Westinghouse Comments and Proprietary Markings Regarding Draft NRC Safety Evaluation for WCAP-16096-P/WCAP-16096-NP, Revision 5, "Software Program Manual for Common Q™ Systems"

(Non-Proprietary)

September 2018

Westinghouse Electric Company
1000 Westinghouse Drive
Cranberry Township, PA 16066

Westinghouse Comments and Proprietary Markings Regarding Draft NRC Safety Evaluation for WCAP-16096-P/WCAP-16096-NP, Revision 5, "Software Program Manual for Common Q™ Systems"

Westinghouse has reviewed the NRCs draft Safety Evaluation (SE) and determined it does not contain any Proprietary information.

The following attachment shows the draft SE with Westinghouse's proposed redline markups. A table has been provided at the end of the SE outlining Westinghouse's comments. Line numbers have been added to the left hand margin of the SE to help locate the comments.

U.S. Nuclear Regulatory Commission Staff

Safety Evaluation for

Westinghouse Topical Report WCAP-16096-P, Revision 5,

"Software Program Manual for Common Q Systems"

August 2018

Principal Contributors:

Rich Stattel

William Roggenbrodt

ENCLOSURE

TABLE OF CONTENTS FOR COMMON Q SAFETY EVALUATION

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

WESTINGHOUSE TOPICAL REPORT WCAP-16096-P, REVISION 5

"SOFTWARE PROGRAM MANUAL FOR COMMON Q SYSTEMS"

(EPID: L-2017-TOP-0059)

1.0 INTRODUCTION

The Software Program Manual (SPM) for Common Qualified (Common Q) Systems was originally submitted as document CE-CES-195-P by Combustion Engineering (CE), for U.S. Nuclear Regulatory Commission (NRC) staff review in 2000. Subsequently, the commercial nuclear power businesses of Asea Brown Boveri (ABB), of which CE was a part, were purchased by British Nuclear Fuels Limited (BNFL) and eventually integrated into the Westinghouse Electric Company (WEC), such that the SPM is now owned by WEC. See References 10 and 11 for Revision 1 of this document and the associated safety evaluation (SE). This document specifies the life cycle planning process for Common Q application software. The SPM specifies the development, documentation, utilization, and maintenance of software to be developed for use with the Common Q platform in nuclear safety applications. It also provides guidance for the maintenance, implementation, and use of commercial-grade hardware and previously developed software (PDS). Revision 4 of the Common Q SPM was submitted by WEC (Refs. 3 and 4) and approved by the NRC (Ref. 17).

The SPM is being updated to Revision Level 5 per Reference ~~0~~ 14 to include a revised test approach that defines testing requirements for Nth of a kind systems of the same design. The revised SPM also addresses corrective actions, implements process improvements, updates several of its references, and includes other minor changes.

The SPM specifies procedures and controls for the complete software development process. This process includes the integration of software into system hardware. Since the application software has not yet been developed, the staff's evaluation does not include the review of the implementation or outputs of the life cycle process, but is limited to the evaluation of the specified planning processes.

2.0 REGULATORY EVALUATION

2.1 Regulatory Criteria

The following regulatory requirements are applicable to the review of the Common Q SPM.

Title 10 of the *Code of Federal Regulations* (10 CFR)

- 10 CFR 50.55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed.

- 10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, "IEEE Standard

Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction dated January 30, 1995.

- Clause 5.3 of IEEE Std. 603-1991 requires that components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. It also requires that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

- Clause 5.6.3 of IEEE Std.603-1991 requires safety system to be designed such that credible failures in and consequential actions by other systems will not prevent safety systems from performing their intended safety functions.

- Clause 5.9 of IEEE Std. 603-1991 requires the design to permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

- 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 1, "Quality Standards and Records," requires, in part, that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.

- 10 CFR Part 50, Appendix A, GDC 21 requires, in part, that protection systems must be designed for high functional reliability commensurate with the safety functions to be performed.

- 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants", Criterion I, "Organization," requires in part that the applicant shall be responsible for the establishment and execution of the quality assurance program.

- 10 CFR Part 50, Appendix B, Criterion II, "Quality Assurance Program," requires in part that the applicant shall establish at the earliest practicable time, consistent with the schedule for accomplishing the activities, a quality assurance program which complies with the requirements of Appendix B.

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

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

- 10 CFR Part 50, Appendix B, Criterion VI, "Document Control," requires, in part that, for safety-related SSCs, measures shall be established to control the issuance of documents which prescribe all activities affecting quality.

- 10 CFR Part 50, Appendix B, Criterion VII, "Control of Purchased Material and Services," requires documented control of purchased material, equipment, and services for safety-related SSCs.

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

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

The following guidance documents are applicable to, and were utilized in support of, the review of the Common Q Software Program Manual.

Regulatory Guides (RGs)

- RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."

- RG 1.168, Revision 2, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

- RG 1.169, Revision 1, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

- RG 1.170, Revision 1, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

- RG 1.171, Revision 1, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

- RG 1.172, Revision 1, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

- RG 1.173, Revision 1, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

NUREG-Series Publications

NUREG-0800, Revision 7, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, "Instrumentation and Controls," March 2007.

  - Branch Technical Position (BTP) 7-14, Revision 6, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."

- NUREG/CR 6101 – "Software Reliability and Safety in Nuclear Reactor Protection Systems," June 1993.

Industry Standards

- IEEE Std. 7-4.3.2-2003, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations," as endorsed by RG 1.152.
- IEEE Std. 730-1998, "Software Quality Assurance Plans,"
- IEEE Std. 828-2005, "Software Configuration Management Plans," as endorsed by RG 1.169.
- IEEE Std. 829-1983, "Software Test Documentation," as endorsed by RG 1.170, September 1997.
- IEEE Std. 829-1998, "Software Test Documentation,"
- IEEE Std. 830-1998, "Guide for Software Requirements Specifications," as endorsed by RG 1.172.
- IEEE Std. 1008-1987 (Reaffirmed 2009), "IEEE Standard for Software Unit Testing."
- IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation Plans," as endorsed by RG 1.168.
- IEEE Std. 1028-2008, "IEEE Standard for Software Reviews and Audits," as endorsed by RG 1.168.
- IEEE Std. 1042-1987, "IEEE Guide to Software Management."
- IEEE Std. 1063-2001, "IEEE Standard for Software Documentation."
- IEEE Std. 1074-2006, "IEEE Std. for Developing Software Life Cycle Processes," as endorsed by RG 1.173.

2.2 Method of Review

The staff used the guidance in RGs and BTP 7-14 to review the software life cycle plans outlined in the Common Q SPM. In BTP 7-14 the information to be reviewed is subdivided into the following three topic areas:

- Software life cycle process planning;
- Software life cycle process implementation; and
- Software life cycle process design outputs.

2.3 Precedents

The NRC previously evaluated the Common Q SPM which was submitted by WEC as document number WCAP-16096-P/NP-A, Revision 4 and the results of this evaluation are documented in the associated SE (Ref. 0).

3.0 TECHNICAL EVALUATION

The regulation at 10 CFR Part 50.55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed. The regulation at 10 CFR Part 50, Appendix A, GDC 1 requires, in part, that a quality assurance program be established and implemented in order to provide adequate assurance that systems and components important to safety will satisfactorily perform their safety functions. The regulation in 10 CFR Part 50, Appendix B, describes criteria that a quality assurance program for systems and components that prevent or mitigate the consequences of postulated accidents must meet. In particular, besides the systems and components that directly prevent or mitigate the consequences of postulated accidents, the criteria of Appendix B also apply to all activities affecting the safety-related functions of such systems and components as designing, purchasing, installing, testing, operating, maintaining, or modifying.

BTP 7-14, provides an acceptable way to meet the regulations cited. The staff reviewed the Common Q SPM in accordance with BTP 7-14.

Acceptability of software for safety system functions is dependent upon (1) confirmation that acceptable plans were prepared to control software development activities as described in BTP 7-14, B.3.1, (2) evidence that the plans were followed in an acceptable software life cycle as described in BTP 7-14, B.3.2, and (3) evidence that the process produced acceptable design outputs as described in BTP 7-14, B.3.3. The Common Q SPM only addresses the first item, the planning phase.

This SE instructs applicants referencing Topical Report WCAP-16096-P (NP), Revision 5 (Ref. 0) to make available specified information. The meaning of the term "make available," however, depends on the type of application referencing the topical report, as follows: A licensee requesting amendment of an existing operating license will make available the identified information by including it in the application. An applicant for certification of a standard design will make available the identified information at the time of presentation of the application or by proposing Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) that address it. Similarly, an applicant for a Combined License (COL) will make available the identified information by providing the necessary information at the time of license application or by (1) proposing ITAAC or by referencing a certified design that does so and (2) addressing any remaining COL action items identified in connection with the topical report in the design certification. A COL holder will ultimately address the information through the process of closing the associated ITAAC if any have been utilized during the licensing process.

BTP 7-14, A.3.1, describes three software planning characteristics: management, implementation, and resource. Management characteristics are significant to the management of the project activities. Implementation characteristics describe the work necessary to achieve the purpose of the planning documents. Resource characteristics describe the material resources necessary to carry out the work defined in the planning document. The Common Q SPM was reviewed against these planning characteristics. These characteristics were assessed and compared to the characteristics described in BTP 7-14 to determine the adequacy of software planning activities implemented for Common Q.

3.1 Design Considerations

The Common Q platform is a distributed, microprocessor-based computer system. It is capable of being configured with three or four independent redundant data-processing paths or divisions,

each with two or three layers of operation. Data processing paths can be run asynchronously with respect to each other. Layers of operation include signal acquisition, data-processing, and actuation signal voting. The Common Q platform uses microprocessor-based digital equipment, operating system software, and plant-specific application software to perform safety-related I&C system functions at nuclear power plants. A full description of the Common Q platform may be found in the Common Q platform TRs (Refs. 1 and 14).

Application software is developed for project-specific applications of the Common Q platform. Software implements plant-specific I&C control and logic functions, and is hardware dependent. Software will be developed using ~~the ABB Master Programming Language Control Configuration (ACC) and Photon~~approved software development tools. The Common Q SPM describes the conditions and objectives to develop application software.

3.2 Life Cycle Planning Process for Application Software

Digital Instrumentation and Control (I&C) safety systems must be designed, fabricated, installed, and tested to quality standards commensurate with the level of the importance of the safety functions to be performed. The development of safety system software should progress according to a formally defined software lifecycle (SLC). Implementation of an acceptable SLC provides reasonable assurance the necessary software quality has been instilled in the final system. BTP 7-14, Section B.2.1 states that the information to be reviewed for the software life cycle process planning should be found under the following topics:

B.3.1.1 Software Management Plan
B.3.1.2 Software Development Plan
B.3.1.3 Software Quality Assurance Plan
B.3.1.4 Software Integration Plan
B.3.1.5 Software Installation Plan
B.3.1.6 Software Maintenance Plan
B.3.1.7 Software Training Plan
B.3.1.8 Software Operations Plan
B.3.1.9 Software Safety Plan
B.3.1.10 Software Verification and Validation Plan
B.3.1.11 Software Configuration Management Plan
B.3.1.12 Software Test Plan

In addition, WEC developed a separate Secure Development and Operating Environment (SDOE) plan to address the criteria of RG 1.152 which provides guidance for the establishment of a SDOE for safety related software. Section 12 of the SPM constitutes the Common Q SDOE Plan.

While most of the information about the above topics is in the SPM, information found in the other submittals and in previous revisions of the SPM is sometimes helpful to the evaluation, and therefore, was considered for this evaluation. The SPM includes sections with the following section numbers and titles:

- (Section 3) Software Safety Plan (SSP)
- (Section 4) Software Quality Assurance Plan (SQAP)
- (Section 5) Software Verification and Validation Plan (SVVP)
- (Section 6) Software Configuration Management Plan (SCMP)

- (Section 7) Software Test Plan (STP)
- (Section 8) Software Installation Plan (SIP)
- (Section 9) Software Maintenance Plan (SMP)
- (Section 12) Secure Development and Operational Environment Plan

The staff found the information needed to support its safety conclusions on the balance of the life cycle topics either in the balance of the SPM or in the Common Q TR WCAP-16097-P "Common Qualified Platform" (Ref. 14) and its appendices. The staff has organized this report to follow the sequence outlined under the topic in BTP 7-14. BTP 7-14, Section B.3.1 describes the acceptance criteria used for reviewing the 12 software plans of the SPM.

3.2.1 Software Management Plan

The Software Management Plan (SMP) describes the management aspects of the software development project. BTP 7-14, Section B.3.1.1 describes acceptance criteria for software management plans. RG 1.173 endorses IEEE Std. 1074-2006, "IEEE Standard for Developing Software Life Cycle Processes." IEEE Std. 1074-2006 describes, in terms of inputs and outputs, a set of processes and constituent activities that are commonly accepted as comprising a controlled and well-coordinated software development process. IEEE Std. 1074-2006 Annex A, Section A.1, "Project Management Section of Activity Groups," describes an acceptable approach for software project management. It states that project management processes are, "the processes that initiate, monitor, and control software projects throughout the software life cycle."

