7 SYSTEM INTEGRATION PHASE 3-11
3.8 INSTALLATION PHASE 3-11
3.9 ALTERNATIVE METHODS TO PROCESSES DEFINED IN WCAP-16096-P-A 3-11
3.10 ALTERNATIVE METHODS TO PROCESSES DEFINED IN WCAP-16097-P-A 3-11

4 REFERENCES 4-1
4.1 INDUSTRY STANDARDS AND CODES 4-1
4.2 WESTINGHOUSE DOCUMENTS 4-1

LIST OF TABLES

Table 3-1 Alternative Methods to the Common Q SPM 3-12

Table 3-2 Alternative Methods to the Common Q Topical Report 3-17

LIST OF FIGURES

Figure 3-1 Development Process 3-18

Figure 3-2 Correlation to Standard Life Cycle Phase 3-19

REVISION HISTORY

RECORD OF CHANGES

Revision	Author	Description	Completed
0	Thomas M. Hayes	Original issue.	9/18/02
1	Steven W. Gore	Class 3 DCP changes as detailed below: Added further definition of the Concept Phase (Section 1). Added additional description of life cycle (Section 1). Removed descriptions also in Common Q NRC docketed reports (Section 1). Added missing acronyms and terms (Section 2). Merged the application and platform design life cycle descriptions into one section to eliminate redundant descriptions common to both (Section 3 and throughout document). Added clarification that critical anomalies had to be completed for each phase (Section 3). Added Functional Design to System Requirements (Section 3.2). Project Master Documents now referred to as Document Index (Section 3.1). Updated Figure 3-1, "Development Process," with additional V&V methods. Updated reference document numbers (throughout document and Section 4). Removed explanation of Platform System Design Phase because it is not applicable to AP1000 PMS since it describes generic architecture (Section 4 of Rev. 0).	11/21/08
2	Warren R. Odess-Gillett	Changes are Class 3 as per NSNP 3.4.1. Updated Figure 3-1 per RAI response RAI-SRP 7.1-ICE-10, reference the SPM for the operation, maintenance and retirement software life cycle phases, and technical editing changes	6/3/09
3	Warren R. Odess-Gillett	Updated to reference the newly NRC-approved Common Q™ Topical Report (WCAP-16097-P-A, Rev. 3). Updated to reference the newly NRC-approved Software Program Manual for Common Q Systems (WCAP-16096-P-A, Rev. 4). Updated Section 3.1 to remove the term Document Index.	4/10/13
4	Matthew A. Shakun	The following change was made to address APP-GW-GEE-4380 and CAPAL 100320452: • Updated to include alternate processes to WCAP-16096-P-A, Rev. 4, "Software Program Manual for Common Q™ Systems" and WCAP-16097-P-A, Rev. 3, "Common Qualified Platform Topical Report"	See EDMS

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

4 (cont.)	Matthew A. Shakun	The following editorial changes were made: • Section 2.1 was updated to fix the acronym for AMPL • Sections 3 and 4 were updated to fix the title for IEEE Std. 1074-1995. • Reference 4.2.3 was deleted since it is not being cited in the document.	See EDMS

1 INTRODUCTION AND SCOPE

This document defines the process for system-level design, software design and implementation, and hardware design and implementation for the AP1000® protection and safety monitoring system development. This document supplements WCAP-16096-P-A, "Software Program Manual for Common Q™ Systems" (Reference 4.2.1). Project definition activities are described in this document as a Conceptual Phase (see Section 3.1). The Conceptual Phase is a preparatory phase before the system design begins; it is described here because it forms the management and technical baseline for the development activities.

The objective of the development process is the production of a high quality instrumentation and control (I&C) system that is to be used for the AP1000 protection and safety monitoring system. The design of the system is derived from functional and other requirements applicable to AP1000 (in addition to general requirements that may apply to all similar applications).

The functional requirements of the software are, for the most part, a direct derivation of the system functional requirements. The end product of application development is an operating I&C system, so the life cycle extends through the retirement phase (the operation, maintenance and retirement phases are sufficiently covered in Reference 4.2.1).

The Common Q™ platform consists primarily of the Asea Brown Boveri, Inc. (ABB) Advant® Controller 160 (AC160) hardware and software product line, including the Advant development tools. The development of the AC160 hardware and software and Advant tools is outside the scope of this document. The AC160 product line is developed commercially, and is qualified for use in Common Q applications by a process of commercial dedication. The commercial dedication process is defined in WCAP-16097-P-A, "Common Qualified Platform Topical Report" (Reference 4.2.2). The Common Q platform also has certain generic hardware and software modules that are developed by Westinghouse specifically for safety system applications and that are reusable for multiple systems of various types. The development of these reusable, generic modules is integrated into the life cycle process as described in this document.

