February 26, 2018

Mr. James A. Gresham, Manager
Regulatory Compliance
Westinghouse Electric Company
1000 Westinghouse Drive
Building 3 Suite 310
Cranberry Township, PA 16066

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION FOR "WCAP-16096-P/NP, REVISION 5, 'SOFTWARE PROGRAM MANUAL FOR COMMON Q™ SYSTEMS'" (CAC NO. MG0220, EPID: L-2018-TOP-0001)

Dear Mr. Gresham:

By letter dated August 28, 2017 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML17241A112), Westinghouse Electric Company (Westinghouse) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review Topical Report (TR) "WCAP-16096-P/NP, Revision 5, 'Software Program Manual for Common Q™ Systems.'" Upon review of the information provided, the NRC staff has determined that additional information is needed to complete the review. The request for additional information (RAI) questions are provided in the enclosure to this letter.

In an email exchange between Mr. Warren Odess-Gillett representing Westinghouse and me, we agreed that the NRC staff will receive your response to the enclosed RAI questions by May 31, 2018.

If you have any questions regarding the enclosed RAI questions, please contact me at 301-415-7297 or via electronic mail at Joseph.Holonich@nrc.gov.

Sincerely,

***/RA/***

Joseph J. Holonich, Senior Project Manager
Licensing Processes Branch
Division of Licensing Projects
Office of Nuclear Reactor Regulation

Docket No. 99902038

Enclosure:
RAI questions

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION FOR "WCAP-16096-P/NP, REVISION 5, 'SOFTWARE PROGRAM MANUAL FOR COMMON Q™ SYSTEMS'" (CAC NO. MG0220, EPID: L-2018-TOP-0001) DATED: FEBRUARY 26, 2018

DISTRIBUTION:

| | | |
|---|---|---|
| PUBLIC | RidsNrrDlp | IJung, NRO |
| RidsACRS_MailCTR | RidsResOd | WRoggenbrodt, NRO |
| RidsNrrLADHarrison | RidsNroOd | RidsNrrDe |
| RidsOgcMailCenter | RidsNrrDlr | JHolonich, NRR |
| RidsNrrDlpPlpb | MWaters, NRR | DMorey, NRR |
| RidsNrrDeEicb | RStattel, NRR | PLPB r/f |

**ADAMS Accession No.: ML18018A005; *concurred via e-mail** **NRR-106**

| | | | |
|---|---|---|---|
| **OFFICE** | NRR/DLP/PLPB/PM | NRR/DLP/PLPB/LA* | NRR/DE/EICB* |
| **NAME** | JHolonich | DHarrison | MWaters |
| **DATE** | 2/1/2018 | 2/22/2018 | 2/23/2018 |
| **OFFICE** | NRR/DLP/PLPB/BC | NRR/DLP/PLPB/PM | |
| **NAME** | DMorey | JHolonich | |
| **DATE** | 2/26/2018 | 2/26/2018 | |

**OFFICIAL RECORD COPY**

**REQUEST FOR ADDITIONAL INFORMATION**

**WCAP-16096-P, "SOFTWARE PROGRAM MANUAL FOR COMMON Q SYSTEMS"**

**1. Compliance with Institute of Electrical and Electronics Engineers Standard 1012**

Title 10, "Energy" of the *Code of Federal Regulations* (CFR) Part 50 requires in Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," in part in Criterion II, "Quality Assurance Program," that, "The [quality assurance] program shall take into account the need for special controls, processes, test equipment, tools, and skills to attain the required quality, and the need for verification of quality by inspection and test." Additionally, in Criterion III, "Design Control," it requires, in part, that, "These measures shall include provisions to assure that appropriate quality standards are specified and included in design documents and that deviations from such standards are controlled…." The design control measures shall provide for verifying or checking the adequacy of design, such as by the performance of design reviews, by the use of alternate or simplified calculation methods, or by the performance of a suitable testing program.