The required elements of a Software Management Plan are contained within Sections 2, 4.3, 5.5.1, and 6.2 of the Common Q SPM. These sections of the SPM define a strategy for managing Common Q software projects. Each of these sections was reviewed against the specific acceptance criteria established by BTP 7-14.

Section 4.3 of the Common Q SPM describes the management principles used for the development of Common Q application software for each phase of the software development life cycle. It includes a description of the software project planning organization which includes a general overview of the organizational structure used by WEC and a discussion of the responsibilities that each of the following organizations has within the Nuclear Automation Organization.

- Quality Organization
- Engineering Organization
  - Design Team
  - V&V Team

The specific tasks and responsibilities performed by these organizations during each of the software lifecycle phases are described within the SPM. These tasks include software design and development, software quality assurance planning, verification reviews, audits, test planning, test execution, and test reporting. The SPM describes the interfaces and boundaries that exist between these organizations.

A level of independence between the Verification and Validation (V&V) Team and the Design Team is established by specifying different reporting structures up to the director level. Beyond the director level, the two teams report to the same vice president. The directors to which the

V&V team and the Design team report are administratively and financially independent of one another. This relationship between the design team and the independent verification and validation (IVV) team is illustrated in Exhibit 2-1, "Design/IV&V Team Organization," of the SPM. The degree of independence between the V&V team and the design team is further reinforced by not allowing V&V team members to participate on the design team.

The SPM calls for the development of a project specific Project Quality Plan (PQP) during the Initiation (Concepts) Phase of the software development life cycle. The PQP allows for alternatives to the SPM processes. Because of this, the PQP should be reviewed to determine if the justification for the use of alternatives to the SPM or other, additional metrics or qualifiers beyond the directions within the SPM is acceptable when an applicant requests approval for installation of a safety-related system based on the Common Q platform. This is plant specific action item 1.

Per BTP 7-14, Sections B.3.2 and B.3.3, the implementation activities and design outputs are to be separately evaluated so that the application design can be evaluated to determine that the software management plan has been followed. This is plant specific action item 2.

The elements of the software management plan are incorporated into the Common Q SPM. The staff has reviewed the Common Q SPM and finds that it establishes adequate organization and authority structure for the design, the procedures to be used, and the relationships between major activities. The staff finds that the management structure in the Common Q SPM provides for adequate project oversight, control, reporting, review, and assessment. The management structure also supports independence of V&V activities. The staff concludes that the Common Q SPM meets the requirements for a software management plan as outlined in IEEE Std. 1074-2006 as endorsed by RG. 1.173 and, is, therefore, acceptable.

3.2.2 Software Development Plan

The Software Development Plan (SDP) describes the plan for technical project development. BTP 7-14, Section B.3.1.2 describes acceptance criteria for software development plans. RG 1.173 endorses IEEE Std. 1074-2006 as providing an acceptable approach to software development processes. BTP 7-14 states that the SDP should clearly state tasks of each life cycle, and state the life cycle inputs and outputs. The review, verification and validation of those outputs should be defined. IEEE Std. 7-4.3.2-2003 provides additional guidance on software development processes.

WEC uses a controlled software development process which is defined within the Common Q SPM. The criteria for the Common Q software development plan are satisfied by a project plan and a Project Quality Plan. These plans are created for each Common Q project in accordance with general criteria that is defined within the SMP. The required elements of a Software Development Plan are defined within the following SPM sections:

- 1.2.1, "Software Classification and Categorization"
- 1.4.1, "Software Life Cycle"
- 4.1.3, "Software Development Process"
- 5.9, "Software Integrity Level Scheme"

Common Q Software Life Cycle

Section 1.4.1 of the SPM defines the software lifecycle (SLC) used for the development of Common Q software. This life cycle is consistent with a classic waterfall model like the model discussed in Section 2.3.1 of NUREG/CR-6101. The Common Q SLC consists of the following life cycle phases:

- Concept
- Requirements Analysis
- Design
- Implementation or Coding
- Test
- Installation and Checkout
- Operation and Maintenance
- Retirement

This model assumes that each phase of the life cycle is completed in sequential order from concept to the retirement phase. The staff finds the WEC choice of SLC acceptable since the waterfall model is well suited for projects with known and stable requirements and where few changes to requirements are anticipated. Since WEC selected an acceptable software life cycle model, the guidance criteria of IEEE Std. 1074-2006, Section A.1 has been satisfied.

Common Q Software Life Cycle Tasks (Inputs & Outputs)

BTP 7-14, Section B.3.1.2.4 states that an applicant should identify which tasks are included with each life cycle phase, and identify the life cycle tasks' inputs and outputs. Exhibit 4-3 of the SPM identifies tasks which are performed for various software categories (defined by the Common Q software integrity scheme described below) during the SLC process and identifies the phases during which each task is performed. Revision 5 of the SPM adds tasks to accommodate the System Validation Testing and Factory Acceptance Testing in accordance with the updated test methods presented in the SPM. In addition, Exhibit 5-1, "Software Tasks and Responsibilities," of the SPM defines the responsibilities for completion of software tasks.

Note: Several exhibits are included in the SPM to show that all required V&V tasks are included as part of the SLC processes. In Exhibits 4-3 and 5-1, WEC has grouped individual tasks into general category headings. For example the task "Design Verification" may include several individual subtasks that are not listed in Exhibit 5-1. As such, specific individual V&V tasks are not delineated in these tables. Exhibit 5-8 was created in conjunction with Section 5 of the SPM to list and define the specific V&V tasks and to map these tasks to the V&V activities defined within IEEE Std. 1012-2004. Exhibit 5-8 was updated in SPM Revision 5 to accommodate System Validation Testing and Factory Acceptance Testing in accordance with the updated test methods presented in the SPM.

IEEE Std. 1012-2004, Clause 1.7, "Conformance," states that the minimum V&V tasks are defined by the software integrity level assigned to the software. Exhibit 5-8 of the SPM includes a table which identifies the minimum tasks for each software integrity level of the Common Q platform. This exhibit contains a mapping of the V&V activities associated with the development lifecycle of a Common Q system to the IEEE Std. 1012-2004 standard. This mapping table also identifies the phase of the development lifecycle in which each activity is performed. Several V&V activities are performed multiple times during the development process. The left-hand

column of this table lists all of the V&V activities from Table 2 of IEEE Std. 1012-2004. Each of these activities has a corresponding activity and reference to the SPM section for the equivalent activity within the Common Q development process. The staff reviewed the activities included in this mapping table and determined that it contains sufficient detail and reference to the SPM to show that the V&V activities performed for safety related Common Q application Protection software are consistent with high criticality software developed to software integrity level (SIL) Level 4 as defined by IEEE Std. 1012-2004 and is therefore acceptable.

Common Q Software Integrity Level Scheme

Section 5.9 of the Common Q SPM discusses the WEC Common Q specific software classification or software integrity level scheme.

Table 5.9.1 of the SPM compares the WEC software integrity level scheme with the scheme presented within IEEE Std. 1012-2004. IEEE Std. 1012-2004 states: "This standard uses software integrity levels to determine the V&V tasks to be performed. High-integrity software requires a larger set of V&V processes and a more rigorous application of V&V tasks." Section 1.2.1 of the SPM defines the software classes used for Common Q software as follows:

- ***Protection*** *(safety critical). Software whose function is necessary to directly perform RPS control actions, ESFAS control actions, and safe shutdown control actions.*

- ***Important-to-Safety****. Software whose function is necessary to directly perform alternate protection system control actions or software that is relied on to monitor or test protection functions, or software that monitors plant critical safety functions.*

- ***Important-to-Availability****. Software that is relied on to maintain operation of plant systems and equipment that are critical to maintaining an operating plant.*

- ***General Purpose****. Software that performs some purpose other than that described in the previous classifications. This software includes tools that are used to develop software in the other classifications, but is not installed in the online plant system. Examples of General Purpose software include commercial grade dedication test software, compilers, assemblers, linkers, comparators, editors, test case generators, and test coverage analyzers.*

Exhibit 4-1 of the SPM identifies assignment of Common Q components to the software classes described above. All Common Q application software on the Advant Controller 160 (AC160) safety processors, the Operator Modules (OM's) and the Maintenance and Test Panels (MTP's) are classified as either Protection, which is equivalent to SIL 4 as defined in IEEE 1012-2004, or Important to Safety. This is consistent with the fact that Common Q system is classified as Class 1E as defined by IEEE Std. 603-1991.

Common Q Components and software that are classified as either Protection or Important to Safety are considered to be safety related. It is however, understood that the subset of safety related software that is classified as Important to Safety does not directly perform RPS or ESFAS safety functions. For this reason, it is acceptable for Important to Safety software to be developed using V&V activities that are not equivalent to SIL Level 4 activities as defined in IEEE Std. 1012-2004.

The staff finds the software integrity level scheme used for the Common Q platform and application development acceptable since it is similar to the software integrity level scheme defined in IEEE Std. 1012-2004, and because the scheme is appropriately used to establish a minimum set of V&V tasks for development of Common Q application software. Section 3.2.10 of this SE provides additional evaluation of the V&V tasks performed on Common Q software.

Management and Oversight of the Software Development Processes

The project manager is responsible for ensuring that the design, verification and validation, and quality assurance (QA) activities are conducted in accordance with the SPM. The corrective action program used during the Common Q development process is defined in Section 11, "Problem Reporting and Corrective Action," of the SPM. This program is designed to promptly identify and correct conditions adverse to safety and quality. This program provides oversight to ensure that development process will be followed and any deviation will be discovered in time to take corrective action. This section of the SPM was updated to accommodate the changed testing processes being implemented within the SPM and to clarify use and management aspects of the corrective action program associated with Revision 5 of the SPM. Also, Exhibit 11-2 was eliminated from the SPM. This exhibit had been a sample printout of a software tool used to implement the corrective action processes. Required information for exception reporting is now captured in Exhibit 11-1 and specific tool usage information is being omitted. The NRC staff considers this acceptable as long as the minimum required information for exception reporting is retained.

Software Tools

BTP 7-14, Section B.3.1.2.4 provides guidance for software tools, and references IEEE Std. 7-4.3.2-2003, Clause 5.3.2, which states, in part, that software tools used to support software development processes and verification and validation processes shall be controlled under configuration management. To confirm the software tools are suitable for use, the clause further states either a test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as intended or the software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

The Common Q SPM Sections 3.3.10, "Tool Support and Approval," and 4.9, "Tools, Techniques and Methodologies," discuss the development support tools used to facilitate Common Q application software development. An evaluation of a tool's readiness for use on a project is performed before such a tool is used to support the development of a Common Q application. This evaluation considers; the tool's past performance, extent of tool validation performed, consistency of tool design with planned use, use of tool upgrades, retirement of the tool, and restrictions on the use of the tool due to its limitations. The configuration management, software quality assurance and IVV processes defined within the SPM apply to software tools and provide a means of ensuring that these tools are only used for their approved and intended purposes. The outputs of software tools undergo the V&V process as defined in the Software Verification and Validation Plan (SVVP), in SPM Section 5.

The staff has reviewed the Common Q SPM and concludes that the software development plan conforms with the criteria provided by IEEE Std. 1074-2006, "IEEE Standard for Developing Software Life Cycle Processes," as endorsed by RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." In addition, the SPM adequately addresses the software development planning activities of

BTP 7-14. The SPM describes acceptable methods of organizing the software life cycle. The staff, therefore, concludes that WEC's application software development plan is acceptable.

3.2.3 Software Quality Assurance Plan

BTP 7-14, Section B.3.1.3 provides guidance in evaluating a Software Quality Assurance Plan (SQAP). The SQAP shall conform to the requirements of 10 CFR Part 50, Appendix B, and the applicant's overall QA program. 10 CFR Part 50, Appendix B states that the applicant shall be responsible for the establishment and execution of the quality assurance program. The applicant may delegate the work of establishing and executing the quality assurance program, or any part thereof, but shall retain responsibility for the quality assurance program. The SQAP would typically identify which QA procedures are applicable to specific software processes, identify particular methods chosen to implement QA procedural requirements, and augment and supplement the QA program as needed for software.

IEEE Std. 7-4.3.2-2003, Clause 5.3.1, which is endorsed by RG 1.152 provides guidance on software quality assurance. IEEE Std.7-4.3.2-2003, Clause 5.3.1, states, "Computer software shall be developed, modified, or accepted in accordance with an approved software QA plan.