2 DEFINITIONS

2.1 ACRONYMS

ABB	Asea Brown Boveri, Inc.
AC160	Part of the ABB Advant open control system family product line
AF100	Advant Fieldbus 100
AMPL	ABB Master Programming Language
CHT	Cabinet Hardware Test
CIT	Channel Integration Test
DCD	Design Control Document
DI	Document Index
EMC	Electromagnetic Compatibility
EST	Element Software Test
HSI	Human System Interface
HSL	High Speed Datalink
I&C	Instrumentation and Control
I/O	Input/Output
PMST	Processor Module Software Test
RSED	Reusable Software Element Document
RTA	Requirements Traceability Analysis
RTM	Requirements Traceability Matrix
SAT	Site Acceptance Testing
SDD	Software Design Description
SDS	System Design Specification
SIT	System Integration Test
SRS	Software Requirements Specification
SSD	System Specification Document
V&V	Verification and Validation

Advant is a trademark or registered trademark of its respective owner. Other names may be trademarks of their respective owners.

AP1000 and Common Q are trademarks or registered trademarks of Westinghouse Electric Company LLC, its affiliates and/or its subsidiaries in the United States of America and may be registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited. Other names may be trademarks of their respective owners.

All other product and corporate names used in this document may be trademarks or registered trademarks of other companies, and are used only for explanation and to the owners' benefit, without intent to infringe.

2.2 TERMS

Advant	An ABB open control system family product line.
Common Q	Common Qualified Platform – a safety system I&C platform as defined in WCAP-16097-P-A, "Common Qualified Platform Topical Report" (Reference 4.2.2).
Data Highway	A serial digital communications circuit that provides communications among several devices.
Datalink	A hardware link used for unidirectional or bi-directional communications between two process modules.
V&V	Verification and validation performed by an organization that is technically, managerially, and financially independent of the development organization.

3 AP1000-SPECIFIC APPLICATION DEVELOPMENT

This section defines the process that is followed in the design of the AP1000 protection and safety monitoring system and in the design and implementation of application hardware and software that are applied to AP1000. The general relationship of hardware, software, and system verification and validation (V&V) (including testing) to this development process is shown, but the details are defined by the V&V Plan.

The following phases occur in the development of the AP1000 protection and safety monitoring hardware and software:

1. Conceptual (Project Definition)
2. System Definition
3. Software Design
4. Hardware Design
5. Software Implementation
6. Hardware Implementation
7. System Integration
8. Installation

Note that testing activities are defined as part of the V&V process.

Figure 3-1 illustrates the relationship of the application development phases to each other and to the V&V process. It also shows the outputs of each phase. The activities and products of these phases are described in the remainder of Section 3. The flow of activities shown in Figure 3-1 is intended to expand on the classic "waterfall" lifecycle model. These activities may be both iterative and overlapping. In particular, because of the constraints of I&C projects, and considering the distributed character of the AP1000 I&C systems, work may commence on a given development phase before preceding phases are complete. For example, it is not necessary for the documentation of system functional requirements to be finished before software design and implementation can start on parts of the system for which the requirements have been defined. However, for a given development phase, all critical anomalies related to that phase must be resolved before the completion of that phase.

Figure 3-2 illustrates the relationship of the development phases defined in this document to the phases (or processes) defined in other documents, specifically IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" (Reference 4.1.1); IEEE/EIA 12207.0-1996, "Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology-Software Life Cycle Processes" (Reference 4.1.2); and WCAP-16096-P-A, "Software Program Manual for Common Q™ Systems" (Reference 4.2.1).

3.1 CONCEPTUAL PHASE

The major tasks of the Conceptual, or Project Definition, Phase are project management planning and project baselining.

The project execution strategy is established and documented. Resources, personnel, and organizational interfaces and dependencies are identified. Planning for schedule, costs, risk management, communication, and project closure is performed. Requisite processes are identified, and may include acquisition, supply, development, operation, and maintenance, and the supporting processes of configuration management, quality assurance, safety, verification, validation, and problem resolution.

The technical baseline is established and documented. Project baseline information typically includes:

- Definition of the scope of the development
- AP1000 Design Control Document (DCD)
- System Specification Documents (SSDs)
- Safety classification of all parts of the system included in the scope of development
- Plant documentation and databases
- Plant-wide I&C requirements
- Applicability of codes and standards, including decomposition of key codes and standards to specific requirements

3.2 SYSTEM DEFINITION PHASE

There are three main tasks in the system definition phase—system requirements analysis, system architectural design, and software requirements analysis. These three tasks overlap in their execution, and there may be considerable iteration among them. The output of this phase is a System Requirements/Functional Design document, a System Design Specification (SDS), and a Software Requirements Specification (SRS).

3.2.1 Platform Requirement Analysis

The Common Q platform is analyzed against the requirements for the AP1000 protection and safety monitoring system. Any modifications or additions to the Common Q platform are identified. These modifications or additions become first-time engineering projects that follow the same design process as described herein.

3.2.2 System Requirements Analysis/Functional Design

In this task, the project technical baseline (Section 3.1) is analyzed to specify the system requirements. This task produces the System Requirements document. Information in the System Requirements document includes system design requirements, system functional requirements (including function-related setpoints, and constants), system interface requirements, and human system interface (HSI) requirements. Detailed requirements for the interface of individual external signals and communications data are documented in an external signal database and an external communications database.

