August 11, 2000

Mr. Philip Richardson
Nuclear Licensing
Westinghouse Electric Company
2000 Day Hill Road
Windsor, Connecticut 06095-0500

SUBJECT: ACCEPTANCE FOR REFERENCING OF TOPICAL REPORT CENPD-396-P, REV. 01, "COMMON QUALIFIED PLATFORM" AND APPENDICES 1, 2, 3 AND 4, REV. 01 (TAC NO. MA1677)

Dear Mr. Richardson:

We have concluded our review of the subject topical report and associated appendices submitted by CE Nuclear Power (CENP) by letter dated June 5, 2000. The appendices are:

Appendix 1, "Common Qualified Platform, Post Accident Monitoring System"
Appendix 2, "Common Qualified Platform, Core Protection Calculator System"
Appendix 3, "Common Qualified Platform, Digital Plant Protection System"
Appendix 4, "Common Qualified Platform, Integrated Solution"
CE-CES-195, Rev. 01, "Software Program Manual for Common Q Systems"

These submittals describe a nuclear safety-related instrumentation and controls (I&C) platform developed by CENP. CENP is proposing one common platform with a modular structure in which various components can be applied to nuclear safety-related applications, including component replacements and/or complete system upgrades. The appendices describe design approaches for implementing the platform into generic I&C systems at nuclear power plants and provide additional information to support the review of the generic design details for the Common Qualified (Common Q) platform. The Common Q platform consists of two parts: (1) the AC160 programmable logic controller (PLC) system, and (2) the non-AC160 hardware.

The staff accepts for referencing the AC160 PLC system portion of the report subject to the limitations specified in the report and in the associated NRC safety evaluation (SE), which is enclosed. The SE defines the basis of acceptance of the report. The CENP submittals do not include sufficient information on non-AC160 PLC hardware for the staff to complete its evaluation. CENP proposes to submit additional information during the coming year for the staff to complete its evaluation.

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 (10) 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.

We do not intend to repeat our review of the matters described in the report, and found acceptable, when the report appears as a reference in license applications, except to assure that the material presented is applicable to the specific plant involved. Our acceptance applies only to matters described in the report.

In accordance with procedures established in NUREG-0390, "Topical Report Review Status," we request that CE Nuclear Power publish accepted versions of this topical report, proprietary and non-proprietary, within three months of receipt of this letter. The accepted versions shall incorporate this letter and the enclosed SE between the title page and the abstract. It must be well indexed such that information is readily located. Also, it must contain in appendices historical review information, such as questions and accepted responses, and original report pages that were replaced. The accepted versions shall include 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, CE Nuclear Power and/or the applicants referencing the topical report will be expected to revise and resubmit their respective documentation, or submit justification for the continued applicability of the topical report without revision of their respective documentation.

Sincerely,

/RA by Stephen Dembek for/

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

Project No. 692

Enclosure: Safety Evaluation

cc w/encl:
Mr. Charles B. Brinkman, Manager
Washington Operations, CE Nuclear Power
12300 Twinbrook Parkway, Suite 330
Rockville, MD 20852

We do not intend to repeat our review of the matters described in the report, and found acceptable, when the report appears as a reference in license applications, except to assure that the material presented is applicable to the specific plant involved. Our acceptance applies only to matters described in the report.

In accordance with procedures established in NUREG-0390, "Topical Report Review Status," we request that CE Nuclear Power publish accepted versions of this topical report, proprietary and non-proprietary, within three months of receipt of this letter. The accepted versions shall incorporate this letter and the enclosed SE between the title page and the abstract. It must be well indexed such that information is readily located. Also, it must contain in appendices historical review information, such as questions and accepted responses, and original report pages that were replaced. The accepted versions shall include 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, CE Nuclear Power and/or the applicants referencing the topical report will be expected to revise and resubmit their respective documentation, or submit justification for the continued applicability of the topical report without revision of their respective documentation.

Sincerely,
/RA by Stephen Dembek for/
Stuart A. Richards, Director
Project Directorate IV & Decommissioning
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Project No. 692

Enclosure: Safety Evaluation

cc w/encl:
Mr. Charles B. Brinkman, Manager
Washington Operations, CE Nuclear Power
12300 Twinbrook Parkway, Suite 330
Rockville, MD 20852

DISTRIBUTION:
PUBLIC
PDIV-2 Reading
SRichards (RidsNrrDlpmLpdiv)
JCushing (RidsNrrPMJCushing)
EPeyton (RidsNrrLAEPeyton)
OGC (RidsOgcMailCenter)
ACRS (RidsAcrsAcnewMailCenter)
JCalvo
KMortensen

Accession No. ML003740165

OFFICE	PDIV-2/PM	PDIV-2/LA	PDIV-2/SC	PDIV/D
NAME	JCushing	EPeyton	SDembek	SDembek for SRichards
DATE	08/11/00	08/11/00	08/11/00	08/11/00

OFFICIAL RECORD COPY

TABLE OF CONTENTS FOR COMMON Q SAFETY EVALUATION

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

CE NUCLEAR POWER TOPICAL REPORT CENPD-396-P

"COMMON QUALIFIED PLATFORM"

PROJECT NO. 692

SUMMARY

By letter dated June 5, 2000, CE Nuclear Power (CENP) (formerly ABB Nuclear Automation) submitted Topical Report CENPD-396-P, Rev. 1, "Common Qualified Platform," to the NRC for review. This safety evaluation (SE) provides the results of the NRC staff's review of the CENP topical report, the accompanying appendices, and other supporting documents. Based on the information provided and the review conducted, the staff concludes that the design of the Common Qualified (Common Q) platform meets the relevant NRC regulatory requirements and is acceptable for safety-related instrumentation and control (I&C) applications in nuclear power plants, subject to the satisfactory resolution of the generic open items listed in Section 7.0 of this SE.

The Common Q platform is a computer system consisting of a set of commercial-grade hardware and previously developed software components dedicated and qualified for use in nuclear power plants. The Common Q platform was developed by CENP from the standard AC 160 computer system developed by ABB Automation Products, GmbH (ABB Products) of Europe. The Common Q platform is to be loaded with plant-specific application software to implement various nuclear plant safety system applications. The hardware components of the platform are:

- Advant Controller 160 (AC160) with PM646 or PM645C processor modules
- S600 input and output (S600 I/O) modules
- Bus communication interface (CI631) modules
- Power supply modules
- Watchdog timer module
- Communication systems
- Flat-panel display system (FPDS)

The AC 160 software, residing on flash PROM in the processor module, consists of a real-time operating system, task scheduler, diagnostic functions, communication interfaces and plant specific application programs. The application program is created using the Asea Brown Boveri (ABB) Master Programming Language (AMPL) Control Configuration (ACC) software development environment that includes a function block library for creating specific logic for the application.

The safety-related I&C systems based on the application of Common Q platforms provide protection against unsafe reactor operation during steady-state and transient power operations. They also initiate selected protective functions to mitigate the consequences of design-basis events and accidents, and to safely shut down the plant by either automatic means or manual actions.

To ensure that the digital I&C systems are implemented properly, the staff considered regulatory requirements, technical positions, guides, and standards in the Standard Review Plan (SRP), (NUREG-0800) Chapter 7, Revision 4, June 1997, in the review of the Common Q platform design.

CENP's "Software Program Manual for Common Q Systems" (SPM) 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. Since the application software has not yet been developed, the staff's evaluation does not include the review of the outputs of the life cycle process, but is limited to the evaluation of the specified process. The staff finds the software program manual acceptable dependent upon the resolution of an open item related to the scope of module testing. Licensees using the Common Q platform for plant-specific applications will be required to implement the application software in accordance with CENP's software program manual.

As regards to the commercial dedication of the Common Q platform, including the previously developed software and tools, CENP conducted a quality evaluation of the AC160 programmable logic controller (PLC) system planned to be used in implementing the safety functions of the reactor protection system for the Oskarshamn Modernization Project in Sweden. The staff finds that the AC160 system planned for the Oskarshamn Modernization Project is the same as that which will be used for the Common Q system, and the quality evaluation done for the Oskarshamn Modernization Project is applicable to the commercial-grade dedication of the Common Q system. The safety-grade application at Oskarshamn is equivalent to Class 1E.

The AC160 PLC system equipment qualification included temperature and humidity tests, seismic tests, and electromagnetic interference/radio frequency interference (EMI/RFI) qualification. These tests passed successfully, except for the EMI/RFI tests on the AC160 system modules. CENP indicated that it will perform additional EMI/RFI tests on the AC160 modules in the future. The staff finds this commitment acceptable and it is documented in Section 7.0 as Open Item 7.5.

CENP has indicated that it will provide additional information regarding the design details and qualification activities of certain Common Q platform hardware items such as the flat panel display system, watchdog timer module, and power supplies. The review of this additional information is documented in Section 7.0 as Open Item 7.6.

Common-mode failures in digital systems and defense-in-depth were the subject of SECY-91-292. Positions addressing those concerns were established and documented in Chapter 7 of the NRC SRP, "Instrumentation and Controls," Branch Technical Position (BTP) HICB-19. BTP HICB-19 identified two criteria for defense against common-mode and common-cause failures: quality and diversity. Maintaining high quality increases the reliability of both

individual components and complete systems. The staff has reviewed the commercial-grade dedication of the Common Q platform and has determined that the Common Q platform has the required quality upon the satisfactory resolution of the outstanding open items. The quality of the plant-specific Common Q system is dependent on the licensee's proper implementation of the CENP software program manual and the resolution of plant-specific items in Section 6.0 of this SE.

In regard to defense-in-depth and diversity (D-in-D&D), the staff has established acceptance guidelines for D-in-D&D assessment and has identified four echelons of defense against common-mode failures: control systems, the reactor trip system, the engineered safety feature actuation system, and the monitoring and indication system. These guidelines are given in BTP HICB-19. The generic methodology proposed by CENP follows the guidance in BTP HICB-19. Applications correctly following this methodology for a plant-specific D-in-D&D assessment will be found acceptable.

The Common Q design is intended to provide a qualified generic digital I&C platform that meets the regulatory requirements and that can be used for a wide range of plant-specific applications. When using this platform for any plant-specific application, the licensee or applicant must verify that the qualification details in this topical report meet the plant license requirements. Because this topical report is for a generic platform, licensees referencing this topical report must describe in detail how they propose to use the Common Q design in plant-specific applications and must address all plant-specific interface items, including those listed in Section 6.0 of this SE.

1.0 INTRODUCTION

By letter dated March 5, 1999, CE Nuclear Power (CENP) (formerly ABB Nuclear Automation) submitted a proprietary topical report and a non-proprietary software program manual for NRC staff review:

- CENPD-396-P, Rev. 00, "Common Qualified Platform"
- CE-CES-195, Rev. 00, "Software Program Manual for Common Q Systems"

By the four letters listed below, CENP submitted five additional proprietary documents for staff review:

- CENPD-396-P, Appendix 1, "Common Qualified Platform Post-Accident Monitoring System" (by letter dated May 10, 1999)
- CENPD-396-P, Appendix 2, "Common Qualified Platform Core Protection Calculator System" (by letter dated June 2, 1999)
- CENPD-396-P, Appendix 3, "Common Qualified Platform Digital Plant Protection System" (by letter dated July 9, 1999)
- CENPD-396-P, Appendix 4, "Common Qualified Platform Integrated Solution" (by letter dated July 2, 1999)

CENP also submitted by letter dated July 2, 1999 a proprietary document entitled "EPRI TR-107330 Generic PLC Requirements." This document is a compliance matrix that CENP developed to compare the capabilities of the Common Qualified platform (Common Q) with the

requirements and acceptance criteria identified in the Electric Power Research Institute (EPRI) report EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants."

By letter dated November 29, 1999, CENP submitted nonproprietary versions of the topical report and four appendices.

By letter dated June 5, 2000, CENP submitted Revision 01 for the proprietary and nonproprietary versions of the topical report and the four appendices and for the nonproprietary SPM. Revision 01 incorporated staff comments and is the version of the topical report that is the subject of this SE.

Revision 01 describes a nuclear safety-related instrumentation and controls (I&C) platform developed by CENP. CENP is proposing one common platform with a modular structure in which various components can be applied to nuclear safety-related applications, including component replacements and/or complete system upgrades. The appendices describe design approaches for implementing the platform into generic I&C systems at nuclear power plants and provide additional information to support the review of the generic design details for the Common Q platform.

The staff made several visits to the CENP sites in Windsor, Connecticut and Rockville, Maryland. During the site visits, the staff inspected CENP procedures that are referenced in the topical report and audited reports of commercial-grade dedication activities. During one site visit to Windsor, Connecticut, the staff saw a representative Common Q system in operation and inspected the hardware. The staff requested that CENP submit six of the reports regarding commercial-grade dedication activities that the staff had audited to be placed on the docket. By letter dated June 20, 2000, CENP submitted the six proprietary reports:

- 2008677-IC-TR560-10, Rev. 00, dated September 24, 1999, "Seismic Qualification Test Report for Common Q Applications"
- 2008677-IC-TR560-11, Rev. 00, dated September 24, 1999, "Environmental Test Report for Module Equipment Qualification for Common Q Applications"
- 2008677-IC-TR560-12, Rev. 00, dated October 8, 1999, "EMI Qualification Test Report for Module Equipment Qualification for Common Q Applications"
- 00000-ICE-37722, Rev 00, dated November 11, 1999, "Commercial Grade Dedication Report for the QNX Operating System for Common Q Applications"
- GWK F 700 778, Rev. 01, dated February 18, 2000, "Generic Operating History Evaluation Report on Previously-Developed Software in ABB AC160, I/O Modules and Tool Software"
- GWK F 700 777, Rev. 02, dated February 22, 2000, "Design and Life Cycle Evaluation Report on Previously-Developed Software in ABB AC160, I/O Modules and Tool Software"

By letter dated June 28, 2000, CENP submitted thirteen missing pages that the staff discovered had been omitted from some of the above reports. This completes the reports.

In addition, public meetings were held between CENP and the staff to discuss various aspects of the Common Q design. These meetings were successful in answering the staff's questions and thus, no requests for additional information from the staff were necessary. These meetings were held on June 9, 1999, at NRC Headquarters in Rockville, Maryland; September 2, 1999, at CENP in Rockville, Maryland; and September 30, 1999, at CENP in Rockville, Maryland.

The staff's review of the information contained in the topical report, SPM, and accompanying appendices is generic. Some plant-specific review items that are not addressed in these submittals will need to be addressed and resolved during plant-specific application reviews. Licensees referencing this topical report will need to document the details regarding the use of the Common Q platform in plant-specific applications and address all plant-specific interface items listed in Section 6.0 of this SE. CENP's submittals do not include sufficient information on some hardware components of the Common Q platform to enable the staff to complete its generic evaluation. Generic open items are identified in Section 7.0 of this SE. CENP must also address unresolved generic open items listed in Section 7.0 of this SE.

The list and definitions of the acronyms used in this SE is attached as Attachment 1.

This SE follows SRP Chapter 7, "Instrumentation and Controls," Revision 4 (June 1997), which provides guidance to the staff for reviewing designs of the I&C systems in nuclear power plants.

The staff has received sufficient information to complete the generic review of the following hardware components:

- Processor 19-inch subrack
- Expansion 19-inch subrack
- PM645C processor module
- PM646 processor module
- CI631 communication interface module
- Eight models of the S600 I/O modules (AI620, AI635, AO650, DI620, DO620, DO625, DO630, DP620)
- TC630 fiber-optic modem
- TC514 fiber-optic modem
- OZDV114 fiber-optic modem
- TC625 wire modem

CENP's submittals do not include sufficient information on the following hardware components of the Common Q platform for the staff to complete its generic evaluation:

- Flat panel display system
- Watchdog timer module
- Power supply modules

This SE includes the following previously developed software (PDS) components for use with the generic AC160 programmable logic controller system in nuclear safety applications:

- AC160 base software Version AC160 1.2/0
- ACC tool software Version ACC 1.7/0

This SE evaluates the following PDS components for use with the generic flat-panel display system for the Common Q platform:

- QNX4 operating system Version 4.25b
- Photon microGUI [graphical user interface] display builder Version 1.13b

CENP has discussed with the staff its projected schedule for submittal of the balance of the needed generic information over the coming several months. When CENP completes these submittals, the staff will prepare a supplement to this safety evaluation.