The staff endorsed a method found to be acceptable when performing the verification and validation (V&V) activities associated with the development of a safety-related software based system via Revision 2 of Regulatory Guide (RG) 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." In the RG, it endorses the Institute of Electrical and Electronic Engineers (IEEE) Standard (Std.) 1012-2004, "IEEE Standard for Software Verification and Validation."

Previous versions of WCAP-16096-P, "Software Program Manual for Common Q Systems" (SPM), up to and including Revision 4, stated that its Software Verification and Validation (SVV) Plan (SVVP) complied with the IEEE Std. 1012, "IEEE Standard for Software Verification and Validation," whether the 1986 or 1998 version – dependent upon the revision of the SPM. This compliance statement was used as a partial basis for the acceptability of the SPM in the original and subsequent safety evaluations (SEs) related to the method of software system development described in the SPM. In Revision 5 of the SPM, the compliance statement to IEEE Std. 1012-2004 has been removed.

The changes made in Revision 5 of the SPM appear to indicate that the SVVP will no longer be required to comply with IEEE Std. 1012-2004. As highlighted in the examples below, please clarify and provide additional information on the revised approach to developing application level software for the Common Q System without compliance to IEEE Std. 1012-2004, along with the basis and justification.

If the SPM intends to take exception to the requirements of IEEE Std. 1012 for V&V activities, then please provide sufficient justification (inputs, tasks/activities, and outputs)

at a similar level of decomposition and granularity within IEEE Std. 1012 to demonstrate an alternative approach that complies with 10 CFR Part 50, Appendix B. In addition, clarify if the SPM is taking exception to compliance with IEEE Std. 7-4.3.2 and, if so, provide similar justification.

a. Section 3.3.9, "Software Verification and Validation Activities" – Reference 8, [IEEE Std. 1012 – 2004], is no longer included in the compliance statement. Please clarify if the V&V activities in this area are taking exception to this standard or taking a different approach for meeting the requirements of 10 CFR Part 50, Appendix B.

b. Section 5.1, "Purpose," of the SVVP – the IEEE Std. 1012 compliance statement has been removed. Beginning in Revision 3 of the SPM, along with the information contained in Exhibit 5.8, "IEEE Standard 1012-1998 Compliance Table" [IEEE Std. 1012-2004 version for Revision 5 of the SPM], that explained where in the SPM the related sections of IEEE Std. 1012 could be located, the staff relied on the more detailed information within IEEE Std. 1012 describing exactly what and how Independent Verification and Validation (IV&V) inputs, tasks/activities, and outputs would be conducted. Please provide a list of what SVV activities and tasks will no longer be conducted as described in Table 1 – "V&V Tasks, Inputs and Outputs" of IEEE Std. 1012 and justification for why the given tasks, inputs, and outputs are no longer required.

c. Table 5.9-1 identifies both 'Important to Availability' and 'General Purpose' software as being, 'IEEE Std. 1012 Not Applicable.' The NRC staff previously determined these classifications to be compliant with IEEE Std. 1012 because V&V tasks for these classifications were defined in Exhibit 5-8. Since there has been no corresponding change to remove 'Important to Availability' or 'General Purpose' software classifications from Exhibit 5-8, please provide a list of what V&V activities that are no longer considered to be compliant with IEEE 1012 and the reasoning behind such changes.

d. Section 10.5, "Software Verification and Validation Documentation" - The IEEE Std. 1012 compliance statement has been removed from this section and replaced by a reference to Section 5.6, "Software Verification and Validation Reporting," of the SPM. Section 5.6 does not contain an IEEE Std. 1012 compliance statement. Please clarify what V&V activities in this area are taking exception to the standard or taking a different approach for meeting the requirements of 10 CFR Part 50, Appendix B.

e. IEEE 7-4.3.2 2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," states, in part, "…the software V&V effort shall be performed in accordance with IEEE Std. 1012." Since, in Section 3.3.9, "Software Verification and Validation Activities," the SPM states that "These activities conform to the requirements in Reference 11," which is IEEE Std. 7-4.3.2. IEEE Std. 7-4.3.2 also requires compliance with IEEE Std. 1012. Please clarify if V&V activities in this area are taking exception to this standard or taking a different approach for meeting the requirements of 10 CFR Part 50, Appendix B.