The Common Q SQAP for application software is described in Section 4 of the SPM, "Software Quality Assurance Plan." The SQAP describes the methodology used for managing Common Q software throughout the development life cycle. Section 4.1.1 of the SPM states that the Common Q SPM complies with IEEE Std. 730-1998. The scope of the Common Q SQAP includes software in all four SIL classifications ~~for~~: protection, ~~and~~ important to safety, important to availability, and general purpose. ~~The Common Q SQAP no longer applies to software classified as: important to availability or general purpose software.~~ The Common Q SQAP applies to original protection and important to safety software that was developed under the requirements of the Common Q SPM.

Evaluations of existing software not created under the controls of the Common Q SPM are performed in order to qualify this software for use under the Common Q SPM. For commercial software, qualification is achieved through the use of WEC's commercial grade dedication program. For non-commercial protection and important to safety software that has actively been used in a nuclear power plant being implemented in Common Q, an evaluation is performed to ensure the quality assurance program being used for development and maintenance of this software is acceptable and includes the following:

- The effective quality assurance program has an active program for problem and corrective action reporting.
- The software has adequate design documentation.
- The software has adequate user documentation.
- The software includes well commented source code.
- The software has been verified and validated under a program that the IVV team determines to be appropriate.

For non-commercial software that has not been actively used in a nuclear power plant being implemented in Common Q, an evaluation is performed to ensure that appropriate quality controls commensurate with the safety classification of the software are implemented.

Quality assurance tasks are listed in Exhibit 4-3 of the SPM. These quality assurance tasks are described in Section 4 of the SPM for each software life cycle phase. These descriptions include a discussion of the tasks and the responsibilities of the organizations performing software quality assurance activities. In addition, Exhibit 5-1 identifies organizational responsibilities for performance of specific software SQA tasks.

Documentation requirements for performance of software Quality Assurance (SQA) activities are described in Section 4.4, "Documentation," of the SMP. Many of the tasks listed in Exhibit 4-3 are in fact documents that will provide evidence for completion of the associated SQA tasks. Furthermore, Section 10 of the SPM, "Documentation," provides guidance for how these documents will be developed.

SPM Section 4.5 identifies the standards, practices, conventions and metrics used for the development of a Common Q based system. It states that, "*compliance with the WEC quality management system standards shall be monitored and assured through the review and audit process."* Standards used for development of Common Q systems include Coding Standards, Software Testing Standards, and Documentation Standards. Coding standards are not established at a generic level and are instead defined within the project specific PQP. Testing standards are defined by the Software Test Plan which is evaluated in Section 3.2.12 of this SE. Documentation Standards are identified in Section 10 of the SPM and include IEEE Std. 830-1998 for Software Requirement Specification (SRS) documentation requirements, IEEE Std. 1016-1998 (Reaffirmed in 2009) for Software Design Description (SDD) documentation requirements, IEEE Std. 1012-2004 for V&V documentation requirements, and IEEE Std. 1063-2001 for Software User documentation requirements.

SPM Section 4.6 describes how software reviews are performed for Common Q applications. Software reviews are performed to verify technical adequacy and to verify completeness of the design and development of Common Q software. The SPM lists several software review activities and defines groups responsible for performance of these activities. The following types of reviews which are defined in IEEE Std. 1028-2008 are performed for Common Q software developed under the SPM:

- Management Reviews,
- Technical Reviews,
- Inspections,
- Walk-through's, and
- Audits.

SPM Section 4.6.2 describes the minimum software reviews and audits to be performed for Common Q software. The staff has determined that this minimum set of review and audit requirements complies with the criteria of IEEE Std. 730-1998 Sections 4.6.2.1 through 4.6.2.10.

IEEE Std.730-1998, Section 4.8 states that the SQAP should describe practices and procedures to be followed for reporting, tracking, and resolving problems. It also stipulates that the SQAP should state specific organizational responsibilities concerned with implementation.

The Common Q SPM Section 11, "Problem Reporting and Corrective Actions," discusses the Common Q processes relating to these criteria. The SPM describes the problem reporting process used to handle discrepancies, deficiencies, or comments identified as a result of

testing, review, or other means. The SPM describes two processes used for reporting errors. One is used for errors identified during the development process prior to approval for use in a nuclear power plant application. The other is used for reporting of errors that are identified after the software has been approved for use. These processes include noncompliance reporting in accordance with 10 CFR Part 21, "Reporting of Defects and Noncompliance." Organizational responsibilities associated with the problem reporting and corrective action processes are also defined in the SPM.

During the Initiation (Concept) phase, the SQAP calls for the development of a PQP which becomes the operative plan for a specific application development process. This PQP may deviate from the SQAP processes defined in Section 4 of the SPM; however, any such deviations must be documented and justified within the PQP. Because such deviations cannot be evaluated during this safety evaluation, a plant specific action item for evaluating these changes has been created. This is plant specific action item 1.

The regulation at 10 CFR Part 50, Appendix B, allows applicants or licensees to delegate the work of establishing and executing the Quality Assurance program, but applicants/licensees shall retain overall responsibility and shall determine if the quality of the software is sufficient. Applicants or licensees referencing this topical report are to make available a SQAP to address these licensee specific responsibilities. This is plant specific action item 3.

The SQAP stipulates that the SQA organization shall participate in formal reviews and audits of the software development activity. Required reviews and audits are indicated in the plan including review documentation requirements, evaluation criteria, anomaly reporting, and anomaly resolution procedures. Additional reporting of the staff's evaluation of the SQAP is detailed in Section 3.2.10, "Software Verification and Validation Plan."

The SQAP describes the process by which WEC manages software and documentation throughout the Common Q software development life cycle, and the SQAP conforms to IEEE Std. 730-1998. The Engineering Project Manager is responsible for ensuring all design team activities are performed in accordance with the QA processes and procedures. The SQAP adequately addresses the software quality planning activities of BTP 7-14. The staff concludes that the Common Q SQAP meets the Guidance in BTP 7-14 Section B.3.1.3 with regard to QA software reviews and audits and is, therefore, acceptable.

Revision 5 to the SPM includes a change to the process for development of a site test plan. This change allows development of the site test plan to occur at a later stage of the development lifecycle to support evaluation of requirement testability on-site. The V&V activity for system V&V test plan generation described in Exhibit 5-8 of the SPM was also revised to facilitate later stage development of the site test plan if necessary. The NRC staff finds this change acceptable because required V&V activities are retained. This change allows for later stage completion of required tasks and does not alter the requirements for task completion.

3.2.4 Software Integration Plan

BTP 7-14, Section B.3.1.4 provides guidance in evaluating a Software Integration Plan (SIntP). IEEE Std. 1074-2006, Clause A.1.2.8, "Plan Integration," which is endorsed by RG 1.173, provides an acceptable approach to an integration plan. Clause A.1.2.8.2 states that during the plan integration activity, the software requirements and the software design description are analyzed to determine the order of combining software components into an overall system. In addition, Clause A.1.2.8.2 states that the integration planned information shall be coordinated

with the evaluation planned information. BTP 7-14, Section B.3.1.4.1 guidance calls for a general description of the software integration process and of the software integration organization.

For the Common Q, WEC does not define a separate software integration organization to perform system integration related activities. Instead, such activities are allocated to different organizations involved with the Common Q software development processes. This allocation of integration activities is defined within various sections within the SMP. For example, Integration Tests are defined in Section 7.3.1.3 of the SPM and Exhibit 5-1 shows that the IVV Team has the responsibility for performing Integration tests for Protection software. Conversely, the design team has the responsibility for performing Integration tests for Important to Availability software.

The testing aspects of Common Q Software Integration are described in Section 7, "Software Test Plan," of the SPM. The Common Q software testing process includes Integration Tests that are conducted on the production hardware or with a system that is functionally equivalent to the production system. This section also specifies that a functionally equivalent system entails a test bed which provides a functionally equivalent configuration to the production hardware.

The NRC staff notes this is a deviation from the integration test description provided in the previous version of the SPM which stated that integration tests were to be performed on actual production hardware. The NRC staff determined that allowing performance of integration tests on non-production hardware is acceptable based on the fact that first of a kind systems undergo system validation tests, which per Section 4.7 of the SPM, encompass the scope of a factory acceptance test (FAT) and subsequent factory tests must still be performed using actual production equipment. Section 7.3.1.5, "Factory Acceptance Test (FAT)," of the SPM states that "FAT includes tests that are performed on the deliverable system for each deliverable system." In addition, Westinghouse confirmed in its response to RAI 7, and RAI 8 (Reference ~~0~~16) that "… the Factory Acceptance Test (FAT) is performed on the delivered equipment." Subsection 7.3.1.3, "Integration Test," describes the details of the integration tests performed during the development of a Common Q application.

Revision 5 of the SPM changed Section 7.3.1.3, "Integration Test," of the SPM such that the following Integration Test Items listed were removed.

- Error Handling
- Communications
- Redundancy
- Diversity

In response to RAI 6 (Ref. 15), Westinghouse stated that because Integration testing is used as part of system validation testing when validating the design and as part of the FAT testing to demonstrate the deliverable system has been properly integrated, the removed test items will continue to be performed and are included as test items in Sections 7.3.1.4, "System Validation Test," and 7.3.1.5, "Factory Acceptance Test (FAT)." The NRC staff confirmed this to be the case and determined that removal of these test items from Section 7.3.1.3 of the SPM is acceptable because all required test activities will continue to be performed.

Subsection 4.5.2.4 of the SPM discusses metrics used for integration tests.

The Common Q system is an integrated suite of hardware and software designed specifically for nuclear safety applications. Software integration of an application that uses Common Q consists of three components.

1. Integration of software modules to form system executable programs. For a Common Q project this level of integration is accomplished by the creation of control functions using ~~the AMPL Control Configuration (ACC)~~an approved~~,~~ development tool. Proper use of ~~ACC~~ the tool involves assembly of pre-approved Program Control (PC) elements into complete control functions. These control functions are converted into code to be used for transfer to the Common Q hardware. Structured design techniques, including the use of data flow diagrams represent interactions among modular elements and the flow of data among these elements. Unit and Module tests are performed to ensure that the module and system requirements have been met by the integrated software.

   Software used in the flat panel display system (FPDS) is developed in accordance with the SPM processes. FPDS software applications are developed using ~~the photon~~an approved graphical user interface software tool. Structured design techniques similar to those used for AC160 are also applied to the development processes of the FPDS components. These FPDS applications are then integrated into the FPDS node box and the FPDS hardware is integrated into the application specific Common Q system design.

2. Integration of the resultant programs with the production hardware and instrumentation or with representative functionally equivalent hardware and instrumentation. This level of integration is performed at the manufacturing facility after the cabinets are assembled and energized. Optionally, this integration testing can be performed using surrogate equipment which is functionally equivalent to the production hardware. The system hardware architecture is established in conjunction with the application software ~~using the ACC tool~~; therefore, specific assignment of software programs to PM646A processors is performed prior to the generation of application executable code. The processor applications are loaded into the PM646A processors as the system is prepared for integration testing. An integration test is performed to verify that the released software correctly integrated with the production hardware or representative test bed hardware. All cabinets within a safety system division are interconnected and integrated as a part of the integration test process.

   The NRC staff notes that even in cases where representative equipment is used for integration test purposes, subsequent factory tests must be performed using actual production equipment. Section 7.3.1.5, "Factory Acceptance Test (FAT)," states that "FAT includes tests that are performed on the deliverable system for each deliverable system."

3. Testing the resulting integrated product. This final level of integration is completed during the System FAT by confirming the correct relationship between test input and output signals. System functions that are implemented across multiple safety divisions are tested to ensure that the overall integrated system meets the systems specifications defined in the System Requirements Specification. For first of a kind systems (FOAKs), certain activities associated with the FAT may have been performed during the system validation tests, and if properly documented, would not need to be re-performed during the FAT. For Nth of a kind systems, the FAT, together with the documentation for prior V&V activities, verifies that all system level functional and performance requirements are satisfied. Regardless of whether the FAT is for a FOAK system or Nth of a kind system,

the purpose of a FAT is to demonstrate the complete system is integrated and functional.

The staff reviewed WEC's application software development and testing processes for both AC160 and FPD software and found they specify how to develop plans for software integration both during the development of the software and during integration with the hardware. The actual integration procedures will be prepared during the planning stage of each project. The staff concludes that the plans for software integration exhibit the management, implementation, and resource characteristics outlined in BTP 7-14 and are, therefore, acceptable.

3.2.5 Software Installation Plan

The acceptance criteria for a Software Installation Plan are contained in BTP 7-14, Section B.3.1.5. IEEE Std. 1074-2006, Clause A.1.2.4, "Plan Installation," endorsed by RG 1.173, provides an acceptable approach for software installation plans. The software installation plan includes the necessary software modifications, checkout in the target environment, and customer acceptance. If a problem arises, it must be identified and reported. BTP 7-14, Section B.3.1.5.4 states that there should be approved procedures for software installation, for combined hardware and software installation, and systems installation. In addition there should be a controlled process to identify, correct, and document errors in the installation procedures.