2.0 SYSTEM DESCRIPTION

The Common Q platform developed by CENP consists primarily of a set of digital hardware and software components from the standard AC160 system, a product developed by ABB Automation Products, GmbH (ABB Products), in Europe. The standard AC160 is a system of PLC products currently used for control systems in industries unrelated to nuclear power. To complete the Common Q platform, CENP combines a FPDS and other components with its set of AC160 system components. The FPDS consists of the flat-panel display module (with touch-screen capability), a single-board computer, and standard communication interfaces for communication with the AC160 system and to electrically isolated external systems.

This section of this safety evaluation briefly describes the proposed Common Q design and some proposed Common Q nuclear applications. As is noted in Section 1.0 above, there are other hardware components, some of which have yet to be finalized.

2.1 Common Q System

The Common Q computer system uses a set of qualified hardware and software components to implement various nuclear safety applications. CENP will procure the hardware and PDS components that make up the Common Q platform from commercial-grade suppliers and dedicate them for use in nuclear power plants. The following discussion applies to equipment in one of two-to-four redundant channels of safety I&C systems.

The hardware building blocks for the Common Q platform are as follows:

- Advant Controller 160 (AC160) with PM646 or PM645C processor modules
- S600 input and output (S600 I/O) modules
- Bus communication interface (CI631) modules
- Power supply modules
- Watchdog timer module
- Communication systems
- FPDS

An AC160 system has three types of hardware modules: processor modules (models PM645C and PM646), the S600 series of analog and digital input and output modules (eight models of S600 I/O), and a communication module (CI631). These hardware modules are designed to be mounted into 19-inch subracks. A minimal AC160 configuration has one or two subracks. The

subrack or subracks contain one or more processor modules, a power supply module, and up to 18 I/O and communication modules.

The AC160 uses between one and six processor modules in an AC160 controller assembly. The number used varies from application to application and is determined by how much processing power and speed are required for the application. The AC160 system covers a range of programmable functions, including logic and sequence control, analog data handling, arithmetic, and pulse counting.

The AC160 uses the S600 I/O system of input and output modules. There are modules for analog and digital inputs and outputs, including temperature measurement, pulse counting, position sensing, rotational speed measurement, and other applications as needed.

The bus communication interface (CI631) module provides the interface with the redundant Advant Fieldbus 100 (AF100) communication bus, which is described below with the other communication buses. The CI631 modules also have global memory, which the AC160 modules in the channel use to share channel process data with other modules in the channel.

With redundant power supplies, diode auctioneering will provide bumpless transfer upon failure of a power supply module. Faults in one half of a redundant supply will not prevent the other half from operating normally. Sufficient hold time (approximately 40 milliseconds) will be provided to prevent momentary loss of power when the external main power buses are transferred.

An external watchdog timer module has a timing function to detect the lack of activity and is used to monitor the activity of the processing system. Depending on the application, the watchdog timer can be used to annunciate a failure, actuate a channel trip, or set output states to predefined conditions. Isolation is provided for applications in which the watchdog timer is connected to external systems.

The Common Q platform uses three types of data communication systems: the AF100 (Advant Fieldbus 100) network communication system; the high-speed link (HSL) serial communication system; and external communication systems such as Ethernet. The AF100 is used for transferring process data and messages within the channel (e.g., between AC160s and the FPDS). The process data are used for monitoring and controlling a process, and the messages are used for program loading and for diagnostic purposes. The HSL is used to transmit data to other channels in a multichannel system. Fiber-optic modems and cables maintain isolation of redundant safety channels. The external communication system is used to transfer calculated data from the Common Q system to the external systems, such as the plant nonsafety control system.

CENP adds the FPDS to the AC160 system to form the Common Q platform. The FPDS consists of the flat-panel display module, a microprocessor-based single-board computer module, and communication interfaces for communication with the AC160 and other components and systems. The display module is a color thin-film transistor flat-panel display readable under high ambient light. The display module provides a graphical user interface (GUI) with pull-down menus and touch-screen capability. (The GUI function provided by the FPDS is similar to the function provided to a common desktop computer by its terminal,

keyboard, and mouse or trackball.) The FPDS is used for the operator's module (OM) and for the maintenance and test panel (MTP) functions.

The OM is used in the main control room (MCR) for operator functions such as changing setpoints or viewing control rod positions. The MTP is used in the equipment cabinet for maintenance and test functions. The MTP allows the operator or technician to bypass a channel, initiate automatic tests, and display detailed system diagnostic messages. Each Common Q safety channel is required to have both an OM and an MTP.

The AC160 PLC system can be used in nuclear safety systems as a stand-alone controller. A licensee or applicant proposing to use the AC160 PLC system may reference this safety evaluation. A diesel generator sequencer is an example of an application for which a licensee or applicant might propose to use the AC160 PLC system without the rest of the Common Q system. This safety evaluation identifies the AC160 components that the staff has approved for use in Class 1E applications.

2.2 Previously Developed Software

CENP defines PDS as software that was developed to satisfy a general market need before being incorporated into the Common Q platform. PDS includes commercial software that is integral to the delivered system and software that supports the delivered system. Some PDS is used to develop the application software to implement the safety functions in the Common Q upgrades. The PDS for the Common Q platform is procured from two vendors: the vendor of the AC160 PLC system and the vendor of the FPDS operating system. Separate software tools are used for AC160 and for FPDS application software. PDS from one vendor is not used on the other vendor's components.

Examples of PDS to be used in the Common Q are as follows:

- Operating systems
- Compilers, linkers, and loaders
- Database software
- Communication drivers
- Man-machine interface software
- Display-building software

There are two types of PDS:

- PDS that resides in Common Q memory when the Common Q is performing its safety functions (i.e., at run time)
- PDS used as development or support tools

The run-time PDS for the AC160 consists of a real-time operating system, a task scheduler, diagnostic functions, and communication functions, all of which reside on flash programmable read-only memory (PROM) in the PM646 processor module. The operating system software executes the control modules of the application program, diagnostic routines, and communication interfaces.

The AC160 operating system provides for the deterministic behavior of the Common Q platform. The AC160 task scheduler receives a signal every 2 milliseconds to schedule the execution of all the control modules, both PDS and application-specific. The control modules are scheduled on the basis of predefined priorities, the assigned cycle time of the control modules, and their entry into the cycle time table. The cycle time table is used to assign priorities to control modules that have the same cycle time. CENP indicates that as long as the measured load of the application programs on a single processor is less than 70%, control module overruns will be avoided. Therefore, for each Common Q application a timing analysis will be performed to ensure that the multiple control modules in the system design are executing deterministically. To achieve a deterministic system behavior, process data are always transferred cyclically. Message transfer is not performed cyclically, but only when one or more of the attached communication interfaces have something to send. Message transfer does not influence process data transfer in any way. Process data transfer remains deterministic since a certain portion of the bandwidth is reserved for message transfer.

The development and support tools include a library of predefined PLC functions that are combined to perform the application functions. The support tools also support the development of new functions by combining functions from the tool library. The development process for the applications is controlled by the SPM.

The run-time PDS for the FPDS consists of a real-time operating system and the GUI system. The PDS for the FPDS also includes development and support tools that will be used in developing the application software. The display builder tool supports the development of human-machine interface (HMI) displays for the FPDS. It contains a symbol library and a visual-display-building tool for creating graphical displays.

The FPDS is used for the OM in the MCR and for the MTP in the AC160 equipment cabinet. The FPDS does not initiate any safety action. If the FPDS halts, the safety-critical applications in the AC160 controllers can continue to operate unimpeded.

Additional details about the operating systems and the functions of the Common Q software are given in Section 4.0 of this SE.

2.3 Application Software

The Common Q platform uses microprocessor-based digital equipment to replace existing safety-related I&C system functions at nuclear power plants. This replacement requires that new software be generated to perform the functions. This new software has not yet been developed.

All software residing on safety system computers at run time must be qualified for its intended application. The new software for the safety-related functions implemented in the Common Q platform will be produced under a quality assurance program. CENP submitted the SPM, CE-CES-195, "Software Program Manual for Common Q Systems," for staff review. The SPM describes CENP’s complete software development process, including hardware integration. The software development process proposed by CENP and described in the SPM derives from the methodology approved by the NRC through the licensing of the System 80+.

In addition to performing the required safety functions, the Common Q application software will also be capable of performing automated diagnostics on the safety systems. Automated diagnostics continuously test the functionality of the applications. Automated diagnostics of the safety functions are performed by the application-specific software. In addition, the Common Q hardware is automatically tested by diagnostics in the PDS delivered with the hardware.

The application program and its control modules in an AC160 coexist in PROM with the other system software programs, such as the diagnostic routines and communication interfaces. The same is true of the FPDS.

2.4 Nuclear Applications

The four appendices describe the use of the Common Q platform in the post-accident monitoring system (PAMS), the core protection calculator system (CPCS), the reactor protection system (RPS), the plant protection system (PPS), and the engineered safeguards features actuation system (ESFAS). Appendix 4 describes integrated combinations of these safety systems and their interfaces with nonsafety systems. The information in the four appendices includes system configuration, failure mode and effects analysis, 10 CFR 50.59 assessment information for digital-to-digital replacements, and other system-specific information. CENP plans to submit additional appendices in the future to address other generic applications such as the diesel generator sequencer.

The scope of the staff's review related to the appendices was limited to only establishing the acceptability of the design approaches for digital implementation of those applications described in the appendices. However, the appendices provide additional information in support of the staff's review of the generic design details of the Common Q platform.

PAMS

The PAMS is described in Appendix 1 to the topical report. It is being implemented as a computer-driven Class 1E safety-related alarm and display system. The PAMS consists of two independent channels of equipment that acquire and process two channels of inputs. The two channels of equipment are located in one or more cabinets, depending upon the plant. The channels are physically separated and electrically isolated from each other. Plant-specific PAMS designs can be developed from the designs included in Appendix 1. A specific PAMS implementation includes one or more of the following subsystems:

- A heated junction thermocouple (HJTC) system and reactor vessel level monitoring system (RVLMS);
- A subcooled margin monitor (SMM);
- A core exit thermocouple monitoring system (CETMS);
- An inadequate core-cooling monitoring system, which includes an SMM, a CETMS, and an HJTC system; and
- A qualified safety parameter display system (QSPDS), which includes all of the above systems.

The PAMS HMI is provided by the OM and the MTP. Both the OM and the MTP will include display and diagnostic capabilities unavailable in the existing design.

CPCS

The CPCS is described in Appendix 2 to the topical report. It provides reactor trip outputs for low departure from nucleate boiling ratio (DNBR) and high local power density (LPD). The low DNBR and high LPD trips (1) ensure that the specified acceptable fuel design limits on departure from nucleate boiling and centerline fuel melting are not exceeded during anticipated operational occurrences and (2) assist the ESFAS in limiting the consequences of certain postulated accidents.

The CPCS generates trip and pretrip signals on low DNBR and high LPD and sends control element assembly (CEA) withdrawal prohibit (CWP) signals to the plant protection system (PPS). The signals are in the form of binary (contact) inputs. The PPS uses these and other inputs to automatically actuate a reactor trip whenever the monitored processes violate predefined limits in at least two of the four redundant PPS channels.

The CPCS consists of four channels of equipment. These are located inside the auxiliary protective cabinet where the channels are physically separated and isolated from each other. The CPCS contains four core protection calculator (CPC)/control element assembly calculator (CEAC) systems, one per channel. Each CPC channel provides contact outputs to its respective PPS channel.

Each CPC/CEAC channel communicates with a CPC OM mounted in the control room. Each of the four OMs is fiber-optically isolated from its associated CPC channel. The OM is used for CPC/CEAC channel monitoring to provide the capability to manually alter addressable constants, to initiate a channel bypass at low power levels, and to initiate periodic surveillance testing.

The Common Q replacement CPCS will run CPC safety-related algorithms functionally identical to the existing core protection calculators in existing Combustion Engineering (CE) plants. Any software changes will be restricted to those required to reflect new hardware platform features (such as diagnostics and error handling) and backplane communications between CPCs and CEACs in the proposed Common Q replacement system.

Digital Plant Protection System (DPPS)

The DPPS is described in Appendix 3 to the topical report. It has both RPS and ESFAS functions. In the earlier CE plants, the RPS and ESFAS were separate systems, with the RPS supplied by the nuclear steam supply system (NSSS) vendor and the ESFAS typically supplied by the architect engineer. In the appendices, these plants, employing separate RPS and ESFAS implementations, are referred to as "RPS" plants. In CE plants of more recent design the RPS and the ESFAS functions share a cabinet, referred to as a PPS cabinet. The PPS cabinet includes the bistable trip functions and two-out-of-four logic to initiate both the reactor trip and the ESFAS function actuation. Plants employing a PPS cabinet also have two separate ESFAS cabinets that house the Train A and Train B component actuation relays, local indication, manual actuation, and selective two-out-of-four actuation logic.

Appendix 3 is applicable to both the RPS and the PPS generations of CE plants. For either generation of plant it is possible to upgrade only the RPS, or only the ESFAS, or both the RPS and the ESFAS.

The proposed DPPS upgrade is limited to replacing the equipment in the PPS cabinet and the ESFAS auxiliary relay cabinets. Sensors and related signal-conditioning equipment outside the PPS cabinet and final actuated devices will not be altered by the DPPS upgrade.

The DPPS comprises four redundant and independent channels that perform the necessary bistable, coincidence, initiation logic, and associated maintenance and test functions. The system includes one redundant remote control module (RCM) for each channel in the MCR.

Monitoring, testing, and maintenance of the DPPS is provided by the MTP and a separate interface test processor (ITP) located in each DPPS channel and ESFAS train. The MTP is used to monitor DPPS status and perform DPPS control functions, such as inserting bistable trip channel bypasses and resetting ESFAS initiation signals.

The ITP in each DPPS channel and ESFAS train performs continuous passive monitoring and either fully automatic, manually initiated automatic, or manually initiated testing of the associated channel. It provides the DPPS cross-channel feedback for cross-channel comparisons and for monitoring the status of automated testing. Independent watchdog timers are used in each channel for both the RPS and the ESFAS functions.

According to CENPD-396-P, Appendix 3, CENP's approach, the implementation of the DPPS will provide protection functions and engineered safety features functions that are functionally identical to those implemented in the equipment that the DPPS is replacing.

Integrated Solution

Appendix 4 to the topical report describes the implementation of the Common Q for a configuration in which the licensee replaces more than one of the systems described in Appendices 1, 2, and 3, i.e., the PAMS, the CPCS, and the PPS (which includes the RPS and the ESFAS). Appendix 4 describes the sharing of some of the Common Q resources, such as display panels and communications buses, when two or more of the above systems are installed in the plant.

Appendix 4 also includes a high-level description of the optional integration of the Common Q replacements with digital nonsafety reactor control systems. The nonsafety control systems are implemented using a different ABB technology from that used in the Common Q. The information on the integration with the nonsafety control systems is mainly conceptual. Design details will be described in future submittals and evaluated by the staff in a supplement to this safety evaluation. Two of the reasons given by CENP for describing the nonsafety control systems in Appendix 4 are (1) to discuss the interfaces with the safety systems, and (2) to indicate the conceptual implementation of the diversity of components in such a nonsafety control system as a credible backup to a postulated common mode failure in the safety systems.

CENP presents many of the high-level descriptions of the nonsafety systems as design concepts, with examples of the technologies in which the concepts might be implemented. In Appendix 4, CENP asked the staff to review certain aspects, especially conceptual aspects, of an integrated system solution to evaluate whether they are acceptable design approaches for an integrated I&C replacement using the Common Q platform.

In many respects, the nonsafety portions of the control systems described in Appendix 4 are essentially the same as those described in Section 7 of the CENP standard design, "CESSAR System 80+," which CENP submitted to the staff for certification on March 30, 1989. The staff issued NUREG-1462, "Final Safety Evaluation Report Related to the Certification of the System 80+ Design," in August 1994. Where applicable, the staff has incorporated evaluations from NUREG-1462 in its evaluation of Appendix 4.

3.0 REVIEW CRITERIA AND METHOD OF REVIEW

3.1 Review Criteria

The staff performed this review using acceptance criteria in Chapter 7 of the SRP, Revision 4 (June 1997). Chapter 7 addresses the requirements for I&C systems in light-water nuclear power plants. Revision 4 has refined the procedures for reviewing digital systems. These procedures are in SRP Appendix 7.0-A; SRP Appendix 7.1-A; SRP Sections 7.1, 7.8, and 7.9; and BTPs HICB-11, HICB-14, HICB-17, HICB-18, HICB-19, and HICB-21. SRP Appendix 7.1-C and SRP Sections 7.2 through 7.7 provide additional criteria that the staff applied to the review of the appendices to the topical report.

