Westinghouse Electric Company
1000 Westinghouse Drive
Cranberry Township, Pennsylvania 16066
USA

U.S. Nuclear Regulatory Commission
Document Control Desk
11555 Rockville Pike
Rockville, MD 20852

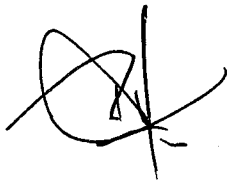
Direct tel: (412) 374-5130
Direct fax: (724) 940-8542
e-mail: hosackkl@westinghouse.com

LTR-NRC-18-36

May 31, 2018

Subject: Responses to NRC Request for Additional Information for Westinghouse Topical Report WCAP-16096-P/WCAP-16096-NP, Revision 5, "Software Program Manual for Common Q™ Systems" (Docket No.: 99902038; EPID: L-2017-TOP-0059)

Enclosed is a copy of the Responses to NRC Request for Additional Information for Westinghouse Topical Report WCAP-16096-P/WCAP-16096 NP, Revision 5, "Software Program Manual for Common Q™ Systems". This submittal contains responses for the thirteen RAIs transmitted via NRC letter to James A. Gresham (Westinghouse) dated February 26, 2018 (ML18018A005). All content in the Responses is non-proprietary, and as such, only a non-proprietary version is provided.



Korey L. Hosack, Manager
I&C Licensing & Regulatory Support

Enclosures

cc: Joseph Holonich
Dennis Morey

Responses to NRC Responses to NRC Request for Additional Information for Westinghouse Topical Report WCAP-16096-P/WCAP-16096 NP, Revision 5, "Software Program Manual for Common Q™ Systems"

(Non-Proprietary)

May 2018

Westinghouse Electric Company
1000 Westinghouse Drive
Cranberry Township, PA 16066

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.

Westinghouse Response:
Westinghouse does not intend to take exception to the requirements for V&V activities in IEEE Std. 1012-2004. The SPM complies with IEEE Std. 1012-2004 requirements for V&V activities as documented in Exhibit 5-8 of the SPM. Therefore, Westinghouse will update the SPM throughout to indicate that it complies with the requirements for V&V activities in IEEE Std. 1012-2004. Accordingly, Westinghouse does not intend to take exception to IEEE Std. 7-4.3.2-2003.

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.

Westinghouse Response:
The SPM complies with IEEE Std. 1012-2004 requirements for V&V activities as documented in Exhibit 5-8 of the SPM. Therefore, Section 3.3.9, "Software Verification and Validation Activities," will be revised to say (as originally stated in Revision 4):
"These activities conform to the requirements in References 8 and 11."

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.

Westinghouse Response:
The SPM complies with IEEE Std. 1012-2004 requirements for V&V activities as documented in Exhibit 5-8 of the SPM. Therefore, Section 5.1, "Purpose," will be revised to say:

"This section explains requirements for the IV&V processes starting with the system design document stage and all necessary IV&V activities to verify and/or validate I&C systems. This SVVP complies with Reference 8 requirements for V&V activities."

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.

Westinghouse Response:
As allowed by IEEE Std. 1012-2004, software classified as SIL 1 and SIL 2 can follow a subset of the V&V activities required for SIL 4 software. Common Q Software classified as General Purpose maps to SIL 1, while software classified as Important to Availability maps

to SIL 2. Exhibit 5-1 provides a listing of the V&V activities that will be performed for ITA and General Purpose software. Therefore, Table 5.9-1 will be updated as follows:

Table 5.9-1. Software Classification Mapping

SPM Classification	IEEE Standard 1012-2004
Protection	4
Important-to-Safety	4 (with noted exceptions identified in **EXHIBIT 5-8 IEEE STANDARD 1012-2004 COMPLIANCE TABLE)**
Important-to-Availability	~~N/A – V&V of non-safety systems is not in accordance with IEEE Std. 10122~~ – See EXHIBIT 5-1 SOFTWARE TASKS AND RESPONSIBILITIES
General Purpose	~~N/A – V&V of non-safety systems is not in accordance with IEEE Std. 10121~~ – See EXHIBIT 5-1 SOFTWARE TASKS AND RESPONSIBILITIES

In order to address the NRC's concern over requirements traceability, Section 5.5.3.2, "IV&V Tasks," will be revised as follows:

"The following are specific IV&V Tasks:

1. Review the adequacy and accuracy of the Requirements Traceability Matrix (RTM) as prepared by the design team. The traceability in the RTM is established in both directions at each decomposition level and allows IV&V to verify the software requirements are complete, correct, and accurate decomposition of allocated system requirements. The review shall include verification that all functional, hardware interface, software, performance, and user requirements have been included."