The Software Installation Plan for Common Q system software is Section 8 of the Common Q SPM. Its purpose is to describe the installation processes to be used for the Common Q system. These processes include loading both operating system and application software into the production Common Q AC160 processor modules and Flat Panel Display system processors.

The staff reviewed the Common Q SPM and found that it included adequate plans for software installation. The procedure(s) for installing the software will be prepared before the installation and checkout phase of the software life cycle. The staff finds that the plans for software installation exhibit the management, implementation, and resource characteristics outlined in BTP 7-14 and are, therefore, acceptable. However, the Common Q Software Installation Plan does not address the installation of the Common Q System into the plant environment. Since the applicant or licensee assumes responsibility, including vendor oversight, for the software installation phase information necessary to address the criteria of BTP 7-14, further evaluation of the site installation activities will be required. This should be accomplished as part of plant specific action item 2.

3.2.6 Software Maintenance Plan

The acceptance criteria for a Software Maintenance Plan are contained in BTP 7-14. Section B.3.1.6. IEEE Std. 7-4.3.2-2003, Clause 5.4.2.3, endorsed by RG 1.152 provides guidance on maintenance and configuration management for commercially dedicated items. IEEE Std. 1074-2006, Clause A.4.2.3, "Maintenance Activity Group," provides an approach for software maintenance plans. IEEE Std. 1074-2006, Clause 6.3.1 states the Maintenance Activity Group is concerned with the identification of enhancements and the resolution of software errors, faults, and failures. NUREG/CR-6101, Section 3.1.9 and Section 4.1.9 also contain guidance on Software Maintenance Plans. These sections identify the maintenance activities to be governed by the Software Maintenance plan as; failure reporting, fault correction, and re-release procedures.

The Software Maintenance Plan for Common Q system software is Section 9 of the Common Q SPM. This plan specifies the requirements for the maintenance and use of Protection class and Important-to-Safety class software used in Common Q Systems. Activities associated with the maintenance phase include:

1. Problem/modification identification, classification and prioritization;
2. Modification analysis;
3. Software maintenance design;
4. Software maintenance implementation;
5. New Software / System test; and
6. Modification delivery.

The staff has reviewed the plan for maintenance of the software as described in the SPM and concludes that it exhibits the characteristics for management, implementation, and resources as set forth in BTP 7-14 and is, therefore, acceptable.

3.2.7 Software Training Plan

The acceptance criteria for a Software Training Plan are contained in BTP 7-14, Section B.3.1.7. IEEE Std. 1074-2006, Clause A.1.2.6, "Plan Training," endorsed by RG 1.173, provides an acceptable approach to software training plans. If the licensee will be performing the digital system maintenance, the training plan(s) will be more involved, since additional knowledge is necessary to perform maintenance.

Personnel involved in Common Q software design and development are required to have documented training in material covered by the SPM. The requirements for training associated with the Common Q system are addressed within the following sections of the SPM:

- 3.3.3, "Staff Qualifications and Training"
- 3.5.1, "Training"
- 4.14, "Training"
- 7.2.2, "Staffing and Training"

In addition requirements for maintaining Training Materials and Training Records are listed in Table 1, "Document Requirements" and Table 2, "Information Requirements," for the Common Q system.

The Common Q SPM specifies the requirements for training programs for end users if within Westinghouse's scope of supply. WEC develops training materials and training programs for use by its Common Q customers. Once delivered, the customer assumes responsibility for providing training to its operators, maintenance and management personnel as appropriate.

All training materials prepared for Common Q customers must be reviewed by the IVV team. For each software system, a separate training program will be developed to ensure safe operation and use of the software within the overall system. The training program will include safety training for the users, operators, and maintenance and management personnel, as appropriate. The SPM stipulates that a training record will be kept on file for each training session, recording the instructor, date, material covered, and personnel attending, to ensure that the appropriate training has been obtained before using the system. The V&V team will review the training documentation for traceability to safety requirements. The training programs

for use at the sites will be developed later. This is an activity that will be influenced by the end users' training facilities and procedures. The staff concludes that the specified plans for training of the software developers and end users meet the criteria outlined in BTP 7-14 and are, therefore, acceptable.

3.2.8 Software Operations Plan

The acceptance criteria for a Software Operations Plan are contained in BTP 7-14, Section B.3.1.8. IEEE Std.1074-2006, Clause A.4.2, endorsed by RG 1.173, provides guidance for software operations plans. IEEE Std.1074-2006, Clause A.4.2 states an operation and support process involves user operation of the system and ongoing support. Support includes providing technical assistance, consulting with the user, and recording user support requests by maintaining a Support Request Log. Thus, the Operation and Support Process may trigger Maintenance Activities, which the Software Maintenance Plan should address. IEEE Std.1074-2006, Clause A.4.2.1.2 states that the Installed Software System shall be utilized in the intended environment and in accordance with the operating instructions.

The revised version of the SPM, does not contain a dedicated section to address the criteria for software operations planning. WEC stated that the Software Operations Plan is either a project specific activity or the Licensee's responsibility.

The Software Operations Plan is not within the scope of the Common Q Software Program Manual. Therefore, a safety determination cannot be made for a Software Operations Plan in this regard. Since the applicant or licensee will assume responsibility, including vendor oversight, for the software operations phase of the software life cycle, relevant information must be evaluated as part of a plant specific action item. An evaluation of compliance with the criteria of BTP 7-14 Section B.3.1.8 shall be performed at the time of system development when the operational aspects of the system have been defined. These requirements are captured as PSAI's 3 and 4.

3.2.9 Software Safety Plan

BTP 7-14, Section B.3.1.9 provides guidance to evaluate software safety plans (SSP). The SSP should require that appropriate safety requirements be included in the software requirements specification. The SSP should define the safety-related activities to be carried out for each set of life cycle activities, from requirements through operation and maintenance. The SSP should describe the boundaries and interfaces between the software safety organization and others. It should show how the software safety activities are coordinated with the development activities and the interactions between software safety organization and the software V&V organization. SSP should designate a single safety officer who has clear responsibility for the safety qualities and has clear authority to accomplish the goals of the safety requirements in the SRS design, and implementation of the software.

The Software Safety Plan for Common Q system software is Section 3, Software Safety Plan," of the Common Q Software Program Manual. The stated purpose of the Common Q Software Safety Plan is, *"…to enable the development of safety critical software for Common Q™ Systems that has reasonable assurance that software defects do not present severe consequences to public health and safety."*

To accomplish this goal, the Common Q SSP defines procedures and methods to be used for the development, procurement, maintenance and ultimately, retirement of all Protection class

Common Q software. The other classes of Common Q software; Important to Safety, Important to Availability, and General Purpose, are not included in the SSP because they are not considered to be safety critical. This is because the failure of this software would not result in severe consequences to public health and safety.

Software Safety Organization:

The Common Q SSP establishes a software safety organization which is composed of two parts. The first part is the quality organization, which is an independent quality assurance department. This quality organization coordinates and reviews quality assurance procedures and directives. The Quality organization has a reporting chain separate from the design team such that the QA organization is independent of project schedule and cost considerations. The Quality organization provides oversight by way of periodic audits to verify that the Automation Engineering organization is correctly abiding by both the procedures and directives generated by both organizations. The SSP is approved by the Manager of the Quality organization, or designee.

The second part of the software safety organization is the Independent Verification and Validation Team (IVV Team). This IVV team performs the safety activities for a given Common Q system implementation project.

The resource requirements needed to perform software safety activities are to be developed by the IVV team leader and the Engineering Project Manager. A plant specific Project Quality Plan will coordinate both the system development, software safety and quality assurance activities to identify the prescribed procedures and provide the resources needed for their execution.

During the requirements phase of the software development life cycle process, an evaluation is performed to identify the safety critical hazards posed by the system through its interfaces. For each hazard identified, the analysis determines whether a software malfunction could produce the hazardous condition. Each software producible hazard is then subsequently evaluated during each development phase of the safety critical software to determine if new hazards have been introduced during that phase, or if the evolving design has altered the results of the hazards analysis. The results of IV&V analyses performed on requirements, design, code, test and other technical documentation are documented in the IVV Phase Summary Reports and the Final IVV Report for the system.

The safety requirements that need to be met by the software in order to mitigate or control system hazards are defined in the system requirements specifications. The software design description will include descriptions of the software design elements that satisfy the software safety requirements. The responsibilities for the execution of the SSP and for ensuring that the software safety activities are completed in accordance with the plan are divided between the IVV Engineering Line Manager (ELM) and the quality manager.

The safety organization defined in the Common Q SSP considers the security risk as well as the risk to the plant if the digital system malfunctions. The critical design review identifies the risks associated with the system design in a manner that is consistent with the software safety strategy.

The staff has reviewed the Common Q SSP and finds that it addresses the topics described in the SRP and in IEEE Std. 1228-1994 (Reaffirmed in 2002), "IEEE Standard for Software Safety Plans." The Common Q SSP describes the organizational structure and responsibilities,

resources, methods of accomplishment, and integration of system safety with other program engineering and management activities. The hazards evaluations required by the SSP will be documented in the V&V documentation. The Common Q SSP identifies the international, national, industry and company standards and guidelines to be followed by the safety organization. The staff determined the software safety activities defined in the SSP will adequately identify and resolve safety issues associated with the Common Q software. The staff concludes that the Common Q SSP adequately addresses the topics outlined in the SRP and is, therefore, acceptable.

3.2.10 Software Verification and Validation Plan

The acceptance criteria for the SVVP are contained in the SRP, BTP 7-14, Section B.3.1.10, "Software Verification and Validation Plan," and Section B.3.2.2, "Acceptance Criteria for Software Verification and Validation Activities. "These sections identify RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" which endorses IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation," as providing methods acceptable to the NRC staff for meeting the regulatory requirements for verification and validation of safety system software. This section also states that further guidance can be found in NUREG/CR-6101, Sections 3.1.4 and 4.1.4.

Verification is defined as the process of determining whether the products of a given phase of the development cycle fulfill the requirements established during the previous phase. Validation is defined as the test and evaluation of the integrated computer system to ensure compliance with the functional, performance, and interface requirements.

Combined, verification and validation is the process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill (i.e., implement) the requirements to meet the criteria imposed by the previous phase, and the final system or component complies with specified requirements.

The Software V&V Plan for Common Q system software is Section 5 of the Common Q Software Program Manual. The stated purpose of the Common Q SVVP is to establish requirements for the IVV process to be applied to Common Q systems. It also defines when, how and by whom specific IVV activities are to be performed.

The aim of the Common Q software V&V program is to provide an acceptable generic methodology of V&V as part of the qualification process for computer software applications developed for the Common Q platform. The Common Q SVVP applies to all new software to be developed under the SPM and to some previously developed application software to be used in the Common Q platform. For the qualification of existing software, either for use in the generic Common Q platform or for use in new applications, the following cases are identified:

- Existing commercial software will be qualified under the Commercial Grade Dedication Program, which is outlined in the Common Qualified Platform Topical Report (Ref. 14).

- Existing non-commercial software that has been actively used in nuclear power plants will be qualified for the Common Q platform by judging its original V&V program. The V&V effort will make this judgment using review criteria similar to those for newly developed software.

Other existing non-commercial software may be used under the conditions that (1) the software fulfills a specific requirement identified in the software requirements specification, (2) the code is well organized and has adequate design documentation and source code commentary to permit the application of the V&V process, and (3) the software is subjected to the V&V process, starting at the design phase.

For the development of new application software, depending on the scope of each specific project, WEC will decide whether to issue a project-specific SVVP or to maintain the generic plan as is. The use of the generic plan will require that the software developers manage the deviations and the project-specific aspects through the project-specific plan to be developed for each project. WEC will hold these project-specific SVVPs for audit. WEC also will hold the project-specific V&V reports for projects developed under the Common Q platform for audit, and the licensees will hold the V&V reports associated with plant-specific applications for audit. Succeeding systems manufactured under the same design as a system that was previously verified and validated in accordance with this SVVP will be certified by performing, as a minimum, the equivalent of the validation tests that were applied to the verified and validated system. The staff considers this approach to be acceptable.

WEC differentiates the span of the V&V activities and the grade of independence required for V&V reviewers according to the classification of each software item. The Common Q software integrity level classifications have been updated in Revision 5 of the SPM and are discussed in Section 3.2.2 of this SE. These Classifications are:

- Protection,
- Important to safety,
- Important to availability, and
- General purpose.

These four levels respectively are matched to the four categories in IEEE Std. 1012-2004 of ~~high~~4, ~~major~~3, ~~moderate~~2, and ~~low~~1. The Software Integrity Levels described in the Common Q SPM are mapped to the activities associated with IEEE Std. 1012-2004, SIL 4 in the SPM.