The following codes are listed in SRP Chapter 7 as being applicable to reviewing digital replacement I&C systems:

- 10 CFR 50.55a(a)(1)
- 10 CFR 50.55a(h)
- 10 CFR 50.34(f)(2)
- 10 CFR 50.62
- 10 CFR 50, Appendix A, General Design Criteria (GDCs) as follows:
    - GDC 1 – Quality Standards and Records
    - GDC 2 – Design Basis for Protection Against Natural Phenomena
    - GDC 4 – Environmental and Dynamic Effects Design Bases
    - GDC 12 – Suppression of Reactor Power Oscillations
    - GDC 13 – Instrumentation and Control
    - GDC 19 – Control Room
    - GDC 20 – Protection System Functions
    - GDC 21 – Protection System Reliability and Testability
    - GDC 22 – Protection System Independence
    - GDC 23 – Protection System Failure Modes
    - GDC 24 – Separation of Protection and Control Systems
    - GDC 25 – Protection System Requirements for Reactivity Control Malfunctions

The following regulatory guides and industry standards provide information, recommendations, and guidance, and in general are an acceptable basis for implementing the above-noted requirements for hardware and software features of safety-related digital systems such as the Common Q platform:

- IEEE Std 7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations," as endorsed by RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants"
- IEEE Std 323-1974/1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," as endorsed by RG 1.89, "Qualifications for Class 1E Equipment for Nuclear Power Plants"
- IEEE Std 338-1987, "IEEE Standard Criteria for Periodic Testing of Nuclear Power Generating Station Safety Systems," as endorsed by RG 1.118, "Periodic Testing of Electric Power and Protection Systems"
- IEEE Std 344-1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"
- IEEE Std 379-1988, "Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems," as endorsed by RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems"
- IEEE Std 384-1992, "Criteria for Independence of Class 1E Equipment and Circuits," as endorsed by RG 1.75, "Physical Independence of Electrical Systems"
- IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as endorsed by RG 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems"
- IEEE Std 730-1989, "Software Quality Assurance Plans," as referenced in BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."
- IEEE Std 828-1990, "Software Configuration Management Plans," as endorsed by RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- IEEE Std 829-1983, "Software Test Documentation," as endorsed by RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- IEEE Std 830-1984, "Guide for Software Requirements Specifications," as endorsed by RG 1.172, "Software Requirements Specification for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans," as endorsed by RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- IEEE Std 1016-1987, "IEEE Standard for Recommended Practices for Software Design Descriptions"
- IEEE Std 1028-1988, "IEEE Standard for Software Reviews and Audits," as endorsed by RG 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- IEEE Std 1042-1987, "IEEE Guide to Software Management," as endorsed by RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Stations"

- IEEE Std 1074-1995, "IEEE Std for Developing Software Life Cycle Processes," as endorsed by RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Systems used in Safety Systems of Nuclear Power Plants"
- MIL-STD-461C, "Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference"
- IEC Std 880, "Software for Computers in the Safety Systems of Nuclear Power Stations," as referenced in the SRP
- ASME NQA-2a-1990, Part 2.7, "Quality Assurance Requirements of Computer Systems for Nuclear Facility Applications," as referenced in the SRP
- EPRI Topical Report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," approved by the NRC on July 30, 1998
- EPRI Topical Report TR-102323-R1, "Guidelines for Electromagnetic Interference Testing in Power Plants," approved by the NRC on April 16, 1996
- EPRI Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," approved by the NRC in April 1997

3.2 Method of Review

CENP submitted its topical report describing the Common Q platform to the staff for generic review.

The suitability of a digital platform for use in safety systems depends on the quality of its components and the implementation of system aspects that present qualification problems when applied to digital systems, such as real-time performance, independence, and online testing. The staff's review of the implementation of these system aspects and the quality of the components of the Common Q platform is contained in Sections 4.1 through 4.3 of this SE.

In the appendices to the topical report, CENP describes the proposed designs for implementing specific safety systems based upon Common Q components. The staff has reviewed these designs against the applicable functional requirements of IEEE Std 603 and the GDCs and the criteria for protection against common-mode failure.

The acceptance process for most commercial-grade digital components can be expected to comprise a variety of complicated technical activities. Guidance on these activities is given in EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." In April 1997, the staff issued a safety evaluation on TR-106439. The staff determined that TR-106439 contains an acceptable method for dedicating commercial-grade digital equipment for nuclear power plant safety applications. CENP submittals have followed the guidance in TR-106439.

EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Application in Nuclear Power Plants," provides a specification in the form of a set of requirements for generically qualifying PLCs for safety-related instrumentation and control systems in nuclear power plants. EPRI TR-107330 was approved by the staff on July 30, 1998.

The staff has applied the guidance in EPRI TR-106439 and TR-107330 in reviewing the CENP program for the qualification of the Common Q hardware and software.

CENP procures the commercial-grade items used in the Common Q platform from different commercial-grade vendors. As part of the commercial-grade dedication (CGD) of these items, CENP teams conducted reviews at the vendors' facilities to determine the quality of the vendors' activities. These reviews focused on the vendor's hardware and software life cycle with regard to the following:

- Well-defined system hardware and software requirements;
- Comprehensive hardware and software development methodologies;
- Comprehensive test procedures;
- Strict configuration management and maintenance procedures; and
- Complete and comprehensive documentation.

The findings of the CENP review teams were documented in CENP proprietary reports and records. The staff reviewed CENP's records of and reports on CGD activities. The staff's evaluations on the CGD activities are documented, and generic open items are identified, in Section 4.2.

4.0 SYSTEM EVALUATION

This section details the staff's evaluation of the Common Q platform. The evaluations include (1) the Common Q design, (2) the commercial-grade dedication of the Common Q platform, (3) the life-cycle planning process for application software, and (4) the Common Q applications. Since hardware and software components need each other to perform any function, the discussion under any given section frequently does not contain all of the details needed for the staff to arrive at a conclusion about the acceptability of the design with regard to specific regulatory criteria. Therefore, the general evaluation of the acceptability of the Common Q platform with regard to the regulatory criteria are stated in Section 5.0. However, where the information in a subsection under Section 4.0 supports a conclusion, the conclusion is stated in that subsection.

The staff has identified some generic open items for which it needs additional information to complete its evaluation (e.g., items involving the power supplies, the watchdog timer module, the FPDS hardware, and communications between the FPDS and the AC160). Generic open items are listed in Section 7.0. (Items that will require plant-specific consideration also are identified throughout the evaluation and are listed in Section 6.0).

4.1 Evaluation of the Common Q Design

In evaluating the adequacy of the Common Q design to perform the functional requirements for nuclear safety applications, the staff considered both the hardware and software components and their performance as a system.

The hardware components for the Common Q are as follows:

- Advant Controller 160 (AC160) with PM646 processor modules;
- S600 input and output (S600 I/O) modules;
- Bus communication interface (CI631) modules;
- Communication systems;
- Power supply modules;
- WDT module; and
- FPDS.

The Common Q software components are as follows:

- Software development tools;
- Real-time operating system;
- Task Scheduler;
- Diagnostic functions;
- Communication interfaces; and
- User application programs.

The hardware and software components for the Common Q platform generally fall into two groups:

- Hardware and software components used with the AC160 PLC products; and
- Hardware and software components used with the FPDS.

Some of the communications systems interface with both groups of components.

4.1.1 AC160 PLC System

The AC160 hardware and software components are discussed below. Since hardware and software components need each other to perform any function, the discussions sometimes overlap.

4.1.1.1 AC160 Hardware

The AC160 PLC system is modular. A typical Common Q configuration consists of one-or-more processor module(s), I/O modules, and communication modules mounted in one or two 19-inch subracks. Each subrack can accommodate up to 10 modules.

The controller subrack is the primary subrack of the AC160. It has positions for processor modules, communication modules, I/O modules, and bus extender modules. The bus connector links the controller subrack to an optional extension subrack via a bus cable. The 10-position extension subrack extends the number of I/O modules of a station. Up to seven additional subrack pairs (I/O stations) can be connected if additional I/O requirements apply.

4.1.1.1.1 PM646 and PM645C Processor Module

Revision 00 of the topical report discussed specifics of the PM645C and Revision 01 of the topical report discusses specifics of the PM646. CENP indicates in Revision 01 that the PM646 is the processor module that CENP will use in the Common Q platform. The PM646 offers

additional diagnostic capabilities over the PM645C. The staff has evaluated both models and has determined that each of the staff's findings in this safety evaluation apply equally to either the PM646 or the PM645C. The generic open items and plant-specific items also apply equally to either model.

The PM646 processor module consists of two hardware sections: (1) the processing section, with a microprocessor and memory for the system software and the application program, and (2) the communication section, with a separate microprocessor and memory for exchanging communication signals with other controllers.

The processing section includes the following:

- A Motorola MC68360 microprocessor, 1 Mbyte of nonvolatile memory (flash PROM) for the user built application and 2 Mbytes of nonvolatile memory (flash PROM) for the system software, and 2 Mbytes of RAM. At startup, the application and system software are copied from the nonvolatile memory into the RAM, where it is executed.

- A memory that is not expandable. The system software flash PROM holds the controller system software executed in run time. The user flash PROM holds the controller system configuration and application program, which is loaded to the RAM at system start.

- A dedicated RS-232-C port to connect a personal computer engineering station used for system maintenance and programming.

The communication section in the PM646 processor module includes the second Motorola MC68360 microprocessor, which is used for HSL communications. It has an extra 512 Kbytes nonvolatile memory (flash PROM) for the system software and an extra 2 Mbytes RAM for communications.

Each PM646 processor module contains two RS-422 high speed serial link ports for signal and data exchange between processor modules for application and system purposes. These ports are used with fiber-optic cables for interchannel communications.

The processing section and the communication section communicate with each other through a dual-port random-access memory, which is housed in the PM646 module, that each section can access through its port. This allows the two sections to share data between them while preventing either from affecting the operation of the other. The two sections communicate with each other by reading from and writing to this dual-port random-access memory. This feature facilitates the capability of designs using the PM646 to satisfy independence and separation requirements for safety systems.

4.1.1.1.2 Input/Output Subsystem

The AC160 PLC system uses the S600 series of I/O modules. Various models of S600 I/O modules are available, including modules for temperature measurement, pulse counting, position sensing, rotational speed measurement, and other applications as needed. Eight S600 I/O models have been qualified for use in nuclear safety applications:

- Two analog-input modules (AI620 and AI635)
- One analog-output module (AO650)
- One digital-input module (DI620)
- Three digital-output modules (DO620, DO625, and DO630)
- One pulse-counting module (DP620)

Any of the S600 I/O modules may be replaced while the system is powered. Removing the front connector disconnects the process signals. A newly inserted module is automatically tested and put into operation if the system identifies the module as the correct model and verifies it to be without faults. The staff's evaluation of the automatic self-testing for the S600 I/O modules is found in Section 4.1.1.3.2.

In addition to meeting the guidance in TR-106439, CENP has committed to redesign some of the above S600 I/O modules, where needed, to meet the requirements of TR-107330. For some applications, the existing S600 I/O modules already satisfy the plant-specific requirements. In other cases, modules designed to meet the requirements of TR-107330 may not satisfy the plant-specific requirements. The staff has stated in its SE for TR-107330 that for any plant-specific application, the licensee will need to verify that the qualification envelope provided by TR-107330 meets the requirements of the application. The qualification envelope includes (1) performance that is capable of performing the functions in the application, and (2) the seismic and environmental qualification. The assessment of the suitability of particular S600 I/O modules for an application is the responsibility of the licensee and is plant-specific action item 6.1.

The staff will evaluate the changes to the S600 I/O modules in a supplement to this safety evaluation. This is Generic Open Item 7.1.

4.1.1.1.3 CI631 Communication Module and Global Memory

The main function of the CI631 is to provide the bus communication interface between the AC160 system and the AF100 bus. The AF100 bus is discussed in Section 4.1.3. The CI631 also houses global memory used for sharing intrachannel data among multiple PM646 modules and I/O modules in an AC160 system. The CI631 is similar in hardware and software to the S600 I/O modules. The CI631 modules may be replaced while the system is powered. A newly inserted module is automatically tested and put into operation if the system identifies the module as the correct type and proper revision number, and verifies it to be without faults. The staff's evaluation of the automatic self-testing for the CI631 module is found in Section 4.1.1.3.2.

4.1.1.2 AC160 Software

The AC160 software consists of a real-time operating system, a task scheduler, diagnostic functions, communication interfaces, and user application programs, all of which reside on flash PROM in the PM646 processor module.

4.1.1.2.1 AC160 System Software

The PM646 processor system software consists of standard AC160 software products developed by ABB Products layered on a commercially available operating system. The system software executes the software functions in the application programs, diagnostic routines, and communication interfaces. The communication interfaces include interfaces with the I/O backplane, the AF100 buses, and the HSL.

The application program and its control modules coexist with the system software programs such as the task scheduler, diagnostic routines, and communication interfaces in the processor module. The task scheduler schedules the execution of the application programs and periodic system software tasks based on predefined priorities. The processing section of the PM646 executes the safety-related application program. The communication section handles the serial communication with other safety channels.

The executable code for the standard set of logic blocks (program control elements) is part of the base software. In addition, custom program control elements can be created as an extension to the base software.

The processing section of the PM646 module executes the safety algorithms. It has one process control program, which consists of several executable units called control modules. Each control module has its own cycle time and execution conditions. When this process control program is compiled into target codes, each control module becomes an operating system's task. On the basis of predefined priorities, the process section schedules all the tasks using the task scheduler in the system software and executes the tasks accordingly. The basic software components of the processing section are the following:

- Task scheduler – The task scheduler schedules the application programs and periodic system tasks. It also performs diagnostic functions.

- Application programs – The application programs are created by the application engineer. The priority of the application program is set by the application tool.

- Service data program – The service data program services all communications on the AC160 subrack backplane. Examples of such communications are I/O module configuration and initialization, communication with the I/O modules, and communication with the AF100 bus.

- System diagnostics – The system diagnostics perform the following:

    - Check proper operation of the window watchdog timer;
    - Validate the RAM diagnostics; and
    - Monitor the health of the serial communications section.

- Background task – The background task is the last in the task sequence. It performs the following diagnostics:

    - Performs a cyclic redundancy check (CRC) of the system firmware in the flash PROMs;
    - Performs a CRC of all static domains in RAM;
    - Performs a CRC of the user programs in flash PROM;
    - Checks parameter set of I/O modules; and
    - Configures I/O modules after they are replaced.

The communication section controls HSL communication. Unlike the process section, the communication section is an event-driven interrupt system. Therefore, execution of a communication section system's task for controlling HSL communication is initiated by an event, such as the reception of data from the process section or the HSL. However, because all the events that initiate an execution of the communication section system's tasks occur cyclically, the system is forced to become a cyclically based system. The acceptability of the event-driven communication section is evaluated in Section 4.1.1.6.

The communication section of the PM646 module handles the serial communication to other channels. The basic software components of this section are the following:

- Main task – The main task creates and starts the supervisor task. Once the supervisor task starts, the main task exits.

- Supervisor program – The supervisor program creates and starts all the other serial communication programs. In addition, it performs the following functions:

    - Monitors the functionality of the application section of the processor module;
    - Notifies the processing section of any errors detected; and
    - Refreshes the processor 2-millisecond watchdog timer.

- Copy program – The copy program copies serial communication data from the application program to the communication section of the PM646 module.

- Transmission program – The transmission program updates the serial transmission buffer with application data copied by the copy program.

- Receiver program – The receiver program puts the serial communication data received from other safety channels into a buffer to be read by the application program.

- Configuration program – The configuration program allocates the resources for serial communication data transfer.

- Diagnostic program – The diagnostic program has two functions: to output messages for software diagnostics and to test the window watchdog timer. After the test activates the relay, the window watchdog timer is quickly retriggered before its relay contacts have a chance to open.

- Background program – The background program performs a CRC on the system flash PROM. The background program is monitored for completion within a specified timeout period.

4.1.1.2.2 Application Software

Creation of the application program utilizes the ACC software development environment that includes a function block library of process control elements. The executable code for the standard set of logic blocks (i.e., process control elements) is part of the base software. In addition, custom process control elements can be created as an extension to the base software. The programmer references the process control element library to create the specific logic for the application.

The application program is written in the ABB Master Programming Language (AMPL) and consists of a process control part and a database part.