3.2.2.1 System Design Requirements

The system design requirements comprise the overall requirements and constraints for the system design, aside from the specific system functions and specific interface signals. The application System Requirements document incorporates, by reference, the platform system design requirements and identifies additions and/or exceptions that apply specifically to AP1000. The system design requirements include the following categories of requirements:

- Applicability of codes and standards, either in whole, or in part, or as guidance (which may be defined by reference to the applicability documented in the technical baseline)
- General design requirements: design basis, single failure criteria, integrity, independence, maintenance, manual capabilities, information display, access control, identification, calibration capabilities, reliability, and availability
- Hardware qualification: environmental, electromagnetic compatibility (EMC), and seismic
- Power and grounding
- External interface capabilities
- Performance requirements: time response, accuracy, and signal noise
- Test and diagnostic capabilities
- Design constraints and objectives

3.2.2.2 System Functional Requirements

The system functional requirements provide a complete definition of the sense and command features within the scope of the system (including non-safety functions, such as provision of data to the plant information system, control interlocks, information displays, etc.). They include the following categories of requirements. The requirements are provided by a combination of textual description, logic diagrams, mathematical formulas, and tables.

- Safety functions and corresponding protective actions (exact definition of the required response of the system for all design basis events)

- Non-safety-related functions (e.g., control interlocks, data to non-safety displays and systems)
- Performance requirements associated with functions (time response, accuracy)
- Setpoints and constants associated with functions (fixed value or range of adjustment, hysteresis)
- Response to failures and out-of-range conditions (internal and external)
- Functional diversity
- Signal diversity
- Separation and isolation requirements for individual functions or interfaces (e.g., assignment of signals and functions to separation divisions)
- Required auxiliary features, such as:
  - Maintenance bypass and trip logic
  - Automatic, manual, and/or continuous test capabilities
  - Maintenance functions

3.2.2.3 System Interface Requirements

The system interface requirements define the interface between the protection system being specified and the rest of the physical plant. The requirements include the following categories:

- System scope (defines what is included in the scope of supply)
- System boundaries:
  - Mechanical system (the plant process; generally, however, the actual boundary between the process and the protection system is the I&C boundary)
  - Electrical system (power and grounding)
  - I&C systems (a general description of the signal interfaces–detailed definition of all external signals is recorded in the external interface database)
  - Functional interfaces (description of the external systems with which the protection system interfaces, and identification of the parameters, controls, indications, and functions that are monitored or actuated)
- Requirements for associated equipment (e.g., time response of actuated equipment)
- Isolation requirements for external interfaces (e.g., individual requirements for Class 1E)

3.2.2.4 HSI Requirements

The HSI requirements identify all of the required operator and maintenance personnel interfaces; for example, displays, alarms, operator controls, and maintenance and test interfaces, including the associated functionality.

3.2.2.5 External Interface Database

The external interface database supplements the System Requirements document and contains two categories of information: external signal information and external communications information.

The database identifies each external physical signal received by or produced by the system. When the database is initially populated, it provides a unique identifier by which each signal can be referenced, and it defines the signal type, signal range, functional description, source or destination (by external system), and external identifier (e.g., tag number) of the signal. As the system design progresses, information is added to each signal to identify where the signal originates and terminates within the protection system, by cabinet, then, ultimately, by specific termination, including terminal identities and identity of the input/output (I/O) or communication module and point that provide the controller interface to each signal.

The database identifies each data item that the protection system receives or transmits via a data channel (datalink or data highway). The database identifies the data channel and defines, where applicable, the data type, range, functional description, update timing, and grouping with other data items. This database provides a unique identifier by which the data item can be referenced.

3.2.3 System Architectural Design

The system architectural design task identifies the major hardware and software elements of the system and their interconnections. This task produces the SDS requirements that are allocated among these items. In particular, the functional, HSI, and interface requirements are mapped to individual subsystems. System hardware requirements are identified. External signals are allocated to individual subsystems, and this information is added to the external interface database, as noted in subsection 3.2.2.5. Intrasystem signals and communications data are identified; details may be documented in an intrasystem interface database.

3.2.3.1 System Architecture

A description is given of the architecture of the protection system as a whole. Information provided includes the following, and typically will include architecture diagrams, hardware configuration diagrams, and textual descriptions of the architectural elements:

- Identification of all parts of the system, to the cabinet and subsystem level
- Interconnections among subsystems
- Assignment of power and grounding interfaces to specific cabinets or subsystems

- Definition of subsystem hardware configuration to a level of detail necessary to support software design and to identify any hardware or software that must be designed or procured (i.e., that is not part of the standard platform hardware and software)

- Evaluation of the selected architecture against the product qualification of the standard platform hardware and software

3.2.3.2 Functional Mapping

The system functions and performance requirements defined in the System Requirements document are assigned to individual subsystems. For most sense and command features (both safety and non-safety) this can be documented as a list or table of the functions that are defined in the system functional requirements (see subsection 3.2.2.2) with the subsystem assignment. If functions must be allocated to a particular processor within a subsystem because of separation requirements defined in the system functional requirements, that assignment is documented here as well. Auxiliary features, such as testing capabilities, are mapped to the architecture at a high level here.