WEC follows the guidance provided in IEEE Std.1012-2004 regarding structure and content for SVVPs when applied to the development of safety-related Common Q software. IEEE Std. 1012-2004 provides the uniform and minimum requirements for the format and content of these plans. Additionally, the standard defines the minimum set of specific V&V tasks to be carried out during each phase of the critical software development life cycle and the required inputs and outputs for these tasks. Exhibit 5-8 of the SPM lists and defines the specific V&V tasks used for Common Q software development and maps these tasks to the V&V activities defined within IEEE Std. 1012-2004. The tables in Exhibit 5-1 and 5-8 identify the minimum set of V&V activities for all classifications of Common Q software including noncritical software. The NRC notes that V&V Tasks for Important to Availability and General Purpose classifications are identified in Exhibit 5-1.

The Common Q SVVP incorporates verification reviews and validation testing. Verification reviews are supported by the use of checklists and requirements traceability analyses for the phases of requirements, design, implementation, test, and installation and checkout. A requirements traceability matrix will be prepared at the beginning of the software development process and updated throughout the phases of the software life cycle.

Validation testing includes structural and functional testing. Structural testing is performed on software modules and units by path testing. Module and unit testing will be performed in accordance with IEEE Std.1008-1987, "IEEE Standard for Software Unit Testing" (endorsed by RG 1.171). Functional testing is performed on the integrated computer system to determine whether the system meets its functional requirements (functional operations, system level performance, external and internal interfaces, stress testing, testability, and other requirements, as stated during the concept phase).

For protection and important to safety software, verification reviews are performed by the V&V staff. V&V activities for the preparation of test plans, procedures, test result reports and execution of tests are performed by either the design team or by the V&V team depending on the classification level of the software being tested. Exhibit 5-1 of the SPM designates which team is responsible for performing these activities. When the design team prepares the material or executes the tests, the V&V team will oversee the conduct of these activities by reviewing documentation and witnessing testing.

Revision 5 of the SPM introduces a System Validation Test process to validate the hardware design, software design, and system integration of first instance applications at a functional level. Section 7.3.1.4, "System Validation Test," of the SPM was added to the SPM to describe the System Validation Testing activities. Section 7.3.1.5 "Factory Acceptance Test," of the SPM has also been rewritten to adopt the new System Validation Test processes and to describe differences between validation activities performed during Factory Acceptance Testing and validation activities to be performed during the new System Validation Test activities. Exhibit 7-1 in the SPM provides a comparison of System Validation Test and Factory Test Processes.

Validation Test requirements are accomplished for each Common Q system through a combination of System Validation Test activities and Factory Acceptance Test activities.

The System Validation process is intended to be used to validate the first application or first instance of a system design while subsequent instances of the same design will undergo integration testing during Factory Acceptance Test processes. Factory Acceptance Tests will be limited in scope such that testing of logic that was previously verified during System Validation Testing will not be performed. For example, Factory Acceptance Testing will only include a subset of voting logic combinations to demonstrate each input to voting logic is effective whereas System Validation Testing of Voting Logic includes testing of all combinations including bypasses and forced trips.

System Validation Testing can also be performed using representative Common Q equipment in lieu of production hardware to be delivered and installed into a licensed facility. Conversely, Factory Acceptance Tests are performed on the deliverable system, both the hardware and software, and are performed for each deliverable Common Q system.

Test documentation will be prepared in accordance with IEEE Std.829-1998, "IEEE Standard for Software Test Documentation." IEEE Std. 829-1983 is endorsed by RG 1.170, September 1997. After the system is validated, a Code certificate is issued certifying that the system is acceptable for use. The SVVP addresses V&V activities associated with the operation and maintenance phase by ensuring that program modifications are submitted to the same V&V program applied to new software development. Software changes will be evaluated by a software safety change analysis, the results of which shall be found in the V&V report. The SVVP addresses the use of regression testing for the V&V of software modifications.

The SVVP also addresses activities designed to verify the adequacy of the software development documentation issued throughout the software life cycle, installation procedures, training materials, and user documentation.

As a result of the V&V activities throughout the software development process, V&V phase summary reports, including discrepancy reports, will be issued. A final V&V report will be issued after the V&V process, including the assessment of the overall software and system quality and a Code certificate. Results of V&V analyses performed on requirements, design, code, test, and other technical documentation are documented in the V&V phase summary reports and the final V&V report. Information on suspected or confirmed safety problems in the pre-released or installed system is recorded in the final V&V report. Results of audits performed on software safety program tasks are documented in the V&V phase summary reports and in the final V&V report. Results of safety tests conducted on all or any part of the entire system are documented in the test report. Software safety certification is documented in the Code certificate. The SVVP is reviewed for adequacy and completeness of the V&V methods by an independent reviewer.

The staff has reviewed the information in the SVVP regarding software module testing and concludes that the procedures used for performance of software module testing satisfy the software V&V program requirements of IEEE Std. 7-4.3.2-2003 and are, therefore, acceptable.

Independence of Verification and Validation

The independence requirements for organizations performing quality control activities are addressed by 10 CFR Part 50 through Criterion I and Criterion III of Appendix B. Criterion I requires in part, that individuals and organizations performing quality assurance functions have sufficient authority, organizational freedom and independence from cost and schedule. Criterion III requires that individuals or groups performing design control activities be different from those who performed the original design, but they may be from the same organization.

The positions reflected in specific standards addressing V&V activities associated with the implementation of digital I&C systems vary from requiring only technical independence, as in RG 1.152 by endorsing IEEE Std.7-4.3.2-2003, to requiring technical, financial and schedule independence, as in RG 1.168. IEEE Std.1012-2004, endorsed by RG 1.168, does not specifically address the level of independence required. IEEE Std.1012-2004 includes an informative annex contemplating the position that for high-integrity-level software, the level of independence required for the V&V organization encompasses technical, managerial, and financial independence.

The organization responsible for ensuring that the Common Q software has been developed according to the quality required by its classification (called the software safety organization in the SPM) is composed of two parts:

- An independent quality assurance organization, which performs the verification of the implementation of quality assurance requirements according to Appendix B of 10 CFR Part 50. This organization, outside the cognizant engineering organization (CEO), generates the quality assurance procedures and directives that are followed by all CEOs.
- An independent V&V Team within the CEO that performs the safety activities of the CEO for a given Common Q system implementation project.

Within the CEO, software activities are organized into two teams: the design team, responsible for the development of the software, and the V&V Team, which performs the testing of the system as well as the V&V activities. The director of the CEO is responsible and accountable for both technical and administrative aspects associated with the development and V&V tasks for each system assigned to the CEO. The director or manager may assign a project manager to be responsible for the development of the software for a specific Common Q project. The CEO Director assigns the appropriate resources to the project manager and the V&V team leader. Members of the V&V team are not allowed to participate on the design team, even on a part-time basis, while a safety-class system is being designed. The V&V team leader, responsible for the V&V, must not be the design team leader. Additionally, the independent reviewer must also be competent to perform the review.

In response to RAI 11 (Refs. 15 and 16), Westinghouse provided clarification of IV&V group membership. The SPM further states that; "The IV&V Team in the context of this SPM refers to those individuals within the IV&V organization who perform V&V functions on the safety system design, implementation, and test (i.e., engineers and technicians). The IV&V organization may include other individuals who perform supporting roles that are not design verification related and the organizational independence does not apply to those individuals."

The SPM states that the V&V leader is responsible for the schedule and budget for the V&V activities, the project manager is responsible for the schedule and budget for the activities associated with the software development and, therefore, financial and managerial independence between the development group and the V&V group is achieved.
The staff finds that the WEC approach on independence of V&V for the Common Q platform is in accordance with the requirements of IEEE Std.7-4.3.2-2003, and is compatible with IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation," as endorsed by RG 1.168 and is, therefore, acceptable.

3.2.11 Software Configuration Management Plan

BTP 7-14, Section B.3.1.11 provides guidance for the evaluation of the Software Configuration Management Plan, and states that IEEE Std.1074-2006, Clause A.1.2.2, "Plan Configuration Management," provides an acceptable approach to software configuration management. IEEE Std.1074-2006, Clause A.2.2.2.2 states that Software configuration management includes the evaluation, coordination, approval or disapproval, and implementation of changes to product components (e.g., code, documentation) after a baseline has been established. Items that are to be managed should include code, documentation, plans, specifications, project policies, procedures, and other artifacts. BTP 7-14, Section B.3.1.11.1 calls for the definition of the responsibilities and authority of the Software Configuration Management (CM) organization.

The Software Configuration Management Plan (SCMP) for Common Q system software is Section 6 of the Common Q SPM. The SCMP is applicable to all Common Q software as well as software tools used in the development of Common Q software. The Common Q SCMP describes the organizational structure that controls the configuration of software. Software Configuration Management is intended to be applied throughout the entire software life cycle, including requirements phase, design phase, implementation phase, test phase, installation and checkout phase, operation and maintenance phase, and retirement phase.

The design team and the IVV Group in the Nuclear Automation organization are responsible for implementation of adequate measures to manage and control the software configuration of a Common Q project. The Common Q SCMP describes the independence of those responsible

for system software configuration management functions from those responsible for verification and validation activities related to configuration management. The SCMP describes the process for configuration control including configuration identification, software change request, software change authorization, module and unit release history, baselines, and backups. The SCMP describes the software configuration management activities related to the software project baselines, the configuration change control authority and management, methods of access control, and the configuration status control log maintenance. Project-specific configuration management data that reflect the specific methods of managing the software configurations will be developed as part of the project plan required for every Common Q project. The SCMP identifies the international, national, industry, and company standards and guidelines to be followed for the software configuration management activity.

The staff concludes the SCMP conforms to the requirements identified in IEEE Std. 828-2005, which is endorsed by RG 1.169. This meets the criteria of BTP 7-14 and is, therefore, acceptable.

3.2.12 Software Test Plan

The acceptance criterion for STP is contained in the SRP, BTP 7-14, Section B.3.1.12, "Software Test Plan," and in Section B.3.2.4, "Acceptance Criteria for Testing Activities." These sections state that both RG 1.170, September 1997, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 829-1983, "IEEE Standard for Software Test Documentation," and RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing," identify acceptable methods to satisfy software unit testing requirements.

The Software Test Plan (STP) for Common Q system software is Section 7 of the Common Q Software Program Manual. This plan identifies the testing activities and test documentation required to verify and validate Common Q safety system software. The scope of the STP includes testing of Common Q platform component software as well as application software that is developed with the Common Q platform.

The Common Q STP describes and defines the test activities for the following test types:

- Module Tests
- Unit Tests
- Integration Tests
- System Validation Tests
- Factory Acceptance Tests

The Module level tests are performed to confirm proper functionality of the platform level software components of Common Q. These tests are not application specific and are used to develop a library of approved building blocks to be used for application development.

Unit tests are performed during the plant specific system design to ensure proper functionality of the platform components as they are incorporated into a specific application.

Integration tests are used to confirm that the program units have been properly connected and are integrated in a manner to ensure proper operation of the overall system. Integration tests

are conducted on the target hardware to be installed at the plant site so they also confirm the proper integration of software to the hardware of the system.

Validation Test requirements are accomplished for each Common Q system through a combination of System Validation Test activities and Factory Acceptance Test activities.

System Validation Tests are performed to validate the hardware design, software design, and system integration of first instance applications at a functional level. The System Validation process is intended to be used to validate the first application or first instance of a system design while subsequent instances of the same design will undergo integration testing during Factory Acceptance Test processes. System Validation Testing can be performed using representative Common Q equipment in lieu of production hardware.

Factory Acceptance Testing of the system is conducted with the final application software installed on the targeted hardware that has been assembled.

Revision 5 of the SPM adds a provision that allows FAT some activities to be performed after system delivery to the site. This position was clarified in Westinghouse's response to RAI 5 (Refs. 15 and 16). The revised Section 7.3.1.5 of the SPM states: *"The FAT is typically performed in the factory but some portion of the test can be performed at site if agreed to with the customer."* The FAT objectives include demonstration that the complete system is integrated and functional. The NRC staff determined this change is acceptable because the objectives of the FAT as stated in Section 7.3.1.5 of the SPM will continue to be accomplished prior to the system being placed into service even if some FAT activities are deferred to the site.

The FAT is the final stage of testing that is conducted prior to acceptance of equipment by the licensee. All subsequent testing activities such as Site Acceptance Testing and Installation testing are considered to be the responsibility of the licensee and are therefore not within the scope of the Common Q STP. The Common Q STP identifies the following two categories of testing that are used in the Common Q software testing process;

- Functional Testing - (otherwise known as black box testing) is used to determine that a module or system has functional performance that is consistent with the requirements specified. Test cases for functional testing are derived from the requirement specifications and are based on manipulating test inputs and monitoring test outputs.

- Structural Testing - (otherwise known as white box testing) is used to evaluate the internal structure of a code module and is only used for module tests. Structural testing is intended to provide one hundred percent of branch execution within the code module.