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.

Westinghouse Response:

Westinghouse does not intend to take exception to the reporting requirements of IEEE Std. 1012-2004. Therefore, Section 10.5 will be revised as follows (as originally stated in Revision 4):

"Software IV&V documentation shall include Software IV&V Reports (SVVR), prepared according to ~~Section 5.6~~Reference 8 as augmented by Reference 18."

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.

Westinghouse Response:
The SPM complies with IEEE Std. 1012-2004 requirements for V&V activities as documented in Exhibit 5-8 of the SPM. Therefore, the SPM complies with IEEE Std. 7-4.3.2-2003.

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.

Westinghouse Response:
Westinghouse intends to take exception to IEEE Std. 829-2008 as endorsed by Regulatory Guide (RG) 1.170, Rev. 1, and instead will use an alternative approach that complies with the requirements of 10 CFR Part 50, Appendix B. To do so, Westinghouse will revise the SPM to state compliance to the previously cited RG revision (i.e., Rev. 0) and IEEE Std. 829-1998. This older RG meets the same underlying regulatory criteria (i.e., GDC 1 and 21 of Appendix A to 10 CFR Part 50, as well as Criteria I, II, III, V, VI, XI, and XVII of Appendix B) as the new RG. As a result, this alternative approach will meet the underlying regulatory criteria of RG 1.170, Rev. 1. Therefore, Reference 14 will be revised as follows (as originally stated in Revision 4):

"IEEE Std 829-~~2008~~1998, "IEEE Standard for Software ~~and System~~ Test Documentation""

And Reference 20 will be revised as follows (as originally stated in Revision 4):

"Reg. Guide 1.170, Rev. ~~10~~ (~~July 2013~~Sept. 1997), "Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants""

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.

   Westinghouse Response:
   As stated above, the SPM will be revised to state compliance to the previously cited RG revision (i.e., Rev. 0) and IEEE Std. 829-1998 as an alternate approach to meet the underlying regulations of RG 1.170, Rev. 1. Therefore, Section 4.3.2.2, "Software Requirements Phase," will be revised as follows (as originally stated in Revision 4):

   "A Common Q™ specific test plan shall start to be developed in accordance with the content, not the format of Reference 14, Section 4, to identify how the test activities will be implemented. ~~Reference 14, Section 8 will be used as guidance in developing the test plan. The test plan shall comply with the requirements of Reference 1 and Reference 4.~~ It shall include the following topics as a minimum:"

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.

Westinghouse Response:
As stated above, the SPM will be revised to state compliance to the previously cited RG revision (i.e., Rev. 0) and IEEE Std. 829-1998 as an alternate approach to meet the underlying regulations of RG 1.170, Rev. 1. Therefore, Section 5.8, "IV&V Test Documentation Requirements," will be revised as follows (as originally stated in Revision 4):

"The purpose of this section is to define the purpose, format and content of required test documentation. The test documentation as a whole shall fulfill the requirements of References 14 and 20 ~~are used as guidance in creating the test documentation~~. ~~The Test Documentation shall be in accordance with the NRC-accepted Westinghouse 10 CFR 50, Appendix B Quality Management System (Reference 1) and quality assurance procedures (Reference 4).~~"

Section 5.8.2, "Test Procedure," will be revised as follows (as originally stated in Revision 4):

"The elements of the test specification and test cases described in Reference 14 can be found in the test procedure. ~~Reference 14, Section 12 will be used as guidance in developing the test procedures.~~ The test procedure shall comply with ~~the requirements of Reference 1 and~~ Reference 14, Section 7."

Section 5.8.3, "Test Report," will be revised as follows (as originally stated in Revision 4):

"The test report also contains the Exception Report log and copies of the Exception Reports. Together, these identify the status of outstanding test exceptions reported during testing. ~~Reference 14, Section 16 will be used as guidance in developing the test reports.~~ The test reports shall comply with ~~the requirements of Reference 1 and~~ Reference 14, Section 11.

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.

Westinghouse Response:
As stated in Westinghouse's response to RAI 2.b, Section 5.8 will be revised to state compliance to the previously cited RG revision and IEEE Std. 829-1998 as an alternate approach to meet the underlying regulations of RG 1.170, Rev. 1.

