

**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

© 2018 Westinghouse Electric Company LLC  
All Rights Reserved

---

**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.

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

**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**

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

1		<b>TABLE OF CONTENTS FOR COMMON Q SAFETY EVALUATION</b>	
2	1.0	INTRODUCTION .....	1
3	2.0	REGULATORY EVALUATION .....	1
4	2.1	Regulatory Criteria .....	1
5	2.2	Method of Review .....	4
6	2.3	Precedents .....	4
7	3.0	TECHNICAL EVALUATION .....	5
8	3.1	Design Considerations .....	5
9	3.2	Life Cycle Planning Process for Application Software .....	6
10	3.2.1	Software Management Plan .....	7
11	3.2.2	Software Development Plan .....	8
12	3.2.3	Software Quality Assurance Plan .....	12
13	3.2.4	Software Integration Plan .....	14
14	3.2.5	Software Installation Plan .....	17
15	3.2.6	Software Maintenance Plan .....	17
16	3.2.7	Software Training Plan .....	18
17	3.2.8	Software Operations Plan .....	19
18	3.2.9	Software Safety Plan .....	19
19	3.2.10	Software Verification and Validation Plan .....	21
20	3.2.11	Software Configuration Management Plan .....	25
21	3.2.12	Software Test Plan (New) .....	26
22	3.2.13	Software Secure Development and Operating Environment Plan .....	29
23	3.2.13.1	Concepts Phase (2.1) .....	30
24	3.2.13.2	Requirements Phase (2.2) .....	31
25	3.2.13.3	Design Phase (2.3) .....	33
26	3.2.13.4	Implementation Phase (2.4) .....	34
27	3.2.13.5	Test Phase (2.5) .....	35
28	4.0	SUMMARY OF REGULATORY COMPLIANCE EVALUATIONS .....	35
29	4.1	Common Q SPM Generic Change Process .....	36
30	4.2	Common Q Record of Changes Document .....	36
31	5.0	PLANT-SPECIFIC ACTION ITEMS .....	37
32	6.0	REFERENCES .....	38
33	7.0	LIST OF ABBREVIATIONS .....	39
34			

1        **SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION**

2                **WESTINGHOUSE TOPICAL REPORT WCAP-16096-P, REVISION 5**

3                        **"SOFTWARE PROGRAM MANUAL FOR COMMON Q SYSTEMS"**

4                                        **(EPID: L-2017-TOP-0059)**

5  
6        **1.0 INTRODUCTION**

7  
8        The Software Program Manual (SPM) for Common Qualified (Common Q) Systems was  
9        originally submitted as document CE-CES-195-P by Combustion Engineering (CE), for U.S.  
10        Nuclear Regulatory Commission (NRC) staff review in 2000. Subsequently, the commercial  
11        nuclear power businesses of Asea Brown Boveri (ABB), of which CE was a part, were  
12        purchased by British Nuclear Fuels Limited (BNFL) and eventually integrated into the  
13        Westinghouse Electric Company (WEC), such that the SPM is now owned by WEC. See  
14        References 10 and 11 for Revision 1 of this document and the associated safety evaluation  
15        (SE). This document specifies the life cycle planning process for Common Q application  
16        software. The SPM specifies the development, documentation, utilization, and maintenance of  
17        software to be developed for use with the Common Q platform in nuclear safety applications. It  
18        also provides guidance for the maintenance, implementation, and use of commercial-grade  
19        hardware and previously developed software (PDS). Revision 4 of the Common Q SPM was  
20        submitted by WEC (Refs. 3 and 4) and approved by the NRC (Ref. 17).

21  
22        The SPM is being updated to Revision Level 5 per Reference 0-14 to include a revised test  
23        approach that defines testing requirements for Nth of a kind systems of the same design. The  
24        revised SPM also addresses corrective actions, implements process improvements, updates  
25        several of its references, and includes other minor changes.

26  
27        The SPM specifies procedures and controls for the complete software development process.  
28        This process includes the integration of software into system hardware. Since the application  
29        software has not yet been developed, the staff's evaluation does not include the review of the  
30        implementation or outputs of the life cycle process, but is limited to the evaluation of the  
31        specified planning processes.

32  
33        **2.0 REGULATORY EVALUATION**

34  
35        **2.1 Regulatory Criteria**

36  
37        The following regulatory requirements are applicable to the review of the Common Q SPM.

38  
39        Title 10 of the Code of Federal Regulations (10 CFR)

- 40        • 10 CFR 50.55a(a)(1) requires, in part, that systems and components be designed,  
41        tested, and inspected to quality standards commensurate with the safety function to be  
42        performed.
- 43        • 10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with Institute  
44        of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, "IEEE Standard

- 1 Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction  
2 dated January 30, 1995.
- 3 ○ Clause 5.3 of IEEE Std. 603-1991 requires that components and modules shall  
4 be of a quality that is consistent with minimum maintenance requirements and  
5 low failure rates. It also requires that safety system equipment be designed,  
6 manufactured, inspected, installed, tested, operated, and maintained in  
7 accordance with a prescribed quality assurance program.
  - 8 ○ Clause 5.6.3 of IEEE Std.603-1991 requires safety system to be designed such  
9 that credible failures in and consequential actions by other systems will not  
10 prevent safety systems from performing their intended safety functions.
  - 11 ○ Clause 5.9 of IEEE Std. 603-1991 requires the design to permit the  
12 administrative control of access to safety system equipment. These  
13 administrative controls shall be supported by provisions within the safety  
14 systems, by provision in the generating station design, or by a combination  
15 thereof.
  - 16 ● 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 1, "Quality Standards and  
17 Records," requires, in part, that systems and components important to safety be  
18 designed, fabricated, erected, and tested to quality standards commensurate with the  
19 importance of the safety functions to be performed.
  - 20 ● 10 CFR Part 50, Appendix A, GDC 21 requires, in part, that protection systems must be  
21 designed for high functional reliability commensurate with the safety functions to be  
22 performed.
  - 23 ● 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and  
24 Fuel Processing Plants", Criterion I, "Organization," requires in part that the applicant  
25 shall be responsible for the establishment and execution of the quality assurance  
26 program.
  - 27 ● 10 CFR Part 50, Appendix B, Criterion II, "Quality Assurance Program," requires in part  
28 that the applicant shall establish at the earliest practicable time, consistent with the  
29 schedule for accomplishing the activities, a quality assurance program which complies  
30 with the requirements of Appendix B.
  - 31 ● 10 CFR Part 50, Appendix B, Criterion III, "Design Control," requires, in part that, for  
32 safety-related structures systems, or components (SSCs), quality standards be specified  
33 and that design control measures shall provide for verifying or checking the adequacy of  
34 design.
  - 35 ● 10 CFR Part 50, Appendix B, Criterion V, "Instructions, Procedures, and Drawings,"  
36 requires, in part that, for safety-related SSCs, activities affecting quality shall be  
37 prescribed by documented...procedures...of a type appropriate to the circumstances....
  - 38 ● 10 CFR Part 50, Appendix B, Criterion VI, "Document Control," requires, in part that, for  
39 safety-related SSCs, measures shall be established to control the issuance of  
40 documents which prescribe all activities affecting quality.

- 1 • 10 CFR Part 50, Appendix B, Criterion VII, "Control of Purchased Material and  
2 Services," requires documented control of purchased material, equipment, and services  
3 for safety-related SSCs.
- 4 • 10 CFR Part 50, Appendix B, Criterion XI, "Test Control," requires, in part, that a test  
5 program be established to demonstrate that safety-related systems and components will  
6 perform satisfactorily in service.
- 7
- 8 • 10 CFR Part 50, Appendix B, Criterion XV, "Nonconforming Materials, Parts, or  
9 Components" requires in part that measures shall be established to control materials,  
10 parts, or components which do not conform to requirements in order to prevent their  
11 inadvertent use or installation.
- 12

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

15

16 Regulatory Guides (RGs)

- 17 • RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear  
18 Power Plants."
- 19 • RG 1.168, Revision 2, "Verification, Validation, Reviews and Audits for Digital Computer  
20 Software Used in Safety Systems of Nuclear Power Plants."
- 21
- 22 • RG 1.169, Revision 1, "Configuration Management Plans for Digital Computer Software  
23 Used in Safety Systems of Nuclear Power Plants."
- 24
- 25 • RG 1.170, **Revision 1**, "Software Test Documentation for Digital Computer Software  
26 Used in Safety Systems of Nuclear Power Plants."
- 27
- 28 • RG 1.171, Revision 1, "Software Unit Testing for Digital Computer Software Used in  
29 Safety Systems of Nuclear Power Plants."
- 30
- 31 • RG 1.172, Revision 1, "Software Requirements Specifications for Digital Computer  
32 Software Used in Safety Systems of Nuclear Power Plants."
- 33
- 34 • RG 1.173, Revision 1, "Developing Software Life Cycle Processes for Digital Computer  
35 Software Used in Safety Systems of Nuclear Power Plants."
- 36

37 NUREG-Series Publications

- 38 NUREG-0800, Revision 7, "Standard Review Plan for the Review of Safety Analysis Reports for  
39 Nuclear Power Plants: LWR Edition," Chapter 7, "Instrumentation and Controls," March 2007.
- 40
- 41 ○ Branch Technical Position (BTP) 7-14, Revision 6, "Guidance on Software  
42 Reviews for Digital Computer-Based Instrumentation and Control Systems."
- 43
- 44 • NUREG/CR 6101 – "Software Reliability and Safety in Nuclear Reactor Protection  
45 Systems," June 1993.
- 46