3.2.3.3 Intrasystem Interface Database

The intrasystem interface database contains two categories of information: intrasystem signal information and intrasystem communications information.

This database identifies each physical signal that is connected between different subsystems within the protection system. The intrasystem interface database defines the signal type, signal range, functional description, and the source and destination(s) (by subsystem) and provides a unique identifier by which the signal can be referenced. Ultimately, this database also includes specific termination information, including terminal identities and identity of the I/O or communication module and point that provide the controller interface to each signal. The termination information, however, does not necessarily need to be included before hardware and software design can proceed.

The Intrasystem Interface Database also identifies each data item that the protection system receives or transmits via an intrasystem data channel (datalink or data highway). It identifies the data channel and defines, where applicable, the data type, range, functional description, update timing, and grouping with other data items. It provides a unique identifier by which the data item can be referenced.

3.2.4 Software Requirements Analysis

The software requirements analysis task completes the identification of the requirements for the software in the system. The outputs of this task are several reusable software element documents (RSEDs) and an SRS for the system-specific software. The requirements for the sense and command features typically will have been documented by the functional mapping documented in the SDS (see subsection 3.2.2.2). Any additional requirements will be identified in the SRS as defined in subsection 3.2.3.2.

3.2.4.1 Reusable Software Element Document (Summary and Requirements)

Reusable common software elements can be created for the AC160 product line in the form of type circuits and custom PC elements. A type circuit is a prearranged group of the smaller pre-existing commercially available software units (PC elements) into a larger, more complex software entity. Type circuits are not compiled code, but more like the ABB Master Programming Language (AMPL) macro definitions that can be saved individually and reused throughout one or more projects. Custom PC elements are compiled from source code and added to the library of standard PC elements available for AMPL programming. Common software elements that are type circuits or general purpose custom PC elements (new PC elements intended for common use in many different safety applications) are documented with a composite document referred to as an RSED. An RSED combines requirements, design description, and user information into a single document.

The portion of an RSED that contains the product of the software requirements analysis contains the following categories of information:

- An element (type circuit, functional unit, custom PC element) summary consisting of a general functional description of the element

- Requirements Specification:

  – Functional requirements (functions implemented, timing, accuracy)
  – I/O terminal descriptions (default values, data types, data ranges)
  – Overflow/error handling (range checking, failure modes, alarming)
  – Truth Table (outputs as a function of input combinations)

3.2.4.2 Software Requirements Specification

The high-level requirements for auxiliary features are refined into detailed requirements in the SRS. The SRS ensures that all requirements are documented for the software in each subsystem. This information may be in the System Requirements as they are mapped to subsystems and processors by the SDS (including information in the signal and communications databases). Additional information is documented as detailed requirements in the SRS. Information in the software requirements analysis includes:

- Software structure

- Software technical description

- Specific inputs and outputs, both those that are physical signals and information that is received from and supplied to human users and external data systems

- Valid input ranges

- Output ranges, if they must be specifically limited

- Required HSI formats (e.g., input screen formats, printed report formats)
- Required sequences of operations (e.g., test sequences, operator dialog sequences)
- Functional processing of the data
- Timing requirements or constraints
- Response to abnormal conditions and error recovery
- Retention, use, and initialization of previous state information, where required
- Safety and security requirements
- Design constraints (e.g., the required use of a particular programming tool or language, or the required use of particular platform software)

3.2.5 System Hardware Requirements

The system hardware requirements describe the hardware requirements needed to support the architecture of the protection system. Information provided includes the following:

- Identification of all the hardware elements used in the system, such as cabinets, panels, subassemblies, wiring, terminations and modules
- Definition of the hardware configuration needed to support the architecture of the protection system
- Cabinet power and grounding requirements
- Cabinet cooling requirements
- Cabinet labeling requirements
- Cabinet environmental requirements
- Cabinet shipping and storage requirements

3.3 SOFTWARE DESIGN PHASE

In the software design phase, the software requirements are decomposed and allocated to individual software components. The use of existing software components to implement the requirements is described within an existing RSED. New software components that must be created are identified and likewise documented within an RSED. The portion of an RSED that contains the product of the Software Design Phase contains any design information that is not obvious from the implementation (AMPL diagram or code comments).

The software design is described in Software Design Description (SDD) documents. A preliminary SDD is produced in the software design phase, while a final SDD is produced in the software implementation phase. There is an SDD generated for each processor module that executes unique code. Redundant processors that execute identical, or nearly identical, code may have a single SDD; this includes processors in separate divisions, if they have essentially identical code (implement the same functions).