The process control part of a user application program describes the control algorithm and the control strategy. It contains the process control elements, their interconnections, and connections to the database elements. A process control program can be divided into several executable units called control modules, each consisting of process control elements. Each executable unit can be given its own cycle time and its own execution conditions. Process control elements are the smallest building blocks in a process control program. The control module is made up of function calls to the process control element library. The process control element library is stored on system flash PROM.

Each AC160 processor has one process control program. Under the process control program are executable control modules. When this process control program is compiled into target code, each of its control modules becomes a task to be executed under the control of the operating system.

The I/O modules continuously scan and store values independent of control module execution. When the control module executes, its first operation is to get the process input values over the backplane I/O bus from the I/O modules.

On processor initialization or restart, the application program is reloaded from flash PROM into RAM and then started.

The database part in an AC160 system contains the database elements that are used to configure the controller. The database elements in an AC160 system describe the following items:

- The hardware configuration of the AC160 system: processor module, I/O modules and communication interfaces (e.g., HSL and AF100);

- Common data elements (e.g., global data); and

- Connection between the hardware and the common data elements (e.g., data set peripheral for AF100 communication and database elements for the HSL).

4.1.1.2.3 Software Tools

The AC160 software development environment is called AMPL Control Configuration (ACC), which is a product of ABB Products. The ACC product consists of the following utilities: Application Builder, Online Builder, Function Chart Builder and Bus Configuration Builder. The tools use the AMPL. AMPL is based on function blocks, called process control elements, which are combined with each other into programs which form a complete control function.

The ACC environment supports the development of type circuits. A type circuit is a logic block composed of process control elements that can be used many times in a control program. The type circuit is considered a module and therefore must undergo documented module tests, as is described in the SPM.

Custom process control elements appear as standard process control elements with input and output terminals when inserted in a control program. They are developed outside of the ACC development environment and then added to the library of process control elements. Once in the library, the custom process control element is available for the programmer to use in a control program. The custom process control element will be classified as a module and therefore undergo documented module tests as described in the SPM for Class 1E software.

4.1.1.3 AC160 Self-Testing

BTP HICB-17 indicates that digital computer-based instrumentation and control systems are prone to different kinds of failures than are traditional analog systems. BTP HICB-17 requires that surveillance testing, taken together with automatic self-testing, should provide a mechanism for detecting all detectable failures. Computer self-testing is only effective at detecting random hardware failures. It is not useful for the detection of latent software errors.

The AC160 performs diagnostic and supervisory functions to continuously monitor the whole system for correct operation. Each type of AC160 module also has its own diagnostic functions. The AC160 monitors the system as a whole by collecting all the diagnostic information and checking the consistency of the hardware configuration and the application software.

The automatic self-test functions for the Common Q fall into the following two main categories:

1. AC160 self-diagnostics, which come with the AC160 as part of the previously developed software and serve to verify the proper operation of the AC160 system.

2. Application automatic self-testing that tests the proper functioning of the Common Q applications, including inputs and outputs, and will be developed as part of the application software for each application.

Both categories of self-test functions run continuously in the AC160 as background operations. There are additional automatic self-tests that run when starting the system. Application automatic self-testing can also be manually initiated by the operator through the OM or the MTP.

AC160 self-diagnostics, together with the watchdog timer in the PM646, ensure that the execution of each control module does not exceed its cycle time and that the AC160 system operates properly. ABB Products designed the processor module so that if the processor module does not complete its operations within specified times or fails the self-diagnostics test, the processor module halts. If the processor module halts, the watchdog timer times out.

The operation of the PM646 is monitored by the process section and the communication section. Each section monitors the other section's life sign. If the process section detects that the communication section is not operating, the process section halts itself and the watchdog timer in the process section. If the communication section that detects the process section is not operating, the communication section halts itself. This causes the watchdog timer in the communication section to time out, signaling the failure. Additionally, the PM646 of one channel is monitored by the PM646 of other channels, which notify the operator if one channel fails to send data or sends bad data. The proper operation of the AC160 self-diagnostics test function is also verified during the power-up of the PM646 module.

Application automatic self-testing is an integral part of the Common Q applications. It is used to continuously monitor the integrity of the application as it performs its function. It can continuously monitor the functionality of the channels from sensor to actuated device and can also perform cross-checks between channels. The automatic self-test software will be developed with the application software under the quality assurance and procedures specified in the SPM.

4.1.1.3.1 PM646 Diagnostics

One component of the AC160 base software is the internal diagnostics that are executed at startup and/or continuously during system operation. Diagnostic functions monitor system operation and report any faults detected. The monitoring functions include the following:

- the functioning of the two microprocessors in the PM646 module;
- the integrity of the data permanently stored in the flash PROM by use of CRC checks;
- the functioning of RAM;
- the functioning of the interrupts and timers; and
- the functioning of the communication buses.

The internal diagnostics check for process, system and device errors. Each type of error is combined into a single bit in a status word. This status word is read by both the system diagnostic routines and the AC160 database element when referenced within an application program.

4.1.1.3.2 Input/Output Module Diagnostics

Diagnostics of the S600 modules I/O and the CI631 communication module are executed by interrogating all modules for errors. The S600 modules have self-contained diagnostics the results of which are reported to the PM646 base software diagnostics routine via a device status word. The system software checks that:

- the module is in the correct slot;
- the module is the correct type;
- the module is functional; and
- the process connector is in place.

4.1.1.3.3 High Speed Link Diagnostics

The HSL diagnostics are executed to detect physical layer failures and failures of the communication link to another PM646 processor module. The bus protocol is secured through a cyclic redundancy check. A keep-alive signal is transmitted over the HSL every 25 milliseconds if an application program has not otherwise requested a transmission. When a PM646 processor module has not received data for 150 milliseconds, the HSL is considered failed. All detected errors are reported to the application program.

4.1.1.3.4 AF100 Diagnostics

The AF100 uses busmastership to continuously monitor the status of the nodes on the bus. The AF100 communication interface, CI631, monitors the validity of the data sets it is supposed to receive. If no data has been received for four cycles or when the communication interface is diagnosed as failed, the database element for the data set will be flagged as failed. The control module programming will constantly monitor the database element flag and perform the appropriate error processing.

4.1.1.3.5 Redundant AF100 Interface

The AC160 redundant CI631 configuration provides online surveillance of these modules to assure that they are in operational condition in case an automatic switchover is required. The primary and secondary communication interface modules contain self-diagnostics and report any errors to the application in the PM646.

If the primary fails, there will be an automatic switchover to the secondary module. When this occurs the new primary module will report an error to the application that the original primary has failed. This error report can be used for alarm or screen indication to direct technicians to the specific AC160 node that has the communication interface failure. Normally the failed module will be indicated by a red light on the front panel. However, if this was a transient error and the PM646 is able to reboot the CI631, the CI631 will return to service (as the standby) and there will be no red light.

Upon detection of an error, the primary CI631 enters the passive state, causing the processor modules to recognize the failure. A technician using an engineering workstation to interrogate the error buffer can collect the diagnostics information to determine the cause of the problem.

The automatic switchover can be periodically tested as follows:

1. The technician verifies that CI631s one and two are functioning (i.e., no error reports and no red lights are on the front panel).

2. The technician removes the primary CI631 module (indicated by the LED light on front plate), and verifies the switchover of the other CI631 from backup to primary (same LED indication).

3. The technician reinserts the CI631 module – this CI631 module now returns to service as the backup CI631 (there is no automatic switch back).

4.1.1.3.6 Application Watchdog Counter

The design of the Common Q platform includes a software watchdog counter in each application program (separate from the external hardware watchdog timers) to override the activation outputs of the safety system should the processor halt. Each program will update a counter or toggle a binary each execution cycle. The counter will be monitored by another application on another processor. When the monitoring application detects the counter not changing for a predefined period of time, it will assume the application has halted and will take appropriate error handling action.

On the basis of the review in Section 4.1.1.3, the staff concludes that the self-testing features of the AC160 system adequately address the self-test issues identified in BTP HICB-17.

4.1.1.4 Throughput and Response Time

The Common Q applications (CPC, PAMS, DPPS, etc.) have system time requirements for responding to specific nuclear plant events. For example, the DPPS must generate a trip signal within a specified time once the steam generator level hits a low trip setpoint. CENP stated that during the design phase of the specific Common Q application, it would perform a throughput calculation of the following:

1. The propagation delay of the input system;
2. The propagation delay of the HSL cross-channel communication;
3. The executing task worst-case timing; and
4. The propagation delay of the output system.

To ensure that the Common Q system meets its application's system response time requirements, CENP will calculate and measure the actual execution time for all the executing tasks (control modules) created for a Common Q application in the PM646. CENP indicates that the predictability of program execution is established by determining whether the measured load of the application in a single processor is less than 70 percent, which will avoid control module overrruns. CENP will then generate a timing diagram that shows the relationship of the tasks to each other. CENP stated that this timing diagram will identify when the maximum number of control modules will be scheduled to execute at the same time.

For each process control program that uses multiple control modules and that is classified as Class 1E, CENP will perform a timing analysis to ensure that:

- The multiple control modules in the system design are executing deterministically; and

- The data dependencies between control modules do not affect the deterministic calculation of results (i.e., that the data used by the multiple control modules are all current).

The Common Q applications will also have response time requirements for displaying calculation results, system anomalies, and input data. The display response time requirements will also include system response time requirements for control action initiated from the display.

During the operation of the Common Q application, the central processing unit (CPU) load will be continuously monitored to ensure that the specified maximum CPU load is never exceeded.

The requirements for the timely operation of the protection features are described in 10 CFR Part 50 Appendix A, GDC 20, 21, 23, and 25. To meet these requirements, BTP HICB-21 provides the following guidance:

- Design timing feasibility may be demonstrated by allocating a timing budget to components of the system architecture (Annex E of IEEE Std 7-4.3.2) so that the entire system meets its timing requirements

- Timing requirements should be satisfied by design commitments

CENP has committed to perform a system response and display response analyses in order to meet the response time requirements identified in BTP HICB-21. Based on its review of the Common Q system architecture and CENP's design commitments to perform throughput and response-time analyses, the staff concludes that for the systems and components reviewed, the Common Q design satisfies the response time requirements identified in BTP HICB-21 and is, therefore, acceptable in this regard. When implementing a Common Q safety system the licensee must review CENP's timing analyses and validation tests for the Common Q system in order to verify that it satisfies its plant-specific requirements for system response and display response time presented in the accident analysis in Chapter 15 of the safety analysis report. This is plant-specific action item 6.6.

4.1.1.5 Hardware Interrupts in the AC160

The hardware-associated interrupts in the AC160 are the following:

2-Millisecond Clock Tick

The task scheduler is the interrupt service routine (ISR) for the 2-millisecond-clock-tick interrupt. It determines which application task is to be executed by decrementing counters associated with each application task. Application tasks have the next highest priority after the task scheduler and the other interrupt service routines described below.

Backplane Interface Module Interrupt

The backplane interface module is the interface between the backplane and the processor module. When the slow background task is polling the other modules in the rack for status, the backplane interface module waits for a reply from each one. When the backplane interface

module receives the status reply, it generates an interrupt. The ISR for this interrupt reads and clears the status registers in the backplane interface module and passes the status information to the slow background task. The slow background task then proceeds to execute unless a higher priority task is ready (e.g., application program).

Dual-Ported Memory Interrupt

The dual-ported memory generates an interrupt on the process section of the processor module if an exception occurs in the communication section. This is the only time an external process can effect an interrupt, e.g., a severed serial cable. The ISR on the process section makes an entry into the processor error buffer and then exits.

Window Watchdog Timer

Every two seconds the processor diagnostics will test the window watchdog timer. In so doing, it causes an interrupt from the window watchdog timer. The ISR reads the window watchdog timer registers and re-triggers the window watchdog timer before its relay contacts have a chance to open.

Microprocessor Exception Interrupt

This hardware interrupt occurs when the processor detects an exception, like a divide-by-zero error or an invalid instruction. In such cases, the processor halts.

Mirror RAM

The mirror RAM checker issues an interrupt when it detects an error in RAM. This occurs every 2 seconds when the system diagnostics task intentionally generates a RAM error to test the mirror RAM device. The ISR looks to see if the error is a test. If it is, the ISR notifies the system diagnostics that the test was successful. Otherwise, the ISR initiates a system halt.

These ISRs can delay the execution of the task scheduler. However, the task scheduler must refresh the 68360 watchdog timer every 2 milliseconds or else the 68360 microprocessor will halt. To prevent this, each ISR is coded to minimize the number of program steps.

Even with this slight delay, the next 2-millisecond tick will always be on time because the internal timer is independent of the interrupt associated with the tick.

All of these hardware interrupts have been designed for strictly deterministic behavior.

4.1.1.6 Deterministic Performance

The process section of the processor module has one process control program, which consists of several executable units called control modules. Each control module has its own cycle time and execution conditions. When this process control program is compiled into target codes, each control module becomes an operating system’s task. On the basis of predefined priorities, the process section schedules all the tasks using the task scheduler in the system software and executes the tasks accordingly.

The task scheduler is a regularly serviced interrupt service routine. It receives an interrupt every 2 milliseconds from the precision interval timer. It schedules all the tasks in the system software and executes the tasks accordingly. In addition to scheduling, the task scheduler monitors whether executed control module codes are completed within the task scheduler's cycle time. A message is written to the PM646's error log every time the control module is not executed within the cycle time. If this failure occurs four consecutive times, the PM646 system halts and the hardware watchdog timer times out. CENP stated that as long as the measured load of the application on a single processor is less than the predefined load condition, the control module will complete its function within the cycle time. Therefore, for each PM646, CENP will require that at least one control module measure the whole system load condition.

On the basis of this review, the staff finds that the use of interrupts for the operation of the process section is acceptable for the following reasons:

- The 2-millisecond interrupt is a scheduled interrupt rather than an event-driven interrupt; therefore, the interrupt does not introduce unpredictability in the operation of the process section.

- Design features, such as the monitoring scheme, the timing analysis, and the throughput analysis to be performed when developing code, assure the execution of tasks (control modules) within the defined cycle time.

The communication section controls HSL communication. Unlike the process section, the communication section is an event-driven interrupt system. Therefore, execution of a communication section system's task for controlling HSL communication is initiated by an event, such as receiving data from the process section or the HSL. All the events that initiate an execution of the communication section system's tasks arer cyclical.

Because the time allowed for completing the execution of communication section tasks is twice the cycle time of the control module that is being executed by the process section, and tasks performed by the communication section for controlling the HSL are predictable, the communication section is assured to have time to complete execution of the communication section tasks. The communication section performs these tasks to obtain the data from either the process section or the HSL and to prepare the data in a format that can be transmitted over the HSL or processed by the process section. Additionally, because the task priority for transmitting data and the task priority for receiving data are the same, the tasks are not going to be interrupted by each other. In addition, the communication section of one channel is indirectly monitored by other channels and the operator is notified if the one channel fails to send data or sends bad data.

On the basis of this review, the staff finds that CENP addressed risks associated with operation of the communication section by the following activities:

- Forcing the event-driven system to operate as a cyclical system. All the events occur cyclically, providing predictable operation of the communication section.

- Allowing ample time to complete the tasks. Because only a small portion of the time allowed is needed to complete a task, there is a large margin for completing the task.

- Assigning the same high priority to all the tasks associated with controlling the HSL. This feature prevents interrupts while executing the tasks that control HSL communications. Usually, tasks associated with diagnostics are interrupted by tasks that control HSL communication.

- Monitoring operation of the communication section using diagnostic tests and a watchdog timer. This provision addresses any deadlocks.

The staff concludes that the design features, the operation of the AC160 PLC system, and CENP's commitments to perform timing analyses and tests provide sufficient confidence that the AC160 will operate deterministically to meet the recommendations in BTP HICB-21 and is, therefore, acceptable in that regard.

4.1.2 Flat-Panel Display System

The FPDS consists of an Intel-microprocessor-based single-board computer for display and communication programs and a flat-panel display similar to the display on a lap-top computer. CENP stated that although the single-board computer has not yet been repackaged in surface-mount technology, it will retain the following design features.

The flat-panel display is a color thin-film-transistor display that is readable under high ambient light conditions. The display has touch-screen capability.

There is an interface with the AF100 communication bus so data can be communicated with the PM646 processors. Other standard interfaces such as Ethernet and serial links are available for communications to external systems over fiber-optic cables. The most typical external system that the FPDS will interface with is the plant control computer. Non-volatile memory is used for operator setpoints or other applications where warm system starts using updated constants is needed.

