

June 22, 2001

Mr. H. A. Sepp, Manager
Regulatory and Licensing Engineering
Westinghouse Electric Company
Energy Center Complex
Northern Pike
Monroville, PA 15146

SUBJECT: SAFETY EVALUATION FOR THE CLOSEOUT OF SEVERAL OF THE
COMMON QUALIFIED PLATFORM CATEGORY 1 OPEN ITEMS RELATED
TO REPORTS CENPD-396-P, REVISION 1, AND CE-CES-195, REVISION 1
(TAC NO. MB0780)

Dear Mr. Sepp:

On August 11, 2000, the staff issued a Safety Evaluation (SE) regarding Topical Reports (TRs) CENPD-396-P, Rev. 01, "Common Qualified Platform" and its Appendices 1, 2, 3 and 4, Revision 1, and CE-CES-195, Revision 1, "Software Program Manual for Common Q Systems." The SE identified (1) 14 plant specific action items (PSAI) requiring the licensee's attention when implementing the Common Qualified Platform (Common Q) design, and (2) 10 generic open items (GOI).

By letter dated May 11, 2001, Westinghouse Electric Company LLC (Westinghouse) submitted: (1) "Westinghouse Nuclear Automation Strategy for the Closeout of the Common Qualified Platform Category 1 Open Items," and (2) "Common Qualified Platform Integrated Solution CENPD-396, Appendix 4, Revision 2, April 2001," for evaluation by the NRC staff. Westinghouse stated that it submitted both proprietary and non-proprietary versions of each document to closeout GOI 7.4, 7.7, 7.9, and 7.10 and provide clarification to PSAI 6.3, 6.11 and 6.14.

By letter dated June 4, 2001, Westinghouse submitted a revised non-proprietary version of "Westinghouse Nuclear Automation Strategy for the Closeout of the Common Qualified Platform Category 1 Open Items," that replaced the May 11, 2001, letter. The June 4, 2001, letter contained the same information as the May 11, 2001, letter only less information was designated as proprietary. By letter dated June 7, 2001, Westinghouse submitted "Westinghouse Nuclear Automation Basis for Change to CENPD-396-P, Appendix 3, "Common Qualified Platform, Digital Plant Protection System," that provided supplemental information for closing PSAI 6.3.

The staff has found that the closeout of the Category 1 open items are acceptable for referencing in licensing applications to the extent specified and under the limitations delineated in the reports and in the enclosed SE. The SE defines the basis for acceptance of the reports.

Pursuant to 10 CFR 2.790, we have determined that the enclosed SE does not contain proprietary information. However, we will delay placing the SE in the public document room for a period of ten working days from the date of this letter to provide you with the opportunity to comment on the proprietary aspects only. If you believe that any information in the enclosure is

proprietary, please identify such information line by line and define the basis pursuant to the criteria of 10 CFR 2.790.

When the subject reports are referenced in plant-specific license applications, we do not intend to review the matters described in the reports and found acceptable, except to ensure that the material presented in the application applies to the specific plant involved.

In accordance with procedures established in NUREG-0390, the NRC requests that an accepted version be published within 3 months of receipt of this letter. The accepted version shall incorporate (1) this letter and the enclosed SE between the title page and the abstract, and (2) an "-A" (designating "accepted") following the report identification symbol.

Should our criteria or regulations change so that our conclusions as to the acceptability of the report are invalidated, Westinghouse and/or the applicants referencing the TR will be expected to revise and resubmit their respective documentation, or submit justification for the continued applicability of the TR without revision of their respective documentation.

Sincerely,

/RA/

Stuart A. Richards, Director
Project Directorate IV
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Project No. 692

Enclosure: Safety Evaluation

cc w/encl: See next page

proprietary, please identify such information line by line and define the basis pursuant to the criteria of 10 CFR 2.790.

When the subject reports are referenced in plant-specific license applications, we do not intend to review the matters described in the reports and found acceptable, except to ensure that the material presented in the application applies to the specific plant involved.