## 1 Industry Standards

- 2 • IEEE Std. 7-4.3.2-2003, "Application Criteria for Programmable Digital Computer  
3 Systems in Safety Systems of Nuclear Power Generating Stations," as endorsed by  
4 RG 1.152.
- 5
- 6 • IEEE Std. 730-1998, "Software Quality Assurance Plans,"  
7
- 8 • IEEE Std. 828-2005, "Software Configuration Management Plans," as endorsed by  
9 RG 1.169.
- 10
- 11 • IEEE Std. 829-1983, "Software Test Documentation," as endorsed by RG 1.170,  
12 September 1997.
- 13
- 14 • IEEE Std. 829-1998, "Software Test Documentation,"  
15
- 16 • IEEE Std. 830-1998, "Guide for Software Requirements Specifications," as endorsed by  
17 RG 1.172.
- 18
- 19 • IEEE Std. 1008-1987 (Reaffirmed 2009), "IEEE Standard for Software Unit Testing."  
20
- 21 • IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation Plans," as  
22 endorsed by RG 1.168.
- 23
- 24 • IEEE Std. 1028-2008, "IEEE Standard for Software Reviews and Audits," as endorsed  
25 by RG 1.168.
- 26
- 27 • IEEE Std. 1042-1987, "IEEE Guide to Software Management."  
28
- 29 • IEEE Std. 1063-2001, "IEEE Standard for Software Documentation."  
30
- 31 • IEEE Std. 1074-2006, "IEEE Std. for Developing Software Life Cycle Processes," as  
32 endorsed by RG 1.173.
- 33

## 34 **2.2 Method of Review**

35  
36 The staff used the guidance in RGs and BTP 7-14 to review the software life cycle plans  
37 outlined in the Common Q SPM. In BTP 7-14 the information to be reviewed is subdivided into  
38 the following three topic areas:

- 39
- 40 • Software life cycle process planning;
- 41 • Software life cycle process implementation; and
- 42 • Software life cycle process design outputs.
- 43

## 44 **2.3 Precedents**

45  
46 The NRC previously evaluated the Common Q SPM which was submitted by WEC as document  
47 number WCAP-16096-P/NP-A, Revision 4 and the results of this evaluation are documented in  
48 the associated SE (Ref. 0).

49



### 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,

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

7  
8 Application software is developed for project-specific applications of the Common Q platform.  
9 Software implements plant-specific I&C control and logic functions, and is hardware dependent.  
10 Software will be developed using ~~the ABB Master Programming Language Control~~  
11 ~~Configuration (AGC) and Photon~~ approved software development tools. The Common Q SPM  
12 describes the conditions and objectives to develop application software.

### 14 3.2 Life Cycle Planning Process for Application Software

15  
16 Digital Instrumentation and Control (I&C) safety systems must be designed, fabricated, installed,  
17 and tested to quality standards commensurate with the level of the importance of the safety  
18 functions to be performed. The development of safety system software should progress  
19 according to a formally defined software lifecycle (SLC). Implementation of an acceptable SLC  
20 provides reasonable assurance the necessary software quality has been instilled in the final  
21 system. BTP 7-14, Section B.2.1 states that the information to be reviewed for the software life  
22 cycle process planning should be found under the following topics:

- 23  
24 B.3.1.1 Software Management Plan  
25 B.3.1.2 Software Development Plan  
26 B.3.1.3 Software Quality Assurance Plan  
27 B.3.1.4 Software Integration Plan  
28 B.3.1.5 Software Installation Plan  
29 B.3.1.6 Software Maintenance Plan  
30 B.3.1.7 Software Training Plan  
31 B.3.1.8 Software Operations Plan  
32 B.3.1.9 Software Safety Plan  
33 B.3.1.10 Software Verification and Validation Plan  
34 B.3.1.11 Software Configuration Management Plan  
35 B.3.1.12 Software Test Plan  
36

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

41  
42 While most of the information about the above topics is in the SPM, information found in the  
43 other submittals and in previous revisions of the SPM is sometimes helpful to the evaluation,  
44 and therefore, was considered for this evaluation. The SPM includes sections with the following  
45 section numbers and titles:

- 46  
47
  - (Section 3) Software Safety Plan (SSP)
  - 48 • (Section 4) Software Quality Assurance Plan (SQAP)
  - 49 • (Section 5) Software Verification and Validation Plan (SVVP)
  - 50 • (Section 6) Software Configuration Management Plan (SCMP)

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

5  
6 The staff found the information needed to support its safety conclusions on the balance of the  
7 life cycle topics either in the balance of the SPM or in the Common Q TR WCAP-16097-P  
8 "Common Qualified Platform" (Ref. 14) and its appendices. The staff has organized this report  
9 to follow the sequence outlined under the topic in BTP 7-14. BTP 7-14, Section B.3.1 describes  
10 the acceptance criteria used for reviewing the 12 software plans of the SPM.

### 11 12 **3.2.1 Software Management Plan**

13  
14 The Software Management Plan (SMP) describes the management aspects of the software  
15 development project. BTP 7-14, Section B.3.1.1 describes acceptance criteria for software  
16 management plans. RG 1.173 endorses IEEE Std. 1074-2006, "IEEE Standard for Developing  
17 Software Life Cycle Processes." IEEE Std. 1074-2006 describes, in terms of inputs and  
18 outputs, a set of processes and constituent activities that are commonly accepted as comprising  
19 a controlled and well-coordinated software development process. IEEE Std. 1074-2006  
20 Annex A, Section A.1, "Project Management Section of Activity Groups," describes an  
21 acceptable approach for software project management. It states that project management  
22 processes are, "the processes that initiate, monitor, and control software projects throughout the  
23 software life cycle."

24  
25 The required elements of a Software Management Plan are contained within Sections 2, 4.3,  
26 5.5.1, and 6.2 of the Common Q SPM. These sections of the SPM define a strategy for  
27 managing Common Q software projects. Each of these sections was reviewed against the  
28 specific acceptance criteria established by BTP 7-14.

29  
30 Section 4.3 of the Common Q SPM describes the management principles used for the  
31 development of Common Q application software for each phase of the software development  
32 life cycle. It includes a description of the software project planning organization which includes  
33 a general overview of the organizational structure used by WEC and a discussion of the  
34 responsibilities that each of the following organizations has within the Nuclear Automation  
35 Organization.

- 36
- 37     ▪ Quality Organization
- 38     ▪ Engineering Organization
- 39         ○ Design Team
- 40         ○ V&V Team
- 41

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

47  
48 A level of independence between the Verification and Validation (V&V) Team and the Design  
49 Team is established by specifying different reporting structures up to the director level. Beyond  
50 the director level, the two teams report to the same vice president. The directors to which the

1 V&V team and the Design team report are administratively and financially independent of one  
2 another. This relationship between the design team and the independent verification and  
3 validation (IVV) team is illustrated in Exhibit 2-1, "Design/IV&V Team Organization," of the SPM.  
4 The degree of independence between the V&V team and the design team is further reinforced  
5 by not allowing V&V team members to participate on the design team.  
6

7 The SPM calls for the development of a project specific Project Quality Plan (PQP) during the  
8 Initiation (Concepts) Phase of the software development life cycle. The PQP allows for  
9 alternatives to the SPM processes. Because of this, the PQP should be reviewed to determine  
10 if the justification for the use of alternatives to the SPM or other, additional metrics or qualifiers  
11 beyond the directions within the SPM is acceptable when an applicant requests approval for  
12 installation of a safety-related system based on the Common Q platform. This is plant specific  
13 action item 1.  
14

15 Per BTP 7-14, Sections B.3.2 and B.3.3, the implementation activities and design outputs are to  
16 be separately evaluated so that the application design can be evaluated to determine that the  
17 software management plan has been followed. This is plant specific action item 2.  
18

19 The elements of the software management plan are incorporated into the Common Q SPM.  
20 The staff has reviewed the Common Q SPM and finds that it establishes adequate organization  
21 and authority structure for the design, the procedures to be used, and the relationships between  
22 major activities. The staff finds that the management structure in the Common Q SPM provides  
23 for adequate project oversight, control, reporting, review, and assessment. The management  
24 structure also supports independence of V&V activities. The staff concludes that the Common  
25 Q SPM meets the requirements for a software management plan as outlined in IEEE  
26 Std. 1074-2006 as endorsed by RG. 1.173 and, is, therefore, acceptable.  
27

### 28 **3.2.2 Software Development Plan**

29  
30 The Software Development Plan (SDP) describes the plan for technical project development.  
31 BTP 7-14, Section B.3.1.2 describes acceptance criteria for software development plans.  
32 RG 1.173 endorses IEEE Std. 1074-2006 as providing an acceptable approach to software  
33 development processes. BTP 7-14 states that the SDP should clearly state tasks of each life  
34 cycle, and state the life cycle inputs and outputs. The review, verification and validation of those  
35 outputs should be defined. IEEE Std. 7-4.3.2-2003 provides additional guidance on software  
36 development processes.  
37

38 WEC uses a controlled software development process which is defined within the Common Q  
39 SPM. The criteria for the Common Q software development plan are satisfied by a project plan  
40 and a Project Quality Plan. These plans are created for each Common Q project in accordance  
41 with general criteria that is defined within the SMP. The required elements of a Software  
42 Development Plan are defined within the following SPM sections:  
43

- 44 • 1.2.1, "Software Classification and Categorization"
- 45 • 1.4.1, "Software Life Cycle"
- 46 • 4.1.3, "Software Development Process"
- 47 • 5.9, "Software Integrity Level Scheme"
- 48

1 Common Q Software Life Cycle

2

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

7

- 8 • Concept
- 9 • Requirements Analysis
- 10 • Design
- 11 • Implementation or Coding
- 12 • Test
- 13 • Installation and Checkout
- 14 • Operation and Maintenance
- 15 • Retirement

16

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

22

23 Common Q Software Life Cycle Tasks (Inputs & Outputs)

24

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

33

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

43

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

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

#### 8 9 Common Q Software Integrity Level Scheme

10  
11 Section 5.9 of the Common Q SPM discusses the WEC Common Q specific software  
12 classification or software integrity level scheme.

13  
14 Table 5.9.1 of the SPM compares the WEC software integrity level scheme with the scheme  
15 presented within IEEE Std. 1012-2004. IEEE Std. 1012-2004 states: "This standard uses  
16 software integrity levels to determine the V&V tasks to be performed. High-integrity software  
17 requires a larger set of V&V processes and a more rigorous application of V&V tasks."