Because the FPDS is used for human-machine interface input and output and is used for transmission of data to nonsafety monitoring systems, the design requires less determinism in its operation. The FPDS must ensure the integrity of its interface with the safety-critical side and ensure that its interface with nonsafety systems and its own operation does not adversely effect the operation of the safety-critical side. The staff finds that the Common Q design assures that errors or failures in FPDS hardware and software components are isolated from the AC160-based subsystems.

The FPDS will be used for the operator display and for maintenance and test functions. Its functions include the displaying of real-time process data, the entering of setpoint data, starting automated surveillance tests, and displaying system status. The display provides HMI functions for the Common Q implementations.

The FPDS design description provides for neither self-diagnostics nor automated self-testing nor an FPDS watchdog timer. If communication is lost between the FPDS and the AC160, the FPDS will be assumed to have failed. Each application program call to the FPDS operating system provides a status. The application program must have an error handler to appropriately

dispatch an FPDS error or failure if one occurs. For the operator or technician, a blinking heartbeat symbol on the FPDS shall provide indication that the display system is in operation.

The application designs indicate that a hardware user interface that replicates existing plant capabilities for an application may be chosen as an alternative to the FPDS. Such an implementation would be a plant-specific action item.

On the basis of this review, the staff concludes that the FPDS conforms to the requirements of IEEE Std 603 as augmented by RG 1.75 related to separation between the FPDS and the AC160 PLC system components. However, the staff could not determine the final acceptability of the FPDS because of insufficient information related to the seismic and environmental qualification testing of the FPDS hardware (see Section 4.2.2.2.).

4.1.3 Communication Subsystems

The Common Q platform uses three types of data communication systems to transfer data:

- AF100 network communication for intrachannel communications and separate AF100 bus will also be used for interchannel communications in the DPPS;
- HSL serial communications for interchannel communication; and
- External communications for communication between the Common Q platform and external computer systems.

4.1.3.1 Advant Field Bus 100

The Common Q equipment connected to the AF100 bus includes the OM, the MTP, the ITP, and the AC160 processor chassis. The OM is used for operator functions, such as changing setpoints or viewing control rod positions. The MTP is used for maintenance and test functions in each of the Common Q system channels. The ITP is a testing system, which is an independent AC160 subrack. The ITP performs continuous passive monitoring of expected outputs based on current inputs, automatic active tests, and manually initiated tests.

The AF100 supports two different types of data communication: process data transfer and message transfer. Process data transfer is used for monitoring a plant or equipment status and controlling a process. Message transfer communication is used for changing parameters, loading a program, and performing a diagnostics test.

The AF100 requires the same amount of process data to be transmitted cyclically at all times and allows the maximum amount of message to transfer within a cycle. Normally, a message is transmitted only if there is a message during the cycle time specifically reserved for the message. Therefore, time reserved for the message transfer is not used if there is no message to send.

All data transfers on the AF100 communication system are controlled by the busmaster. The busmaster function is performed by any one of the nodes that have some cyclic data packets to transmit. A node is a communication interface of a module, which is connected to the AF100

bus. When an application software is developed, the nodes that will become the busmaster are identified, and during an initialization, those identified nodes are configured so that they have the capability to become the busmaster. There can be only one busmaster at any given time. Busmastership is normally transferred every cycle. The other nodes that have the capability to become a busmaster will monitor whether the busmaster is operating correctly. If they detect that the busmaster has failed, one of the nodes takes over the busmaster responsibilities. The FPDS never serves as busmaster. If the FPDS fails or halts, the AC160 continues to run without it. It is not required in the safety functions.

The busmaster controls the transmission of data on the AF100 by allowing a node to transmit cyclic data packets according to a scan table. The busmaster broadcasts information on which node to transmit, and that node responds by broadcasting its cyclic data packets. The scan table contains the transmission schedule information on each of the cyclic data packets. The scan table schedule is divided into 1-millisecond intervals, and within those intervals the cyclic data packets to be transmitted from a particular node are identified.

To ensure that the Common Q response time capabilities are maintained, CENP will perform throughput analysis and response time analysis. CENP stated that the Common Q applications have display response time requirements for how quickly the calculation results, system anomalies, and input data need to be displayed. The display response time requirements also include the system's response time requirements for responding to a control action initiated from the display. In addition, to ensure that these display response time requirements are met, CENP will determine the AF100 data set peripherals transfer cycle time from the AF100 network throughput analysis. CENP stated that during the testing phase of the Common Q application it will perform response time tests to validate the design's compliance with both the system response and the display response requirements (see Section 4.1.1.4).

The Common Q uses the AF100 communication system for intrachannel communications, and the AF100 communication system for one channel is completely isolated from the AF100 system of other channels. Therefore, a failure in the AF100 system in one channel does not affect the AF100 communication systems in the other channel(s).

On the basis of this review, the staff concludes that the AF100 communication system satisfies the requirements in IEEE Std 7-4.3.2, Section 5.6, "Independence."

4.1.3.2 High Speed Link

The HSL is a serial RS 432 link that is used for exchanging data between the safety channels. The data transmission cycle time and the amount of data transferred during a cycle is determined by application-specific design. CENP stated that the timing analysis of the communication section is performed as part of the propagation delay analysis of the HSL cross-channel communication. After the configuration of the plant-specific process control program is determined, the data the PM646 transmits are also determined, and fixed for that configuration.

Each processor module has two serial link ports. Each port is a bi-directional link, however, each direction works independently of the other. The transmission is purely unidirectional without acknowledgment from the other side. When a control module transmits data over the HSL, the data is transmitted through both ports. When a control module receives data from the

HSL it specifies the HSL port it wants data from. Therefore, the receive lines on the HSL ports can have different data. Additionally, the devices are also optically isolated from each other. The other channels have the same HSL system. Therefore, a fatal fault in one link or one HSL channel does not propagate to other links.

The integrity of the links and the data transmitted is monitored by the processor module that receives data from the HSL. The receiving processor module declares a link has failed if it has not received data for 150 milliseconds and reports the failure to the application software; the application software takes appropriate action. At the sending end, the processor module transmits a keep-alive signal every 25 milliseconds, even if it has no data to send within that time period. The integrity of data transmitted is monitored by using CRC. The receiving processor module calculates the CRC of the received data and compares it with CRC bits received with the data. If the CRC comparison fails three consecutive times, the processor module declares the link has failed and reports the failure to the application software, which takes appropriate action.

To ensure that safety systems meet the response time requirement, CENP stated that it will perform throughput analysis and response time analysis. In addition, CENP stated that during the testing phase of the Common Q application it will perform response time tests to validate the design's compliance with both the system response and the display response requirements.

On the basis of this information, the staff concludes that the HSL communications meet the requirements of Section 5.6 of IEEE Std 7-4.3.2, 1993, for communication independence.

4.1.3.3 External Communications

The FPDS single-board computer will have two separate hardware communication interfaces: an Ethernet/serial interface and an AF100 interface. Each interface will have its own buffers and software for data communication. The microprocessor and the application codes on the single-board computer will move data from buffers on the AF100 interface card to buffers on the Ethernet/serial interface. The data will then be broadcasted on an external communication bus. This design feature will eliminate propagation of any fault from nonsafety systems to the Common Q systems that perform safety functions. On the basis of this information, the staff concludes that the external communication system meets the requirements of Section 5.6 of IEEE Std 7-4.3.2, 1993, for communication independence.

4.1.4 Power Supply

The selections of the Common Q power supplies have not been finalized. The review of the design and dedication of the power supplies is Generic Open Item 7.2.

4.1.5 Watchdog Timer Module

An external and independent hardware watchdog timer module (WDT) module is planned to monitor the activity of the processing system. The hardware watchdog timer will have a separate timing circuit to detect the lack of activity. Depending on the specific system application, the hardware watchdog timer can be used to annunciate a failure, actuate a

channel trip, or set output states to predefined conditions. Isolation will be provided for those applications where the watchdog timer is connected to external systems.

CENP has not submitted information on the design or dedication of the hardware watchdog timer and it has not yet been subjected to testing for environmental qualification. The review of the dedication of the hardware watchdog timer is Generic Open Item 7.3.

4.1.6 Defense-in-Depth and Diversity

The staff described concerns with common-mode failures and other digital system design issues in SECY-91-292. Common-mode failures could defeat the redundancy achieved by the hardware architectural structure, and also result in the loss of several echelons of defense in depth (provided by the monitoring, control, reactor protection, and engineered safety functions performed by the digital I&C systems).

The staff has established acceptance guidelines for D-in-D&D assessments and has identified four echelons of defense against common-mode failures:

- Control system – The control system echelon consists of nonsafety equipment which routinely prevents reactor excursions toward unsafe regimes of operation, and is used for normal operation of the reactor.

- Reactor trip system (RTS) – The reactor trip echelon consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

- Engineered safety feature actuation system – The ESFAS echelon consists of safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers (cladding, vessel, and containment) to radioactive release.

- Monitoring and indication – The monitoring and indication echelon consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.

As a result of the reviews of advanced light-water reactor (ALWR) design certification applications that used digital protection systems, the staff documented its position in SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Design," with respect to common-mode failure in digital systems and defense-in-depth for the advanced reactors. This position also documented in the SRP BTP HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer Based Instrumentation and Control Systems." There are four points in the position as applied to ALWR design certification applications. These four positions are quoted below.

1. The applicant/licensee should assess the diversity and defense-in-depth of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed.

2. In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of those events.

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, should be required to perform either the same function or a different function. The diverse or different function may be performed by a nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above.

The staff stated in BTP HICB-19 that Points 1, 2, and 3 of this position apply to digital system modifications for U.S. operating plants. Point 4 of this position applies particularly to ALWR design certification applications, but also offers guidance that CENP has applied in the design description for the integrated solution. Depending upon how many of its I&C systems a licensee elects to upgrade in Common Q technology, it may need to apply Point 4. When fully implemented, the Common Q design described in the integrated solution for safety and nonsafety systems is similar to the System 80+ ALWR. The staff has approved this approach of relying on non-safety systems for defense against common mode failures in safety systems in NUREG-1462, the safety evaluation report for the System 80+ ALWR.

The integrated solution appendix describes the implementation of the Common Q Platform for an integrated configuration where some or all of the safety systems are upgraded in Common Q technology. It discuses the replacement of the nonsafety plant control system with ABB computer technology that is diverse from the Common Q. It also describes a set of displays and controls located in the main control room designed to comply with the requirements of Point 4 of BTP HICB-19. A review of the differences between the Common Q and the nonsafety control system implemented using ABB technology is outside the scope of this evaluation and must be addressed in a plant-specific safety analysis. Any Common Q implementations must be supported by a plant-specific safety analysis to be submitted by the licensee. This is plant-specific action item 6.11.

On the basis of its review, the staff found that CENP's D-in-D&D assessment methodology is consistent with the staff position stated in BTP HICB-19 and is, therefore, acceptable. Applications correctly following this methodology for a plant-specific diversity and defense-in-depth assessment will be found acceptable.

4.2 Evaluation of the Commercial-Grade Dedication of the Common Q Platform

Commercial-grade dedication is an acceptance process for demonstrating that a commercial-grade item to be used as a basic component will perform its intended safety functions and, in this respect, is equivalent to an item designed and manufactured under a 10 CFR Part 50 Appendix B quality assurance program. Dedication of commercial-grade items may be performed by licensees or by third-party dedicators. CENP is a third-party dedicator for the Common Q platform.

Under "Requirements on the Dedicator" EPRI TR-106439 states the following:

> The process of performing commercial-grade item procurement and dedication activities is itself a safety-related process and, as such, must be controlled and performed in accordance with a quality assurance (QA) program that meets the requirements of 10 CFR 50 Appendix B. This applies to the dedicating entity whether it is the utility or a third-party dedicator.

CENP is an approved 10 CFR Part 50 Appendix B supplier. The staff does not attempt in this review to renew CENP's status as an approved 10 CFR Part 50 Appendix B supplier. However, during a visit to a CENP site, the staff did audit a sampling of CENP's manuals for CGD activities. On the basis of the audit, the staff finds that the procedures and processes in the manuals correspond to the requirements of IEEE 7-4.3.2 and the guidance of EPRI TR-106439 and, therefore, provide an acceptable program for the dedication of commercial-grade items.

In the topical report, CENP has committed to meeting the requirements of IEEE Std 7-4.3.2 and the guidance of EPRI TR-106439 for the commercial-grade dedication of the Common Q platform. TR-106439 discusses four methods of commercial-grade dedication: (1) special tests and inspections, (2) a commercial-grade survey of the supplier, (3) source verification, and (4) acceptable supplier and item performance records. As noted in TR-106439 (supported by Generic Letters 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products," and 91-05, "Licensee Commercial-Grade Procurement and Dedication Programs"), typical applications will require more than one method, and will likely require that methods 1, 2, and 4 all be used. CENP uses methods 1, 2, and 4 for the qualification of the Common Q platform.

The CGD of the Common Q platform includes the CGD of both the PDS and the hardware. The vendor survey applies to both the PDS and the hardware. The seismic and environmental qualification of the hardware also includes operation of the PDS and some new software to verify continued operation of the hardware throughout the qualification testing.

There are two main categories of PDS for the Common Q. These are (1) the PDS for the AC160 system, and (2) the PDS for the FPDS. Two separate CENP review teams surveyed the vendors for these two categories and issued separate reports of the commercial-grade dedication effort. Similarly, there are two groups of hardware to receive the seismic and environmental qualification testing. These are (1) the AC160 components that will be used in the Common Q and (2) the balance of the Common Q hardware. The former group has been tested and the staff has reviewed the test reports. The latter group has yet to be tested. The staff's evaluation of CENP's dedication activities follows.

4.2.1 Vendor Surveys

4.2.1.1 Vendor Survey for AC160 PLC System

The CENP audit team conducted the quality evaluation of the AC160 PLC system planned to be used to develop and implement the custom-application, safety functions of the RPS for the Oskarshamn Modernization Project (O1 MOD) in Sweden. The staff finds that the PLC system planned for the O1 MOD at Oskarshamn is the same as that which will be used for the AC160 hardware and software components in the Common Q and, therefore, that the quality evaluation done for the O1 MOD is applicable to the commercial-grade dedication of the PDS for the AC160 in the Common Q. The safety grade application at Oskarshamn is equivalent to Class 1E.

The CENP audit team has issued two reports for that Oskarshamn audit. These are "Design and Life Cycle Evaluation Report on Previously Developed Software in AC160, I/O Modules and Tools (DLCE)," and "Generic Operating History Evaluation Report on Previously Developed Software in AC160, I/O Modules and Tool Software (GOHE)." For both reports, the title mentions the previously developed software while omitting reference to the associated hardware. The staff found, however, that both reports also included the necessary details of the evaluation of the associated hardware.

The DLCE report covers the following areas:

- Product descriptions;
- Functional requirements;
- Design requirements;
- Software development;
- Hardware/software integration;
- Validation (testing);
- User documentation; and
- Maintenance.

The DLCE report is augmented by the GOHE report, which covers the following areas:

- The release history of the products being evaluated (including the history of the AC110 as predecessor version of the AC160);

- Review of all hardware and software problems since the original release and when they were resolved (including release updates);

- The error notification procedure; and

- The change notification procedure.

The AC160 PDS is composed of the AC160 software, S600 I/O Module(s) software, and ABB Tool software. The evaluation is based on the requirements specified in International Electrotechnical Commission (IEC) standard IEC 880, "Software for Computers in the Safety Systems of Nuclear Power Stations." IEC 880 is referenced in IEEE Std 7-4.3.2, "IEEE

Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." IEC 880 is comparable to IEEE Std 7-4.3.2, and the staff has found standard IEC 880 to be an acceptable equivalent.

CENP stated that the purpose for these reviews was to assess the quality of the following during the vendor's software life cycle:

- System requirements;
- Development methodologies;
- Test procedures;
- Configuration management and maintenance procedures; and
- Documentation.

The CENP review team reports show that they performed the following activities at each of the vendor sites they visited in their review:

- Provided introduction/training to the vendor personnel on the audit process.

- Conducted interviews with quality assurance personnel and engineers.

- Reviewed documents from each phase of the development life cycle (planning, requirements, SW requirements, design, integration, validation, commissioning, exploit/maintenance).

- For the exploit/maintenance life cycle phase:

    - Examined error reporting process
    - Examined error resolution process
    - Examined error notification process
    - Obtained AC110, AC160, S600, and tool error reports
    - Determined what training was available

The CENP team discovered some discrepancies in the comparisons between the IEC 880 life cycle phase requirements and activities and those which were performed during the development of the AC160 PDS. The team reported the discrepancies at the end of each section of the report. Each discrepancy was evaluated and, if resolved, its resolution is discussed. A summary of the discrepancies and the team's resolution of these is found in Section 7 of the DLCE report.