In accordance with procedures established in NUREG-0390, the NRC requests that an accepted version be published within 3 months of receipt of this letter. The accepted version shall incorporate (1) this letter and the enclosed SE between the title page and the abstract, and (2) an "-A" (designating "accepted") following the report identification symbol.

Should our criteria or regulations change so that our conclusions as to the acceptability of the report are invalidated, Westinghouse and/or the applicants referencing the TR will be expected to revise and resubmit their respective documentation, or submit justification for the continued applicability of the TR without revision of their respective documentation.

Sincerely,
/RA/
Stuart A. Richards, Director
Project Directorate IV
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Project No. 700

Enclosure: Safety Evaluation

cc w/encl: See next page

DISTRIBUTION:

PUBLIC
PDIV-2 Reading
SRichards (RidsNrrDlpmLpdiv)
JCushing (RidsNrrPMJCushing)
EPeyton (RidsNrrLAEPeyton)
JCalvo
EMarinos
WKMortensen

RidsOgcRp
RidsAcrcAcnwMailCenter

Accession No.: ML011690170

* See Memo dated June 14, 2001

OFFICE	PDIV-2/PM	PDIV-2/LA	EEIB/SC	PDIV-2/SC	PDIV-2/PD
NAME	JDonohew for:JCushing:am	EPeyton	EMarinos*	SDembek	SRichards
DATE	6/22/01	6/22/01	06/14/01	6/22/01	6/22/01

CE Owners Group

Project No. 692

cc:

Mr. Gordon C. Bischoff, Project Director
CE Owners Group
Westinghouse Electric Company
CE Nuclear Power, LLC
M.S. 9615-1932
2000 Day Hill Road
Post Office Box 500
Windsor, CT 06095

Mr. Richard Bernier, Chairman
CE Owners Group
Mail Stop 7868
Arizona Public Service Company
Palo Verde Nuclear Generating Station
P.O. Box 52034
Phoenix, Arizona 85072-2034

Mr. Charles B. Brinkman, Manager
Washington Operations
Westinghouse Electric Company
CE Nuclear Power, LLC
12300 Twinbrook Parkway, Suite 330
Rockville, MD 20852

Mr. Virgil Paggen
CE Nuclear Power LLC
M. S. 9383-1922
2000 Day Hill Road
Windsor, CT 06095-1922

Mr. Philip W. Richardson, Manager
Windsor Nuclear Licensing
Westinghouse Electric Company
CE Nuclear Power, LLC
P.O. Box 500
2000 Day Hill Road
Windsor, CT 06095-0500

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION
RELATED TO THE CLOSEOUT
OF SEVERAL OF THE COMMON QUALIFIED PLATFORM CATEGORY 1 OPEN ITEMS
PROJECT NO. 692

1.0 INTRODUCTION

On August 11, 2000, the staff issued a Safety Evaluation (SE) regarding Topical Report (TR) CENPD-396-P, Rev. 01, "Common Qualified Platform" and its Appendices 1, 2, 3 and 4, Rev. 01 and CE-CES-195, Rev. 01, "Software Program Manual for Common Q Systems." These TRs are for the Common Qualified Platform (Common Q) for use in digital upgrades in nuclear power plants. The SE dated August 11, 2000, included the identification of (1) 14 plant specific action items (PSAI) requiring the licensee's attention when implementing the Common Qualified Platform (Common Q) design, and (2) 10 generic open items (GOI).

In its letter dated May 11, 2001, Westinghouse Electric Company LLC (Westinghouse) submitted: (1) "Westinghouse Nuclear Automation Strategy for the Closeout of the Common Qualified Platform Category 1 Open Items," and (2) "Common Qualified Platform Integrated Solution CENPD-396, Appendix 4, Revision 2, April 2001," for evaluation by the NRC staff. Westinghouse stated that it submitted both proprietary and non-proprietary versions of each document to close GOI 7.4, 7.7, 7.9, and 7.10 and provide clarification to PSAI 6.3, 6.11 and 6.14, in the SE dated August 11, 2000.