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.

Westinghouse Response:
As stated in Westinghouse's response to RAI 2.a, Section 4.3.2.2 will be revised to state compliance to the previously cited RG revision and IEEE Std. 829-1998 as an alternate approach to meet the underlying regulations of RG 1.170, Rev. 1.

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.

Westinghouse Response:
As stated in Westinghouse's response to RAI 2.b, Section 5.8 will be revised to state compliance to the previously cited RG revision and IEEE Std. 829-1998 as an alternate approach to meet the underlying regulations of RG 1.170, Rev. 1.

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.

Westinghouse Response:
As stated in Westinghouse's response to RAI 2.a, Section 4.3.2.2 will be revised to state compliance to the previously cited RG revision and IEEE Std. 829-1998 as an alternate approach to meet the underlying regulations of RG 1.170, Rev. 1.

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.

Westinghouse Response:
As stated in Westinghouse's response to RAI 2.b, Section 5.8 will be revised to state compliance to the previously cited RG revision and IEEE Std. 829-1998 as an alternate approach to meet the underlying regulations of RG 1.170, Rev. 1.

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.

Westinghouse Response:
As stated in Westinghouse's response to RAI 2.b, Section 5.8 will be revised to state compliance to the previously cited RG revision and IEEE Std. 829-1998 as an alternate approach to meet the underlying regulations of RG 1.170, Rev. 1.

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.

Westinghouse Response:
IEEE Std. 1012-2004 does not differentiate between a Factory Acceptance Test (FAT) plan and a Site Acceptance Test (SAT) plan. Therefore, the FAT plan will be generated during the requirements phase as shown in Exhibit 5-8 of the SPM. If Westinghouse is contracted to perform site acceptance testing, Westinghouse will work with the Licensee to develop the required inputs for the SAT plan. The contract schedule will then define when the SAT plan will be developed. Therefore, the text for "Acceptance V&V test plan generation" in Exhibit 5-8 will be revised as follows:

"One test plan covers ~~Acceptance, integration, system, and componentall~~ phases of testing, except SAT. A separate SAT plan will be developed in accordance with the contract schedule with the licensee."

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.

Westinghouse Response:
A software module can be generically produced (existing software not to be modified) or maybe specifically developed or modified for a particular project (new software, or existing software to be modified). In the former, pre-validated modules are used in the application software and the project's validation testing starts with Unit Testing of the released application. In the latter case, however, the validation of the software module (module test) can be performed while the application software that uses the module is concurrently undergoing downstream validation tests. This is a calculated risk in the project execution where rework in the downstream validation activities may be required should the module test failed. Nevertheless, the scope of module test, or any downstream test activities, is not changed due to this provision.

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).

Westinghouse Response:

Per paragraph 7.3.1.5 the purpose of the FAT is to demonstrate that the complete system is integrated and functional. Further, it states that the FAT provides evidence to the customer that the system meets its requirements and provides confidence that the site installation and integration activities will be successful. These activities are the tests that show to the customer that the equipment is acceptable to transfer from the equipment vendor to the customer. As stated, deferring of FAT activities to site is based on customer agreement and is a contractual decision. From a technical perspective the ability to demonstrate acceptable integrated performance can be achieved in the factory or at site when it is integrated with site infrastructure. In this way the actual power grid, grounding plane, interconnecting cabling and other prototypic interface are available, thereby providing a more prototypic environment.

Per SPM paragraph 7.2.5.1 in the FAT paragraph “FAT is the equivalent of the description of Acceptance tests in IEEE Std. 1012.”

IEEE Std 1012-2004, “ acceptance testing: (A) Formal testing conducted to determine whether or not a system satisfies its acceptance criteria and to enable the customer to determine whether or not to accept the system. (B) Formal testing conducted to enable a user, customer, or other authorized entity to determine whether to accept a system or component.”

The statement of deferring the testing to site does not eliminate the testing requirement of the equipment provider. Westinghouse experience is that customer and project schedules may benefit from delivering tested equipment and completing the final integration testing that represents part of the FAT at the site. An example or a condition where this may occur is when a system has completed system validation testing. In this testing the hardware was fully exercised but a future software baseline is planned due to identified design changes. The system can be delivered and installed and a follow on FAT test could be run at site at the new baseline. In this scenario the equipment vendor performs testing with the customer support to complete the intent of an acceptance tests. The controls and reporting of this type of scenario would be based on customer agreement and contractual obligation. The important aspect is that the correct amount of testing is performed on the system consistent with the test plan and the agreed acceptance criteria.