**2. Compliance with IEEE Standard 829 Requirements**

The regulation at 10 CFR Part 50, Appendix B requires, in part, that, "The [quality assurance] program shall take into account the need for special controls, processes, test equipment, tools, and skills to attain the required quality, and the need for verification of quality by inspection and test." Additionally, in Criterion III, "Design Control," it requires,

in part, that, “These measures shall include provisions to assure that appropriate quality standards are specified and included in design documents and that deviations from such standards are controlled….” The design control measures shall provide for verifying or checking the adequacy of design, such as by the performance of design reviews, by the use of alternate or simplified calculation methods, or by the performance of a suitable testing program.

The staff endorsed a method found to be acceptable when performing the testing and documenting the test activities associated with the development of a safety-related software based system via Revision 1 of RG 1.170, “Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants.” In the RG, it endorses the IEEE Std. 829-2008, “IEEE Standard for Software and System Test Documentation.”

Previous versions of the SPM, including Revision 4, stated that the SVVP complied with IEEE Std. 829. As highlighted in the examples below, which describe how the test plans, procedures, test summary reports, and other SVV test documentation will be managed, it appears to indicate that testing documentation will no longer be required to comply with IEEE Std. 829-2008 [or in some cases in content, but not necessarily in format]. For each example below, please clarify if documentation activities in this area are taking exception to this standard or taking a different approach for meeting the requirements of 10 CFR Part 50, Appendix B.

If the SPM intends to take exception to some or all of the requirements of IEEE Std. 829, then please provide sufficient justification (inputs, tasks/activities, and outputs) at a similar level of decomposition and granularity within IEEE Std. 829 to demonstrate how an alternative approach complies with the requirements of 10 CFR Part 50, Appendix B.

a. Section 4.3.2.2, “Software Requirements Phase,” of Revision 5 of the SPM states, in part, “A Common Q [Qualification] specific test plan shall start to be developed to identify how the test activities will be implemented. Reference 14 [IEEE Std. 829-2008], Section 8 will be used as guidance in developing the test plan.” However, in Revision 4 of the SPM the Common Q specific test plan shall start to be developed in accordance with the content, but not the format of Reference 14 [IEEE Std. 829-1998], Section 7, “Test Procedure Specification,” and Section 11, “Test Summary Report,” respectively.

b. Section 4.5.2.2, “Software Testing Standards,” of Revision 5 of the SPM states, in part, “Specific format and content for test procedures and test reports shall also be provided in the Test Plan and shall comply with Section 5.8 [of the SPM].” In Revision 4 of the SPM, it states, in part, “Specific format and content for test procedures and test reports shall also be provided in the Test Plan and shall comply with Reference 14 [IEEE Std. 829-1998] Sections 7 and 11 [‘Test Procedure Specification’ and ‘Test Summary Report’ respectively].” However, in Revision 5 of the SPM, Section 5.8 does not contain an IEEE Std. 829 compliance statement.

c. Section 5.4.5.2 “IV&V Core Activities,” Item 3 and Item 4 replace compliance commitment to documentation requirements of IEEE Std. 829-2008, with a reference to Section 5.8 of the SPM. However, in Revision 5 of the SPM, Section 5.8 does not contain an IEEE Std. 829 compliance statement.

d. Section 5.5.3.2, "[Requirements Phase] IV&V Tasks," V&V Task 10 (Task 9 in Revision 4 of the SPM) replaces the compliance commitment to test plan development requirements of IEEE Std. 829 with a reference to Section 4.3.2.2 of the SPM. In Revision 5 of the SPM, Section 4.3.2.2 no longer contains an IEEE Std. 829 compliance statement. Instead it replaced the previous compliance statement in Revision 4 of the SPM with a statement that IEEE Std. 829 will be used as guidance in developing the test plan.