The preliminary SDD contains the following categories of information:

- Decomposition of the required functions into software entities (modules, procedures, type circuits, etc.), including entity names and the reason for the existence of the entity
- Module timing and priority
- A description, where applicable, of how safety (sense and command) functions and auxiliary functions are combined (e.g., the functionality required in bistable and logic processors to implement periodic testing; local functionality required to support maintenance functions, such as calibration data changes). In typical cases, this description may be made generic and included in the "Design Constraints" section of the application SRS, or even in platform (non-project-specific) documentation; a reference to such generic information should be made where applicable.
- Identification of any generic type circuits or custom PC elements that need to be developed. These may be project-universal elements, applicable in multiple processors in a specific project, or they may be new platform software. In either case, their design and implementation follows the platform software development process.
- Where applicable, handling of software initialization, redundancy, and tracking

3.4 HARDWARE DESIGN PHASE

In the hardware design phase, the final construction configuration of the production hardware is specified. The production unit specific cabinet assembly drawings and cabinet configuration drawings are issued at this stage. These drawings contain all of the information necessary to produce the production unit hardware. The drawings include the following information:

- Cabinet layout details
- Cabinet assembly details
- Cabinet bill of materials
- Cabinet configuration details
- Cabinet termination frame details
- Cabinet internal wiring details

3.5 SOFTWARE IMPLEMENTATION PHASE

In the software implementation phase, the executable code modules are created, typically by use of the AMPL tools. (Non-AC160 subsystems require different tools.) The application modules are integrated with platform software to produce code modules that are downloaded into subsystem processors for V&V testing (described in a V&V plan). The final version of the RSED for all of the defined software components is an output of this phase. Descriptive information about the implementation is added to the preliminary SDD to produce the final SDD.

3.5.1 Final RSED

The implementation description (a printout of the AMPL diagram) is added to the RSED and a User's Guide section is added (providing the developer with adequate instruction to incorporate the common element into an application program). The complete RSED then contains the following information:

- The element summary
- The requirements specification
- Design information (as described in Section 3.3)
- Implementation (printout of AMPL diagram for the type circuits)
- Users Guide:
  - Detailed instantiation procedure (prerequisites, applicability, restrictions, signal connections)
  - Configuration/applications (database elements connections, I/O interfaces, high speed datalink [HSL] interfaces, Advant Fieldbus 100 (AF100) interfaces, default values used)

3.5.2 Final Software Definition Document

The following categories of information are added to produce the final SDD:

- Mapping of signal names used in the code to names used in the requirements documents and databases, where these differ
- Printouts of the AMPL function chart diagrams
- Any other non-obvious information that is needed to understand the software implementation and its interfaces. The intention is that this is an aid to the individuals who will verify or maintain the code. This should not repeat information that is clear to a knowledgeable individual reading the diagrams (or non-AMPL source code listings).

3.6 HARDWARE IMPLEMENTATION (ASSEMBLY) PHASE

In this phase, the construction of the production unit hardware system is completed using the drawings specified in Section 3.4.

3.7 SYSTEM INTEGRATION PHASE

In this phase, completed cabinets containing the applications software are connected together as an integrated system. Validation testing (described in the V&V plan) is performed to test system functionality that was not covered by the cabinet-level validation testing. System integration and testing may be done on appropriate portions (e.g., individual divisions) of the system or on the complete system.

3.8 INSTALLATION PHASE

The completed system is installed at the site. Site Acceptance Testing (SAT), described in the V&V plan, is performed to assure that the system has not been damaged by shipping and installation. The SAT also confirms proper operation of any interfaces that were not completely tested by the factory validation testing; e.g., interfaces to other plant systems.

3.9 ALTERNATIVE METHODS TO PROCESSES DEFINED IN WCAP-16096-P-A

Table 3-1 identifies alternatives to the processes defined in WCAP-16096-P-A, “Software Program Manual for Common Q Systems” (Reference 4.2.1).

3.10 ALTERNATIVE METHODS TO PROCESSES DEFINED IN WCAP-16097-P-A

Table 3-2 identifies alternatives to the processes defined in WCAP-16097-P-A, “Common Qualified Platform Topical Report” (Reference 4.2.2).

Table 3-1 Alternative Methods to the Common Q SPM

WCAP-16096-P-A Section	WCAP-16096-P-A Text	Alternative
Glossary of Terms: Project Quality Plan (PQP) 4.3.2.1 Initiation (Concept) Phase	A document that specifies alternatives or supplements to the Westinghouse 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 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.	Alternative A document that specifies alternatives or supplements to the Westinghouse 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.
4.3.1 Organization Exhibit 2-1 Design/IV&V Team Organization	The NA organization includes a Quality organization and an Engineering organization. The design team and the IV&V team are organized within the Engineering organization.	Alternative The NA organization includes a Quality organization and an Engineering organization. The design team and the IV&V team are in separate organizations at least to the Director level. See updated SPM Exhibit 2-1 Design/IV&V Team Organization following this table.
4.3.2.6 Site Installation and Checkout Phase	The preparation of the site test plan will be initiated during the requirements phase to support evaluation of requirement testability on-site.	Alternative 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.

Table 3-1 Alternative Methods to the Common Q SPM (cont.)

