September 3, 2004

Mr. James A. Gresham, Manager
Regulatory and Licensing Engineering
Westinghouse Electric Company
P.O. Box 355
Pittsburgh, PA 15230-0355

SUBJECT: DRAFT SAFETY EVALUATION FOR TOPICAL REPORT WCAP-16096-NP-A, REVISION 1, "SOFTWARE PROGRAM MANUAL FOR COMMON Q SYSTEMS" (TAC NO. MC2294)

Dear Mr. Gresham:

On January 29, 2004, Westinghouse Electric Company (Westinghouse) submitted Topical Report (TR) WCAP-16069-NP-A, Revision 1, "Software Program Manual for Common Q Systems," to the staff for review. Enclosed for Westinghouse's review and comment is a copy of the staff's draft safety evaluation (SE) for the TR.

Twenty working days are provided to you to comment on any factual errors or clarity concerns contained in the SE. The final SE will be issued after making any necessary changes and will be made publicly available. The staff's disposition of your comments on the draft SE will be discussed in the final SE.

To facilitate the staff's review of your comments, please provide a marked-up copy of the draft SE showing proposed changes and provide a summary table of the proposed changes.

If you have any questions, please contact Bill Macon at 301-415-3965.

Sincerely,

/RA/

Stephen Dembek, Chief, Section 2
Project Directorate IV
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Project No. 700

Enclosure: Draft Safety Evaluation

cc w/encl: See next page

September 3, 2004

Mr. James A. Gresham, Manager
Regulatory and Licensing Engineering
Westinghouse Electric Company
P.O. Box 355
Pittsburgh, PA 15230-0355

SUBJECT: DRAFT SAFETY EVALUATION FOR TOPICAL REPORT WCAP-16096-NP-A, REVISION 1, "SOFTWARE PROGRAM MANUAL FOR COMMON Q SYSTEMS" (TAC NO. MC2294)

Dear Mr. Gresham:

On January 29, 2004, Westinghouse Electric Company (Westinghouse) submitted Topical Report (TR) WCAP-16069-NP-A, Revision 1, "Software Program Manual for Common Q Systems," to the staff for review. Enclosed for Westinghouse's review and comment is a copy of the staff's draft safety evaluation (SE) for the TR.

Twenty working days are provided to you to comment on any factual errors or clarity concerns contained in the SE. The final SE will be issued after making any necessary changes and will be made publicly available. The staff's disposition of your comments on the draft SE will be discussed in the final SE.

To facilitate the staff's review of your comments, please provide a marked-up copy of the draft SE showing proposed changes and provide a summary table of the proposed changes.

If you have any questions, please contact Bill Macon at 301-415-3965.

Sincerely,
/RA/
Stephen Dembek, Chief, Section 2
Project Directorate IV
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Project No. 700

Enclosure: Draft Safety Evaluation

cc w/encl: See next page

DISTRIBUTION:
PUBLIC
PDIV-2 Reading
RidsNrrDlpmLpdiv (HBerkow)
RidsNrrWMacon
RidsNrrLAEPeyton
RidsOgcRp
RidsAcrsAcnwMailCenter
EMarinos

ADAMS Accession No.: ML042510034 NRR-106

OFFICE	PDIV-2/PM	PDIV-2/LA	EEIB-A/SC*	PDIV-2/SC
NAME	WMacon	EPeyton	EMarinos	SDembek
DATE	9/3/04	9/3/04	8/25/04	9/3/04

DOCUMENT NAME: C:\ORPCheckout\FileNET\ML042510034.wpd
OFFICIAL RECORD COPY

***SE dated**

cc:
Mr. Gordon Bischoff, Manager
Owners Group Program Management Office
Westinghouse Electric Company
P.O. Box 355
Pittsburgh, PA 15230-0355

DRAFT SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

TOPICAL REPORT WCAP-16096-NP-A, REVISION 1

"SOFTWARE PROGRAM MANUAL FOR COMMON Q SYSTEMS"

WESTINGHOUSE ELECTRIC COMPANY

PROJECT NO. 700

1.0 INTRODUCTION

By letter dated January 29, 2004 (ADAMS Accession Number ML040360115), Westinghouse Electric Company (Westinghouse) submitted Topical Report (TR) WCAP-16069-NP-A, Revision 1, "Software Program Manual for Common Q Systems," to the NRC for review.