Some AC160 software error reports have not been closed by CENP. These errors are being tracked by CENP for resolution. The selected version of the AC160 base software is AC160 1.2/0. The selected version of the ACC tool software is ACC 1.7/0. Both are being considered for revisions before use for the Common Q. The V&V team for the nuclear application must formally examine the existing PDS error reports, including any recent PDS error reports, open at the time of the development of the application software to ensure that the nuclear application is not impacted. It is CENP's responsibility to perform these actions. Because the process for doing so is controlled by the SPM, this need not be considered a generic open item. (See Section 4.3 for the evaluation of the SPM.)

IEEE Std 7-4.3.2 does not require V&V on the ABB software development tools if the end products developed from these tools are subjected to a V&V process that will detect flaws introduced by these tools. The application V&V and testing program prescribed in the SPM includes provisions to detect these types of flaws. Therefore, CENP has excluded the software development tools to be used when writing the project-specific application software from the V&V requirements of the program for commercial-grade dedication. The staff concludes that this is acceptable.

There are no open error reports for the hardware. The staff's review of the seismic and environmental qualification for the AC160 hardware is reported in Section 4.2.2.1.

CENP created BA AUT-99-ADVANT-00, "Agreement for the Supply of Advant Hardware and Software Components," dated February 2, 1999. This is a value-added reseller agreement entered into with ABB Automation Products (ABB Products) located in Vasteras, Sweden that establishes the basis for configuration control and continued availability for the safety system AC160 equipment. BA AUT-99-ADVANT-00 describes required documentation and configuration control parameters that, when placed into effect and verified, will ensure that the resulting product is suitable for safety system applications.

The AC160 products manufactured in Sweden that conform to the requirements of BA AUT-99-ADVANT-00 are supplied to CENP in Windsor, Connecticut. The individual modules and assemblies are subjected to an incoming receipt inspection by CENP. Configuration information is maintained in a documentation database that contains the reference details, including the makes, models, and revisions, etc.

ABB Products controls the detailed arrangement and fabrication drawings of all printed circuit boards (PCBs) and module assemblies. The drawings show the physical location and identification of all parts. Digital images will be taken of the PCBs for all AC160 equipment. The digital images will serve as a record of the actual assembly of each AC160 module used for safety system applications. The digital images will be contained in a database to support configuration by the serial number and the date code of delivered units. The resolution of the digital image allows for detailed inspection (i.e., high-resolution zoom) of each PCB. The digital images will be controlled by CENP.

These requirements and processes establish a detailed configuration for the safety-related AC160 equipment. The traceability aspect of the configuration will be a trail that defines an explicit original manufacturer of completed assemblies that are identified by unique serial numbers and date codes. Only parts defined on the Approved Parts List from approved suppliers will be used.

The staff visited CENP's site, reviewed BA AUT-99-ADVANT-00, and concludes that it conforms to the procurement guidance in EPRI TR-106439 and is, therefore, acceptable.

The staff has reviewed the reports of the dedication of commercial-grade AC160 hardware and software for use in nuclear safety systems. On the basis of the foregoing, the staff concludes that the AC160 PLC system meets the requirements set forth in BTP HICB-18 and follows the guidance in EPRI TR-106439 and is, therefore, acceptable for use in nuclear power plants.

4.2.1.2 Vendor Survey for the FPDS

The FPDS is used in the Common Q as both the OM and the MTP. The OM is placed in the MCR to permit operators to monitor the safety channels. The MTP is mounted in the equipment cabinets and is used by technicians to perform maintenance and test functions on the Common Q platforms in the safety channels. Neither the OM or the MTP is required to be operational when the Common Q is called upon to initiate automatic safety functions. The Common Q safety functions are initiated by the AC160 system components and software, independent of whether the FPDS is operational at the time.

The evaluation of the CGD for the FPDS PDS is based on the requirements specified in IEEE Std 7-4.3.2 as endorsed by RG 1.152 and the guidance in EPRI TR-106439. The qualification process is accomplished by comparing the commercial-grade item to the design criteria of the standard. This standard allows the use of compensating factors to substitute for missing elements of the software development process.

A CENP CGD audit team visited the site of QNX Software Systems Limited (QSSL). Because QSSL did not use a formal software design life cycle process in the development of its products, the CGD audit plan focused on the following:

- Tools used to develop software products;
- Software architecture;
- Software version control;
- Customer service performance record;
- Vendor performance record; and
- Product performance record.

The two products that will be used for the run-time environment for the FPDS for Common Q applications are:

- QNX operating system including the TCP/IP module, and
- Photon microGUI GUI system.

The tools used to develop QNX and Photon are:

- Watcom compiler/linker, Version 10.6, and
- QNX photon application builder (PhAB), Version 1.13.

QNX only used the Watcom C compiler and not the C++ compiler.

The CENP team prepared their audit plan and developed the checklists to be used in the audit. The CENP team examined the vendors' records and reports and interviewed members of the vendors' staff.

The CENP audit team documented their findings in the report, "ABB Commercial Grade Dedication Report for the QNX Operating System for Common Q Applications," Rev 00, dated November 11, 1999 (QNX CGD Report). The checklists and findings for each of the above

parts of the plan are presented in the appendices to the QNX CGD report. The staff has reviewed the report and its appendices and has documented its findings below.

Appendix 1 in the QNX CGD report lists the open errors for both Watcom 10.6 and PhAB 1.13 tools. The staff concurs with the CENP assessment that the identified open errors can be adequately dealt with by requiring the software engineers that will develop the application programs for the Common Q to acquaint themselves with this list before generating application programs. The SQAP in the SPM also dictates that the software engineers shall become familiar with any open errors or problems, and that includes any that become known up to the time of the programming activity.

Appendix 2 in the QNX CGD Report presents the checklist and findings for software architecture. The CENP audit team and the CENP SPM each stipulate that before the initiation of any Common Q project, the software engineers assigned to the project must review this appendix so as to use recommended coding practices in their design.

The CENP audit team reviewed the QSSL program for tracking problem reports and their resolution. The team identified 52 problem reports that related to the products that will be used in the FPDS. These are listed in Appendix 3 in the QNX CGD Report. Several of the problem reports have not been closed by QSSL. In the QNX CGD Report and its appendices the CENP audit team discusses and resolves each of its negative findings.

One negative finding is with regard to problem report number 264. This remains open because the problem description, which is reported to cause QNX to halt, is not detailed enough to determine the cause of the failure. CENP stated that if this reported problem should occur in the operation of the FPDS the halt of the FPDS will be detected by the AC160 and annunciated in the MCR. Also, the flashing "heartbeat" indicator on the display of the FPDS would stop flashing, giving notification to anyone viewing the display that it had stopped. CENP indicates that this event is acceptable because the FPDS is not required to be operating when the AC160 initiates a safety function. The staff finds this limitation on the use of the FPDS to be acceptable.

The CENP V&V team for the nuclear application must formally examine the existing PDS error reports, including any recent PDS error reports, open at the time of the development of the application software to ensure that the nuclear application is not impacted. It is CENP's responsibility to perform these actions. Because the process for doing so is controlled by the SPM, this need not be considered a generic open item. (See Section 4.3 for the evaluation of the SPM.)

CENP did not dedicate the software development tools. IEEE Std 7-4.3.2 does not require that the software tools be dedicated if the V&V process will detect errors that the tools may introduce. The CENP V&V procedures are specified in the SPM and have been evaluated in this safety evaluation. IEEE Std 7-4.3.2 requires that the tools be identified and placed under software configuration management control. CENP configuration management is evaluated and found acceptable in Section 4.3.1.k. On the basis of the above, the staff concludes that it is acceptable that the PDS development tools from QSSL not be dedicated.

In the QNX CGD Report CENP noted that QSSL does not provide a maintenance manual for their software products. CENP has committed to develop a technical manual for each of the Common Q system. The CENP audit team indicates that the CENP technical manual will provide error diagnostic and trouble shooting information. The staff observes that CENP's SPM specifies that CENP will develop and provide a technical manual for each Common Q system. The staff concludes that the above provisions for a technical manual are acceptable.

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 completion and staff review of the value-added reseller agreement with QSSL is Generic Open Item 7.4.

Even though there is a newer version of QNX available (called Neutrino) that has better documentation of the software design life cycle, CENP selected QNX4 on the basis of its maturity and stability of product. Operating history data for QNX4 is estimated to be in excess of 6000 product years. Operating history data for Photon microGUI is in excess of 1000 product years. On the basis of the guidance in EPRI TR-106439, the staff concurs in this selection of the older QNX4 over the newer Neutrino.

CENP selected the vendor's products QNX4, Version 4.25b and Photon microGUI, Version 1.13b as suitable for use as the FPDS operating system and display system, respectively. CENP plans to use the selected versions of these two products in all future FPDS installations in Common Q applications.

On the basis of the review of the QNX CGDR, the staff concludes that CENP has acceptably dedicated the commercial-grade QNX4, Version4.25b and Photon microGUI, Version 1.13b in accordance with the guidance in EPRI TR-106439 for use as the operating system and display builder for the FPDS in the Common Q. 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 it is required to be operational when the Common Q system is called upon to initiate safety functions. This is plant-specific action item 6.3.

For the qualification of the FPDS hardware, see Section 4.2.2.2.

4.2.2 Seismic and Environmental Qualification

4.2.2.1 Environmental, Seismic and Electromagnetic Qualification of the AC160

This section is the staff's evaluation of the environmental, seismic and electromagnetic qualification of the AC160 PLC system hardware components that will be used in the Common Q platform. CENP decided to test both the PM645C and the PM646 processor modules. The items that were tested are:

- Processor 19-inch subrack
- Expansion 19-inch subrack
- PM645C processor module

- PM646 processor module
- CI631 communication interface module
- Eight models of S600 I/O modules to include:
    - AI620
    - AI635
    - AO650
    - DI620
    - DO620
    - DO625
    - DO630
    - DP620
- TC630 fiber-optic modem
- TC514 fiber-optic modem
- OZDV 114 fiber-optic modem
- TC625 wire modem

Common Q platform equipment is qualified for a mild environment, such as a main control room and auxiliary electrical equipment rooms. CENP performed the following tests: EMI/RFI testing, environmental testing, and seismic testing. For these tests, CENP used two groups of test specimens: one for the EMI/RFI test and one for all the other tests. For the EMI/RFI test, the test group AC160 system is configured to replicate the worst case hardware configuration that encompasses the intended applications of the Common Q platform equipment. For the other tests, the AC160 system is configured to represent the loading conditions of the anticipated Common Q applications.

Criteria for environmental qualifications of safety-related equipment are provided in 10 CFR Part 50, Appendix A, GDC 2, "Design Bases for Protection Against Natural Phenomena," and GDC 4, "Environmental and Dynamic Effects Design Bases." The staff conducted its reviews in accordance with the guidance provided in SRP Appendix 7.1-A, which references Appendix 7.1-B, item 5, and Appendix 7.1-C, item 9. These two items reference ANSI/IEEE Std 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," and EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants."

4.2.2.1.1 Temperature and Humidity

CENP demonstrated that the Common Q platform equipment will function under applicable temperature and humidity conditions by subjecting the test specimen to a series of temperature and humidity conditions and monitoring the performance of the test specimen. The test shows that none of the AC160 modules failed to function as a result of the environmental conditions imposed by the test. The environmental conditions imposed by this test envelop the test conditions specified in EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," dated 1998.

CENP stated that the temperature inside the cabinet is determined on the basis of an assumption that there is a maximum temperature rise of 18^{o}F inside the cabinet. Additionally, CENP stated that an analysis will be performed for each application to ensure that the design basis temperature (test temperature minus the IEEE Std 323 margin requirement) of the

Common Q equipment is not exceeded when installed in the cabinet. The analysis demonstrates, using extrapolated test data, that individual component and equipment temperature specifications are not exceeded within the cabinet/enclosure when the cabinet is exposed to the environmental conditions as specified in Table 8.2-1 of the topical report. Therefore, the staff concludes that the tests provide assurance that the Common Q equipment will operate properly in its environmental conditions. Additionally, the staff concludes that for plant-specific Common Q systems, the licensee should validate that CENP's temperature analysis is applicable to its plant-specific application before installing the Common Q system for a safety system in a nuclear power plant. This is plant-specific action item 6.4.

4.2.2.1.2 Seismic Testing

CENP mounted the test specimens to a tri-axial seismic simulator table and subjected the test specimens to a series of seismic simulation tests. The tests performed on the test specimens include resonance search tests and random multifrequency tests. The random tri-axial multifrequency tests, which simulate a series of earthquake environments were performed in accordance with IEEE Std 344-1987. CENP stated that Common Q equipment is designed to withstand the cumulative effects of a minimum of five operating basis earthquakes and one safe shutdown earthquake without loss of either safety function or physical integrity.

On the basis of this review, the staff concludes that the tested AC160 equipment is qualified to the triaxial seismic simulator table limits shown in Figure 4-2 of the Wyle report attached to Test Report 2008677-IC-TR560-10, Revision 00, "Seismic Qualification Report for Module Equipment Qualification for Common Q Applications." Therefore, the staff finds that before installing the plant-specific Common Q equipment, a licensee needs to verify that the required response spectra for the Common Q equipment to be qualified are enveloped by the response spectra shown in Figure 4-2, as cited above. Additionally, because CENP configured the test specimen using dummy modules to fill all the used rack slots, the licensee also needs to verify that its Common Q system does not have any unfilled rack slots. This is plant-specific action item 6.4.

4.2.2.1.3 Electromagnetic Interference and Radio Frequency Interference

EPRI submitted Topical Report TR-102323, "Guideline for Electromagnetic Interference Testing in Power Plants," for staff review in 1994. The topical report was developed by EPRI to recommend alternatives for performing site-specific EMI surveys for qualifying digital plant safety instrumentation and control equipment in a plant's electromagnetic environment. The recommendations in TR-102323 include (1) a set of EMI/RFI susceptibility testing levels, (2) EMI eliminating practices, and (3) equipment EMI/RFI emission testing levels. The above recommendations are based on EMI/RFI emission data collected during 1993 and 1994 at seven nuclear power plants and data collected before 1993 at other nuclear power plant sites. In 1996, the staff issued a safety evaluation concluding that the TR-102323 recommendations and guidelines provided an adequate method for qualifying digital I&C equipment for a plant's electromagnetic environment without the need for plant-specific EMI surveys if the plant-specific electromagnetic environment is confirmed to be similar to that identified in TR-102323.

CENP performed electromagnetic compatibility (EMC) tests and measurements on the AC160 portions of the Common Q platform equipment in accordance with EPRI TR-102323. The details of the test and measurements are described in 2008677-IC-TR560-12, "EMI Qualification Test Report for Common Q Applications."

Before starting the tests, CENP decided to use four PM645C modules and one PM646 module in the test. Including both models into the qualification process does not affect the physical configuration because PM646 and PM645C have the same physical configuration. However, the staff finds that using PM646s where the PM645Cs were used in the EMC tests might affect how the Common Q equipment responds to the EMI/RFI signals. Therefore, to resolve any issues that might arise from replacing PM645Cs with PM646s, CENP stated that it will perform additional EMC tests and measurements on the PM646 during planned EMC testing of the new Common Q equipment. The staff's review of this planned testing is Generic Open Item 7.5.

CENP stated that the test specimen hardware configuration was configured to simulate the worst case hardware configuration to encompass the expected applications of the equipment. CENP simulated the worst case hardware configuration by configuring the AC160 to the maximum load without going to a bus extension, which would allow the addition of up to another two AC160 racks. CENP stated that it does not expect to configure the AC160 beyond the tested configuration. In addition, to create the worst-case operating conditions during the tests and measurements, all the modules are actively used.

CENP performed four emission tests and seven susceptibility tests on the test specimen. Table 6-0 of 2008677-IC-TR560-12 shows the list of tests and measurements performed on the test specimen and Table 7-0 of that report shows the results of those tests and measurements. Table 7-0 shows that during the tests and measurement, CENP recorded some anomalies.

Therefore, the staff finds that the AC160 equipment did not meet the EMI susceptibility requirements of TR-102323. The staff, however, accepts the EMI test results reported in 2008677-IC-TR560-12, and concludes that AC160 equipment is acceptable to the levels to which the equipment is tested. Before an installation of AC160 equipment in a nuclear power plant, the licensee needs to perform analysis to ensure that the plant environment is enveloped by the test levels and the EMI emission from the AC160 system does not affect the surrounding equipment. This is plant-specific action item 6.4.