18 Section 1.2.1 of the SPM defines the software classes used for Common Q software as follows:

- 19  
20 • **Protection** (*safety critical*). Software whose function is necessary to directly perform  
21 RPS control actions, ESFAS control actions, and safe shutdown control actions.
- 22  
23 • **Important-to-Safety**. Software whose function is necessary to directly perform alternate  
24 protection system control actions or software that is relied on to monitor or test  
25 protection functions, or software that monitors plant critical safety functions.
- 26  
27 • **Important-to-Availability**. Software that is relied on to maintain operation of plant  
28 systems and equipment that are critical to maintaining an operating plant.
- 29  
30 • **General Purpose**. Software that performs some purpose other than that described in  
31 the previous classifications. This software includes tools that are used to develop  
32 software in the other classifications, but is not installed in the online plant system.  
33 Examples of General Purpose software include commercial grade dedication test  
34 software, compilers, assemblers, linkers, comparators, editors, test case generators, and  
35 test coverage analyzers.

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

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

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

## 6 Management and Oversight of the Software Development Processes

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

## 21 22 Software Tools

23  
24 BTP 7-14, Section B.3.1.2.4 provides guidance for software tools, and references  
25 IEEE Std. 7-4.3.2-2003, Clause 5.3.2, which states, in part, that software tools used to support  
26 software development processes and verification and validation processes shall be controlled  
27 under configuration management. To confirm the software tools are suitable for use, the clause  
28 further states either a test tool validation program shall be developed to provide confidence that  
29 the necessary features of the software tool function as intended or the software tool shall be  
30 used in a manner such that defects not detected by the software tool will be detected by V&V  
31 activities.

32  
33 The Common Q SPM Sections 3.3.10, "Tool Support and Approval," and 4.9, "Tools,  
34 Techniques and Methodologies," discuss the development support tools used to facilitate  
35 Common Q application software development. An evaluation of a tool's readiness for use on a  
36 project is performed before such a tool is used to support the development of a Common Q  
37 application. This evaluation considers; the tool's past performance, extent of tool validation  
38 performed, consistency of tool design with planned use, use of tool upgrades, retirement of the  
39 tool, and restrictions on the use of the tool due to its limitations. The configuration  
40 management, software quality assurance and IVV processes defined within the SPM apply to  
41 software tools and provide a means of ensuring that these tools are only used for their approved  
42 and intended purposes. The outputs of software tools undergo the V&V process as defined in  
43 the Software Verification and Validation Plan (SVVP), in SPM Section 5.

44  
45 The staff has reviewed the Common Q SPM and concludes that the software development plan  
46 conforms with the criteria provided by IEEE Std. 1074-2006, "IEEE Standard for Developing  
47 Software Life Cycle Processes," as endorsed by RG 1.173, "Developing Software Life Cycle  
48 Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." In  
49 addition, the SPM adequately addresses the software development planning activities of

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

### 3 4 **3.2.3 Software Quality Assurance Plan**

5  
6 BTP 7-14, Section B.3.1.3 provides guidance in evaluating a Software Quality Assurance Plan  
7 (SQAP). The SQAP shall conform to the requirements of 10 CFR Part 50, Appendix B, and the  
8 applicant's overall QA program. 10 CFR Part 50, Appendix B states that the applicant shall be  
9 responsible for the establishment and execution of the quality assurance program. The  
10 applicant may delegate the work of establishing and executing the quality assurance program,  
11 or any part thereof, but shall retain responsibility for the quality assurance program. The SQAP  
12 would typically identify which QA procedures are applicable to specific software processes,  
13 identify particular methods chosen to implement QA procedural requirements, and augment and  
14 supplement the QA program as needed for software.

15  
16 IEEE Std. 7-4.3.2-2003, Clause 5.3.1, which is endorsed by RG 1.152 provides guidance on  
17 software quality assurance. IEEE Std.7-4.3.2-2003, Clause 5.3.1, states, "Computer software  
18 shall be developed, modified, or accepted in accordance with an approved software QA plan.

19  
20 The Common Q SQAP for application software is described in Section 4 of the SPM, "Software  
21 Quality Assurance Plan." The SQAP describes the methodology used for managing Common Q  
22 software throughout the development life cycle. Section 4.1.1 of the SPM states that the  
23 Common Q SPM complies with IEEE Std. 730-1998. The scope of the Common Q SQAP  
24 includes software in all four SIL classifications ~~for: protection, and important to safety, important~~  
25 ~~to availability, and general purpose. The Common Q SQAP no longer applies to software~~  
26 ~~classified as: important to availability or general purpose software.~~ The Common Q SQAP  
27 applies to original protection and important to safety software that was developed under the  
28 requirements of the Common Q SPM.

29  
30 Evaluations of existing software not created under the controls of the Common Q SPM are  
31 performed in order to qualify this software for use under the Common Q SPM. For commercial  
32 software, qualification is achieved through the use of WEC's commercial grade dedication  
33 program. For non-commercial protection and important to safety software that has actively  
34 been used in a nuclear power plant being implemented in Common Q, an evaluation is  
35 performed to ensure the quality assurance program being used for development and  
36 maintenance of this software is acceptable and includes the following:

- 37  
38
- 39 • The effective quality assurance program has an active program for problem and  
40 corrective action reporting.
  - 41 • The software has adequate design documentation.
  - 42 • The software has adequate user documentation.
  - 43 • The software includes well commented source code.
  - 44 • The software has been verified and validated under a program that the IVV team  
45 determines to be appropriate.

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



1 Quality assurance tasks are listed in Exhibit 4-3 of the SPM. These quality assurance tasks are  
2 described in Section 4 of the SPM for each software life cycle phase. These descriptions  
3 include a discussion of the tasks and the responsibilities of the organizations performing  
4 software quality assurance activities. In addition, Exhibit 5-1 identifies organizational  
5 responsibilities for performance of specific software SQA tasks.  
6

7 Documentation requirements for performance of software Quality Assurance (SQA) activities  
8 are described in Section 4.4, "Documentation," of the SMP. Many of the tasks listed in  
9 Exhibit 4-3 are in fact documents that will provide evidence for completion of the associated  
10 SQA tasks. Furthermore, Section 10 of the SPM, "Documentation," provides guidance for how  
11 these documents will be developed.  
12

13 SPM Section 4.5 identifies the standards, practices, conventions and metrics used for the  
14 development of a Common Q based system. It states that, "*compliance with the WEC quality  
15 management system standards shall be monitored and assured through the review and audit  
16 process.*" Standards used for development of Common Q systems include Coding Standards,  
17 Software Testing Standards, and Documentation Standards. Coding standards are not  
18 established at a generic level and are instead defined within the project specific PQP. Testing  
19 standards are defined by the Software Test Plan which is evaluated in Section 3.2.12 of this SE.  
20 Documentation Standards are identified in Section 10 of the SPM and include IEEE  
21 Std. 830-1998 for Software Requirement Specification (SRS) documentation requirements,  
22 IEEE Std. 1016-1998 (Reaffirmed in 2009) for Software Design Description (SDD)  
23 documentation requirements, IEEE Std. 1012-2004 for V&V documentation requirements, and  
24 IEEE Std. 1063-2001 for Software User documentation requirements.  
25

26 SPM Section 4.6 describes how software reviews are performed for Common Q applications.  
27 Software reviews are performed to verify technical adequacy and to verify completeness of the  
28 design and development of Common Q software. The SPM lists several software review  
29 activities and defines groups responsible for performance of these activities. The following  
30 types of reviews which are defined in IEEE Std. 1028-2008 are performed for Common Q  
31 software developed under the SPM:  
32

- 33 • Management Reviews,
- 34 • Technical Reviews,
- 35 • Inspections,
- 36 • Walk-through's, and
- 37 • Audits.
- 38

39 SPM Section 4.6.2 describes the minimum software reviews and audits to be performed for  
40 Common Q software. The staff has determined that this minimum set of review and audit  
41 requirements complies with the criteria of IEEE Std. 730-1998 Sections 4.6.2.1 through  
42 4.6.2.10.  
43

44 IEEE Std.730-1998, Section 4.8 states that the SQAP should describe practices and procedures  
45 to be followed for reporting, tracking, and resolving problems. It also stipulates that the SQAP  
46 should state specific organizational responsibilities concerned with implementation.  
47

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

1 testing, review, or other means. The SPM describes two processes used for reporting errors.  
2 One is used for errors identified during the development process prior to approval for use in a  
3 nuclear power plant application. The other is used for reporting of errors that are identified after  
4 the software has been approved for use. These processes include noncompliance reporting in  
5 accordance with 10 CFR Part 21, "Reporting of Defects and Noncompliance." Organizational  
6 responsibilities associated with the problem reporting and corrective action processes are also  
7 defined in the SPM.  
8

9 During the Initiation (Concept) phase, the SQAP calls for the development of a PQP which  
10 becomes the operative plan for a specific application development process. This PQP may  
11 deviate from the SQAP processes defined in Section 4 of the SPM; however, any such  
12 deviations must be documented and justified within the PQP. Because such deviations cannot  
13 be evaluated during this safety evaluation, a plant specific action item for evaluating these  
14 changes has been created. This is plant specific action item 1.  
15

16 The regulation at 10 CFR Part 50, Appendix B, allows applicants or licensees to delegate the  
17 work of establishing and executing the Quality Assurance program, but applicants/licensees  
18 shall retain overall responsibility and shall determine if the quality of the software is sufficient.  
19 Applicants or licensees referencing this topical report are to make available a SQAP to address  
20 these licensee specific responsibilities. This is plant specific action item 3.  
21

22 The SQAP stipulates that the SQA organization shall participate in formal reviews and audits of  
23 the software development activity. Required reviews and audits are indicated in the plan  
24 including review documentation requirements, evaluation criteria, anomaly reporting, and  
25 anomaly resolution procedures. Additional reporting of the staff's evaluation of the SQAP is  
26 detailed in Section 3.2.10, "Software Verification and Validation Plan."  
27

28 The SQAP describes the process by which WEC manages software and documentation  
29 throughout the Common Q software development life cycle, and the SQAP conforms to  
30 IEEE Std. 730-1998. The Engineering Project Manager is responsible for ensuring all design  
31 team activities are performed in accordance with the QA processes and procedures. The SQAP  
32 adequately addresses the software quality planning activities of BTP 7-14. The staff concludes  
33 that the Common Q SQAP meets the Guidance in BTP 7-14 Section B.3.1.3 with regard to QA  
34 software reviews and audits and is, therefore, acceptable.  
35

36 Revision 5 to the SPM includes a change to the process for development of a site test plan.  
37 This change allows development of the site test plan to occur at a later stage of the  
38 development lifecycle to support evaluation of requirement testability on-site. The V&V activity  
39 for system V&V test plan generation described in Exhibit 5-8 of the SPM was also revised to  
40 facilitate later stage development of the site test plan if necessary. The NRC staff finds this  
41 change acceptable because required V&V activities are retained. This change allows for later  
42 stage completion of required tasks and does not alter the requirements for task completion.  
43

#### 44 **3.2.4 Software Integration Plan**

45

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

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

4  
5 For the Common Q, WEC does not define a separate software integration organization to  
6 perform system integration related activities. Instead, such activities are allocated to different  
7 organizations involved with the Common Q software development processes. This allocation of  
8 integration activities is defined within various sections within the SMP. For example, Integration  
9 Tests are defined in Section 7.3.1.3 of the SPM and Exhibit 5-1 shows that the IVV Team has  
10 the responsibility for performing Integration tests for Protection software. Conversely, the  
11 design team has the responsibility for performing Integration tests for Important to Availability  
12 software.