Two previous versions of this Software Program Manual (SPM) have been submitted and reviewed. The original version was submitted by CE Nuclear Power on June 5, 2000 (ADAMS Accession Number ML003722925), as a part of CENPD-396-P, Revision 1, "Common Qualified Platform." This TR and the SPM were approved in a safety evaluation (SE) dated August 11, 2000 (ADAMS Accession Number ML003740165). When Westinghouse acquired the Common Qualified (Common Q) platform product line, an updated version of the SPM was submitted on August 14, 2002 (ADAMS Accession Number ML003721618), as WCAP-16096-NP-A, Revision 0. This TR was approved in a SE dated February 24, 2003 (ADAMS Accession Number ML030550776).

WCAP-16096-NP-A, Revision 1 specifies plans for implementing a structured software life cycle process for application software and provides guidance for configuration management of commercial-grade hardware and previously-developed software.

2.0 REGULATORY EVALUATION

The basic review criteria for the evaluation of the changes to the SPM is that the changes do not compromise the characteristics of the Common Q platform that were critical to its acceptability in the initial SE. Therefore, the review criteria for the changes are essentially all of the criteria that applied to the previously approved the Common Q platform. These criteria are identified in Section 3.1, "Review Criteria," in the initial SE dated August 11, 2000. Since this SPM has been previously approved, this SE will only evaluate the changes to ensure that they continue to meet these criteria. For this review, the staff has determined that the following subset of regulatory guides (RG) and standards applies to the acceptability of the changes:

- RG 1.152-1996, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants" (which endorses the Institute of Electrical and Electronic Engineers (IEEE) Standard (Std) 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations").

- RG 1.168-1997, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (which endorses the American National Standards Institute (ANSI)/IEEE Std 1012, "IEEE Standard for Software Verification and Validation Plans," and IEEE Std 1028, "IEEE Standard for Software Reviews and Audits").

- RG 1.170-1997, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (which endorses IEEE Std 829, "IEEE Standard for Software Test Documentation").

- RG 1.171-1997, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (which endorses ANSI/IEEE Std 1008, "IEEE Standard for Software Unit Testing").

- RG 1.173-1997, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (which endorses IEEE Std 1074, "IEEE Standard for Developing Software Life Cycle Processes").

3.0 TECHNICAL EVALUATION

The Westinghouse SPM for Common Q systems specifies plans for implementing a structured software life cycle process for application software and provides guidance for configuration management of commercial-grade hardware and previously developed software. As stated in the initial SE, licensees using the Common Q platform for plant-specific applications are required to implement the application software in accordance with the SPM. As stated above in this SE, the staff has already reviewed the SPM twice before; therefore, this SE will only evaluate the changes to ensure that they continue to meet the applicable review criteria.

Westinghouse has stated that the SPM was modified for the following reasons:

- To ensure consistency with updated Westinghouse Repair, Replacement and Automation Services (RRAS) quality program requirements and to meet the RRAS documentation standards.

- Experience with the Palo Verde Core Protection Calculator System (CPCS).

- Implemented changes based on NRC review and audit experience.

- Corrected errors and inconsistencies discovered during early experience with Common Q projects.

- To correct typographical errors and to clarify some of the process descriptions.

3.1 Changes Based on RRAS Program Requirements

These changes are primarily format changes. The acronym section, definitions section, and references section were moved to different locations. References to the ABB Quality Assurance Manual were removed, and some definitions were added or modified. The title of

"V&V Team Leader" was replaced with "V&V Engineering Line Manager;" however, the administrative and financially independence from the design team manager was not changed. The other change was to show that the Quality organization is responsible for auditing the software safety plan implementation and performing process certification rather than the verification and validation (V&V) team and that the results of the audit are documented in the Quality organization's Audit Report. These changes do not compromise the characteristics that were critical in the initial SE to meet the review criteria, and are, therefore, acceptable.