4.2.2.2 Seismic and Environmental Qualification of Non-AC160 Hardware

CENP has not yet conducted seismic and environmental qualification testing on the non-AC160 hardware components. Items not yet tested include:

- FPDS
- WDT
- Power supply modules

The review of the seismic and environmental qualification of non-AC160 hardware is Generic Open Item 7.6.

4.3 Evaluation of the Life Cycle Planning Process for Application Software

CENP submitted CE-CES-195-P, "Software Program Manual for Common Q Systems" (SPM) for staff review. It specifies the life cycle planning process for application software. It is essentially an updated version of the software program manual for the System 80+, NPX80-SQP-0101.0, "Software Program Manual for NUPLEX 80+," Revision 02, dated February 10, 1994 (SPM80). The staff's review of the SPM80+ is found in NUREG-1462, "Final Safety Evaluation Report Related to the Certification of the System 80+ Design," dated August 1994.

The SPM specifies the development, documentation, utilization and maintenance of software to be developed for use with the Common Q platform in nuclear safety applications . It also provides guidance for the maintenance of commercial-grade hardware and previously developed software.

Where applicable, the staff has referenced the evaluation of the SPM80, however, the staff finds that there have been many changes made to the SPM80 to meet the needs for digital upgrades of existing plants and to address new regulatory requirements. Therefore, the staff has reviewed the SPM according to the guidance in BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." In BTP HICB-14 the information to be reviewed is subdivided into the following three topic areas:

- Software life cycle process planning;
- Software life cycle process implementation; and
- Software life cycle process design outputs.

The SPM specifies procedures and controls for the complete software development process including hardware integration. Since the application software has not yet been developed, the staff's evaluation does not include the review of the outputs of the life cycle process, but is limited to the evaluation of the specified process.

4.3.1 Evaluation of the Software Life Cycle Process Planning

HICB BTP-14, Section 2.1 states that the information to be reviewed for the software life cycle process planning should be found under the following topics:

a. Software Management Plan
b. Software Development Plan
c. Software Quality Assurance Plan
d. Software Integration Plan
e. Software Installation Plan
f. Software Maintenance Plan
g. Software Training Plan
h. Software Operations Plan
i Software Safety Plan
j. Software Verification and Validation Plan
k. Software Configuration Management Plan

While most of the information about the above topics is in the SPM, information found in the other submittals is sometimes helpful to the evaluation, and is considered. The SPM includes sections with the following titles:

- Software Safety Plan (SSP)
- Software Quality Assurance Plan (SQAP)
- Software Configuration Management Plan (SCMP)
- Software Verification and Validation Plan (SVVP)
- Operations and Maintenance Plan

The staff also found the needed information on the balance of the life cycle topics either in the balance of the SPM or in the topical report and its appendices. The staff has organized this report to follow the sequence outlined under the topic in BTP HICB-14. For ease of reference, the lower case letter in each section heading below matches the lower case letter in the list of topics above, which is the same as in BTP HICB-14.

4.3.1.a Software Management Plan

The elements of the software management plan are incorporated into the SPM. The staff has reviewed the SPM and finds that it establishes the organization and authority structure for the design, the procedures to be used, and the relationships between major activities. The staff finds that the management structure in the SPM provides adequate project oversight, control, reporting, review, and assessment. The staff concludes that the SPM meets the requirements for the software management plan as outlined in BTP HICB-14 and is, therefore, acceptable.

4.3.1.b Software Development Plan

The staff found the elements of the Common Q application software development plan to be distributed throughout the SPM. The staff has reviewed the SPM and concludes that the software development plan conforms with the guidance in IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," as endorsed by RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." These documents describe acceptable methods of organizing the software life cycle. The staff, therefore, concludes that CENP's application software development plan is acceptable.

4.3.1.c Software Quality Assurance Plan

The Common Q SQAP for application software is described in Section 4 of the SPM, "Software Quality Assurance Plan." Each quality assurance task is described in the SQAP for each software life cycle phase. The plan stipulates that the software QA organization shall participate in formal reviews and audits of the software development activity. Required reviews and audits are indicated in the plan including review documentation requirements, evaluation criteria, anomaly reporting, and anomaly resolution procedures. Additional reporting of the staff's evaluation of the SQAP is detailed in Section 4.3.1.j, "Software Verification and Validation Plan." The staff has reviewed the SQAP and concludes that it meets the requirements of 10 CFR Part 50, Appendix B with regard to QA software reviews and audits and is, therefore, acceptable.

4.3.1.d Software Integration Plan

The staff reviewed CENP's application software development process and found that it specified how to develop plans for software integration both during the development of the software and during integration with the hardware. The actual integration procedures will be prepared during the planning stage of each project. The staff concludes that the plans for software integration exhibit the management, implementation, and resource characteristics outlined in BTP HICB-14 and are, therefore, acceptable.

4.3.1.e Software Installation Plan

The staff reviewed CENP's SPM and found that it included adequate plans for software installation. The procedure(s) for installing the software will be prepared before the installation and checkout phase of the software life cycle. The staff finds that the plans for software installation exhibit the management, implementation, and resource characteristics outlined in BTP HICB-14 and are, therefore, acceptable.

4.3.1.f Software Maintenance Plan

CENP treats both the maintenance and the operation phases of the software life cycle together in SPM Section 7, "Software Operation and Maintenance Plan." CENP used IEEE Std 1219-1992, "IEEE Standard for Software Maintenance," as a guide. Activities associated with the operation and maintenance phase include:

1. Problem/modification identification, classification and prioritization;
2. Problem analysis;
3. Solution design;
4. Solution implementation;
5. Solution / system test; and
6. Delivery.

The staff has reviewed the plan for maintenance of the software as described in the SPM and concludes that it exhibits the characteristics for management, implementation, and resources as set forth in BTP HICB-14 and is, therefore, acceptable.

4.3.1.g Software Training Plan

The SPM specifies the requirements for training programs for end users. For each software system, a separate training program will be developed to ensure safe operation and use of the software within the overall system. The training program will include safety training for the users, operators, and maintenance and management personnel, as appropriate. The SPM stipulates that a training record will be kept on file for each training session recording the instructor, date, material covered, and personnel attending, to ensure that the appropriate training has been obtained before using the system. The V&V team will review the training documentation for traceability to safety requirements. The training programs for use at the sites will be developed later. This is an activity that will be influenced by the end users' training facilities and procedures. The staff concludes that the specified plans for training of the

software developers and end users meet the criteria outlined in HICB BTP-14 and are, therefore, acceptable.

4.3.1.h Software Operations Plan

CENP treats both the operation and the maintenance phases of the software life cycle together in SPM Section 7, "Software Operation and Maintenance Plan." CENP plans for the operation of the software are also discussed in other places in the topical report and its appendices. Application-specific data that reflect the specific methods of managing the software operation will be developed as part of the specific applications. The staff has reviewed CENP's plans for management of software operations and concludes that they are acceptable.

4.3.1.i Software Safety Plan

The staff has reviewed CENP's Software Safety Plan and finds that it addresses the topics described in the SRP and in IEEE Std 1228, "IEEE Standard for Software Safety Plans," as endorsed by RG 1.168. CENP's SSP describes the organizational structure and responsibilities, resources, methods of accomplishment, and integration of system safety with other program engineering and management activities. The hazards evaluations required by the SSP will be documented in the V&V documentation. The SSP identifies the international, national, industry and company standards and guidelines to be followed by the safety organization. The staff concludes that the SSP adequately addresses the topics outlined in the SRP and is, therefore, acceptable.

4.3.1.j Software Verification and Validation Plan

A V&V program for the application software is provided by CENP throughout the SPM. Section 5 of the SPM specifically outlines the proposed SVVP.

The staff reviewed the Common Q SVVP for application programs against the criteria of the Chapter 7 of the SRP. BTP HICB-14 describes a software engineering process for software development that provides adequate V&V. Section 5.3.4 of IEEE Std 7-4.3.2-1993, as endorsed by RG 1.152, provides minimum requirements for V&V. ANSI/IEEE Std 1012-1986, as endorsed by RG 1.168, provides acceptable guidance on developing SVVPs. ANSI/IEEE Std 829-1983, as endorsed by RG 1.170, describes acceptable methods for preparing software test documentation. ANSI/IEEE Std 1008-1987, as endorsed by RG 1.171, describes acceptable methods for software unit testing.

CENP references all of the above-mentioned standards, as well as other standards, as the criteria to be applied to the software V&V process for the Common Q platform. Therefore, the staff finds the standards applied by CENP to be in accordance with the SRP.

The aim of the software V&V program proposed by CENP is to provide an acceptable generic methodology of V&V as part of the qualification process for application computer systems developed under the Common Q platform. CENP plans to apply the SVVP to all the new software to be developed under the SPM and to some previously developed application software to be used in the Common Q platform. For the qualification of existing software, either

for use in the generic Common Q platform or for use in new applications, CENP identifies the following three cases:

- Existing commercial software will be qualified under the Commercial Grade Dedication Program, which is outlined in the topical report.

- Existing non-commercial software that has been actively used in nuclear power plants will be qualified for the Common Q platform by judging its original V&V program. The V&V effort will make this judgment using review criteria similar to those for newly developed software.

- Other existing non-commercial software may be used under the conditions that (1) the software fulfills a specific requirement identified in the software requirements specification, (2) the code is well organized and has adequate design documentation and source code commentary to permit the application of the V&V process, and (3) the software be subjected to the V&V process, starting at the design phase.

For the development of new application software, depending on the scope of each specific project, CENP will decide whether to issue a project-specific SVVP or to maintain the generic plan as is. The use of the generic plan will require that the software developers manage the deviations and the project-specific aspects through the project-specific plan to be developed for each project. CENP will hold these project-specific SVVPs for audit. CENP also will hold the project-specific V&V reports for projects developed under the Common Q platform for audit, and the licensees will hold the V&V reports associated with plant-specific applications for audit. Succeeding systems manufactured under the same design as a system that was previously verified and validated in accordance with this SVVP will be certified by performing, as a minimum, the equivalent of the validation tests that were applied to the verified and validated system. The staff considers this approach to be acceptable.

CENP differentiates the span of the V&V activities and the grade of independence required for V&V reviewers according to the classification of each software item. The SPM classifies software into four integrity levels: protection, important to safety, important to availability and general purpose. These four levels respectively are matched to the four categories in IEEE Std 1012-1998 of high, major, moderate, and low.

CENP has followed the guidance provided in IEEE Std 1012-1986 regarding structure and content for SVVPs when developing the Common Q SVVP. IEEE Std 1012-1986 requires that a SVVP be written for both critical and noncritical software, and provides the uniform and minimum requirements for the format and content of these plans. Additionally, the standard defines the minimum set of specific V&V tasks to be carried out during each phase of the critical software development life cycle and the required inputs and outputs for these tasks. For noncritical software, this standard does not specify a minimum set of required tasks, but states that all other requirements of the standard shall be satisfied and recommends that the minimum tasks for critical software also be employed for noncritical software.

The Common Q SVVP incorporates verification reviews and validation testing. Verification reviews are supported by the use of checklists and requirements traceability analyses for the phases of requirements, design, implementation, test, and installation and checkout. A

requirements traceability matrix will be prepared at the beginning of the software development process and updated throughout the phases of the software life cycle.

Validation testing includes structural and functional testing. Structural testing is performed on software modules and units by path testing. Module and unit testing will be performed in accordance with IEEE Std 1008-1987 (endorsed by RG 1.171). Functional testing is performed on the integrated computer system to determine whether the system meets its functional requirements (functional operations, system level performance, external and internal interfaces, stress testing, testability, and other requirements, as stated during the concept phase).

For protection and important to safety software, verification reviews are performed by the V&V staff. Preparation of test plan, procedures, and result reports and execution of the tests are carried out by the design team or by the V&V team itself. When the design team prepares the material or executes the tests, the V&V team will oversee the conduct of these activities by reviewing documentation and witnessing testing.

Test documentation will be prepared in accordance with IEEE Std 829-1983 (endorsed by RG 1.170). After the system is validated, a Code certificate is issued certifying that the system is acceptable for use. The SVVP addresses V&V activities associated with the operation and maintenance phase by ensuring that program modifications are submitted to the same V&V program applied to new software development. Software changes will be evaluated by a software safety change analysis, the results of which shall be found in the V&V report. The SVVP addresses the use of regression testing for the V&V of software modifications.

The SVVP also addresses activities designed to verify the adequacy of the software development documentation issued throughout the software life cycle, installation procedures, training materials, and user documentation.

As a result of the V&V activities throughout the software development process, V&V phase summary reports, including discrepancy reports, will be issued. A final V&V report will be issued after the V&V process, including the assessment of the overall software and system quality and a Code certificate. Results of V&V analyses performed on requirements, design, code, test, and other technical documentation are documented in the V&V phase summary reports and the final V&V report. Information on suspected or confirmed safety problems in the pre-released or installed system is recorded in the final V&V report. Results of audits performed on software safety program tasks are documented in the V&V phase summary reports and in the final V&V report. Results of safety tests conducted on all or any part of the entire system are documented in the test report. Software safety certification is documented in the Code certificate.

The SVVP is reviewed for adequacy and completeness of the V&V methods by an independent reviewer meeting the qualifications of QPM-101 "ABB CENO Quality Procedures Manual."

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 Generic Open Item 7.7.

On the basis of this review, the staff finds that the content of the Common Q SVVP for the development of application programs to be in accordance with the SRP, the requirements of HICB BTP-14, and the guidance of IEEE Std 7-4.3.2 and ANSI/IEEE Std 1012-1986 and is, therefore, acceptable, provided the staff accepts the resolution of the foregoing generic open item.

Independence of Verification and Validation

Part 50 of 10 CFR addresses the independence requirements for organizations performing quality control activities through Criterion I and Criterion III of Appendix B. Criterion I requires that individuals and organizations performing quality assurance functions have sufficient independence from cost and schedule. Criterion III requires that individuals or groups performing design control activities be different from those who performed the original design, but they may be from the same organization.

The positions reflected in specific standards addressing V&V activities associated with the implementation of digital I&C systems go from requiring only technical independence, as in RG 1.152 by endorsing IEEE Std 7-4.3.2-1993, to requiring technical, financial and schedule independence, as in RG 1.168. IEEE Std 1012-1986, endorsed by RG 1.168, does not specifically address the level of independence required, but it does address it in the most recent revision, IEEE Std 1012-1998. The 1998 version of the standard, not yet endorsed by any RG, includes an informative annex contemplating the position that for high-integrity-level software, the level of independence required for the V&V organization encompasses technical, managerial, and financial independence.

The organization responsible for ensuring that the Common Q software has been developed according to the quality required by its classification (called the software safety organization in the SPM) is composed of two parts:

- An independent quality assurance organization, which performs the verification of the implementation of quality assurance requirements according to Appendix B of 10 CFR Part 50. This organization, outside the cognizant engineering organization (CEO), generates the quality assurance procedures and directives that are followed by all CEOs in CENP.

- An independent V&V Team within the CEO that performs the safety activities of the CEO for a given Common Q system implementation project.

Within the CEO, software activities are organized into two teams: the design team, responsible for the development of the software, and the V&V Team, which performs the V&V activities. The manager of the CEO is responsible and accountable for both technical and administrative aspects associated with the development and V&V tasks for each system assigned to the CEO. The manager may assign a project manager to be responsible for the development of the software for a specific Common Q project. The CEO manager shall assign the appropriate resources to the project manager and the V&V team leader. Members of the V&V team are not allowed to participate on the design team, even on a part-time basis, while a safety-class system is being designed. The V&V team leader, responsible for the V&V, must not be the

design team leader. Additionally, the independent reviewer must also be competent to perform the review.

CENP states that the V&V leader is responsible for the schedule and budget for the V&V activities, the project manager is responsible for the schedule and budget for the activities associated with the software development and, therefore, financial and managerial independence between the development group and the V&V group is achieved.

The staff finds that the CENP approach on independence of V&V for the Common Q platform is in accordance with the requirements of IEEE Std 7-4.3.2, and is compatible with IEEE Std 1012, "Software Verification and Validation Plans," as endorsed by RG 1.168 and is, therefore, acceptable.