13  
14 The testing aspects of Common Q Software Integration are described in Section 7, "Software  
15 Test Plan," of the SPM. The Common Q software testing process includes Integration Tests  
16 that are conducted on the production hardware or with a system that is functionally equivalent to  
17 the production system. This section also specifies that a functionally equivalent system entails  
18 a test bed which provides a functionally equivalent configuration to the production hardware.

19  
20 The NRC staff notes this is a deviation from the integration test description provided in the  
21 previous version of the SPM which stated that integration tests were to be performed on actual  
22 production hardware. The NRC staff determined that allowing performance of integration tests  
23 on non-production hardware is acceptable based on the fact that first of a kind systems undergo  
24 system validation tests, which per Section 4.7 of the SPM, encompass the scope of a factory  
25 acceptance test (FAT) and subsequent factory tests must still be performed using actual  
26 production equipment. Section 7.3.1.5, "Factory Acceptance Test (FAT)," of the SPM states  
27 that "FAT includes tests that are performed on the deliverable system for each deliverable  
28 system." In addition, Westinghouse confirmed in its response to RAI 7, and RAI 8  
29 (Reference 016) that "... the Factory Acceptance Test (FAT) is performed on the delivered  
30 equipment." Subsection 7.3.1.3, "Integration Test," describes the details of the integration tests  
31 performed during the development of a Common Q application.

32  
33 Revision 5 of the SPM changed Section 7.3.1.3, "Integration Test," of the SPM such that the  
34 following Integration Test Items listed were removed.

- 35
- 36 • Error Handling
- 37 • Communications
- 38 • Redundancy
- 39 • Diversity
- 40

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

48  
49 Subsection 4.5.2.4 of the SPM discusses metrics used for integration tests.  
50

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

- 4
- 5 1. Integration of software modules to form system executable programs. For a Common Q  
6 project this level of integration is accomplished by the creation of control functions using  
7 ~~the AMPL Control Configuration (ACC)~~an approved; development tool. Proper use of  
8 ~~ACC~~the tool involves assembly of pre-approved Program Control (PC) elements into  
9 complete control functions. These control functions are converted into code to be used  
10 for transfer to the Common Q hardware. Structured design techniques, including the  
11 use of data flow diagrams represent interactions among modular elements and the flow  
12 of data among these elements. Unit and Module tests are performed to ensure that the  
13 module and system requirements have been met by the integrated software.

14

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

- 21
- 22 2. Integration of the resultant programs with the production hardware and instrumentation  
23 or with representative functionally equivalent hardware and instrumentation. This level  
24 of integration is performed at the manufacturing facility after the cabinets are assembled  
25 and energized. Optionally, this integration testing can be performed using surrogate  
26 equipment which is functionally equivalent to the production hardware. The system  
27 hardware architecture is established in conjunction with the application software ~~using~~  
28 ~~the ACC tool~~; therefore, specific assignment of software programs to PM646A  
29 processors is performed prior to the generation of application executable code. The  
30 processor applications are loaded into the PM646A processors as the system is  
31 prepared for integration testing. An integration test is performed to verify that the  
32 released software correctly integrated with the production hardware or representative  
33 test bed hardware. All cabinets within a safety system division are interconnected and  
34 integrated as a part of the integration test process.

35

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

- 41
- 42 3. Testing the resulting integrated product. This final level of integration is completed during  
43 the System FAT by confirming the correct relationship between test input and output  
44 signals. System functions that are implemented across multiple safety divisions are  
45 tested to ensure that the overall integrated system meets the systems specifications  
46 defined in the System Requirements Specification. For first of a kind systems (FOAKs),  
47 certain activities associated with the FAT may have been performed during the system  
48 validation tests, and if properly documented, would not need to be re-performed during  
49 the FAT. For Nth of a kind systems, the FAT, together with the documentation for prior  
50 V&V activities, verifies that all system level functional and performance requirements are  
51 satisfied. Regardless of whether the FAT is for a FOAK system or Nth of a kind system,

1 the purpose of a FAT is to demonstrate the complete system is integrated and  
2 functional.  
3

4 The staff reviewed WEC's application software development and testing processes for both  
5 AC160 and FPD software and found they specify how to develop plans for software integration  
6 both during the development of the software and during integration with the hardware. The  
7 actual integration procedures will be prepared during the planning stage of each project. The  
8 staff concludes that the plans for software integration exhibit the management, implementation,  
9 and resource characteristics outlined in BTP 7-14 and are, therefore, acceptable.  
10

### 11 **3.2.5 Software Installation Plan**

12  
13 The acceptance criteria for a Software Installation Plan are contained in BTP 7-14,  
14 Section B.3.1.5. IEEE Std. 1074-2006, Clause A.1.2.4, "Plan Installation," endorsed by  
15 RG 1.173, provides an acceptable approach for software installation plans. The software  
16 installation plan includes the necessary software modifications, checkout in the target  
17 environment, and customer acceptance. If a problem arises, it must be identified and reported.  
18 BTP 7-14, Section B.3.1.5.4 states that there should be approved procedures for software  
19 installation, for combined hardware and software installation, and systems installation. In  
20 addition there should be a controlled process to identify, correct, and document errors in the  
21 installation procedures.  
22

23 The Software Installation Plan for Common Q system software is Section 8 of the Common Q  
24 SPM. Its purpose is to describe the installation processes to be used for the Common Q  
25 system. These processes include loading both operating system and application software into  
26 the production Common Q AC160 processor modules and Flat Panel Display system  
27 processors.  
28

29 The staff reviewed the Common Q SPM and found that it included adequate plans for software  
30 installation. The procedure(s) for installing the software will be prepared before the installation  
31 and checkout phase of the software life cycle. The staff finds that the plans for software  
32 installation exhibit the management, implementation, and resource characteristics outlined in  
33 BTP 7-14 and are, therefore, acceptable. However, the Common Q Software Installation Plan  
34 does not address the installation of the Common Q System into the plant environment. Since  
35 the applicant or licensee assumes responsibility, including vendor oversight, for the software  
36 installation phase information necessary to address the criteria of BTP 7-14, further evaluation  
37 of the site installation activities will be required. This should be accomplished as part of plant  
38 specific action item 2.  
39

### 40 **3.2.6 Software Maintenance Plan**

41  
42 The acceptance criteria for a Software Maintenance Plan are contained in BTP 7-14.  
43 Section B.3.1.6. IEEE Std. 7-4.3.2-2003, Clause 5.4.2.3, endorsed by RG 1.152 provides  
44 guidance on maintenance and configuration management for commercially dedicated items.  
45 IEEE Std. 1074-2006, Clause A.4.2.3, "Maintenance Activity Group," provides an approach for  
46 software maintenance plans. IEEE Std. 1074-2006, Clause 6.3.1 states the Maintenance  
47 Activity Group is concerned with the identification of enhancements and the resolution of  
48 software errors, faults, and failures. NUREG/CR-6101, Section 3.1.9 and Section 4.1.9 also  
49 contain guidance on Software Maintenance Plans. These sections identify the maintenance  
50 activities to be governed by the Software Maintenance plan as; failure reporting, fault correction,  
51 and re-release procedures.

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

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

12

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

### 16

### 17 **3.2.7 Software Training Plan**

### 18

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

24

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

- 28
- 29 • 3.3.3, "Staff Qualifications and Training"
- 30 • 3.5.1, "Training"
- 31 • 4.14, "Training"
- 32 • 7.2.2, "Staffing and Training"
- 33

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

37

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

42

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

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

### 5 6 **3.2.8 Software Operations Plan** 7

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

17  
18 The revised version of the SPM, does not contain a dedicated section to address the criteria for  
19 software operations planning. WEC stated that the Software Operations Plan is either a project  
20 specific activity or the Licensee's responsibility.

21  
22 The Software Operations Plan is not within the scope of the Common Q Software Program  
23 Manual. Therefore, a safety determination cannot be made for a Software Operations Plan in  
24 this regard. Since the applicant or licensee will assume responsibility, including vendor  
25 oversight, for the software operations phase of the software life cycle, relevant information must  
26 be evaluated as part of a plant specific action item. An evaluation of compliance with the criteria  
27 of BTP 7-14 Section B.3.1.8 shall be performed at the time of system development when the  
28 operational aspects of the system have been defined. These requirements are captured as  
29 PSAI's 3 and 4.

### 30 31 **3.2.9 Software Safety Plan** 32

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

43  
44 The Software Safety Plan for Common Q system software is Section 3, Software Safety Plan,"  
45 of the Common Q Software Program Manual. The stated purpose of the Common Q Software  
46 Safety Plan is, "...to enable the development of safety critical software for Common Q<sup>TM</sup>  
47 Systems that has reasonable assurance that software defects do not present severe  
48 consequences to public health and safety."