3.2 Changes Based on Palo Verde CPCS Experience

These changes are to provide clarification rather than to make substantive changes. The first change is to provide clarification that the independent managerial review to assess the execution of all of the actions and the items identified in the Software Quality Assurance Plan (SQAP) that is included in the SPM, as required by IEEE Std 730, is the responsibility of the Quality organization. The second change is to provide clarification that the requirements for the hardware design process are defined in the Westinghouse Policy and Procedures Manual and that hardware verification is performed as part of the hardware quality assurance activities, which is also defined in the Westinghouse Policy and Procedures Manual.

These changes do not compromise the characteristics that were critical in the initial SE to meet the review criteria, and are, therefore, acceptable.

3.3 Changes Based on NRC Review and Audit Experience

These changes provide clarification of items based on comments and observations during staff reviews, rather than to make substantive changes.

These changes provide a clearer definition of responsible groups and organizational structure, such as the responsibilities of the V&V Group, the Software Librarian and the Automation Engineering groups. In addition, the Requirements Traceability Analysis, Requirements Traceability Matrix, and the documentation requirements are better defined.

These changes do not compromise the characteristics that were critical in the initial SE to meet the review criteria, and are, therefore, acceptable.

3.4 Changes to Implemented Design Process Improvements and Corrected Errors and Inconsistencies Based on Early Experience with Common Q Projects

There are a number of minor changes to the SPM which further clarify or modify the software processes. Some of these changes are as follows:

- Define when software will be entered into a controlled access account.
- State that the results of physical reviews shall be documented with a Certificate of Conformance.
- Add a statement that non-commercial software (freeware) cannot be used for Protection Class Software.

- Add a statement that the coding standards to be applied to a project shall be referenced in the Project Quality Plan, and that the V&V team shall review the applicable coding standards for each project for acceptability.

- Consistently use "SDD" to mean Software Design Description rather than Software Design Document and "SCR" to mean Software Change Request rather than System Change Request.

- Require that Westinghouse personnel assigned to work on any activity in the software life cycle process must complete training on the SPM in accordance with the "NA Policy and Procedures Manual," and that the V&V team must review training materials prepared for the customer.

- Revise the statement so that in-process audits shall be performed by the Quality organization rather than the V&V team, and that these audits shall be documented in an audit report rather than the V&V report.

- Require that the Software quality assurance plan be required for all quality classifications defined for the Common Q system: protection, important-to-safety, important-to-availability, and general purpose software, not just software "within the scope of Westinghouse software."

- Revise the responsibilities within the SPM so that:

    1. Verification of the implementation of quality assurance requirements is performed by the Quality organization, and that the V&V Team Leader shall verify that software and associated documentation has been developed in accordance with the standards specified in the SQAP.

    2. The responsibility for performing the Physical Review is moved from the V&V team to the design team.

    3. Stating that the Preliminary Hazards Analysis Report can be either completed by the V&V team or completed by the design team and reviewed by the V&V team.

There are a number of other minor changes to terminology, documentation requirements and processes, Westinghouse standard forms, and dates on references and standards. The staff has reviewed these changes, and has determined that these changes are minor, and do not alter the SPM in a significant manner.

These changes do not compromise the characteristics that were critical in the initial SE to meet the review criteria, and are, therefore, acceptable.

3.5 Changes to Correct Typographical Errors and to Clarify Some of the Process Descriptions

These changes are being made to correct some errors in the original document, and to provide clarification of some process descriptions. The staff has reviewed these changes, and has

determined that these changes are minor, and do not alter the SPM in a significant manner. Since these changes do not compromise the characteristics that were critical in the initial SE to meet the review criteria, they are acceptable.

4.0 CONCLUSION

On the basis of this review, the staff has determined that the proposed changes to the Westinghouse SPM for Common Q systems continue to meet the applicable review criteria and do not compromise any of the characteristics that were critical in the initial SE. Therefore, the changes in WCAP-16096-NP-A, Revision 1, are acceptable.

Principal Contributor: P. Loeser, NRR

Date: September 3, 2004