This allowance is to recognize the many combinations and conditions I&C systems are developed and delivered, such as entire systems, subsystems, back fits into existing systems, etc. The two aspects of a FAT are the scope of the testing that is the responsibility of the supplier and at what location the test is performed. By allowing testing

that is considered to be the responsibility of the supplier performed at the site recognizes that the scope of the test is as important as or more important than where it is conducted. Therefore, the SPM will be revised in Sections 7.2.4, 7.2.5.1, and 7.3.1.5 to clarify that a FAT is performed prior to the customer accepting the equipment or system:

Section 7.2.4, "Schedule," will be revised as follows:
"Factory Acceptance Test (FAT) – The FAT is to be executed on a deliverable system and must be completed and meet its approved requirements before ~~shipping the safety system to~~ the customer accepts the system. The FAT is typically performed in the factory but some portion of the test can be performed at site if agreed to with the customer. When performed on a deliverable system, the System Validation Test can fulfill the role of the Factory Acceptance Test."

Section 7.2.5.1, "Testing Hardware," will be revised as follows:
"Factory Acceptance Tests – These tests shall be conducted on the deliverable hardware assembled in cabinet(s) ~~for shipment to the customer~~ and configured with the application software. The integration and system validation test can be credited for applicable parts of the Factory Acceptance Test (FAT) when conducted on deliverable hardware. FAT is the equivalent of the description of Acceptance tests in IEEE Std. 1012 (Reference 8)."

Section 7.3.1.5, "Factory Acceptance Test (FAT)," will be revised as follows:
"The purpose of the FAT is to demonstrate that the complete system is integrated and functional. To this end, the optimum scenario is to perform this test in the manufacturing facility ~~with full interconnection of the deliverable system cabinets (across all divisions) and with application software~~. Prior to ~~shipment of equipment to the site~~acceptance of equipment by the customer, a Factory Acceptance Test (FAT) is performed as a manufacturing test to provide evidence to the customer that the system meets its requirements and provides confidence that the site installation and integration activities will be successful."

"FAT is performed to:
- Demonstrate that the system ~~being delivered~~ has been manufactured correctly and is acceptable to the customer"

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.

Westinghouse Response:
Integration testing is defined as a functional test that is performed on a system that is now integrated. This integration is referring to the integration of released software with deliverable equipment or equivalent. Section 7.3.1.3 states, "Integration testing is used as part of system validation testing when validating the design and as part of the FAT testing to demonstrate the deliverable system has been properly integrated." Therefore, there are two types of integrated tests, System Validation Tests and FAT. For first of a kind testing, a System Validation Testing proves that the design meets detailed functional requirements and it demonstrates that the design is correct and adequate. The tests that you identified above have not been removed but are listed along with other functions in paragraph 7.3.1.4:

- Safety Functions
- Communications
- Displays
- Diagnostics
- Performance
- Error Handling – potential errors shall be handled with known consequences
- Communications – all defined outputs shall be broadcast and received correctly within the channel
- Redundancy – all shared inputs shall produce the same output from redundant processors
- Diversity – all functionally diverse signals shall be verified for correctness in termination

The Factory Acceptance Test (FAT) is also an Integration Test. It's performed to demonstrate that the delivered equipment has been manufactured correctly and integrated properly. The FAT also has a list of test that fulfills this definition as applicable for the system under test. These are listed in section 7.3.1.5:

The following test items shall be included or demonstrated in the FAT:
- Safety Functions
- Communications
- Operability of Displays
- Diagnostics associated with hardware specific inputs (door alarms, temperature alarms, breaker status, etc.)
- Performance (accuracy, time response, etc.)

As can be seen by this list, the FAT contains the tests from the previous list that are applicable to a FAT and the FAT is an extensive test of the integrated system and will demonstrate a proper operating system.

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.