49  
50 To accomplish this goal, the Common Q SSP defines procedures and methods to be used for  
51 the development, procurement, maintenance and ultimately, retirement of all Protection class

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

5  
6 Software Safety Organization:

7  
8 The Common Q SSP establishes a software safety organization which is composed of two  
9 parts. The first part is the quality organization, which is an independent quality assurance  
10 department. This quality organization coordinates and reviews quality assurance procedures  
11 and directives. The Quality organization has a reporting chain separate from the design team  
12 such that the QA organization is independent of project schedule and cost considerations. The  
13 Quality organization provides oversight by way of periodic audits to verify that the Automation  
14 Engineering organization is correctly abiding by both the procedures and directives generated  
15 by both organizations. The SSP is approved by the Manager of the Quality organization, or  
16 designee.

17  
18 The second part of the software safety organization is the Independent Verification and  
19 Validation Team (IVV Team). This IVV team performs the safety activities for a given Common  
20 Q system implementation project.

21  
22 The resource requirements needed to perform software safety activities are to be developed by  
23 the IVV team leader and the Engineering Project Manager. A plant specific Project Quality Plan  
24 will coordinate both the system development, software safety and quality assurance activities to  
25 identify the prescribed procedures and provide the resources needed for their execution.

26  
27 During the requirements phase of the software development life cycle process, an evaluation is  
28 performed to identify the safety critical hazards posed by the system through its interfaces. For  
29 each hazard identified, the analysis determines whether a software malfunction could produce  
30 the hazardous condition. Each software producible hazard is then subsequently evaluated  
31 during each development phase of the safety critical software to determine if new hazards have  
32 been introduced during that phase, or if the evolving design has altered the results of the  
33 hazards analysis. The results of IV&V analyses performed on requirements, design, code, test  
34 and other technical documentation are documented in the IVV Phase Summary Reports and the  
35 Final IVV Report for the system.

36  
37 The safety requirements that need to be met by the software in order to mitigate or control  
38 system hazards are defined in the system requirements specifications. The software design  
39 description will include descriptions of the software design elements that satisfy the software  
40 safety requirements. The responsibilities for the execution of the SSP and for ensuring that the  
41 software safety activities are completed in accordance with the plan are divided between the  
42 IVV Engineering Line Manager (ELM) and the quality manager.

43  
44 The safety organization defined in the Common Q SSP considers the security risk as well as the  
45 risk to the plant if the digital system malfunctions. The critical design review identifies the risks  
46 associated with the system design in a manner that is consistent with the software safety  
47 strategy.

48  
49 The staff has reviewed the Common Q SSP and finds that it addresses the topics described in  
50 the SRP and in IEEE Std. 1228-1994 (Reaffirmed in 2002), "IEEE Standard for Software Safety  
51 Plans." The Common Q SSP describes the organizational structure and responsibilities,



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

### 9 10 **3.2.10 Software Verification and Validation Plan**

11  
12 The acceptance criteria for the SVVP are contained in the SRP, BTP 7-14, Section B.3.1.10,  
13 "Software Verification and Validation Plan," and Section B.3.2.2, "Acceptance Criteria for  
14 Software Verification and Validation Activities. "These sections identify RG 1.168, "Verification,  
15 Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of  
16 Nuclear Power Plants" which endorses IEEE Std. 1012-2004, "IEEE Standard for Software  
17 Verification and Validation," as providing methods acceptable to the NRC staff for meeting the  
18 regulatory requirements for verification and validation of safety system software. This section  
19 also states that further guidance can be found in NUREG/CR-6101, Sections 3.1.4 and 4.1.4.

20  
21 Verification is defined as the process of determining whether the products of a given phase of  
22 the development cycle fulfill the requirements established during the previous phase.

23 Validation is defined as the test and evaluation of the integrated computer system to ensure  
24 compliance with the functional, performance, and interface requirements.

25  
26 Combined, verification and validation is the process of determining whether the requirements for  
27 a system or component are complete and correct, the products of each development phase  
28 fulfill (i.e., implement) the requirements to meet the criteria imposed by the previous phase, and  
29 the final system or component complies with specified requirements.

30  
31 The Software V&V Plan for Common Q system software is Section 5 of the Common Q  
32 Software Program Manual. The stated purpose of the Common Q SVVP is to establish  
33 requirements for the IVV process to be applied to Common Q systems. It also defines when,  
34 how and by whom specific IVV activities are to be performed.

35  
36 The aim of the Common Q software V&V program is to provide an acceptable generic  
37 methodology of V&V as part of the qualification process for computer software applications  
38 developed for the Common Q platform. The Common Q SVVP applies to all new software to be  
39 developed under the SPM and to some previously developed application software to be used in  
40 the Common Q platform. For the qualification of existing software, either for use in the generic  
41 Common Q platform or for use in new applications, the following cases are identified:

- 42
- 43 • Existing commercial software will be qualified under the Commercial Grade Dedication  
44 Program, which is outlined in the Common Qualified Platform Topical Report (Ref. 14).
  - 45
  - 46 • Existing non-commercial software that has been actively used in nuclear power plants  
47 will be qualified for the Common Q platform by judging its original V&V program. The  
48 V&V effort will make this judgment using review criteria similar to those for newly  
49 developed software.
- 50

1 Other existing non-commercial software may be used under the conditions that (1) the software  
2 fulfills a specific requirement identified in the software requirements specification, (2) the code is  
3 well organized and has adequate design documentation and source code commentary to permit  
4 the application of the V&V process, and (3) the software is subjected to the V&V process,  
5 starting at the design phase.  
6

7 For the development of new application software, depending on the scope of each specific  
8 project, WEC will decide whether to issue a project-specific SVVP or to maintain the generic  
9 plan as is. The use of the generic plan will require that the software developers manage the  
10 deviations and the project-specific aspects through the project-specific plan to be developed for  
11 each project. WEC will hold these project-specific SVVPs for audit. WEC also will hold the  
12 project-specific V&V reports for projects developed under the Common Q platform for audit, and  
13 the licensees will hold the V&V reports associated with plant-specific applications for audit.  
14 Succeeding systems manufactured under the same design as a system that was previously  
15 verified and validated in accordance with this SVVP will be certified by performing, as a  
16 minimum, the equivalent of the validation tests that were applied to the verified and validated  
17 system. The staff considers this approach to be acceptable.  
18

19 WEC differentiates the span of the V&V activities and the grade of independence required for  
20 V&V reviewers according to the classification of each software item. The Common Q software  
21 integrity level classifications have been updated in Revision 5 of the SPM and are discussed in  
22 Section 3.2.2 of this SE. These Classifications are:  
23

- 24 • Protection,
- 25 • Important to safety,
- 26 • Important to availability, and
- 27 • General purpose.  
28

29 These four levels respectively are matched to the four categories in IEEE Std. 1012-2004 of  
30 **high4**, **major3**, **moderate2**, and **low1**. The Software Integrity Levels described in the Common Q  
31 SPM are mapped to the activities associated with IEEE Std. 1012-2004, SIL 4 in the SPM.  
32

33 WEC follows the guidance provided in IEEE Std.1012-2004 regarding structure and content for  
34 SVVPs when applied to the development of safety-related Common Q software. IEEE  
35 Std. 1012-2004 provides the uniform and minimum requirements for the format and content of  
36 these plans. Additionally, the standard defines the minimum set of specific V&V tasks to be  
37 carried out during each phase of the critical software development life cycle and the required  
38 inputs and outputs for these tasks. Exhibit 5-8 of the SPM lists and defines the specific V&V  
39 tasks used for Common Q software development and maps these tasks to the V&V activities  
40 defined within IEEE Std. 1012-2004. The tables in Exhibit 5-1 and 5-8 identify the minimum set  
41 of V&V activities for all classifications of Common Q software including noncritical software.  
42 The NRC notes that V&V Tasks for Important to Availability and General Purpose classifications  
43 are identified in Exhibit 5-1.  
44

45 The Common Q SVVP incorporates verification reviews and validation testing. Verification  
46 reviews are supported by the use of checklists and requirements traceability analyses for the  
47 phases of requirements, design, implementation, test, and installation and checkout. A  
48 requirements traceability matrix will be prepared at the beginning of the software development  
49 process and updated throughout the phases of the software life cycle.  
50

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

8  
9 For protection and important to safety software, verification reviews are performed by the V&V  
10 staff. V&V activities for the preparation of test plans, procedures, test result reports and  
11 execution of tests are performed by either the design team or by the V&V team depending on  
12 the classification level of the software being tested. Exhibit 5-1 of the SPM designates which  
13 team is responsible for performing these activities. When the design team prepares the material  
14 or executes the tests, the V&V team will oversee the conduct of these activities by reviewing  
15 documentation and witnessing testing.

16  
17 Revision 5 of the SPM introduces a System Validation Test process to validate the hardware  
18 design, software design, and system integration of first instance applications at a functional  
19 level. Section 7.3.1.4, "System Validation Test," of the SPM was added to the SPM to describe  
20 the System Validation Testing activities. Section 7.3.1.5 "Factory Acceptance Test," of the SPM  
21 has also been rewritten to adopt the new System Validation Test processes and to describe  
22 differences between validation activities performed during Factory Acceptance Testing and  
23 validation activities to be performed during the new System Validation Test activities.  
24 Exhibit 7-1 in the SPM provides a comparison of System Validation Test and Factory Test  
25 Processes.

26  
27 Validation Test requirements are accomplished for each Common Q system through a  
28 combination of System Validation Test activities and Factory Acceptance Test activities.

29  
30 The System Validation process is intended to be used to validate the first application or first  
31 instance of a system design while subsequent instances of the same design will undergo  
32 integration testing during Factory Acceptance Test processes. Factory Acceptance Tests will  
33 be limited in scope such that testing of logic that was previously verified during System  
34 Validation Testing will not be performed. For example, Factory Acceptance Testing will only  
35 include a subset of voting logic combinations to demonstrate each input to voting logic is  
36 effective whereas System Validation Testing of Voting Logic includes testing of all combinations  
37 including bypasses and forced trips.