WCAP-16096-P-A Section	WCAP-16096-P-A Text	Alternative
4.6.2.10 Post Mortem Review	Suggestions for improvement and/or best practices that are identified during the Post Mortem Review should be documented via EXHIBIT 11-2 CORRECTIVE ACTIONS PROCESS.	Alternative 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.
5.5.1 Management of IV&V	The resources for performing the IV&V shall be identified in the Project Quality Plan (Reference 4) that is prepared by the Project Manager during the conception phase of the software life cycle.	Alternative The resources for performing the IV&V shall be identified in the AP1000 PMS SVVP that is prepared by the IV&V team during the conception phase of the software life cycle.
6.3.2 Configuration Change Control	Software Change Request Procedure, Step 5: Revised System Baseline: The SCR forms will be used as the basis to track all system changes and to verify that changes have been properly implemented and that documentation has been updated.	Alternative DCPs, 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 documentation has been updated.
6.3.4 Configuration Audits and Reviews	Configuration Audits and Reviews 3. External audits by customers or regulators shall be coordinated by the EPM [Engineering Project Manager] who will schedule personnel to be available if additional support is required.	Alternative 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.

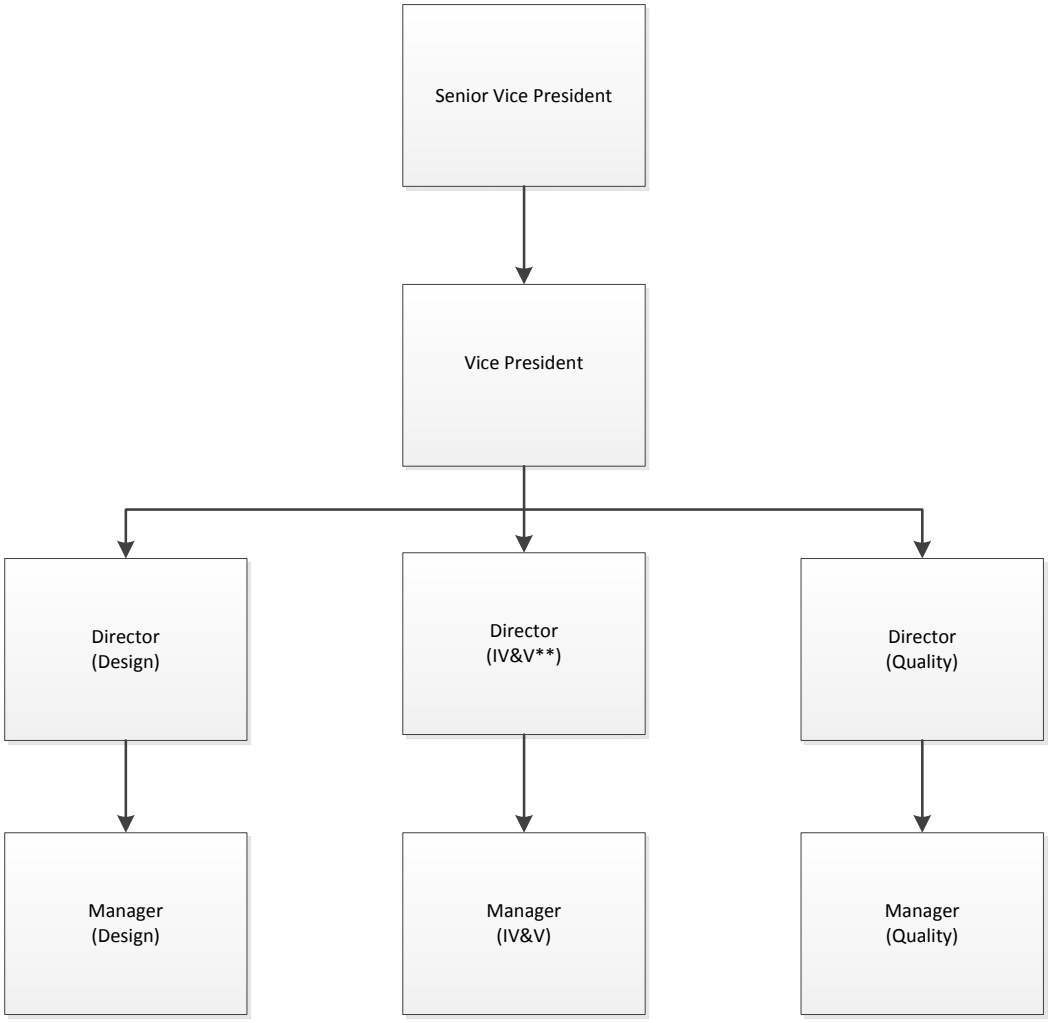
Table 3-1 Alternative Methods to the Common Q SPM (cont.)

WCAP-16096-P-A Section	WCAP-16096-P-A Text	Alternative
6.4 SCM Schedule	SCM milestones that shall be indicated on the project schedule include: • CCB establishment • Establishment of a configuration baseline, and • Implementation of change control procedures.	Alternative 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.
9.2.3 Control	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 this log.	Alternative Per the Common Q RITS Work Instruction, the RITS system maintains the SCR log. The Software Lead shall confirm that the approved SCR is entered into this log.
10.5.1 Software Verification and Validation Plan	The PQP shall also define the tracking and recording process for the hardware configuration pertinent to the software verification and validation process during all phases of the software life cycle.	Alternative 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.
10.10 Computer Code Certificate	The completion of the implementation 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).	Alternative 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).