e. Section 5.5.4.2, "[Design Phase] IV&V Tasks," Item 9 replaces the compliance commitment to test procedure development requirements of IEEE Std. 829 with a reference to Section 5.8 of the SPM. However, in Revision 5 of the SPM, Section 5.8 does not contain an IEEE Std. 829 compliance statement.

f. Section 9.3.2.2, "Detailed Analysis," replaces the compliance content commitment to test plan requirements of IEEE Std. 829 with a reference to Section 4.3.2.2 of the SPM. When compared to Revision 4 of the SPM, Section 4.3.2.2 no longer contains an IEEE Std. 829 compliance statement. Instead it replaced the previous compliance statement with a statement that IEEE Std. 829 will be used as guidance in developing the test plan.

g. Section 9.4.2, "Design Process," replaces the compliance commitment to test procedure development requirements of IEEE Std. 829 with a reference to Section 5.8 of the SPM. However, when compared to Revision 4 of the SPM, Section 5.8 does not contain an IEEE Std. 829 compliance statement.

h. Section 9.6.2, "Test Process," replaces the compliance commitment to test procedure development requirements of IEEE Std. 829 with a reference to Section 5.8 of the SPM. However, when compared to Revision 4 of the SPM, Section 5.8 does not contain an IEEE Std. 829 compliance statement.

3. **Preparation of Site Test Plan**

In Revision 5 to the SPM, Section 4.3.2.6 includes a change to the process for development of a site test plan which allows development of such a plan to occur at a later stage of the development lifecycle to support evaluation of requirement testability on-site. There does not appear to be a corresponding change to the V&V activities associated with this issue.

In Revision 4 to the SPM, the preparation of a site test plan occurred during the requirements phase, which is consistent with the requirements of IEEE Std. 1012. This was reflected in Exhibit 5-8 as an item titled "Acceptance V&V Test Plan Generation" and this test plan covered acceptance, integration, system, and component levels. The staff needs to understand where this site testing activity now fits in relation to the V&V activities in the "IEEE Standard 1012 – 2004 Compliance Table" (Exhibit 5-8) now that an allowance for Site Acceptance Test Plan development at a later stage is described. Please provide additional information to identify the specific V&V activity requirement for development of the Site Acceptance Test Plan. Provide a discussion of when the required activity is to be performed in relation to the development lifecycle, and why doing so at that particular phase of system development is acceptable.

4. **Testing Sequence** - Section 7.2.4 of the SPM now includes provisions for deferring completion of test activities to allow commencement of the subsequent tests before the

preceding test level is complete. Please provide additional information to explain why these new provisions for the testing sequence are being made and provide justification for allowing testing levels to proceed in a sequence other than previously prescribed.

5. **Deferral of Factory Acceptance Test Activities to Site**

Section 7.3.1.5, "Factory Acceptance Test (FAT)," of the revised SPM now allows for deferral of FAT activities to be conducted at the site following installation. Considering the stated objective of the FAT as demonstrating that the complete system is integrated and functional, it is unclear how these objectives will be achieved prior to shipment of equipment to the site when FAT activities are deferred. Please provide additional information describing how FAT objectives will be achieved when FAT activities are deferred to the site. Include a discussion of required reasoning/justification for deferring FAT activities and criteria which must be satisfied before FAT activity deferral can be performed and the post FAT activities that would have to be accomplished on site (versus the factory).

6. **Integration Test Items**

The following Integration Test Items listed in Section 7.3.1.3, "Integration Test," have been removed from the SPM in Revision 5:

- Error Handling
- Communications
- Redundancy
- Diversity

Since the SPM no longer lists test items for integration, it is unclear to the NRC how the stated objectives for integration testing can be achieved. The NRC staff needs to understand why these test items were removed and how the objectives of integration testing will continue to be achieved in absence of these test items. Please provide additional information explaining removal of integration test items as well as justification for no longer performing these test activities as a part of integration testing.