38  
39 System Validation Testing can also be performed using representative Common Q equipment in  
40 lieu of production hardware to be delivered and installed into a licensed facility. Conversely,  
41 Factory Acceptance Tests are performed on the deliverable system, both the hardware and  
42 software, and are performed for each deliverable Common Q system.

43  
44 Test documentation will be prepared in accordance with IEEE Std.829-1998, "IEEE Standard for  
45 Software Test Documentation." IEEE Std. 829-1983 is endorsed by RG 1.170,  
46 September 1997. After the system is validated, a Code certificate is issued certifying that the  
47 system is acceptable for use. The SVVP addresses V&V activities associated with the  
48 operation and maintenance phase by ensuring that program modifications are submitted to the  
49 same V&V program applied to new software development. Software changes will be evaluated  
50 by a software safety change analysis, the results of which shall be found in the V&V report. The  
51 SVVP addresses the use of regression testing for the V&V of software modifications.

1 The SVVP also addresses activities designed to verify the adequacy of the software  
2 development documentation issued throughout the software life cycle, installation procedures,  
3 training materials, and user documentation.  
4

5 As a result of the V&V activities throughout the software development process, V&V phase  
6 summary reports, including discrepancy reports, will be issued. A final V&V report will be issued  
7 after the V&V process, including the assessment of the overall software and system quality and  
8 a Code certificate. Results of V&V analyses performed on requirements, design, code, test, and  
9 other technical documentation are documented in the V&V phase summary reports and the final  
10 V&V report. Information on suspected or confirmed safety problems in the pre-released or  
11 installed system is recorded in the final V&V report. Results of audits performed on software  
12 safety program tasks are documented in the V&V phase summary reports and in the final V&V  
13 report. Results of safety tests conducted on all or any part of the entire system are documented  
14 in the test report. Software safety certification is documented in the Code certificate. The SVVP  
15 is reviewed for adequacy and completeness of the V&V methods by an independent reviewer.  
16

17 The staff has reviewed the information in the SVVP regarding software module testing and  
18 concludes that the procedures used for performance of software module testing satisfy the  
19 software V&V program requirements of IEEE Std. 7-4.3.2-2003 and are, therefore, acceptable.  
20

#### 21 Independence of Verification and Validation

22

23 The independence requirements for organizations performing quality control activities are  
24 addressed by 10 CFR Part 50 through Criterion I and Criterion III of Appendix B. Criterion I  
25 requires in part, that individuals and organizations performing quality assurance functions have  
26 sufficient authority, organizational freedom and independence from cost and schedule.  
27 Criterion III requires that individuals or groups performing design control activities be different  
28 from those who performed the original design, but they may be from the same organization.  
29

30 The positions reflected in specific standards addressing V&V activities associated with the  
31 implementation of digital I&C systems vary from requiring only technical independence, as in  
32 RG 1.152 by endorsing IEEE Std.7-4.3.2-2003, to requiring technical, financial and schedule  
33 independence, as in RG 1.168. IEEE Std.1012-2004, endorsed by RG 1.168, does not  
34 specifically address the level of independence required. IEEE Std.1012-2004 includes an  
35 informative annex contemplating the position that for high-integrity-level software, the level of  
36 independence required for the V&V organization encompasses technical, managerial, and  
37 financial independence.  
38

39 The organization responsible for ensuring that the Common Q software has been developed  
40 according to the quality required by its classification (called the software safety organization in  
41 the SPM) is composed of two parts:  
42

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

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

12  
13 In response to RAI 11 (Refs. 15 and 16), Westinghouse provided clarification of IV&V group  
14 membership. The SPM further states that; "The IV&V Team in the context of this SPM refers to  
15 those individuals within the IV&V organization who perform V&V functions on the safety system  
16 design, implementation, and test (i.e., engineers and technicians). The IV&V organization may  
17 include other individuals who perform supporting roles that are not design verification related  
18 and the organizational independence does not apply to those individuals."

19  
20 The SPM states that the V&V leader is responsible for the schedule and budget for the V&V  
21 activities, the project manager is responsible for the schedule and budget for the activities  
22 associated with the software development and, therefore, financial and managerial  
23 independence between the development group and the V&V group is achieved.  
24 The staff finds that the WEC approach on independence of V&V for the Common Q platform is  
25 in accordance with the requirements of IEEE Std.7-4.3.2-2003, and is compatible with IEEE  
26 Std. 1012-2004, "IEEE Standard for Software Verification and Validation," as endorsed by  
27 RG 1.168 and is, therefore, acceptable.

### 28 29 **3.2.11 Software Configuration Management Plan**

30  
31 BTP 7-14, Section B.3.1.11 provides guidance for the evaluation of the Software Configuration  
32 Management Plan, and states that IEEE Std.1074-2006, Clause A.1.2.2, "Plan Configuration  
33 Management," provides an acceptable approach to software configuration management. IEEE  
34 Std.1074-2006, Clause A.2.2.2.2 states that Software configuration management includes the  
35 evaluation, coordination, approval or disapproval, and implementation of changes to product  
36 components (e.g., code, documentation) after a baseline has been established. Items that are to  
37 be managed should include code, documentation, plans, specifications, project policies,  
38 procedures, and other artifacts. BTP 7-14, Section B.3.1.11.1 calls for the definition of the  
39 responsibilities and authority of the Software Configuration Management (CM) organization.

40  
41 The Software Configuration Management Plan (SCMP) for Common Q system software is  
42 Section 6 of the Common Q SPM. The SCMP is applicable to all Common Q software as well  
43 as software tools used in the development of Common Q software. The Common Q SCMP  
44 describes the organizational structure that controls the configuration of software. Software  
45 Configuration Management is intended to be applied throughout the entire software life cycle,  
46 including requirements phase, design phase, implementation phase, test phase, installation and  
47 checkout phase, operation and maintenance phase, and retirement phase.

48  
49 The design team and the IVV Group in the Nuclear Automation organization are responsible for  
50 implementation of adequate measures to manage and control the software configuration of a  
51 Common Q project. The Common Q SCMP describes the independence of those responsible

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

12  
13 The staff concludes the SCMP conforms to the requirements identified in IEEE Std. 828-2005,  
14 which is endorsed by RG 1.169. This meets the criteria of BTP 7-14 and is, therefore,  
15 acceptable.

### 16 17 **3.2.12 Software Test Plan**

18  
19 The acceptance criterion for STP is contained in the SRP, BTP 7-14, Section B.3.1.12,  
20 "Software Test Plan," and in Section B.3.2.4, "Acceptance Criteria for Testing Activities." These  
21 sections state that both RG 1.170, September 1997, "Software Test Documentation for Digital  
22 Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE  
23 Std. 829-1983, "IEEE Standard for Software Test Documentation," and RG 1.171, "Software  
24 Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,"  
25 which endorses IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing," identify  
26 acceptable methods to satisfy software unit testing requirements.

27  
28 The Software Test Plan (STP) for Common Q system software is Section 7 of the Common Q  
29 Software Program Manual. This plan identifies the testing activities and test documentation  
30 required to verify and validate Common Q safety system software. The scope of the STP  
31 includes testing of Common Q platform component software as well as application software that  
32 is developed with the Common Q platform.

33  
34 The Common Q STP describes and defines the test activities for the following test types:

- 35  
36
- 37 • Module Tests
  - 38 • Unit Tests
  - 39 • Integration Tests
  - 40 • System Validation Tests
  - 41 • Factory Acceptance Tests

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

45  
46 Unit tests are performed during the plant specific system design to ensure proper functionality of  
47 the platform components as they are incorporated into a specific application.

48  
49 Integration tests are used to confirm that the program units have been properly connected and  
50 are integrated in a manner to ensure proper operation of the overall system. Integration tests

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

3  
4 Validation Test requirements are accomplished for each Common Q system through a  
5 combination of System Validation Test activities and Factory Acceptance Test activities.

6  
7 System Validation Tests are performed to validate the hardware design, software design, and  
8 system integration of first instance applications at a functional level. The System Validation  
9 process is intended to be used to validate the first application or first instance of a system  
10 design while subsequent instances of the same design will undergo integration testing during  
11 Factory Acceptance Test processes. System Validation Testing can be performed using  
12 representative Common Q equipment in lieu of production hardware.

13  
14 Factory Acceptance Testing of the system is conducted with the final application software  
15 installed on the targeted hardware that has been assembled.

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

25  
26 The FAT is the final stage of testing that is conducted prior to acceptance of equipment by the  
27 licensee. All subsequent testing activities such as Site Acceptance Testing and Installation  
28 testing are considered to be the responsibility of the licensee and are therefore not within the  
29 scope of the Common Q STP. The Common Q STP identifies the following two categories of  
30 testing that are used in the Common Q software testing process;

- 31
- 32 • Functional Testing - (otherwise known as black box testing) is used to determine that a  
33 module or system has functional performance that is consistent with the requirements  
34 specified. Test cases for functional testing are derived from the requirement  
35 specifications and are based on manipulating test inputs and monitoring test outputs.  
36
  - 37 • Structural Testing - (otherwise known as white box testing) is used to evaluate the  
38 internal structure of a code module and is only used for module tests. Structural testing  
39 is intended to provide one hundred percent of branch execution within the code module.  
40

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

48  
49 When pre-validated modules are used for an application, the project's validation testing can  
50 begin with Unit Testing of the released application. When specifically developed modules are  
51 used, validation of the software module (module test) can be performed while the application

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

5  
6 The NRC staff determined this change is acceptable because all testing requirements for each  
7 level of test will continue to be met even though the test sequence can, in some cases, be  
8 changed to support application specific requirements.

9  
10 The risks associated with software testing are addressed through regression analysis. The STP  
11 states that *"regression analysis shall be performed to determine extent of retesting activities that*  
12 *may be necessary to re-verify and/or re-validate any changes to a tested element."* The results  
13 of this analysis are intended to identify latent design errors or programming bugs that have been  
14 introduced by software design modifications.