Section 7.2.4 of the SPM Revision 5 includes new provisions for deferring completion of test activities to allow commencement of the subsequent tests before the preceding test level is complete. This change was further clarified in Westinghouse's response to RAI 4 (Refs. 15 and 16). This change is being made to account for the fact that modules can either be generically produced (existing software not to be modified during application development) or may be specifically developed or modified for a particular project (new software, or existing software to be modified during application development).

When pre-validated modules are used for an application, the project's validation testing can begin with Unit Testing of the released application. When specifically developed modules are used, validation of the software module (module test) can be performed while the application

software that uses the module is concurrently undergoing downstream validation tests. Westinghouse recognizes this is a calculated risk in project validation testing, and should the module test fail while downstream testing is occurring concurrently, the downstream validation testing may be required to be reperformed to demonstrate valid downstream testing results.

The NRC staff determined this change is acceptable because all testing requirements for each level of test will continue to be met even though the test sequence can, in some cases, be changed to support application specific requirements.

The risks associated with software testing are addressed through regression analysis. The STP states that *"regression analysis shall be performed to determine extent of retesting activities that may be necessary to re-verify and/or re-validate any changes to a tested element."* The results of this analysis are intended to identify latent design errors or programming bugs that have been introduced by software design modifications.

The Common Q STP prescribes the scope, approach, resources, and schedule of the testing activities and it identifies the items and features to be tested. Testing tasks as well as the personnel responsible for each task are identified. The software test plan includes module testing, unit testing, integration testing, System Validation Testing and factory acceptance testing.

Revision 5 of the SPM removes the requirement for test plans to contain all the requirements for all acceptance test procedures and to define each required test to be conducted. The reason for this change was provided by Westinghouse in response to RAI 12 (Refs. 15 and 16). This response states the following:

> The reason for the change in the SPM is due to the typical sequence and progression of a project. Requirements analysis, testing coverage and tracing of the requirements to test cases are significant testing activities. The Test Plan is needed to outline these activities. The test planning and initial engineering work occurs in parallel with the finalization of the design requirements and the implementation specifications. Therefore, the specific requirements to be tested are not available or issued in their final form when the test plan is written.

The NRC staff determined this change to be acceptable because Westinghouse's processes will continue to establish traceability between system requirements and test procedures and/or test cases even if these are determined after the test plan is written. As such, the individual requirements for lower level acceptance test procedures and identification of individual, specific required tests to be conducted do not need to be included in the test plan itself at the requirements phase of development and can instead be established at a later stage of the development process.

Site acceptance testing and installation testing are not covered under the Common Q STP because they are considered to be licensee actions and 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. This is addressed in plant specific action item 5.

The Common Q STP is understandable and it includes adequate provisions for retest in the event of failure of the original test. The Common Q Software Test Plan adequately addresses the test planning guidance of BTP 7-14, Section B.3.1.12, and based on WEC's commitment to

conformance with IEEE Std. 829-1998 and IEEE Std.1008-1987, the staff finds the Common Q Software Test Plan acceptable.

3.2.13 Secure Development and Operating Environment (SDOE) Evaluation

The staff evaluated the Common Q platform requirements against RG 1.152. It contains five regulatory positions that describe methods acceptable to the staff for establishing a SDOE for digital safety systems. Each of these positions correlates to a phase of a typical software development life cycle. These regulatory positions support compliance with portions of 10 CFR Part 50 – specifically Appendix A GDC 21 (Protection System Reliability and Testability), Appendix B Criterion III (Design Control) and IEEE Std. 603-1991 Clauses 5.6.3 (Independence from Interconnected Equipment) and 5.9 (Access Control).

Section 12 of the Common Q Software Program Manual (Ref. 0) addresses the SDOE planning aspects of the Common Q platform from the Concepts Phase through the Test Phase of the software development life cycle per the guidance provided by RG 1.152.

The lifecycle structure, for which criteria on development environment controls are to be established, consists of the following phases:

- Concept
- Requirements
- Design
- Implementation
- Test
- Installation, Checkout, and Acceptance Testing
- Operation
- Maintenance
- Retirement

This SE evaluates the secure development environment controls applied to the Common Q safety system development from concept phase through the test phase. The last four phases: Installation, Operation, Maintenance, and Retirement will need to be evaluated via follow-up activities once a safety system application is developed using the Common Q platform.

The operating software for the Common Q platform was developed prior to the issuance of RG 1.152. Thus the discussion of development activities is focused on those secure development environment considerations applied during the commercial grade dedication effort applicable to the life cycle processes for maintenance of the previously developed software. Although application software is not within the scope of this review, platform features that contribute to the SDOE for the application are identified and discussed. Credit may be taken for the use of these security capabilities in establishing a secure operational environment for a plant specific safety-related application.

A security evaluation for the Common Q platform was not conducted by the NRC when the Common Q platform SE (Ref. 2) was performed because the applicable regulatory guidance was not available at the time of that safety evaluation. Nonetheless, the security measures discussed below were in place during the Common Q platform development.

3.2.13.1 Concepts Phase (2.1)

~~System Security~~Secure Operational Environment Capabilities

The Common Q platform was developed prior to the issuance of regulatory guidance on security capabilities. The security enabling capabilities of the Common Q platform were not implemented to fulfill a specific security concept, but were rather the product of good design practices. The NRC staff review of the Common Q development documentation determined that the development process incorporated several security features in the original design that apply to the secure development and operating environment of the system. Even though a formal concepts phase security analysis was not performed, the WEC SDOE plan supports the security concepts used during the development of the Common Q platform. The basic concepts used in defining the system security capabilities of the Common Q platform were ensuring confidentiality, and integrity. The vulnerabilities associated with these concepts are defined in the SPM as follows.

- *Confidentiality Vulnerability - the inadvertent loss of information related to the security of a system and related development systems.*

- *Integrity Vulnerability - the inadvertent change to a system and related development system design requirements that could adversely affect security*

The security capabilities of the Common Q platform that include physical and logical access controls, safety to non-safety isolation, and control of the various life cycle activities, were derived from these security concepts. These security capabilities were used to establish the security requirements for the system hardware and software. Even though the Common Q platform was developed several years prior to the issuance cyber security regulatory guidance, the NRC staff review concludes that the WEC SDOE plan satisfies the criterion for identifying safety system security capabilities.

~~Identification of~~General Life Cycle Vulnerabilities

A formal security assessment for the Common Q platform design was not performed at the time of development because the platform was designed prior to the availability of guidance in this area. Instead, WEC provided a SDOE plan which includes an analysis of the vulnerabilities applicable to the development of the Common Q platform. This is an acceptable alternative approach considering the fact that the Common Q platform design was completed prior to the issuance of RG 1.152.

The SPM calls for ~~a software life cycle vulnerabilities assessment~~ V&V activities to be performed during the Concept, Requirements, Design, Implementation, and Test phases to verify correct implementation of secure operational environment requirements. ~~The SPM also identifies human factors to be used for mitigation of system vulnerabilities.~~

The vulnerabilities of the Common Q platform development are initially assessed during the concepts phase. ~~Subsequent assessments~~These vulnerabilities ~~are also performed during the requirements~~become platform restrictions that are confirmed ~~,~~through the ~~-~~design, implementation, and test phases. The NRC staff finds that these identified vulnerabilities and the applicants response to them adequately address the potential for tampering with the Common Q platform during its developmental phases. The vulnerabilities identified by WEC were used to derive the security controls for the system hardware and software development. Based on the review of identified vulnerabilities and the fact that requirements to address these

vulnerabilities through the various life cycle phases are described in the SDOE plan, the staff has determined that the Common Q SPM adequately identifies and addresses the vulnerabilities associated with software development.

Remote Access and One-Way Communication

The Software Program Manual states that Isolated Development Infrastructures (IDI) are created to preclude inadvertent and remote access or changes that could affect the confidentiality or integrity of a system and related development system hardware or software during the implementation phase. The NRC staff understands this to mean that Common Q systems under development will be configured in an isolated manner which precludes any remote access to the safety system. Though the Common Q system can be configured to provide remote access capability, measures are taken by the design and development team to prevent the implementation of these features. WNA-DS-01070-GEN-P Rev. 6, "Westinghouse Application Restrictions for Generic Common Q," (Reference 5) is used to identify generic restrictions that are applied to all Common Q projects. This document identifies several measures that are taken to prevent remote access to the PM646A safety processors including a measure to prevent software installation over the AF-100 bus, as well as a measure to restrict network connectivity of the serial interfaces on the processor module. An additional requirement to disable the remote access capabilities in the application is also described. The NRC staff determined that the Common Q SPM provides adequate provisions to establish one way communications where required and to prevent remote access to the safety system.

The staff finds that the Common Q SDOE plan adequately addresses the criteria of position C.2.2.1 of RG 1.152.

3.2.13.2 Requirements Phase (2.2)

System Features (2.2.1)

Security functional performance requirements are implemented to address vulnerabilities identified in the concept phase for the Common Q system. All such requirements are subject to independent verification and validation as part of the overall IVV process.

NRC staff finds that the requirements pertaining to the security functions, system configuration, external interfaces, qualification, human factors, data definitions, and documentation for hardware and software have been properly established and are therefore acceptable.

The Common Q SPM has provisions for a security assessment to be performed during the ~~requirements~~ concept phase. The results of the security assessment are security related design features. Security related design features are implemented into the system requirements specifications. The Common Q SVVP states that the IVV team evaluates the software design and test documentation, which includes the system requirements specification. As such, the system requirements specification which includes security related design features is evaluated by the IVV team.

NRC staff finds that the verification process used for security related design features provides an adequate means of ensuring the correctness, completeness, accuracy, testability, and consistency of the system's security features and is therefore acceptable.

Previously Developed Common Q software

The previously developed operating software of the Common Q platform is dedicated for use in safety-related applications. As described in Section 4.2 of the Common Q platform Topical Report SE (Refs. 1 and 14), commercial-grade dedication is an acceptance process for demonstrating that a commercial grade item to be used as a basic component will perform its intended safety functions and, in this respect, is equivalent to an item designed and manufactured under a 10 CFR Part 50 Appendix B quality assurance program. Testing performed as part of the commercial grade dedication effort further establishes the quality and security characteristics of the previously developed software. The dedicated operating software is controlled under the Common Q software configuration management program (SCMP) as evaluated in Section 3.2.11 of this SE and is maintained under the Common Q Quality Assurance program which is evaluated in Section 3.2.3 (SQAP) of this SE. Based on the review of the evidence for the previously developed software and its ongoing management under the WEC quality processes, the NRC staff determined that the Common Q previously developed software satisfies the criterion of regulatory position C.2.2.1 in RG 1.152.

Development Activities (2.2.2)

Among the identified vulnerabilities of the Common Q system was its vulnerability to inadvertent change to the design requirements of a system or related development system that could adversely affect the security of the system. If appropriate controls are not placed within the requirements development process, then the opportunity exists for inappropriate requirements to be inserted and/or necessary requirements to be omitted. The actions taken by WEC to prevent requirements tampering are described below.

During development of the Common Q platform software, the SPM defines configuration management, quality assurance, and life cycle development processes used to control activities performed in the requirements phase. The engineering procedures used by WEC govern the organization, content and structure of requirements specifications for the Common Q platform.

The software review process, including responsibilities, review methods, review processes, and specific review activities are defined in the Common Q SQAP. The Reviews section of the SPM (Section 4.6) addresses the review requirements throughout the software life cycle. A Software Requirements Review (SRR) is required to be performed by the IVV team after the completion of the requirements phase. During this SRR, an examination of the software requirements specifications is performed to verify that they are clear, verifiable, consistent, modifiable, traceable and usable during the operations and maintenance phases. The SRR includes an evaluation of the traceability and completeness of the requirements as well as the adequacy of rationale for derived requirements. The NRC staff review of the Common Q review processes found them to be acceptable and compatible with IEEE Std. 1028-~~2005~~ 2008 "IEEE Standard for Software Reviews."

The staff finds the measures identified in the Common Q SDOE Plan (Section 12 of the SPM) adequate to prevent inadvertent, unintended, or unauthorized modifications to the system during the requirements phase. The staff also finds the verification activities completed by the IVV team, to be sufficient to identify and mitigate any unauthorized modifications of the Common Q platform requirements specifications. The Common Q SDOE Plan therefore satisfies the requirements of regulatory position C.2.2.2 in RG 1.152.

3.2.13.3 Design Phase (2.3)

The Common Q system development process has provisions for the creation of a Software Design Description (SDD) which includes descriptions of the software design elements that are used to satisfy software safety and security requirements. The documentation requirements for the SDD are provided in SPM Section 10.3. Here it is stated that *"the SDD … complies with the system requirements specification and the software requirements specification"*. All design features including those that are security related are described in the SDD.

Verification

Section 10.3 of the SPM states that; *"…each software safety design element identified that satisfy the software safety requirements, such that its achievement is capable of being verified and validated per the SVVP."* Therefore, the security design elements of the SDD will be subject to a formal verification and validation process. The evaluation of the Common Q SVVP is documented in Section 3.2.10 of this SE. The staff finds the verification activities completed by the IVV team during the design phase to be sufficient to identify and mitigate any unauthorized modifications of the Common Q platform design products.