By letter dated June 4, 2001, Westinghouse submitted a revised non-proprietary version of "Westinghouse Nuclear Automation Strategy for the Closeout of the Common Qualified Platform Category 1 Open Items," that replaced the May 11, 2001, letter. The June 4, 2001, letter contained the same information as the May 11, 2001, letter only less information was designated as proprietary.

By letter dated June 7, 2001, Westinghouse submitted an addendum to CENPD-396-P, Appendix 3, "Common Qualified Platform, Digital Plant Protection System," with additional proprietary information for insertion into the Digital Plant Protection System (DPPS) failure mode and effects analysis (FMEA) regarding the failure of the flat panel display system (FPDS) that provided supplemental information for closing PSAI 6.3.

2.0 EVALUATION

The staff's evaluation of the seven GOI and PSAI listed above are given below.

Generic Open Item 7.4

GOI 7.4 as stated in the SE dated August 11, 2000:

CENP has committed to arrange a value-added reseller agreement with QSSL that is similar to BA AUT-99-ADVANT-00, the value-added reseller agreement it has with ABB Products. A value-added reseller agreement is needed to satisfy the configuration control and incoming inspection requirements of EPRI TR-106439. The staff's review of the value-added reseller agreement with QSSL is discussed in Section 4.2.1.2.

The staff has reviewed the value-added reseller agreement with QNX Software Systems Limited (QSSL), the vendor for the FPDS operating system and display system and concludes that it satisfies the configuration control and incoming inspection guidance of EPRI TR-106439 and is, therefore, acceptable. This closes GOI 7.4.

Generic Open Item 7.7

GOI 7.7 as stated in the SE dated August 11, 2000:

The staff has reviewed the information in the SVVP about software module testing and finds that the information provided is not sufficient for the staff to arrive at a conclusion about the adequacy of the scope of the tests for validating a software module. The staff's review of this information is discussed in Section 4.3.1.j.

Westinghouse submitted additional information indicating in which sections of CE-CES-195, Rev. 01, "Software Program Manual for Common Q Systems", and TR CENPD-396-P, Rev. 1, "Common Qualified Platform," the staff would find the Westinghouse Nuclear Automation (WNA) procedures for performing software module testing. The staff has reviewed the indicated sections and concludes that the procedures specified therein satisfy the software verification and validation program (SVVP) requirements of IEEE Std 7-4.3.2-1993 with regard to testing of software modules and are, therefore, acceptable. This closes GOI 7.7.

Generic Open Item 7.9

GOI 7.9 as stated in the SE dated August 11, 2000:

The staff has reviewed the approach for the integrated solution of using the ITPs and the AF100 buses to provide separation of safety and non-safety signals and finds that there is not sufficient detail to permit an evaluation against the independence requirements set forth in IEEE Std 7-4.3.2. This must be the subject of a future CENP submittal. This is discussed in Section 4.4.4.3.4.

Westinghouse has revised Appendix 4, "Common Qualified Platform Integrated Solution," to provide additional information on the use of the interface and test processors (ITPs) and the AF100 buses to provide separation of safety and non-safety signals. The staff has reviewed the revised information in Appendix 4, Rev. 2 on the use of the ITPs and the AF100 buses to provide separation of safety and non-safety signals and finds that the conceptual approach as

presented therein is consistent with the independence requirements set forth in IEEE Std 7-4.3.2. The staff, therefore, concludes that this conceptual approach may be used for guidance for the anticipated application-specific and plant-specific designs involving the integration of multiple Common Q digital instrumentation and control (I&C) upgrades. This closes GOI 7.9 as far as the conceptual approach is concerned, but the evaluation of each forthcoming design remains a PSAI because the staff finds that the forthcoming details of the actual designs may require an evaluation against the independence requirements for safety systems in specific nuclear power plants.