Table 3-1 Alternative Methods to the Common Q SPM (cont.)

WCAP-16096-P-A Section	WCAP-16096-P-A Text	Alternative
11.4 Corrective Action	Corrective actions shall be documented on Exception Reports and Common Q™ Comment Records by the design team and shall be completed by the due date specified on the form…Once the independent reviewer is satisfied with the corrective action taken, the report form shall be signed.	Alternative 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.
12 Secure Development and Operational Environment Plan	Secure Development and Operational Environment	Alternative 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."

Exhibit 2-1
Westinghouse Organization Chart*



*This example organization chart shows the minimum level of separation required for the Design, IV&V, and Quality Teams

**System level validation testing is performed by another group, which meets the same level of independence as the IV&V group depicted in this organization chart

Table 3-2 Alternative Methods to the Common Q Topical Report		
WCAP-16097-P-A Section	**WCAP-16097-P-A Text**	**Alternative**
References	27. WCAP-17266, Rev. 0, "Common Q Platform Generic Change Process," Westinghouse Electric Company LLC.	Alternative 27. WCAP-17266, "Common Q Platform Generic Change Process," Westinghouse Electric Company LLC.

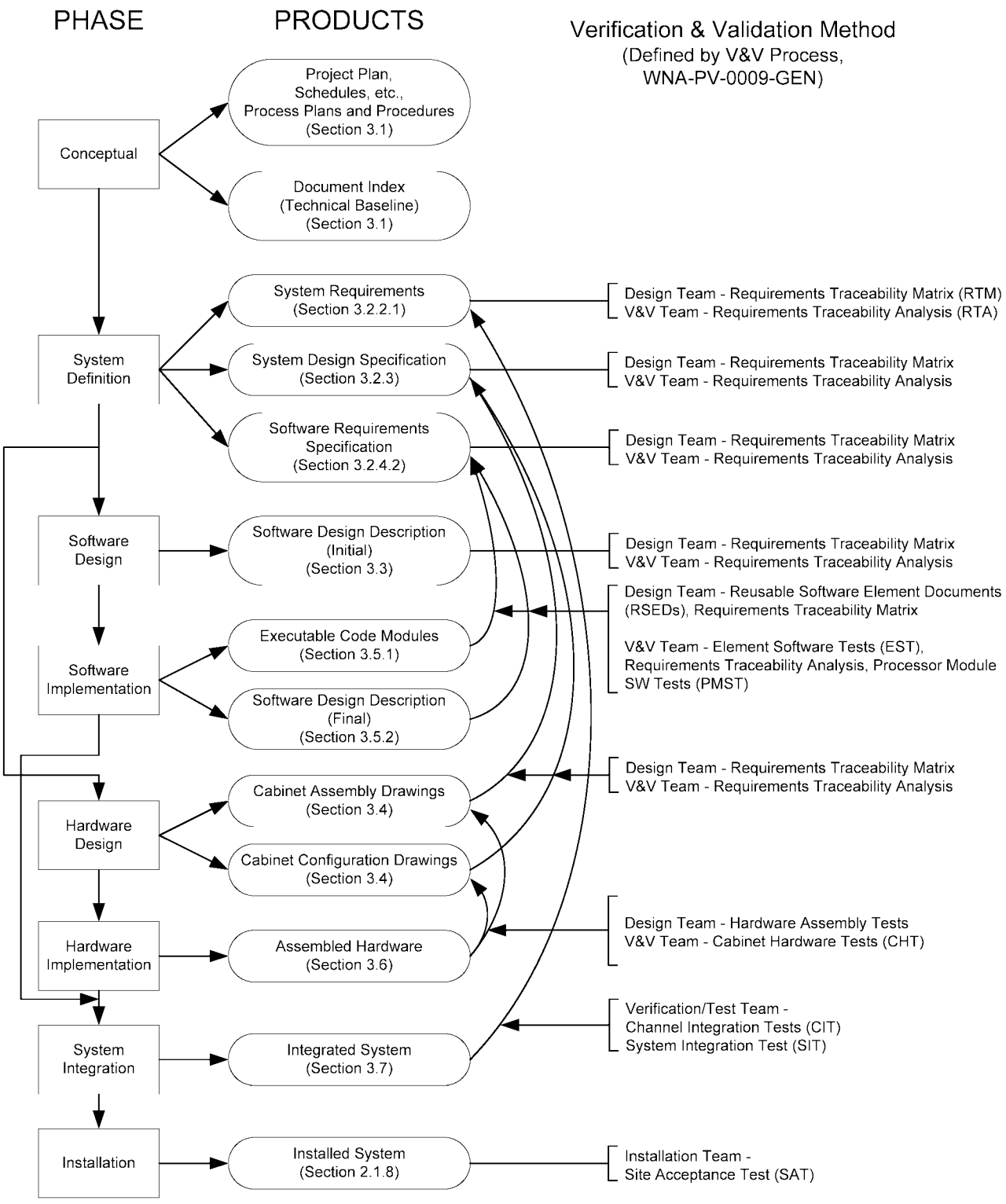


Figure 3-1 Development Process

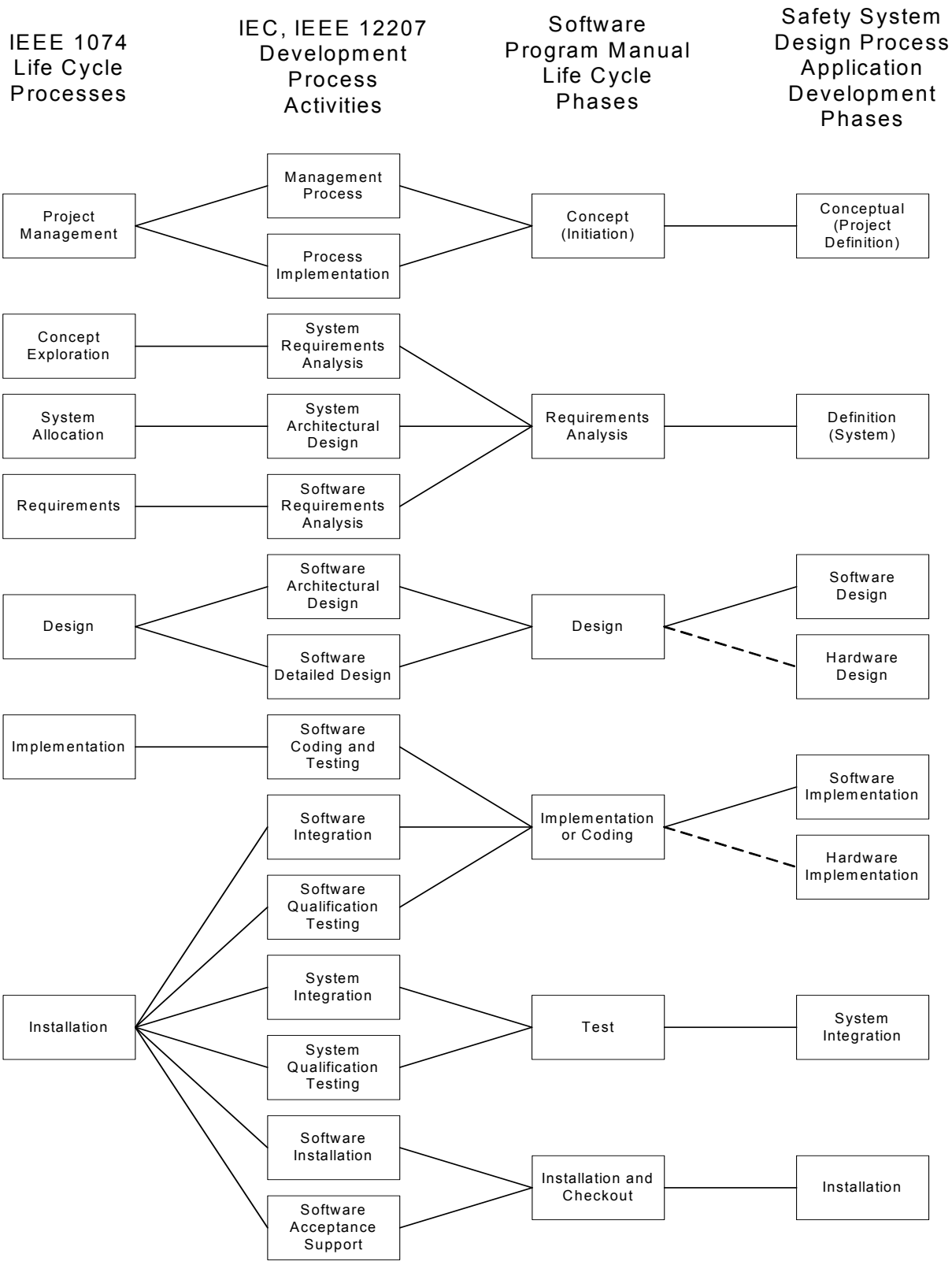


Figure 3-2 Correlation to Standard Life Cycle Phase

4 REFERENCES

4.1 INDUSTRY STANDARDS AND CODES

4.1.1 IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," Institute of Electrical and Electronics Engineers, 1995.

4.1.2 IEEE/EIA 12207.0-1996, "Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology-Software Life Cycle Processes," Institute of Electrical and Electronics Engineers/Electronic Industries Alliance, 1996.

4.2 WESTINGHOUSE DOCUMENTS

4.2.1 WCAP-16096-P-A (Proprietary), Rev. 4, "Software Program Manual for Common Q™ Systems," Westinghouse Electric Company LLC.

4.2.2 WCAP-16097-P-A (Proprietary), Rev. 3, "Common Qualified Platform Topical Report," Westinghouse Electric Company LLC.