October 26, 2011

J. A. Gresham, Manager
Regulatory Compliance and Plant Licensing
Westinghouse Electric Company
Nuclear Services
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION, WESTINGHOUSE TOPICAL REPORT WCAP-16096, REVISION 2, SOFTWARE PROGRAM MANUAL FOR COMMON- Q SYSTEMS (TAC NO.ME5159)

Dear Mr. Gresham

By letter dated August 26, 2010, Westinghouse Electric Company submitted for U.S. Nuclear Regulatory Commission (NRC) staff review Topical Report (TR) WCAP-16096, Revision 2, "Software Program Manual for Common Q Systems" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML103220086).

Upon review of the above information provided, the NRC staff has identified that additional information is needed to complete the review. On October 12, 2011, Stephanie Smith, Westinghouse Project Manager, and I agreed that the NRC staff will receive your response to the enclosed Request for Additional Information (RAI) in 30 days from the date of this letter which contains no proprietary information. If you have any questions regarding the enclosed RAI questions, please contact me at 301-415-8480.

Sincerely,

/RA/

Andrew L. Hon, Project Manager
Licensing Processes Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Project No. 280

cc:
Mark Stofko
Westinghouse Electric Company
20 International Drive
Windsor, CT 06095

J. A. Gresham, Manager
Regulatory Compliance and Plant Licensing
Westinghouse Electric Company
Nuclear Services
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION, WESTINGHOUSE TOPICAL REPORT WCAP-16096, REVISION 2, SOFTWARE PROGRAM MANUAL FOR COMMON- Q SYSTEMS (TAC NO.ME5159)

Dear Mr. Gresham

By letter dated August 26, 2010, Westinghouse Electric Company submitted for U.S. Nuclear Regulatory Commission (NRC) staff review Topical Report (TR) WCAP-16096, Revision 2, "Software Program Manual for Common Q Systems" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML103220086).

Upon review of the above information provided, the NRC staff has identified that additional information is needed to complete the review. On October 12, 2011, Stephanie Smith, Westinghouse Project Manager, and I agreed that the NRC staff will receive your response to the enclosed Request for Additional Information (RAI) in 30 days from the date of this letter which contains no proprietary information. If you have any questions regarding the enclosed RAI questions, please contact me at 301-415-8480.

Sincerely,
/RA/
Andrew L. Hon, Project Manager
Licensing Processes Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Project No. 280

cc:
Mark Stofko
Westinghouse Electric Company
20 International Drive
Windsor, CT 06095

DISTRIBUTION:

PUBLIC	PLPB Reading File	RidsNrrDpr	RidsNrrDprPlpb
RidsNrrLADBaxley	RidsAcrsAcnwMailCenter	RidsNrrPMAhon	RidsOgcMailCenter
RidsNrrDeEicb	RidsNroDeIce1	RidsNroDnrlNrga	

ADAMS ACCESSION NO.: ML112850828 *concurred by email **NRR-106**

OFFICE	PLPB/PM	PLPB/LA	EICB/BC	PLPB/BC	PLPB/PM
NAME	AHon	DBaxley*	GWilson*	JJolicoeur	AHon
DATE	10/12/2011	10/18/2011	10/21/2011	10/26/11	10/26/11

OFFICIAL RECORD COPY

Software Program Manual Request for Additional Information

The U.S. Nuclear Regulatory Commission (NRC) staff conducted an audit of the Common Q Post Accident Monitoring (PAMS) system used at Watts Bar Nuclear Plant, Unit Two (WBN2) on February 28 through March 4, 2011. During this audit, the staff reviewed the implementation of several aspects of the Software Program Manual (SPM) and several discrepancies were noted. The resulting audit report (Agencywide Documents Access and Management System (ADAMS) Accession No. ML110980761) identified several generic actions in which Westinghouse Electric Company (Westinghouse) agreed to revise the SPM in order to accurately reflect the processes being used for the development of safety related software applications. For each of these items, the staff requests that the revised SPM text be provided in the request for additional information (RAI) response to facilitate completion of this safety evaluation.

1. SPM Section 6.3.1, "Configuration Identification," specifies guidance for information to be included in header blocks for source files in order to maintain configuration identification. In the source files for the AC160, the header does not strictly follow this SPM guidance due to the process that creates those source files. Most of this information, including revision history, is instead contained in the footer of those files.

   Please provide revised SPM text used to address the issue described above.

2. SPM Section 5.4.3.2.2, "Verifiers," under Validation and Verification (V&V) Team Roles states that "The verifier is also the independent reviewer for the design team." The audit team observed however that the V&V team did not perform this role.