15  
16 The Common Q STP prescribes the scope, approach, resources, and schedule of the testing  
17 activities and it identifies the items and features to be tested. Testing tasks as well as the  
18 personnel responsible for each task are identified. The software test plan includes module  
19 testing, unit testing, integration testing, System Validation Testing and factory acceptance  
20 testing.

21  
22 Revision 5 of the SPM removes the requirement for test plans to contain all the requirements for  
23 all acceptance test procedures and to define each required test to be conducted. The reason  
24 for this change was provided by Westinghouse in response to RAI 12 (Refs. 15 and 16). This  
25 response states the following:

26  
27 The reason for the change in the SPM is due to the typical sequence and  
28 progression of a project. Requirements analysis, testing coverage and tracing of  
29 the requirements to test cases are significant testing activities. The Test Plan is  
30 needed to outline these activities. The test planning and initial engineering work  
31 occurs in parallel with the finalization of the design requirements and the  
32 implementation specifications. Therefore, the specific requirements to be tested  
33 are not available or issued in their final form when the test plan is written.

34  
35 The NRC staff determined this change to be acceptable because Westinghouse's processes will  
36 continue to establish traceability between system requirements and test procedures and/or test  
37 cases even if these are determined after the test plan is written. As such, the individual  
38 requirements for lower level acceptance test procedures and identification of individual, specific  
39 required tests to be conducted do not need to be included in the test plan itself at the  
40 requirements phase of development and can instead be established at a later stage of the  
41 development process.

42  
43 Site acceptance testing and installation testing are not covered under the Common Q STP  
44 because they are considered to be licensee actions and are to be addressed during the  
45 development of a Common Q based application. As such, a project specific test plan should be  
46 developed and used to address these aspects of software test planning. This is addressed in  
47 plant specific action item 5.

48  
49 The Common Q STP is understandable and it includes adequate provisions for retest in the  
50 event of failure of the original test. The Common Q Software Test Plan adequately addresses  
51 the test planning guidance of BTP 7-14, Section B.3.1.12, and based on WEC's commitment to



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

### 4 **3.2.13 Secure Development and Operating Environment (SDOE) Evaluation**

5  
6 The staff evaluated the Common Q platform requirements against RG 1.152. It contains five  
7 regulatory positions that describe methods acceptable to the staff for establishing a SDOE for  
8 digital safety systems. Each of these positions correlates to a phase of a typical software  
9 development life cycle. These regulatory positions support compliance with portions of 10  
10 CFR Part 50 – specifically Appendix A GDC 21 (Protection System Reliability and Testability),  
11 Appendix B Criterion III (Design Control) and IEEE Std. 603-1991 Clauses 5.6.3 (Independence  
12 from Interconnected Equipment) and 5.9 (Access Control).

13  
14 Section 12 of the Common Q Software Program Manual (Ref. 0) addresses the SDOE planning  
15 aspects of the Common Q platform from the Concepts Phase through the Test Phase of the  
16 software development life cycle per the guidance provided by RG 1.152.

17  
18 The lifecycle structure, for which criteria on development environment controls are to be  
19 established, consists of the following phases:

- 20
- 21 • Concept
- 22 • Requirements
- 23 • Design
- 24 • Implementation
- 25 • Test
- 26 • Installation, Checkout, and Acceptance Testing
- 27 • Operation
- 28 • Maintenance
- 29 • Retirement
- 30

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

35  
36 The operating software for the Common Q platform was developed prior to the issuance of  
37 RG 1.152. Thus the discussion of development activities is focused on those secure  
38 development environment considerations applied during the commercial grade dedication effort  
39 applicable to the life cycle processes for maintenance of the previously developed software.  
40 Although application software is not within the scope of this review, platform features that  
41 contribute to the SDOE for the application are identified and discussed. Credit may be taken for  
42 the use of these security capabilities in establishing a secure operational environment for a plant  
43 specific safety-related application.

44  
45 A security evaluation for the Common Q platform was not conducted by the NRC when the  
46 Common Q platform SE (Ref. 2) was performed because the applicable regulatory guidance  
47 was not available at the time of that safety evaluation. Nonetheless, the security measures  
48 discussed below were in place during the Common Q platform development.

49

## 1 3.2.13.1 Concepts Phase (2.1)

2 ~~System Security~~Secure Operational Environment Capabilities

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

- 14
- 15 • *Confidentiality Vulnerability - the inadvertent loss of information related to the security of*  
 16 *a system and related development systems.*
- 17
- 18 • *Integrity Vulnerability - the inadvertent change to a system and related development*  
 19 *system design requirements that could adversely affect security*
- 20

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

## 28

29 ~~Identification of General~~ Life Cycle Vulnerabilities

30

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

37

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

42

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

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

#### 4 Remote Access and One-Way Communication

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

23  
24 The staff finds that the Common Q SDOE plan adequately addresses the criteria of position  
25 C.2.2.1 of RG 1.152.

#### 26 27 3.2.13.2 Requirements Phase (2.2)

##### 28 29 System Features (2.2.1)

30  
31 Security functional performance requirements are implemented to address vulnerabilities  
32 identified in the concept phase for the Common Q system. All such requirements are subject to  
33 independent verification and validation as part of the overall IVV process.

34  
35 NRC staff finds that the requirements pertaining to the security functions, system configuration,  
36 external interfaces, qualification, human factors, data definitions, and documentation for  
37 hardware and software have been properly established and are therefore acceptable.

38  
39 The Common Q SPM has provisions for a security assessment to be performed during the  
40 **requirements-concept** phase. The results of the security assessment are security related design  
41 features. Security related design features are implemented into the system requirements  
42 specifications. The Common Q SVVP states that the IVV team evaluates the software design  
43 and test documentation, which includes the system requirements specification. As such, the  
44 system requirements specification which includes security related design features is evaluated  
45 by the IVV team.

46  
47 NRC staff finds that the verification process used for security related design features provides  
48 an adequate means of ensuring the correctness, completeness, accuracy, testability, and  
49 consistency of the system's security features and is therefore acceptable.

50

1 Previously Developed Common Q software

2

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

17

18 Development Activities (2.2.2)

19

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

26

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

31

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

43

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

50

1 3.2.13.3 Design Phase (2.3)

2

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

9

10 Verification

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

18

19 Access Controls

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

25

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

30

31 Software Configuration Management

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

34

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

41

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

49

## 1 Development Activities (2.3.2)

2

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

8

## 9 3.2.13.4 Implementation Phase (2.4)

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

18

## 19 System Features (2.4.1)

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

25

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

35

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

39

## 40 Development Activities for the Implementation Phase (2.4.2)

41

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

47

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

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

3

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

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

9

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

12

#### 13 3.2.13.5 Test Phase (2.5)

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

#### 21 System Features (2.5.1)

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

28

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

34

#### 35 Development Activities (2.5.2)

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

41

## 42 4.0 SUMMARY OF REGULATORY COMPLIANCE EVALUATIONS

43 On the basis of the foregoing review of the Common Q software development process for  
44 application software, the staff concludes that the SPM specifies plans that will provide a quality  
45 software life cycle process, and that these plans commit to documentation of life cycle activities  
46 that will permit the staff or others to evaluate the quality of the design features upon which the  
47 safety determination will be based. A review of the implementation of the life cycle process and

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

4  
5 On the basis of the review of WEC's software development process for application software, the  
6 staff concludes that the Common Q application development procedures will provide a quality  
7 software life cycle process, and that these plans commit to documentation of life cycle activities  
8 that will permit the staff or others to evaluate the quality of the design features upon which the  
9 safety determination will be based. The staff, therefore, concludes that the software program  
10 manual as applied to Common Q safety systems meets the guidance of RG 1.152 and that the  
11 special characteristics of computer systems have been adequately addressed. Based on its  
12 review, the staff finds, therefore, that the Common Q safety system software development  
13 processes when properly implemented are capable of producing software that will satisfy the  
14 requirements of GDC 1 and 21.

15  
16 Cyber security to address malicious events is addressed under the purview of 10 CFR 73.54,  
17 "Protection of Digital Computer and Communication Systems and Networks," and thus has not  
18 been evaluated as part of this SPM review. Conformance to 10 CFR 73.54 is the responsibility  
19 of COL applicants or licensees who choose to reference the SPM.

#### 20 21 4.1 Common Q SPM Generic Change Process

22  
23 Per letter dated August 12, 2010 (Reference 6), WEC submitted WCAP-17266, "Common Q  
24 Platform Generic Change Process, (Reference 7) for NRC review and approval.

25  
26 The Common Q generic change process defined by WCAP-17266 describes methods used by  
27 WEC to screen, and evaluate proposed changes to Common Q components, software or  
28 processes defined within the Common Q Platform and Software Program Manual topical reports  
29 subsequent to NRC review and approval. The scope of this process includes changes that are  
30 made to the Common Q SPM subsequent to the issuance of this SE. This process defines  
31 criteria to be used for the determination of whether the safety conclusions of the NRC safety  
32 evaluation remain valid following the proposed change or if the changes will require submittal to  
33 the NRC for evaluation and approval prior to implementation.

34  
35 The staff has reviewed this document and acknowledges the benefits provided by  
36 implementation of a formal topical report screening, evaluation, and change process however,  
37 the NRC is unable to perform a safety evaluation of the processes defined by this document or  
38 make any safety conclusions regarding these processes at this time. This document is included  
39 as a reference within this safety evaluation in order to provide future reviewers of Common Q  
40 applications that reference this SE with information on how WEC evaluates and documents  
41 changes to the Common Q SPM. It is also beneficial for reviewers of Common Q applications  
42 to have access to the WEC generic change process in order to interpret the information  
43 provided in the Record of Changes document discussed below.

#### 44 45 4.2 Common Q Record of Changes Document

46  
47 Per letter dated August 25, 2010 (Reference 8), WEC submitted WCAP-16097, "Common  
48 Qualified Platform Record of Changes, "(Reference 9) for NRC review and approval.

49  
50 The staff reviewed the Common Q Record of Changes (ROC) and confirmed that the changes  
51 to the Common Q SPM are consistent with the revised topical report evaluated by this SE.