Generic Open Item 7.10

GOI 7.10 as stated in the SE dated August 11, 2000:

The evaluation of the design for the multichannel operator station control for the integrated solution requires detail beyond the scope of the present submittals. This is discussed in Section 4.4.4.3.5.

Westinghouse has revised Appendix 4 to provide additional information on the multichannel operator station control. Westinghouse does not intend that Appendix 4, Rev. 2 should contain sufficient detail to permit the staff to evaluate any plant-specific multiple upgrade. However, Westinghouse requests that the staff evaluate the concept of the multichannel operator station with regard to potential adverse multichannel interaction. Accordingly, the staff has reviewed the design concepts as presented in Appendix 4, Rev. 2, and finds the following.

The multichannel operator stations can control most Class 1E components directly and use the ITPs and the AF100 buses discussed in GOI 7.9 above, to provide separation of safety and non-safety signals. The WNA design provides that Class 1E control signals will override any erroneous signal that may originate from non-safety equipment. Where there are no overriding Class 1E control signals, manual release switches are used in conjunction with the multichannel operator station.

In the Integrated Solution concept, Class 1E devices within each safety division provide backups to the non-safety multichannel operator stations. One variation of the non-safety multichannel operator station design is the compact workstation (CW) to be used in control rooms for the Integrated Solution. In the CW design, the multichannel operator stations are part of the safety system. They utilize the Common Q FPDS which the staff has approved as a Class 1E HMI device, subject to its successful performance during qualification testing that is scheduled for this summer. Westinghouse has determined that each CW console meets all qualification and single failure requirements for display and control of Class 1E functions. As a result, the channelized operator modules and channelized post accident monitoring instrumentation (PAMI) and safe shutdown displays (SSD), which serve as credited backup HMI devices for the non-safety multichannel operator station design, would not be required in the CW version of the implementation of the multichannel operator station.

The staff has reviewed the revised information in Appendix 4, Rev. 2 with regards to the use of the multichannel operator station including the Integrated Solution CW variation and finds the conceptual approach to be free of potential for adverse multichannel interaction and is consistent with the Class 1E independence requirements set forth in IEEE Std 7-4.3.2. The staff, therefore, concludes that the conceptual approach employing multichannel operator stations may be used for guidance for the anticipated application-specific and plant-specific designs involving the integration of multiple Common Q digital I&C upgrades. This closes GOI 7.10 as far as the conceptual approach is concerned, but the evaluation of each forthcoming design remains a PSAI because the staff finds that the forthcoming details of the actual designs may require an evaluation against the independence requirements for safety systems in specific nuclear power plants.

Plant-Specific Action Item 6.3

PSAI 6.3 as stated in the SE dated August 11, 2000:

If a licensee installs a Common Q application that encompasses the implementation of FPDS, the licensee must verify that the FPDS is limited to performing display and maintenance functions only, and is not to be used such that is required to be operational when the Common Q system is called upon to initiate automatic safety functions. The use of the FPDS must be treated in the plant-specific FMEAs. See Section 4.2.1.2.

A previously unresolved QSSL software error report is discussed in Section 4.2.1.2 of the SE. QSSL, the vendor for the operating system in the FPDS, has resolved this error report and the staff has reviewed the resolution report. The staff concludes that the error report has been satisfactorily resolved.

The FPDS does not execute protection algorithms in the safety-related applications. Should the FPDS fail for any reason, its failure will be electrically isolated from the processors executing the protection algorithms. The protection algorithms can continue to execute their intended functions independent of the FPDS failure. On the basis of its evaluation of the Common Q submittals previously evaluated and based on the above findings, the staff concludes that the FPDS software operating systems are acceptable for use in the Class 1E operators module and Class 1E maintenance and test panel in Common Q digital upgrades. Therefore, based on the foregoing, the staff finds that PSAI 6.3 has been resolved and is therefore closed.

However, an evaluation of the human factors considerations remains as PSAI 6.7.