   Please document in the response that the SPM will be revised to clarify that the V&V team verifier does not perform the role of independent reviewer for the design team.

   Westinghouse has also agreed to ensure that consistent terminology is used in the SPM and quality assurance implementing procedures. Please provide all changes to SPM terminology that will be made to address this generic action.

3. SPM Section 4.6.2.9 states that:

   "The Software Configuration Management Plan (SCMP) Review is held to evaluate the adequacy and completeness of the configuration management methods defined in the SCMP (SECTION 6) and their implementation. The review shall be performed by the V&V team, and results documented to identify all deficiencies found. The design team shall plan for the resolution of deficiencies."

   Westinghouse stated that no review of the adequacy and completeness of Section 6, "SCMP," was performed by the WBN2 V&V Team since the NRC had approved the SPM (i.e., the NRC found the SCMP – SPM Section 6- to be adequate).

ENCLOSURE

The NRC approved the SPM, in part, based on requirements it contained for future actions. The staff however understands this clause to mean that the V&V team will specifically evaluate the SCMP for acceptability and completeness for each development project. If the generic SCMP is determined to be unacceptable, then a project specific SCMP would need to be developed.

Please clarify how and when SCMP review activities will be performed in the next revision of the SPM. The staff also requests that a clarification of the objectives and scope of the SCMP review be included in this discussion.

4. SPM Section 6.2.2.1, "Requirements Phase" states:

   "*1. Define the software items that are to be controlled via this SCMP*."

   However, the V&V team for the WBN2 did not perform this activity during the requirements phase. Instead, the design team used the project plan to define the generic software that was used for WBN2 PAMS.

   Please include a discussion in the revised SPM on generic vs. project-specific requirements. The SPM will also be updated to include a discussion to clarify in which part of the software life cycle these software items are to be defined.

5. SPM Section 4.5.2.1, "Coding Standards," states:

   "*The V&V team shall review the applicable coding standards for each project for acceptability."*

   Westinghouse credits the V&V signature on the generic coding standards document as addressing this requirement.

   Please clarify in the SPM to address project requirements for reviewing applicable codes and standards for acceptability.

6. Table 5.9-1 in Section 5.9 of the SPM provides software classification mapping to Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 1012-1998 which implies that the same or equivalent V&V tasks defined in IEEE 1012 are performed for the equivalent Westinghouse software classifications.

   Section 5.1 of the SPM also states this SVVP complies with IEEE 1012-1998. However, the V&V tasks defined in Section 5 of the SPM and in Exhibit 5-1 do not match the V&V tasks that are prescribed in IEEE 1012 Table 1, "V&V Tasks, Inputs and Outputs".

   In addition, Regulatory Guide 1.168 states that "software used in nuclear power plant safety systems should be [assigned software integrity level (SIL) 4] or equivalent as demonstrated by mapping between the applicants or licensee approach and SIL 4 as defined in IEEE Std. 1012-1998." The mapping provided in Table 5.9 and in Exhibit 5-1 does not demonstrate that an equivalent level of V&V is ensured for Software classified as "Protection."

Specifically, the Westinghouse SPM specifies a total of 23 tasks in Exhibit 5-1 while IEEE 1012 Table 1 specifies 62 V&V tasks that are required for SIL 4 software. Please provide documentation (mapping) to demonstrate that each of the V&V tasks specified in IEEE 1012 for SIL 4 software is being performed for Westinghouse "Protection" class software.

7. Many of the V&V tasks described in Section 5.2 of the SPM are not included in the table in Exhibit 5-1. Therefore, this table does not provide a complete mapping of all V&V activities required for the various classifications of software. In addition Section 5.5.2 of the SPM does not specify which organization is responsible for performance of these V&V activities. Please provide a complete listing of all V&V activities which includes the responsible organization for each activity. This list should either include all V&V activities specified for SIL 4 software in IEEE 1012 or provide mapping to those activities so that the staff can determine compliance with RG 1.168.

8. There are no dedicated sections in the Westinghouse SPM for the following planning documents that are delineated in BTP 7-14 Section B.2.1.

    a. Software Management Plan
    b. Software Development Plan
    c. Software Integration Plan
    d. Software Installation Plan
    e. Software Operations Plan

    Each of these plans was previously evaluated on the basis of the required elements being contained within the existing sections of the Westinghouse SPM. However, with the exception of the Software Operation and Maintenance Plan (see RAI #9), no specific references were provided in the safety evaluation to SPM sections that can be credited to satisfy regulatory guidance or an acceptable, equivalent methodology or plans for the items listed above. The staff will need to evaluate the revised SPM against the acceptance criteria provided by the SRP for each of these planning areas. Please provide mapping to the applicable sections within the SPM or provide additional information to support the evaluation for each of these planning topics.