7. **Performance of FAT on Deliverable System**

SPM Section 7.3.1.5, "Factory Acceptance Test (FAT)," includes a description of the FAT which states that the FAT is to be executed on a deliverable system. The reworded description of FAT however seems to imply that some portion of the FAT may now be performed on a non-deliverable or surrogate system as follows:

*FAT includes tests that are performed for each deliverable system.*

Please confirm that FAT will not include tests that are performed on non-deliverable or surrogate equipment or provide a description and justification for crediting FATs performed on surrogate equipment to apply to deliverable systems.

8. **Surrogate System Testing**

The revised test strategy outlined in the SPM includes provisions for using a test bed, proxy, or surrogate system in lieu of actual production equipment to be delivered to the site for performance of Integration and System Validation Tests. SPM, Section 7.3.1.5, "Factory Acceptance Test (FAT)," includes a description of the FAT which states that the FAT is to be executed on a deliverable system (i.e., not a surrogate system). However, Section 7.3.1.5 also states that System Validation Tests, which can be credited to fulfill the role of FAT, may be performed on surrogate equipment. These statements appear to contradict the purpose of the System Validation Test or the FAT and the conditions under which the testing is to be conducted (actual deliverable system versus surrogate system). Please clarify these statements and justify what specific conditions are appropriate to test a surrogate system, for either the FAT or System Validation Test rather than the production-based system.

Please provide additional information on the process for crediting system validation tests to meet FAT objectives. The NRC staff needs to understand any limitations or conditions for crediting System Validation Tests to meet FAT requirements before a safety determination can be made for this change.

9. **Time Response Testing**

The Table in Exhibit 7-1, "Comparison of System Validation Test and FAT," includes a Test Item of "Performance" with a "Design Aspect" of "Time Response Testing." The corresponding System Validation Test and FAT items to demonstrate compliance refer to tests using representative functions and representative samples of tests instead of actual safety functions performed on production equipment. Please justify the use of representative tests and representative functions to assure compliance with time response requirements in lieu of testing actual functions using production equipment and the basis for doing so.

10. **Archival Requirements - Section 4.11.2, "Archival Requirements"**

In Revision 4 of the SPM, the archival requirements are the responsibility of the software librarian and should be performed in accordance with Reference 4 (Westinghouse Level II Policies and Procedures). In Revision 5 of the SPM, the commitment is changed to, in part, "the requirements of this section 'can be' performed by the software librarian." Provide additional detail explaining what individual or group of individuals, by position, is (are) specifically responsible for completion of archival requirements associated with the development, control, storage, and distribution of all project software deliverable physical media.

11. **Independent Verification and Validation Organization – Section 2, "Organization"**

In Revision 4 of the SPM it was not permitted for IV&V team members to participate on the design team. In Revision 5 of the SPM, the requirement was relaxed such that only IV&V 'engineers' are not allowed to participate on design activities. Provide additional information related to the type of design activities and justification why some IV&V team members (i.e., not IV&V engineers) would be allowed to participate in design activities.

12. **Test Plans**

Section 3.3.5.7.1, “Test Plans,” of Revision 5 of the SPM describes that the test plan will contain the method for defining requirements to be tested and the method for establishing the acceptance criteria and how it will be documented. In Revision 4 of the SPM, the text stated, in part, “They [the test plans] shall contain all the requirements for all acceptance test procedures and define each required test to be conducted.” Please provide additional information explaining why it is acceptable to provide only a method for defining requirements and acceptance criteria rather than defining the actual test requirements and acceptance criteria as was previously required by the SPM and consistent with the definition and content of a “test plan” in accordance with IEEE Std. 829.

13. **Software V&V Plan Review**

Section 4.6.2.4, “Software Verification and Validation Plan Review,” of Revision 5 of the SPM states, in part, “The SVVP (Section 5) *has been* reviewed for adequacy and completeness of the verification and validation methods for Common Q.” In Revision 4 of the SPM it states, in part, that, “The SVVP *is* reviewed for adequacy and completeness of the verification and validation methods for Common Q.” Why is it acceptable for the SVVP to no longer be reviewed for a new or ongoing project as part of the Westinghouse Global Management System Quality Procedures, the descendant of Reference 4 in Revision 4 of the SPM?