Based on its review of the addendum to the FMEA for Appendix 3 and its previous review of the model FMEAs in Appendices 1, 2, and 3, the staff concludes that a similar approach may be used by a licensee implementing a Common Q design when preparing its plant-specific FMEAs covered by PSAI 6.10.

Plant-Specific Action Item 6.11

PSAI 6.11 as stated in the SE dated August 11, 2000:

If a licensee installs a Common Q PAMS, CPCS, DPPS or Integrated Solution, the licensee shall demonstrate that the plant-specific Common Q application complies with the criteria for defense against common-mode failure in digital instrumentation and control systems and meets the DID&D requirements of HICB BTP-19. See Sections 4.1.6, 4.4.2.3, 4.4.3.3, 4.4.4.3.3, and 5.0.

Westinghouse has revised the Common Qualified Platform Integrated Solution, Appendix 4, Section A4.5.3 to address this topic. Appendix 4, Rev. 2, now provides the basis for a strategy of using the Integrated Solution as the model for a modernization project and performing a plant-specific diversity and defense-in-depth (DID&D) assessment that addresses the plant as it will be after the implementation of all of the planned digital upgrades. Westinghouse proposes that a licensee that plans to implement Common Q digital upgrades in phases over a series of planned outages could submit a one-time, plant-specific, bounding analysis that assumes a simultaneous common-mode failure in all of the licensee's planned Common Q digital upgrades. This one-time analysis would then be applicable for each phase of a system-by-system phased upgrade. For each phase the licensee would confirm by additional analysis as needed, that the diverse equipment credited in the bounding analysis remains available. The staff finds the foregoing plan for the implementation on a one-time, plant-specific, bounding DID&D analysis to be acceptable.

Plant-Specific Action Item 6.14

PSAI 6.14 as stated in the SE dated August 11, 2000:

The licensee must ascertain that the implementation of the Common Q does not render invalid any of the previously accomplished TMI action items. See Section 5.0.

Westinghouse asked the staff to explain why the TMI actions appear to receive more emphasis than other design basis items. They asked the staff if there were special actions required by the licensees to meet the staff's expectations with regard to TMI action items when implementing digital upgrades.

The staff answered that there was no intent to elevate the importance of TMI action items over the importance of the General Design Criteria (GDCs), Appendix A of 10 CFR Part 50, or any design-basis items, nor has the staff identified any special actions required by the licensees to meet the staff's expectations with regard to TMI action items. The staff uses Chapter 7 of the Standard Review Plan (SRP) (NUREG-0800), for guidance when evaluating plant safety systems. The TMI action plan requirements are treated individually in the SRP and are found to require 10 rows in SRP Table 7-1, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems," whereas the long-established GDCs receive only one row each. Licensees may anticipate that these 10 points relating to TMI might get individual attention in the submittals the staff reviews regarding digital upgrades. However, the licensee must ascertain that the implementation of a Common Q digital replacement does not render invalid any of the plant's previously accomplished protection or safety functions, TMI-related or otherwise.

The staff has no changes to PSAI 6.14.

3.0 CONCLUSIONS

The staff has concluded that GOI 7.4 and 7.7 have been fully resolved. The staff considers that GOI 7.9 and 7.10 have been resolved with regard to the acceptability of the design concept, however, the review of the details of these future designs remain as system-specific generic reviews or as plant-specific considerations.

PSAI 6.3 has been resolved generically and may be closed as a requirement in the SE. In connection with its resolution, the staff also found that the FPDS, subject to its successful performance during scheduled qualification testing, to be acceptable for use in Common Q designs as a Class 1E HMI device.

With regard to PSAI 6.11, the staff concluded that the Westinghouse plan for the implementation of a one-time, plant-specific, bounding DID&D analysis for phased digital upgrades, accompanied by appropriate phase-specific analysis, is acceptable.

Principal Contributor: Keith Mortensen

Date: June 22, 2001