9. In the previous version of the SPM, Section 7 had been credited for combining the Operations and Maintenance aspects of the Common Q systems, however, in the new version; Section 8 is titled "Software Maintenance Plan." Was it Westinghouse's intent to limit the scope of this section to the Maintenance aspects of the software lifecycle or does this section still apply to both Operational and Maintenance aspects of the system lifecycle?

10. Westinghouse referenced WCAP-16096 Section 11, "Secure Development and Operational Environment (SDOE) Plan," to address Interim Staff Guidance (ISG 6) Item 1.26 "Vulnerability Assessment." In reviewing Section 11 of WCAP-16096, the staff determined this planning document does not include all of the information needed to complete its assessment of the development aspects for the Common Q SDOE. The staff also performed a review of the Westinghouse Application Restrictions for Generic

Common Q document and determined the required information is contained within the application restriction tables therein. The staff requests that the applicant submit the "Applications Restrictions for Generic Common Q" onto the docket to support the SDOE evaluation.

11. Revision 3 of RG. 1.152 has already been issued; please clarify how Westinghouse intends to address this new version in the SPM.

    RG 1.152 Revision 1 (January 2006) is provided as Reference 17 in WCAP-16096, however, the staff will evaluate the common Q platform against the criteria of the current version of this standard. To support its review of the Common Q SDOE, the staff requests that Westinghouse provide an assessment of the Common Q system conformance to the criteria of RG 1.152 Revision 3. This assessment should address the criteria for each of the following software life cycle phases as specified in RG 1.152 Sections 2.1 through 2.5.

    a. concepts,
    b. requirements,
    c. design,
    d. implementation, and
    e. test.

12. In Table I., "Document Requirements," within the Documentation Requirements Section of the Common Q SPM several items specify that the listed document would be prepared by one of two or more individuals or teams. For example, the Test Plan (Item 25) is listed as being prepared by either the Design Team or the V&V Team. Please specify the conditions which would determine which of these individuals or teams would perform these activities.

13. In Table II. "Information Requirements," several of the Output Documents are listed as "V&V Report" with no delineation of what type of V&V Report would need to be created to document this activity or identification of during what part of the development life cycle this report would be generated. Is there only one V&V Report which is updated as the development process progresses or are there multiple V&V reports created throughout the development process?

14. It is unclear to the staff at which phase of the development process each output document listed in Table II would be created to document the associated activity. Please provide additional information to identify the phase within the software development process during which each listed output document would be created.

15. In Table II. "Information Requirements," what is meant by the requirement listed in SPM Section Number 10.2 describing the, "Justification for not performing complete system testing"? Section 10.2 describes error reporting and includes a discussion of determining the extent of retest but does not include any discussion of not performing complete system testing. If this document is only referring to the retest requirements as described in Section 10.2 then the document title should not imply that a test

requirement is being omitted.

16. In Subsection 1.2.1 “Software Classification and Categorization,” the use of the term “General Purpose software” is used. The examples cited reference test software such as that utilized for a commercial dedication process. Any such software would be subject to the restrictions of IEEE 7-4.3.2 Section 5.3.2 and would have to be qualified based upon the tool usage and the subsequent downstream testing performed on the safety related components being tested by the tool. Please include appropriate qualifiers for the examples listed so that the implication that all test software being used could be classified as general purpose software.

17. Within Section 3.3.1 “Organization and Responsibilities,” the SPM discusses that the Quality organization has a matrix reporting relationship to the Senior VP of the NA business unit. The staff requires additional information in order to determine if an adequate level of independence has been established. Please provide a detailed listing of all reporting relationships established to demonstrate that an adequate level of separation exists between the Quality organization and the organizations with which it conducts its business function.

18. Within Section 3.3.2 “Resources,” of Section 3, Software Safety Plan, the SPM previously stated that, “*Project schedules and resource allocations are established and maintained in SAP*.”

    It now states, “*Project schedules and resource allocations are established via the Project Plan*.”

    However, in Table II “Information Requirements” of the Documentation Requirements Section it states that a detailed schedule and Resource Plan are documented in the Systems, Applications and Products in Data Processing (SAP), an enterprise software system utilized by Westinghouse.

    Please explain which information is correct?