Access Controls

Control over the use of safety system services is addressed by the Development System Requirements. These include physical and logical access controls to Common Q system functions. Control of data communication between the Common Q safety system and other systems has been evaluated in Section 4.1.3.4 of the Common Q Platform Topical Report SE (Refs. 1 and 14).

Common Q physical and logical access features are included in the development system requirements and were derived from the vulnerability assessments performed starting in the concept phase of software development. The staff finds this approach to establishing physical and logical access controls for the Common Q system to be acceptable.

Software Configuration Management

The Common Q SCMP defines the process used for identifying software configuration items. During the requirements phase, the Design team and the IVV group perform the tasks of:

- identifying software items developed under SPM for generic application that are to be controlled via the SCMP,
- assuring that the qualification of these items are complete and appropriate for the project (including appropriateness of software classification), and
- describing how the software will be integrated with the project-specific software development.

During the design phase, the system security requirements are translated into these design configuration items. The secure operational environment requirements for the Common Q platform correspond to security-related features, capabilities, and design elements that serve as design configuration items. The staff finds that the process employed for Common Q systems to transfer security functional performance requirements into system design elements is acceptable. The staff has therefore determined that the Common Q SDOE Plan satisfies the requirements of regulatory position C.2.3.1 in RG 1.152.

Development Activities (2.3.2)

The security measures implemented in the design phase included; system features, verification, access controls, and software configuration management. The staff finds the measures identified in the Common Q SDOE plan adequate to prevent inadvertent, unintended, or unauthorized modifications to the system during the design phase to address Regulatory Position C.2.3.2 of RG 1.152.

3.2.13.4 Implementation Phase (2.4)

Module coding is performed and existing qualified software is integrated into the software system during the Implementation phase of the Common Q software development process. The IVV team also reviews the design team's implementation products during this phase. The SPM states that *"The purpose of the implementation verification is to ascertain the implementation documents are clear, understandable, logically correct and a faithful translation of the design specifications."* It also states that *"The objectives of the implementation documents are to facilitate the effective production, testing, use, transfer, conversion to a different environment, future modifications, and traceability to design specifications."*

System Features (2.4.1)

The V&V activities to be performed during the implementation phase ~~include performing a security assessment of the system to~~ verify that the security controls chosen in the design phase ~~are~~ have been ~~adequate~~properly implemented. ~~If system vulnerabilities are identified during this security assessment then requirements for additional security controls are added to the system requirements in order to address or otherwise mitigate these vulnerabilities.~~

These V&V activities defined in the SPM provide a means by which the correctness and accuracy of the design configuration items produced during the implementation phase can be confirmed. The Common Q development process also includes a process for establishing and maintaining requirements traceability as is described in Section 5.4.5.3 of the SPM. This process involves associating requirements with documentation and software design configuration items. During the requirements traceability analyses that are performed throughout the development process, assessments of completeness are made in order to ensure that; a) all system requirements are implemented and that b) no features are implemented within the design that are not associated with an approved specification.

The NRC staff has reviewed the implementation controls outlined in the SPM and has determined that the Common Q platform development process contains features that comply with the criterion in Section 2.4.1 of RG 1.152.

Development Activities for the Implementation Phase (2.4.2)

The secure development environment established during development of the Common Q system software involves creation of Isolated Development Infrastructures (IDI). These IDI's are intended to preclude inadvertent and remote access or changes that could affect the confidentiality or integrity of a system and related development system hardware or software during the implementation phase.

The SPM establishes requirements for security procedures and standards to minimize and mitigate tampering with the developed system. The security program established by these procedures addresses hidden functions and vulnerable features embedded in the code. Where

possible, the program requires these functions to be disabled, removed, or addressed to prevent any unauthorized access.

Use of Commercial-Off-the-Shelf Systems (COTS)

The security program established by the Common Q SPM includes assessments of COTS systems to confirm that the features within the COTS system do not compromise the security requirements of the integrated Common Q system. Additionally, these assessments ensure that security functions are not compromised by the other system functions.

The NRC staff determined that the criterion of regulatory position C.2.4.2 of RG 1.152 has been met.

3.2.13.5 Test Phase (2.5)

The Common Q software test process is outlined in Section 7, "Software Test Plan," of the SPM and is evaluated in Section 3.2.12 of this SE. This process includes module and unit testing performed during the implementation phases as well as integration, factory acceptance and site acceptance testing that are performed in the later phases of the Common Q software development life cycle. The integration and acceptance tests are performed with all application software installed into actual plant hardware so these tests are performed on the completed design implementation of the system.

System Features (2.5.1)

The testing performed on Common Q systems is intended to verify that all system requirements are validated. Because security requirements are integrated into the overall system requirements, they will also be validated by tests. Design validation is accomplished by the execution of integration, system, and acceptance tests. These tests are performed on the system configured as it is intended to be installed in the plant. Test configurations also include interfaces to other external systems.

Common Q system testing confirms that security controls are implemented and functioning to mitigate the corresponding vulnerabilities. ~~In addition, Vulnerability assessments are performed on the system during the test phase in order to identify the introduction of vulnerabilities or to confirm that no new vulnerabilities are introduced into the system.~~ The NRC staff determined that the criterion of Regulatory Position C.2.5.1 of RG 1.152 has been met.

Development Activities (2.5.2)

Testing environments are isolated and maintained in accordance with the security program established by WEC. This program includes the establishment of an IDI to preclude inadvertent and remote access or changes that could affect the confidentiality or integrity of a system and related development system hardware or software. The NRC staff determined that the criterion of Regulatory Position C.2.5.2 of RG 1.152 has been met.

4.0 SUMMARY OF REGULATORY COMPLIANCE EVALUATIONS

On the basis of the foregoing review of the Common Q 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 the design features upon which the safety determination will be based. A review of the implementation of the life cycle process and

the software life cycle process design outputs for specific applications will be performed on a plant-specific basis. This is addressed in Section 6.5 of the SE on LTR WCAP-16097-PINP Common Qualified Platform (ML12241A101).

On the basis of the review of WEC's software development process for application software, the staff concludes that the Common Q application development procedures 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 the design features upon which the safety determination will be based. The staff, therefore, concludes that the software program manual as applied to Common Q safety systems meets the guidance of RG 1.152 and that the special characteristics of computer systems have been adequately addressed. Based on its review, the staff finds, therefore, that the Common Q safety system software development processes when properly implemented are capable of producing software that will satisfy the requirements of GDC 1 and 21.

Cyber security to address malicious events is addressed under the purview of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," and thus has not been evaluated as part of this SPM review. Conformance to 10 CFR 73.54 is the responsibility of COL applicants or licensees who choose to reference the SPM.

4.1 Common Q SPM Generic Change Process

Per letter dated August 12, 2010 (Reference 6), WEC submitted WCAP-17266, "Common Q Platform Generic Change Process, (Reference 7) for NRC review and approval.

The Common Q generic change process defined by WCAP-17266 describes methods used by WEC to screen, and evaluate proposed changes to Common Q components, software or processes defined within the Common Q Platform and Software Program Manual topical reports subsequent to NRC review and approval. The scope of this process includes changes that are made to the Common Q SPM subsequent to the issuance of this SE. This process defines criteria to be used for the determination of whether the safety conclusions of the NRC safety evaluation remain valid following the proposed change or if the changes will require submittal to the NRC for evaluation and approval prior to implementation.

The staff has reviewed this document and acknowledges the benefits provided by implementation of a formal topical report screening, evaluation, and change process however, the NRC is unable to perform a safety evaluation of the processes defined by this document or make any safety conclusions regarding these processes at this time. This document is included as a reference within this safety evaluation in order to provide future reviewers of Common Q applications that reference this SE with information on how WEC evaluates and documents changes to the Common Q SPM. It is also beneficial for reviewers of Common Q applications to have access to the WEC generic change process in order to interpret the information provided in the Record of Changes document discussed below.

4.2 Common Q Record of Changes Document

Per letter dated August 25, 2010 (Reference 8), WEC submitted WCAP-16097, "Common Qualified Platform Record of Changes, "(Reference 9) for NRC review and approval.

The staff reviewed the Common Q Record of Changes (ROC) and confirmed that the changes to the Common Q SPM are consistent with the revised topical report evaluated by this SE.

Furthermore, the staff reviewed the information provided in the Tables within the ROC and determined that these tables provide valuable information that should be used during application specific reviews to determine acceptability of changes to the Common Q SPM subsequent to the NRC review and approval of this License Topical Report (LTR). Plant-Specific action item 6 is therefore being included in this SE to provide direction for plant specific safety evaluations to include a review of the current Common Q record of changes to assess the validity of previously derived safety conclusions in light of the changes made to the Common Q SPM.

5.0 PLANT SPECIFIC ACTION ITEMS

An application may reference the approved WEC Common Q Topical Report provided the application satisfies the following conditions and limitations. The conditions and limitations are intended to ensure that all aspects of the digital safety system are properly designed and implemented. The following information is to be submitted or made available for staff audit/inspection upon receipt of an application for a license amendment, a design certification, or a combined license when referencing or incorporating by reference, TR WCAP-16096. The Common Q SPM and this safety evaluation provide the context and basis for the required additional information.

The following plant-specific actions must be performed by an applicant when requesting NRC approval for installation of a safety-related system based on the Common Q platform.

1. As noted in Sections 3.2.1 and 3.2.3, WEC 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.

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.

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 quality assurance, additional evaluations, audits or inspections must be performed to ensure that these licensee responsibilities are fulfilled.

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.

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, site acceptance and installation 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.

6. 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 SPM.

7. Secure Development and Operational Environment – An applicant or licensee referencing the Common Q SPM for a safety-related plant specific application should ensure that a secure development and operational environment has been established for its plant specific application, and that it satisfies the applicable regulatory evaluation criteria of RG 1.152, Revision 3.

6.0 REFERENCES

1. WCAP-16097-P-A, Revision 3, "Common Qualified Platform Topical Report" (Proprietary/Non-Proprietary), February 28, 2013, Agencywide Documents Access and Management System (ADAMS) Accession No. ML13112A110/ML13112A108.

2. Common Qualified Platform Topical Report WCAP-16097-P and 16097-NP Revision 3, June 30, 2012, ADAMS Accession Nos. ML12207A512 and ML12207A510.

3. Submittal of WCAP-16096-P and WCAP-16096-NP, Revision 4, "Software Program Manual for Common Qualified Platform," (Proprietary/Non-Proprietary) for Review and Approval, July 17, 2012, ADAMS Accession No. ML12205A051.

4. Software Program Manual for Common Q Systems, Revision 4 WCAP-16096-P and 16096-NP Revision 4, June 30, 2012, ADAMS Accession Nos. ML12205A053 and ML12205A052.

5. WNA-DS-01070-GEN, Revision 6, "Application Restrictions for Generic Common Q Qualification," December 31, 2011, ADAMS Accession Nos. ML11364A030 and ML11364A029.

6. Transmittal Letter for WCAP-17266-P/NP "Common Q Platform Generic Change Process," Revision 0, August 12, 2010, ADAMS Accession No. ML102290175.

7. Common Q Platform Generic Change Process (WCAP-17266-P/NP), Revision 0, August 31, 2010, ADAMS Accession Nos. ML102290177 and ML102290176.

8. Transmittal Letter for WCAP-16097-P/NP "Common Qualified Platform Record of Changes", Revision 1, April 19, 2012, ADAMS Accession No. ML12115A213.

9. Common Qualified Platform Record of Changes (WCAP-16097-P/NP), Revision 1, March 31, 2012, ADAMS Accession Nos. ML12115A215 and ML12115A214.

10. Software Program Manual for Common Q Systems (WCAP-16096-NP-A) Revision 1, January 29, 2004, ADAMS Accession No. ML040360115.

11. Safety Evaluation for Topical Report WCAP-16096-NP-A "Software Program Manual for Common Q Systems," Revision 1, September 28, 2004, ADAMS Accession No. ML042730580.

12. Request for Additional Information, License Topical Report (WCAP-160096) "Software Program Manual for Common Q Systems," September 29, 2011, ADAMS Accession No. ML112490485.

13. Response to NRC Request for Additional Information on WCAP-16096, Revision 2 "Software Program Manual for Common Q Systems," January 31, 2012, ADAMS Accession No. ML12034A212.

14. Submittal of WCAP-16096-P/WCAP-16096-NP, Revision 5, "Software Program Manual for Common Q™ Systems" (Proprietary/Non-Proprietary), August 28, 2017, ADAMS Accession No. ML17241A112.
15. Request for Additional Information, License Topical Report (WCAP-160096) "Software Program Manual for Common Q Systems," February 26, 2018, ADAMS Accession No. ML118018A005.