Westinghouse Response:
It is agreed and confirmed that the Factory Acceptance Test (FAT) is performed on the deliverable equipment. The statement about surrogate equipment is referring to system validation testing and regression testing, which can be performed on surrogate equipment. This paragraph in section 7.3.1.5 is providing clarification for the scenario where a previous validation test has been performed on the first of a kind system but during the Nth of a kind, a design change has been identified. Such a change could be either hardware, software or both. A System Validation test would need to be run for the design change to prove that the design implementation is correct for all of the systems that are considered the same design, (i.e. the first of a kind and all Nth of kind systems). It is the System Validation test that can be run on surrogate equipment. Another option would be that the deliverable system that is going through the FAT test program can be the surrogate equipment for the purposes of System Validation testing for all other systems. Either way the system that is going through the FAT would need to obtain the change and appropriate FAT testing would be conducted for that deliverable system. Therefore, Section 7.3.1.5, "Factory Acceptance Test," will be revised as follows:

"~~As design changes are introduced, regression analysis shall be performed to determine what tests need to be repeated or introduced to maintain the level of system design validation achieved during the first of a kind system validation test program. The system validation tests required by the regression analysis may be performed on the deliverable equipment as a separate section of the FAT or on surrogate equipment consistent with the regression testing methods described in subsection 7.3.2.2.~~"

With that sentence moving to Section 7.3.1.4, "System Validation Test," as follows:
"As design changes are introduced, regression analysis needs to be performed to determine what tests need to be repeated or introduced to maintain the level of system validation achieved during the first of a kind test program. The system validation tests required by the regression analysis may be performed on the deliverable equipment as a separate section of the FAT or on surrogate equipment consistent with the regression testing methods described in subsection 7.3.2.2.

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.

Westinghouse Response:
For system validation test to be credited as FAT it must be performed on the delivered equipment.

In this version of the SPM, “Integration Test” is now a term that describes a condition of the test (e.g. integrated). There are two types of integrated testing that performs two different functions; System Validation Testing and Factory Acceptance Testing (FAT). The System Validation Testing is a test of the design (system design, Hardware design and the software design) that proves that the design as implemented meets the requirements. The FAT is a manufacturing integrated test that demonstrates that the deliverable equipment is working properly and consistent with the System Validation Test (e.g. within acceptance criteria). If the System Validation Test is performed on the deliverable system then it can also be credited as the FAT for that system. This has been the model for many plants where the System Validation Test was also the FAT. Once the design has been validated via the System Validation Test, it can now be credited for other systems of the same design.

Therefore, for every system delivered, either first of a kind or Nth of a kind (follow on units), we must show that it has passed a System Validation Test and a FAT. The System Validation Test can be performed on Surrogate equipment. This can be a test bed that is configured to be functionally equivalent to the production hardware or it could be production equipment destined to be delivered. Either way, it is considered to be surrogate equipment for follow on units.

The FAT is never performed on surrogate equipment as its purpose is to demonstrate acceptability of the delivered system.

Inherent in this strategy is that the FAT is a functional subset of the System Validation Test. For example, an analog input and accuracy test is performed as part of both tests. To prove the system is meeting all of its requirements in the design of hardware and software the system validation test checks every signal. And for the FAT each signal is also checked to confirm the correct manufacturing of every signal path. However, the detailed software that displays the information to the operator needs only be fully tested once during the System Validation Test and not during the FAT. The FAT needs to demonstrate the display is working and data communication to the display are working properly. Therefore, the FAT is a functional subset of the System Validation Test. The term functional subset is used because there may be a different and more efficient method of testing these features than to just rerun a subset of the System Validation Tests.

Therefore, every system delivered must show that it passed a FAT and a system validation test. And the system validation test may have been run on the delivered system in question, another delivered system of the same design or on other appropriate surrogate equipment. But all delivered systems must have a FAT run on that system. Therefore, Section 7.3.1.4, “System Validation Test,” will be revised as follows:

"See EXHIBIT 7-1 COMPARISON OF SYSTEM VALIDATION TEST AND FAT for a detailed description of the tests performed during system validation testing and FAT.

For system validation test to be credited as FAT, it must be performed on the delivered equipment.

As an alternative to functional testing with production hardware, a system validation test can be performed with a test bed…"

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.