19. Section 3,”Software Safety Plan,” Section 3.3.5.7.3 ”Test Reports,” it states:

    > *The test reports document the execution of the acceptance test procedures. In addition to attaching the signed and checked off test procedure, the test reports provide an overall summary of the test results and the resulting Exception Reports generated during the test. The system configuration at the time of test execution is also documented in the test reports. Test Reports are prepared in accordance with Reference 14, Section 10.*

    In reviewing Section 10 of Reference 14 – IEEE Std. 829 – 2008, the section is the “Level Test Design” section which has nothing to do with Test Reports as is implied. On the other hand, Section 14 Anomaly Report, of IEEE Std. 829 – 2008 describes a similar process and may have been the intended reference.

    For reference, in IEEE Std. 829 – 1998, Section 10 is the Test Incident Report.

    Please explain the reason for referencing Section 10 of Reference 14 in relation to Test

Reports or provide a corrected reference.

20. Section 4, “Software Quality Assurance Plan,” Section 4.1.1 “Purpose,” it previously stated, “NuCARs [now referred to as RECARs] shall be prepared by the design team and reviewed by the V&V team. The text has been modified to remove the requirement for the V&V team to conduct a review of the software classification determination. Please provide justification for removal of this requirement including a discussion of what organization now performs this validation and/or verification activity?

21. In Section 4.3.2.6 “Site Installation and Checkout Phase,” the SPM discusses the use of an Exception Report Log. Additionally, the detailed record of changes states that “The Test Exception Report (TER) form is used to document all software anomalies, not just test exceptions”.

    Because of this characterization, it is not clear to the staff why is there no mention of this formal corrective action mechanism earlier in the development process in Sections 4.3.2.1 through 4.3.2.4. Please provide a definition of the TER which includes a discussion of when during the development process they will be used to document software anomalies.

22. Section 4.4 “Documentation,” Section 4.4.1 “Purpose,” the text states, “If required, documents listed shall be made lifetime quality records in accordance with Reference 4” [Westinghouse Level II Policies & Procedures, Revision 15]. Where in the SPM or other appropriately cited Westinghouse document does the text describe the requirements for the need to create lifetime quality records?

23. Section 4.4 “Documentation,” Section 4.4.1 “Purpose,” the text states, “If required, documents listed shall be made lifetime quality records in accordance with Reference 4” [Westinghouse Level II Policies & Procedures, Revision 15. Please provide a description of the criteria that is used to determine the retention requirements for Common Q records.

24. Section 4.5 “Standards, Practices, Conventions and Metrics,” Section 4.5.2.2 “Software Testing Standards,” states:

    > *“Specific format and content…shall comply with Reference 14, Sections 6 and 10.”*

    However in the new revision of Reference 14 [IEEE Std. 829 – 2008], Section 10 is the Level Test Design” section, not the Test Incident Report section as was the case in the 1998 revision of the IEEE Std.

25. Section 4.5.3 “Life Cycle Application of Standards” informs the reader to refer to Section 5.5 “Life Cycle Verification and Validation,” for the application of *these* standards, practices, conventions, and metrics at each life cycle phase. It is not clear to the staff what specific standards and/or conventions and/or metrics are being referred to in the text. Section 5.5 does not appear to include a discussion of any specific standards, practices, conventions or metrics either. Please provide an explanation of which standards, practices, conventions, and metrics are applicable to which phases of the software development life cycle.

26. Within Section 5.4.3.2.3 “Librarian,” the individual previously had responsibility for records retention and revision control of the software product(s) and ensures procedures concerning the management of software recordkeeping were enforced. It is not clear to the staff whether that responsibility has been removed or if the responsibilities described in the re-worded sentence are equivalent. Please explain the purpose of this revised wording and include a discussion of who (by position or title) has the responsibility for performing the following activities:

    a. Records retention
    b. Revision control of software products
    c. Enforcement of procedures for managing software record keeping

27. In Section 5.4.5.2 “V&V Core Activities,” Item 6 discusses that either the design team or the V&V Team will provide the report qualifying such an item. Please explain the criteria used to determine which organization will perform this activity. This discussion should include a description of how the required levels of independence are maintained for all Common Q software.

28. In Section 5.4.5.3, Requirements Traceability Analysis, the second paragraph below the “Requirements, Design, Code and Test” diagram, the word analysis has been replaced with matrix. However, the next sentence within the paragraph goes back to describing the analysis. Please describe the relationship between the RTA and the RTM including a discussion of how one affects the other and which individuals and organizations will perform given functions for both the RTA and RTM.

29. The software Problem Report Exhibit 6-3 was deleted from Section 10 per detailed record of changes (see page ix). However, within Section 6.1.1 Purpose, of Section 6.1 Software Configuration Management Plan, Item 5 reads, “Maintain the status of released software, users of this software and associated **problem reports**.” The term Problem Report is also used elsewhere in the document (Item 5 of Section 6.2.2.6, Section 4.1.2, 8.2.4, and in Section 9.5.2). This RAI applies to Item 8 of Section 6.1.1 also.