16. Response to NRC Request for Additional Information on WCAP-16096, Revision 5 "Software Program Manual for Common Q Systems," May 31, 2018, ADAMS Accession No. ML18156A479.

17. Safety Evaluation for Topical Report WCAP-16096-P(NP)-A "Software Program Manual for Common Q Systems," Revision 4, February 28, 2013, ADAMS Accession Nos. ML13081A046 and ML13081A047.

7.0 LIST OF ABBREVIATIONS

ABB	Asea Brown Boveri
AC160	Advant Controller 160
~~ACC~~	~~AMPL Control Configuration~~
AF100	Advant Fieldbus 100
AISC	Application Specific Integrated Circuit
ALWR	Advanced Light Water Reactor
~~AMPL~~	~~ABB Master Programming Language~~
API	Application Programming Interface
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transients Without Scram
BIOB	Backplane I/O Bus
BTP	Branch Technical Position
CE	Combustion Engineering
CENP	Combustion Engineering Nuclear Power
CEA	Control Element Assembly
CEAC	Control Element Assembly Calculator
CEAPD	CEA Position Display
CENP	CE Nuclear Power (Westinghouse)
CEO	Cognizant Engineering Organization
CETMS	Core Exit Thermocouple Monitoring System
CGD	Commercial-Grade Dedication

1	Common Q	Common Qualified
2	COTS	Commercial-Off-The-Shelf
3	CPC	Core Protection Calculator
4	CPCS	Core Protection Calculator System
5	CPU	Central Processing Unit
6	CRC	Cyclic Redundancy Check
7	CS	Communication Section
8	CWP	CEA Withdrawal Prohibit
9	D-in-D&D	Defense in Depth and Diversity
10	DB	Database
11	DBE	Design Basis Event
12	DESFAS	Digital ESFAS
13	DI	Digital Input
14	DLCE	Design Life Cycle Evaluation
15	DNBR	Departure from Nucleate Boiling Ratio
16	DPPS	Digital Plant Protection System
17	DPRAM	Dual Port Random Access Memory
18	DSP	Data Set Peripheral
19	EIA	Electronic Industries Association
20	EMC	Electromagnetic Compatibility
21	EPRI	Electric Power Research Institute
22	EPLD	Erasable Programmable Logic Device
23	ESF	Engineered Safety Features
24	ESFAS	Engineered Safeguards Features Actuation System
25	FAT	Factory Acceptance Test
26	FCB	Function Chart Builder
27	FE	Function Enable
28	FMEA	Failure Modes and Effect Analysis
29	FOM	Fiber Optic Modem
30	FPD	Flat Panel Display
31	FPDS	Flat-Panel Display System
32	FSAR	Final Safety Analysis Report
33	GDC	General Design Criteria
34	GUI	Graphical User Interface
35	HDD	Hard Disk Drive
36	HDLC	High Level Data Link Control
37	HJTC	Heated Junction Thermocouple
38	HMI	Human Machine Interface
39	~~HIS~~HSI	Human System Interface
40	HSL	High Speed Link
41	I/O	Input/Output
42	I&C	Instrumentation and Control
43	IEC	International Electrotechnical Commission
44	IEEE	Institute of Electrical and Electronics Engineers
45	IPC	Interprocess Communication
46	ISR	Interrupt Service Routine
47	ITP	Interface and Test Processor
48	LC	Loop Controller
49	LCLP	Local Coincidence Logic Processor
50	LED	Light Emitting Diode
51	LPD	Local Power Density

1	MCR	Main Control Room
2	MTBF	Mean Time Between Failures
3	MTP	Maintenance and Test Panel
4	NEI	Nuclear Energy Institute
5	NSSS	Nuclear Steam Supply System
6	OM	Operator's Module
7	OBE	Operational Basic Earthquake
8	PAMS	Post-accident Monitoring System
9	PAS	Plant Annunciator System
10	PC	Process Control
11	PCB	Printed Circuit Board
12	PCE	Program Control Element
13	PDS	Previously Developed Software
14	PIT	Precision Interval Timer
15	PLC	Programmable Logic Controller
16	PM	Processor Module
17	PPS	Plant Protection System
18	PROM	Programmable Read-only Memory
19	PS	Processing Section
20	QA	Quality Assurance
21	QSPDS	Qualified Safety Parameter Display System
22	~~QSSL~~	~~QNX Software Systems Limited~~
23	RAM	Random Access Memory
24	RCM	Remote Control Module
25	RCP	Reactor Coolant Pump
26	RFI	Radio Frequency Interference
27	RG	Regulatory Guide
28	RPS	Reactor Protection System
29	RSP	Remote Shutdown Panel
30	RSPT	Reed Switch Position Transmitter
31	RTC	Real Time Clock
32	RTD	Resistance Temperature Detector
33	RTS	Reactor Trip System
34	RTCB	Reactor Trip Circuit Breaker
35	RVLMS	Reactor Vessel Level Monitoring System
36	SAR	Safety Analysis Report
37	SBC	Single Board Computer
38	SCADA	Supervisory Control and Data Acquisition
39	SCMP	Software Configuration Management Plan
40	SCR	Software Change Request
41	SDM	Service Data Manager
42	SDP	Service Data Protocol
43	SE	Safety Evaluation
44	SLC	Software Life-Cycle
45	SLE	Software Load Enable
46	SMM	Subcooled Margin Monitor
47	SPM	Software Program Manual
48	SQAP	Software Quality Assurance Plan
49	SRAM	Static RAM
50	SRP	Standard Review Plan
51	SSP	Software Safety Plan

STS	Standard Technical Specifications
SVVP	Software Verification and Validation Plan
SW	Software
SWC	Surge Withstand Capability
TCB	Task Control Block
TMI	Three Mile Island
TS	Technical Specification(s)
TSTF	Technical Specification Task Force
V&V	Verification and Validation
WWDT	Window Watchdog Timer

Advant® is a registered trademark of ABB Process Automation Corporation.
~~QNX® and Photon® are registered trademarks of QNX Software Systems GmBH & Co. KG ("QSSKG", formerly "QSSL") and are used under license by QSS.~~
Unix® is a registered trademark of The Open Group in the US and other countries.
Windows® is a registered trademark of Microsoft group of companies.

Comment Number	Comment Location	Comment Type	Comment	NRC Response
1	Page 1/Line 22	Editorial	“Reference 0” should be “Reference 14”	
2	Page 3/Line 25	Editorial	Should “Revision 1” be added to RG 1.170?	
3	Page 6/Lines 10 – 11	Editorial	Westinghouse (WEC) suggests changing “the ABB Master Programming Language Control Configuration (ACC) and Photon” to “approved”. WEC would like to remove references to specific software tools (e.g., AMPL and Photon) because the SPM does not specifically cite these tools; they are only cited in the Common Qualified Platform Topical Report (WCAP-16097).	

Comment Number	Comment Location	Comment Type	Comment	NRC Response
4	Page 12/Lines 24 – 26	Clarification	The SER states that the "SQAP no longer applies to software classified as: important to availability or general purpose software." However, this is not consistent with the text in the SQAP, Section 4.1.2, "Scope," which states: "This SQAP is required for all quality classifications defined for the Common Q™ system: protection, important-to-safety, important-to-availability, and general purpose software." Therefore, WEC suggests reverting to the wording from the previous revision of the SER: "The scope of the Common Q SQAP includes software in all four SIL classifications; protection, important to safety, important to availability, and general purpose. The Common Q SQAP applies to original software that was developed under the requirements of the Common Q SPM."	
5	Page 15/Line 29	Editorial	"Reference 0" should be "Reference 16"	

Comment Number	Comment Location	Comment Type	Comment	NRC Response
6	Page 16/Line 7	Editorial	WEC suggest changing “the AMPL Control Configuration (ACC)” to “an approved”. WEC would like to remove references to specific software tools because the SPM does not specifically cite these tools; they are only cited in the Common Qualified Platform Topical Report (WCAP-16097).	
7	Page 16/Line 8	Editorial	WEC suggests changing “ACC” to “the tool”. WEC would like to remove references to specific software tools because the SPM does not specifically cite these tools; they are only cited in the Common Qualified Platform Topical Report (WCAP-16097).	
8	Page 16/Lines 16 - 17	Editorial	WEC suggests changing “the photon” to “an approved”. WEC would like to remove references to specific software tools because the SPM does not specifically cite these tools; they are only cited in the Common Qualified Platform Topical Report (WCAP-16097).	
9	Page 16/Lines 27 – 28	Editorial	WEC suggests deleting “using the ACC tool”. WEC would like to remove references to specific software tools because the SPM does not specifically cite these tools; they are only cited in the Common Qualified Platform Topical Report (WCAP-16097).	

Comment Number	Comment Location	Comment Type	Comment	NRC Response
10	Page 18/Lines 38 – 39	Clarification	WEC suggests adding "if within Westinghouse's scope of supply" to the end of the first sentence because creating training materials for end users may not be in Westinghouse's supply contract. This is clarified in section 5.5.7.2 of the SPM, which states: "Review training materials (if within Westinghouse's scope of supply) for the following:"	
11	Page 22/Line 30	Editorial	WEC suggests changing "high, major, moderate, and low" to "4, 3, 2, and 1". IEEE Std. 1012-2004 now uses "4, 3, 2, and 1" for their software integrity level scheme.	
12	Page 30/Line 2	Editorial	WEC suggests changing "System Security Capabilities" to "Secure Operational Environment Capabilities" to be consistent with the revised heading in the SDOE section of the SPM.	
13	Page 30/Line 29	Editorial	WEC suggests changing "Identification of Life Cycle Vulnerabilities" to "General Life Cycle Vulnerabilities" to be consistent with the revised heading in the SDOE section of the SPM.	

Comment Number	Comment Location	Comment Type	Comment	NRC Response
14	Page 30/Lines 38 - 40	Clarification	WEC suggests changing “The SPM calls for a software life cycle vulnerabilities assessment V&V activities to be performed during the Concept, Requirements, Design and Test phases.” to “The SPM calls for V&V activities to be performed during the Concept, Requirements, Design, Implementation, and Test phases to verify correct implementation of secure operational environment requirements.” This revision better aligns with the revised SDOE section.	
15	Page 30/Lines 40 – 41	Clarification	WEC suggests deleting “The SPM also identifies human factors to be used for mitigation of system vulnerabilities.” This revision better aligns with the revised SDOE section.	
16	Page 30/Lines 44 – 46	Clarification	WEC suggests changing “Subsequent assessments are also performed during the requirements, design, implementation and test phases.” to “These vulnerabilities become platform restrictions that are confirmed through the design, implementation, and test phases.” This revision better aligns with the revised SDOE section.	
17	Page 31/Line 40	Clarification	WEC suggests changing “requirements phase” to “concept phase” in order to better align with the revised SDOE section.	

Comment Number	Comment Location	Comment Type	Comment	NRC Response
18	Page 32/Line 41	Editorial	"IEEE Std. 1028-2005" should be "IEEE Std. 1028-2008"	
19	Page 34/Lines 20 – 22	Clarification	WEC suggests changing "The V&V activities to be performed during the implementation phase include performing a security assessment of the system to verify that the security controls chosen in the design phase are adequate" to "The V&V activities to be performed during the implementation phase verify that the security controls chosen in the design phase have been properly implemented". This revision better aligns with the revised SDOE section.	
20	Page 34/Lines 22 – 24	Clarification	WEC suggests deleting "If system vulnerabilities are identified during this security assessment then requirements for additional security controls are added to the system requirements in order to address or otherwise mitigate these vulnerabilities" in order to better align with the revised SDOE section.	
21	Page 35/Lines 30 – 32	Clarification	WEC suggests deleting "In addition, Vulnerability assessments are performed on the system during the test phase in order to identify the introduction of vulnerabilities or to confirm that no new vulnerabilities are introduced into the system" in order to better align with the revised SDOE section.	

Comment Number	Comment Location	Comment Type	Comment	NRC Response
22	Page 38/Lines 11 – 15	Clarification	Normally a PSAI is cited in the text of the SER, but it's not in this case. Having corresponding text in the SER helps provide context for the reason behind the PSAI.	
23	Page 39/Line 33	Editorial	WEC suggests deleting the “ACC” acronym since it is not cited in the SER text.	
24	Page 39/Line 37	Editorial	WEC suggests deleting the “AMPL” acronym since it is not cited in the SER text.	
25	Page 40/Line 39	Editorial	“HIS” should be changed to “HSI”	
26	Page 41/Line 22	Editorial	WEC suggests deleting the “QSSL” acronym since it is not cited in the SER text.	
27	Page 42/Lines 13 – 14	Editorial	WEC suggests deleting “QNX® and Photon® are registered trademarks of QNX Software Systems GmbH & Co. KG ("QSSKG", formerly "QSSL") and are used under license by QSS” since “QNX” and “Photon” are not used in the SER.	

---------- End of Table of Comments ----------