Westinghouse Response:
In this table the term representative means typical. It also means that it is not exhaustive for all combinations of every factor or path. Time response for a typical software based design has historically shown that the largest contributor to the variability of the response has been the software loop times and the asynchronous nature of signal propagation through such systems. During the System Validation Testing real trips and actuations are caused by the real inputs and the time is measured for multiple runs. These times are compared to the requirements and to the analyzed and predicted times to bound the response of the system. For the FAT, the design has been validated and the time response has been well characterized. Because these systems are highly digital, very little of the time response path are susceptible to latency issues that are not detectable during functional testing or identified as part of the system diagnostics. Therefore the FAT is intended to be a subset of the System Validation Testing but still tests the hardware paths or uses commercial dedication test data for time sensitive components. For example, signal conditioning front ends that have filters and latency limits can be better tested independently during the commercial dedication process on the bench. However, FAT time response testing exercises the actual safety function actuations and trips on the deliverable equipment. Therefore, the column, "FAT (Nth Application)" in Exhibit 7-1 will be revised as follows:

A representative sample of safety function tests on the deliverable hardware with the deliverable software to demonstrate critical safety trips, consistency with analytic model and first application response tests

- One path through ~~each relative~~critical hardware component; e.g., each PM, I/O module, high-speed datalink, etc.
- Component response confirmed by commercial grade dedication process (similar to spare parts).

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.

Westinghouse Response:
Archival requirements are per the Westinghouse Level II Policies and Procedures. Ultimately the group managers are responsible for their group's work products being archived according to the procedures. Software Librarian is a role within the context of IV&V activities in addition to being a position within the IV&V Group. The activities of the role could be performed by individual other than the person whose title is Software Librarian. This provision was necessary to allow flexibility in task assignments within the IV&V group with discretion of the IV&V manager who ultimately is responsible for IV&V archival requirements.

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.

Westinghouse Response:
The IV&V Group consists of positions including engineers, administrative assistants, software librarians and escorts. The wording in this section was changed to 'engineers' to differentiate those resources who do perform design verification and validation activities. Individuals who are not performing design related IV&V functions can be shared by other organizations as their work scope are not related to 'design activities' and does not jeopardize independence. For instance, escorts (who are hired to escort foreign nationals and customers) can be loaned to other groups with no impact to IV&V work performed on any project. Therefore, Section 2, "Organization," will be modified as follows:

"Reference 11 requires that the IV&V team for a safety system is organized independently of the design team. The IV&V organization meets this requirement by not allowing IV&V ~~engineers~~ team members to participate on design activities, even on a part time basis, if they are involved in the verification of that design.

The IV&V Team in the context of this SPM refers to those individuals within the IV&V organization who perform V&V functions on the safety system design, implementation, and test (i.e. engineers and technicians). The IV&V organization may include other individuals who perform supporting roles that are not design verification related and the organizational independence does not apply to those individuals."

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.

Westinghouse Response:
Per IEEE Std 829-1998 overview states:
“The test plan prescribes the scope, approach, resources, and schedule of the testing activities. It identifies the items to be tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the risks associated with the plan.”

Additionally in section 4.2 on Test Plan the following is stated:

“If some or all of the content of a section is in another document, then a reference to that material may be listed in place of the corresponding content. The referenced material must be attached to the test plan or available to users of the plan.”

Additionally in section 4.2.3 on Test Items for the test plan the following is stated:

“Supply references to the following test item documentation, if it exists:

a) Requirements specification;”

This allows for a reference to the item if it exists. Review of IEEE 829-2008 also includes the allowance of references to requirements in paragraph “9.2.1 (LTP Section 2.1) Test items and their identifiers”

The reason for the change in the SPM is due to the typical sequence and progression of a project. Requirements analysis, testing coverage and tracing of the requirements to test cases are significant testing activities. The Test Plan is needed to outline these activities. The test planning and initial engineering work occurs in parallel with the finalization of the design requirements and the implementation specifications. Therefore, the specific requirements to be tested are not available or issued in their final form when the test plan is written. Our processes include an extensive requirements management process and analysis for coverage using appropriate tools. This includes linking to test procedures and/or test cases depending on the requirement level. The requirements that are being tested are tied to the test section or test procedure either directly or by reference to a requirements tracing document for testing.

Since IEEE 829 recognizes and allows the ability to provide a reference to the requirements to be tested, and the normal progression of a test program determines the

specific requirements and coverage at a lower level than what is available for the test plan, the SPM was changed to better reflect the typical process.

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?

Westinghouse Response:

The SPM will be revised as follows (as originally stated in Revision 4):

"The SVVP (Section 5) ~~has been~~ is reviewed for adequacy and completeness of the verification and validation methods ~~for Common Q™~~ defined in the SVVP. An independent reviewer meeting the qualifications of Reference 4 performed this review as part of the review process for this SPM. Compliance to the SVVP is covered by the in-process audits described in subsection 4.6.2.7."