    It is not clear what the “problem reports” being referred to are, in light of the fact that the software problem report has been deleted from Section 10. It is the staffs understanding that “Exception Reports” are now used to identify internal software problems. Please explain what is meant by the term problem report throughout the document and what, if any similar document or documents replaced the problem report.

30. Section 6 “Software Configuration Management Plan,” Section 6.3.4 “Configuration Audits and Reviews,” Item 5 states the V&V team will conduct a functional review to verify “actual” functionality and performance is consistent with the System Requirements Specification. The staff understands that equipment functionality is not exercised during a functional review activity. Additionally, the stated purpose of a functional review in Section 4.6.2.5 differs from the purpose stated in Section 6.3.4. In Section 4.6.2.5 it states that a functional review is conducted to “verify that all requirements specified in the Software Requirements Specification have been met.” Please explain how a functional review can satisfy the statement in Section 6.3.4.

31. Section 6, Software Configuration Management Plan, Section 6.3.6.1 “Subcontractor Software,” of the last sentence states, “Proprietary item ownership security and

traceability does not apply since Westinghouse owns the rights of subcontractor software." The term "Proprietary Item Ownership security and traceability" is not used elsewhere in the SPM so it is not clear to the staff what specific activities are not applicable for Subcontractor Software. Please explain, in greater detail, what is meant by that statement.

32. Section 7 "Software Test," Section 7.3.1.2 "Unit Testing, Plan," describes the steps taken by Westinghouse for Unit Testing. In Section 4.2.3.5 "Testing Phase" of Section 4, *Software Quality Assurance Plan*, the text states that Module and Unit Testing will be conducted in accordance with Reference 12, IEEE Std. 1008 – 1987, *IEEE Standard for Software Unit Testing*. IEEE Std. 1008 – 1987 specifies when conducting unit testing to test for input, output and internal states of software units. However, the following statement in Section 7.3 of the SPM implies that internal states are not tested during unit testing.

    SPM Section 7 "Software Test Plan," Section 7.3 "Testing Process Activities and Tasks," of states that testing for internal states will only be conducted for module tests.

    Please provide a description of how the Unit testing that is performed on Common Q software tests for internal states of the software to comply with IEEE Std. 1008 – 1987.

33. Section 10 "Problem Reporting and Corrective Action," Section 10.2 "Error Reporting Before Software Approval for Use," the third paragraph that previously contained requirements that the Exception Reports be forwarded to the EPM, the ELM, and the V&V team have been removed.

    Please provide an explanation of why these actions were taken including a description of what equivalent mechanisms have been put in place to ensure errors are properly identified, captured, tracked, resolved and placed into a records management system to ensure the issue is available for historical reference.

34. In Section 1.4 and throughout the SPM, it is unclear to the staff whether the requirements invoked by the use of the word "shall" would apply to the platform hardware and software, or to the application specific hardware and software, or to both. Please explain whether the use of "Shall" or "Should" in the SPM is intended to document activities to be performed on each application.

35. The staff would like to know if this version of the SPM is intended to supersede all previous versions that have been referenced in Common Q applications. Because this revision describes several substantial process changes, it is unclear to the staff what actual processes were used for development of specific applications that refer to previous versions of the SPM. For applications that are currently under review, the staff would like to have a clear understanding of the processes that are being used for system development.

    Please describe how the revised processes defined in Revision 3 of the SPM have been applied to those applications under review that currently reference previous versions of the SPM.

36. The Common Q Platform Topical Report WCAP-16097 discusses the use of Custom PC Elements in Section 5.2.1.2.3 which states that these elements will be subject to the

requirements set forth in the SPM. However, Custom PC elements are not mentioned in the SPM.

Please provide additional information on how the SPM controls are applied to the development of Custom PC elements.

37. Section 4.6.2.3 “Code Verification,” discusses the use of Code Reviews as a means of ensuring that source code conforms to software coding standards and guidelines. The staff requires additional information on how these code reviews are performed in order to determine if this SQA activity adequately satisfies the criteria of BTP 7-14 Sections B.3.3.4 and B.3.1.3.4. Please provide a detailed description of the Code Review process. This description should include a discussion of how the code which is developed for Custom PC elements is reviewed in a manner to ensure that high quality software which is capable of performing all required safety functions is produced.

38. Please confirm if the checklists in Exhibits 5-2, through 5-6 will be included in the V&V summary reports. If not, then how will completion of these checklists be documented? Please provide a description of how these checklists will be used including a description of all documentation requirements associated with performance of these activities.