1 Furthermore, the staff reviewed the information provided in the Tables within the ROC and  
2 determined that these tables provide valuable information that should be used during application  
3 specific reviews to determine acceptability of changes to the Common Q SPM subsequent to  
4 the NRC review and approval of this License Topical Report (LTR). Plant-Specific action item 6  
5 is therefore being included in this SE to provide direction for plant specific safety evaluations to  
6 include a review of the current Common Q record of changes to assess the validity of previously  
7 derived safety conclusions in light of the changes made to the Common Q SPM.  
8

## 9 **5.0 PLANT SPECIFIC ACTION ITEMS**

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

18 The following plant-specific actions must be performed by an applicant when requesting NRC  
19 approval for installation of a safety-related system based on the Common Q platform.  
20

- 21 1. As noted in Sections 3.2.1 and 3.2.3, WEC may choose to use alternatives to the SPM  
22 defined processes when performing Initiation phase activities for individual projects.  
23 These alternatives are required to be documented in the Project Quality Plan (PQP).  
24 This PQP should be reviewed to determine if alternatives to the SPM are being used for  
25 development of project specific software. When such alternatives are being used, the  
26 PQP should be evaluated to determine if the justifications for the use of alternatives to  
27 the SPM processes are acceptable.  
28
- 29 2. The Common Q SPM only includes the Software Life Cycle Process Planning  
30 Documentation as outlined in SRP BTP 7-14, Section B.2.1. As such, the plant-specific  
31 documentation outlined in SRP BTP 7-14, Sections B.2.2, "Software Life Cycle Process  
32 Implementation," and B.2.3, "Software Life Cycle Process Design Outputs," is to be  
33 evaluated separately for any application that references the Common Q SPM.  
34
- 35 3. The Common Q SPM only addresses the vendor software planning processes for a  
36 Common Q-based system. For all activities in which the applicant or licensee assumes  
37 responsibility within a given project (including vendor oversight) for quality assurance,  
38 additional evaluations, audits or inspections must be performed to ensure that these  
39 licensee responsibilities are fulfilled.  
40
- 41 4. Because the Common Q SPM does not address the criteria of BTP 7-14 Section  
42 B.3.1.8.4, "Software Operations Plan," an evaluation of compliance must be performed  
43 at the time of system development when the operational aspects of the system have  
44 been defined.  
45
- 46 5. Site acceptance testing and installation testing are not covered under the Common Q  
47 Software Test Plan because they are considered to be licensee actions that are to be  
48 addressed during the development of a Common Q based application. As such, a  
49 project specific, site acceptance and installation test plan should be developed and used

1 to address these aspects of software test planning. Because the Common Q SPM does  
2 not address all aspects of the BTP 7-14 Section B.3.2.4 criteria, an evaluation of  
3 compliance must be performed at the time of system development when the site and  
4 installation testing activities have been defined.

- 5  
6 6. A licensee implementing an application based upon the Common Q platform should  
7 perform a review of the current Common Q Record of Changes document to assess the  
8 validity of previously derived safety conclusions if changes have been made to the  
9 Common Q SPM.
- 10  
11 7. Secure Development and Operational Environment – An applicant or licensee  
12 referencing the Common Q SPM for a safety-related plant specific application should  
13 ensure that a secure development and operational environment has been established for  
14 its plant specific application, and that it satisfies the applicable regulatory evaluation  
15 criteria of RG 1.152, Revision 3.

## 16 17 **6.0 REFERENCES**

- 18  
19 1. WCAP-16097-P-A, Revision 3, "Common Qualified Platform Topical Report"  
20 (Proprietary/Non-Proprietary), February 28, 2013, Agencywide Documents Access and  
21 Management System (ADAMS) Accession No. ML13112A110/ML13112A108.
- 22  
23 2. Common Qualified Platform Topical Report WCAP-16097-P and 16097-NP Revision 3,  
24 June 30, 2012, ADAMS Accession Nos. ML12207A512 and ML12207A510.
- 25  
26 3. Submittal of WCAP-16096-P and WCAP-16096-NP, Revision 4, "Software Program  
27 Manual for Common Qualified Platform," (Proprietary/Non-Proprietary) for Review and  
28 Approval, July 17, 2012, ADAMS Accession No. ML12205A051.
- 29  
30 4. Software Program Manual for Common Q Systems, Revision 4 WCAP-16096-P and  
31 16096-NP Revision 4, June 30, 2012, ADAMS Accession Nos. ML12205A053 and  
32 ML12205A052.
- 33  
34 5. WNA-DS-01070-GEN, Revision 6, "Application Restrictions for Generic Common Q  
35 Qualification," December 31, 2011, ADAMS Accession Nos. ML11364A030 and  
36 ML11364A029.
- 37  
38 6. Transmittal Letter for WCAP-17266-P/NP "Common Q Platform Generic Change  
39 Process," Revision 0, August 12, 2010, ADAMS Accession No. ML102290175.
- 40  
41 7. Common Q Platform Generic Change Process (WCAP-17266-P/NP), Revision 0,  
42 August 31, 2010, ADAMS Accession Nos. ML102290177 and ML102290176.
- 43  
44 8. Transmittal Letter for WCAP-16097-P/NP "Common Qualified Platform Record of  
45 Changes", Revision 1, April 19, 2012, ADAMS Accession No. ML12115A213.
- 46  
47 9. Common Qualified Platform Record of Changes (WCAP-16097-P/NP), Revision 1,  
48 March 31, 2012, ADAMS Accession Nos. ML12115A215 and ML12115A214.
- 49  
50 10. Software Program Manual for Common Q Systems (WCAP-16096-NP-A) Revision 1,  
51 January 29, 2004, ADAMS Accession No. ML040360115.

- 1  
2 11. Safety Evaluation for Topical Report WCAP-16096-NP-A "Software Program Manual for  
3 Common Q Systems," Revision 1, September 28, 2004, ADAMS Accession  
4 No. ML042730580.  
5  
6 12. Request for Additional Information, License Topical Report (WCAP-160096) "Software  
7 Program Manual for Common Q Systems," September 29, 2011, ADAMS Accession  
8 No. ML112490485.  
9  
10 13. Response to NRC Request for Additional Information on WCAP-16096, Revision 2  
11 "Software Program Manual for Common Q Systems," January 31, 2012, ADAMS  
12 Accession No. ML12034A212.  
13  
14 14. Submittal of WCAP-16096-P/WCAP-16096-NP, Revision 5, "Software Program Manual  
15 for Common Q™ Systems" (Proprietary/Non-Proprietary), August 28, 2017, ADAMS  
16 Accession No. ML17241A112.  
17 15. Request for Additional Information, License Topical Report (WCAP-160096) "Software  
18 Program Manual for Common Q Systems," February 26, 2018, ADAMS Accession  
19 No. ML118018A005.  
20  
21 16. Response to NRC Request for Additional Information on WCAP-16096, Revision 5  
22 "Software Program Manual for Common Q Systems," May 31, 2018, ADAMS Accession  
23 No. ML18156A479.  
24  
25 17. Safety Evaluation for Topical Report WCAP-16096-P(NP)-A "Software Program Manual  
26 for Common Q Systems," Revision 4, February 28, 2013, ADAMS Accession  
27 Nos. ML13081A046 and ML13081A047.  
28

## 29 7.0 LIST OF ABBREVIATIONS

31	ABB	Asea Brown Boveri
32	AC160	Advant Controller 160
33	<del>ACC</del>	<del>AMPL Control Configuration</del>
34	AF100	Advant Fieldbus 100
35	AISC	Application Specific Integrated Circuit
36	ALWR	Advanced Light Water Reactor
37	<del>AMPL</del>	<del>ABB Master Programming Language</del>
38	API	Application Programming Interface
39	ASME	American Society of Mechanical Engineers
40	ATWS	Anticipated Transients Without Scram
41	BIOB	Backplane I/O Bus
42	BTP	Branch Technical Position
43	CE	Combustion Engineering
44	CENP	Combustion Engineering Nuclear Power
45	CEA	Control Element Assembly
46	CEAC	Control Element Assembly Calculator
47	CEAPD	CEA Position Display
48	CENP	CE Nuclear Power (Westinghouse)
49	CEO	Cognizant Engineering Organization
50	CETMS	Core Exit Thermocouple Monitoring System
51	CGD	Commercial-Grade Dedication

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

- 40 -

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	DPSS	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	HSHSI	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

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

- 41 -

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	<del>QSSL</del>	<del>QNX Software Systems Limited</del>
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

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

- 42 -

1	STS	Standard Technical Specifications
2	SVVP	Software Verification and Validation Plan
3	SW	Software
4	SWC	Surge Withstand Capability
5	TCB	Task Control Block
6	TMI	Three Mile Island
7	TS	Technical Specification(s)
8	TSTF	Technical Specification Task Force
9	V&V	Verification and Validation
10	WWDT	Window Watchdog Timer

11

12 Advant<sup>®</sup> is a registered trademark of ABB Process Automation Corporation.

13 ~~QNX<sup>®</sup> and Photon<sup>®</sup> are registered trademarks of QNX Software Systems GmbH & Co. KG~~  
14 ~~("QSSKG", formerly "QSSL") and are used under license by QSS.~~

15 Unix<sup>®</sup> is a registered trademark of The Open Group in the US and other countries.

16 Windows<sup>®</sup> is a registered trademark of Microsoft group of companies.

17

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

- 2 -

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).	

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

- 3 -

Comment Number	Comment Location	Comment Type	Comment	NRC Response
4	Page 12/Lines 24 – 26	Clarification	<p>The SER states that the “SQAP no longer applies to software classified as: important to availability or general purpose software.”</p> <p>However, this is not consistent with the text in the SQAP, Section 4.1.2, “Scope,” which states:</p> <p>“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.”</p> <p>Therefore, WEC suggests reverting to the wording from the previous revision of the SER:</p> <p>“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.”</p>	
5	Page 15/Line 29	Editorial	“Reference 0” should be “Reference 16”	



**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

- 4 -

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).	

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

- 5 -

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.	

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

- 6 -

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.	

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

- 7 -

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.	

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

**OFFICIAL USE ONLY – PROPRIETARY INFORMATION**

- 8 -

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 -----