4.3.1.k Software Configuration Management Plan

CENP's SCMP is found in Section 6 of the SPM. CENP's SCMP describes the organizational structure that controls the configuration of the software during the development and during the operation and maintenance phases. It describes the independence of those responsible for system software configuration management functions from those responsible for verification and validation activities related to configuration management. The SCMP describes the process for configuration control including configuration identification, software change request, software change authorization, module and unit release history, baselines, and backups. The SCMP describes the software configuration management activities related to the software project baselines, the configuration change control authority and management, methods of access control, and the configuration status control log maintenance. Project-specific configuration management data that reflect the specific methods of managing the software configurations will be developed as part of the project plan required for every Common Q project. The SCMP identifies the international, national, industry, and company standards and guidelines to be followed for the software configuration management activity.

The staff concludes that the SCMP conforms to the requirements identified in IEEE Std 828 and IEEE Std 1042, which are endorsed by RG 1.169. This conforms to the guidance in HICB BTP-14 and is, therefore, acceptable.

4.3.2 Summary of the Evaluation of the Life Cycle Planning Process

On the basis of the foregoing review of CENP's software development process for application software, the staff concludes that the SPM specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the staff or others to evaluate the quality of the design features upon which the safety determination will be based. The staff will review the implementation of the life cycle process and the software life cycle process design outputs for specific applications on a plant-specific basis. This is plant-specific action item 6.5.

4.4 Evaluation of the Common Q Applications

CENP has submitted Appendices 1 through 4, which describe proposed design approaches for implementing the Common Q platform in various safety systems at nuclear power plants. None of the designs proposed in the Appendices are complete and, therefore, the staff is not able to evaluate all portions of the proposed designs. For example, some of the hardware has not been fully tested yet, some is still subject to change, and final selection for some of the components has not yet been made. However, these appendices provide additional information to support the staff's review of the generic design details of the Common Q platform. The staff has evaluated the content of the appendices and includes in this safety evaluation the report of its findings.

4.4.1 Appendix 1 – Post-accident Monitoring System

4.4.1.1 Description

CENP's CENPD-396-P, Appendix 1, "Post Accident Monitoring Systems," provides the functional requirements and conceptual design approach for upgrading an existing PAMS based upon Common Q components.

The PAMS is a Class 1E safety-related alarm and display system. Each PAMS system consists of two independent channels of equipment (Channels A & B), which acquire and process two separate channels of inputs. The channels are physically separated and electrically isolated from each other. The proposed PAMS system also includes the QSPDS and PAMS channel implementation includes automatic self-testing.

4.4.1.2 Specific Evaluation Criteria for PAMS

The replacement components described in Appendix 1 must provide functionality and safety that are at least equivalent to that of the PAMS equipment being replaced. SRP Section 7.5, "Information Systems Important to Safety," provides review criteria that are applicable to PAMS. The staff's review of Appendix 1 draws especially upon the guidance and criteria in the following codes and standards:

- 10 CFR 50.55a(h), IEEE Std 279, item 4.7.2, "Isolation Devices"
- BTP HICB-10, "Guidance on Application of Regulatory Guide 1.97"
- RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems""
- RG 1.75, "Physical Independence of Electrical Systems" (endorses IEEE Std 384-1992, "Criteria for Independence of Class 1E Equipment and Circuits")
- RG 1.97, "Instrumentation for Light-water-cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident"
- GDC 13, "Instrumentation and Control"
- GDC 19, "Control Room"
- GDC 24, "Separation of Protection and Control Systems"

4.4.1.3 PAMS Evaluation

In Appendix 1, CENP stipulates that the Common Q PAMS will be designed to provide the same functionality as that of the existing PAMS system. The process parameters and corresponding ranges will be designed to conform to the respective plant's requirements for RG 1.97. The licensee must verify that these have been met as a plant-specific action item (see plant-specific action item 6.8).

NUREG-0737, "Clarification of TMI [Three Mile Island] Action Plan Requirements," specifies TMI-related actions which utilities must complete for emergency response facilities, inadequate core cooling and accident monitoring. The PAMS upgrade will replace equipment that presently provides for accident monitoring and inadequate core cooling monitoring. The replacement equipment will continue to provide information and data to the plant monitoring/SPDS (safety parameters display system) computers for use in its control room displays. The PAMS OM will be used to provide control room displays. Electrically isolated PAMS outputs are provided from the AC160 to the plant annunciators.

The PAMS channels must have a response time consistent with that of the present qualified safety parameters display system (QSPDS) implementation. A licensee implementing a Common Q PAMS shall determine that it satisfies the plant requirements with regard to the Chapter 15 accident analysis. This is plant-specific action item 6.6.

Each PAMS channel is electrically independent and physically separated from the redundant PAMS channel, including the isolation of the data link to the SPDS. The Common Q is designed to maintain the plants' existing capability to meet the two channel separation and mechanical isolation requirements of IEEE Std 384 and RG 1.75. Also, each PAMS channel is powered by a separate Class 1E power source.

The PAMS will permit administrative control of access to module calibration. Setpoint changes will be made through software entries. Each PAMS channel will have a key-switch or a password permissive to provide the capability of bypassing any input signals and for changing selected alarm setpoints and parameters. This permissive will be referred to as the bypass permissive. If a key-switch is implemented, it shall be located in the respective PAMS channel cabinet.

When the bypass permissive is actuated, an MTP display will also allow selection of an alarm setpoint value and input of a new value to replace the current value. Reasonability checks will be performed on the new value before it is accepted for alarm processing.

The PAMS HMI is provided by the OM and the MTP. Both the OM and the MTP will include display and diagnostic capabilities unavailable in the existing system. The review of the design details of the HMI for the PAMS is not within the scope of this topical report. The review of human factors considerations for a specific PAMS implementation is plant-specific action item (see plant-specific action item 6.7).

The design will permit periodic checking, testing, calibration and calibration verification. A capability for testing during power operation will be provided. Automated testing will facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or

modules. This automated testing will be designed to run continuously and may perform some of the surveillance functions that are presently performed manually in existing plants. Any resulting changes in plant procedures is beyond the scope of Appendix 1. Such a request by the licensee would constitute a plant-specific action item (see plant-specific action item 6.9).

The PAMS uses the FPDS to perform the alarm and display safety functions. The FPDS is scheduled to receive the same level of seismic and environmental qualification as did the AC160 system. The staff's evaluation of the test results for seismic and environmental qualification for the FPDS is Generic Open Item 7.6.

The PAMS is designed so that any single failure, in either channel, will not prevent proper monitoring, display and alarm action of the other PAMS channels, or inhibit operation of any other system, including the PPS/DPPS, at the system level. CENP submitted a failure modes and effect analysis (FMEA) for the Common Q PAMS with the intent that it might serve as a model for the plant-specific FMEA that the licensee will be required to submit.

The staff reviewed the FMEA prepared by CENP for the PAMS design and finds that a similar approach may be used by a licensee implementing a PAMS design when preparing its specific model and the FMEA. This is plant-specific action item 6.10.

In Section 4.2.1.2, the staff noted that the FPDS may halt in a common mode failure due to an unresolved error report in the QNX operating history. CENP has not analyzed the case of the common-mode failure of the two PAMS channels. Licensees implementing a PAMS design shall demonstrate that the system complies with the criteria for defense against common-mode failure by analyzing the common-mode failure of both PAMS channels. The safe shutdown systems design should be compatible with the SAR Chapter 15 design bases accident analyses. It is not sufficient to evaluate the adequacy of the safe shutdown systems only on the basis of the design meeting the specific requirements of ANSI/IEEE Std 279 or IEEE Std 603. This is plant-specific action item 6.10.

The staff finds that the acceptability of the PAMS design is highly dependent upon the final resolution of the generic open items and plant specific items that relate to the PAMS implementation. Some plants may be more dependent upon the continuous operation of the FPDS than others. On the basis of the above review, the staff concludes that Appendix 1 does not contain sufficient information to establish the generic acceptability of the proposed PAMS design. The staff will review the resolution of the above-mentioned findings and, therefore, the acceptability of a PAMS implementation on a plant-specific basis.

4.4.2 Appendix 2 – Core Protection Calculator System

4.4.2.1 Description

CENPD-396-P, Appendix 2, "Common Qualified Platform Core Protection Calculator System," provides the functional requirements and a design concept for upgrading an existing core protection calculator system in a CE plant with Common Q components. These requirements and concepts include CPC functional design, testing, system block diagrams, and the interface with the existing analog PPS or with the Common Q digital plant protection system (DPPS).

The CPC/CEAC system is composed of four redundant channels that perform the necessary calculation, bistable, and maintenance/test functions. The system includes four redundant OMs, one per CPC/CEAC channel, located on the MCR panels. The CPC OM is implemented using a FPDS. There is one MTP in each CPC/CEAC channel, implemented using an FPDS identical to that of the OM, used for diagnosing the system, providing electrically isolated communications to external systems, and displaying the same information as the OM. The MTP is local to the CPC processors and is the primary HMI for routine maintenance and surveillance testing by plant technicians.

One CPC/CEAC channel is associated with each PPS channel, and provides low DNBR trip and pretrip, high local power density (LPD) trip and pretrip, and CWP discrete (contact) outputs to its associated PPS channel. The CPC/CEAC processors in each channel receive channelized process sensor analog inputs, to perform the detailed DNBR and LPD calculations, and to provide the associated bistable trip functions. The CPC/CEAC channel inputs consist of hot and cold leg temperature, RCS pressure, reactor coolant pump (RCP) speed, and CEA position via reed switch position transmitters (RSPTs). CPC/CEAC processing of this CEA position input is functionally unchanged from that in the present design.

The CPCS will be installed into the auxiliary protective cabinet (APC), physically separate from the PPS, as is done in the present CPC/CEAC system. The CPC/CEAC processor assembly in each channel consists of two chassis:

1. The controller subrack, which contains the PM646 processors, global memory, communications, and the RCP speed pulse count input modules; and

2. The I/O subrack, which contains the I/O modules.

4.4.2.2 Specific Evaluation Criteria for CPCS

The CPCS replacement described in Appendix 2 must provide functionality and safety that is at least equivalent to that of the CPCS equipment being replaced.

The staff's review of Appendix 2 draws especially upon the guidance and criteria in the following codes and standards:

- GDC 12, "Suppression of Reactor Power Oscillations"
- GDC 13, "Instrumentation and Control"
- GDC 19, "Control Room"
- RG 1.22, "Periodic Testing of Protection System Actuation Functions"
- RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"
- RG 1.62, "Manual Initiation of Protection Actions"
- RG 1.75, "Physical Independence of Electrical Systems" (endorses IEEE Std 384-1992, "Criteria for Independence of Class 1E Equipment and Circuits")
- RG 1.118, "Periodic Testing of Electric Power and Protection Systems" (endorses IEEE Std 338, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems")
- BTP HICB-17, "Guidance on Self-Test and Surveillance Test Provisions"

- BTP HICB-19, "Guidance on Evaluation for Defense-in-Depth and Diversity in Digital Computer-based Instrumentation and Control Systems"

4.4.2.3 CPCS Evaluation

Each CPC/CEAC channel will communicate with a CPC OM mounted in the MCR. Each of the four OMs is fiber-optically isolated from its associated CPC channel. The OM will be used for CPC/CEAC channel monitoring, to provide the capability to manually alter addressable constants, to initiate channel operating bypass at low power levels, and to initiate periodic surveillance testing.

The CPC/CEAC system will include manually initiated automatic test capability for determining system operability. It will also perform automatic hardware diagnostic testing. It will be possible for the operator to initiate surveillance testing from the OM or from a locally mounted MTP.

Each CPC channel is equipped with five PM646 processors. One of these is used as the CPC processor, one as a CEAC 1 and 2 processor, and three for redundant HSL CEA position communication to the other CPC channels.

The CPC and CEAC processor modules are each equipped with separate watchdog timers. If the CPC or CEAC processor fails to refresh its module, the module will open its respective trip and annunciation output contacts. The CPC watchdog timer will cause the CPCS to generate low DNBR and high LPD channel trips to the PPS. This provides a failsafe condition should the CPCS computer system fail. The CEAC watchdog timer will cause the CEAC processor to indicate alarm conditions for both CEAC outputs in that channel. Self-testing of the AC160 and application-specific automated testing of the proper functioning of the CPC run in the AC160 as well. The high LPD channel trips to the PPS conform to the requirements of GDC 12, "Suppression of Reactor Power Oscillations."

For the CPCS, a single non-Class 1E CEA position display (CEAPD) will be mounted on the main control board in the MCR. The CEAPD will provide CEA position-related information on a large screen display, and will be connected to the CPC/CEAC system MTPs in all four channels by fiber-optically isolated ethernet connections. The display will also provide alarm on CEA deviations, CEA sensor failure, and data-link failure. Several display formats will be available. Operator display format and CPC/CEAC channel input selection will be via an operator's keypad located on the main control board. The proposed CEAPD provides enhanced CEA position monitoring compared to the present CEAC/CEA position display on the main control board.

The existing CPC/CEAC system uses four redundant sets of inputs, one set per channel, for all input parameters except CEA position. CEA position is provided by only two RSPT inputs on each CEA. While this remains true for the CPCS, it will still provide additional functionality that will result in enhanced operator displays and may contribute to an increased reactor availability.

Each CEA position is measured by two redundant and independent RSPTs associated with each CEA. In the current CPC/CEAC design, each RSPT provides an analog input to one of the two redundant CEACs. In the proposed design, the disposition of CEA inputs to CEACs will be retained, but there will be eight CEACs, two in each CPC channel. Each CPC channel will

have a CEAC 1, using RSPT 1 inputs from all CEAs, and a CEAC 2, using RSPT 2 inputs from all CEAs. RSPT inputs to each CPC/CEAC channel will be converted to digital format in the channel analog input module A/D converter, and transmitted to the other three CPC/CEAC channels via optically isolated data links.

Increased availability may be achieved because the failure of a CEAC affects only the associated CPC channel. Additionally, for the Common Q platform, the failed module can be exchanged for a good one without removing power from the channel.

Each CPCS channel is electrically independent and capable of being physically separated from a redundant CPCS channel as required by RG 1.75. Each CPCS channel is powered by a separate Class 1E power source.

The trip channel bypasses allow for channel maintenance and surveillance testing at power in accordance with the requirements of IEEE Std 338 and IEEE Std 603, as endorsed by RG 1.22.

The replacement CPCS will run CPC safety-related algorithms functionally identical to the existing CPCS so that program structure will experience little change. Software changes will be restricted to those required to reflect new hardware platform features such as diagnostics and error handling and backplane communications between CPC and CEAC in the proposed system.

CENP states that the proposed design maintains the same functionality as the existing CPCS and meets or exceeds present licensing requirements. A licensee implementing the Common Q CPCS must verify that the replacement CPCS provides the functionality required for its plant. This is plant-specific action item 6.8.

CENPD-396-P, Appendix 2, includes a proposal for changes to the standard technical specifications (STS) in connection with the implementation of a CPCS design. The changes to the STS are not approved (see Section 5.0). The staff finds the proposed changes to be consistent with the CPCS upgrading proposed. However, a licensee implementing a CPCS shall provide its specific proposal for changing the technical specifications (TS). The staff will review changes to the TS or plant procedures as a plant-specific action item (see plant-specific action item 6.9).

The CPCS channels must have a response time consistent with that of the present CPC implementation. A licensee implementing a digital CPCS shall verify that the Common Q system response time accomplishes the specific time requirements for its plant. This is plant-specific action item 6.6.

The CPCS is designed so that any single failure will not prevent proper monitoring, display and alarm action of the other CPCS channels, or inhibit operation of any other system, including the PPS/DPPS, at the system level. CENP submitted a FMEA for the Common Q CPCS with the intent that it might serve as a model for the plant-specific FMEA that the licensee will be required to submit. The staff reviewed the FMEA prepared by CENP for the CPCS design and finds that a similar approach may be used by a licensee implementing a CPCS design when preparing its specific model and the FMEA. This is plant-specific action item 6.10.

CENP considered the case of the common-mode failure of all CPCS channels. The FMEA presumes that the ESFAS system has not been upgraded from analog components and is, therefore, diverse from the Common Q components in the replacement CPCS. Licensees implementing a CPCS design shall demonstrate that the system complies with the criteria for defense against common-mode failure by analyzing the failure of all CPCS channels. This is plant-specific action item 6.11.

The review of human factors considerations for a specific CPCS implementation is a plant-specific action item (see plant-specific action item 6.7).

In summary, the staff concludes that the proposed design approach for replacing existing CPCS functions with the Common Q platform as set forth in Appendix 2 is acceptable, subject to the satisfactory resolution of generic open items identified in this safety evaluation.

4.4.3 Appendix 3 – Digital Plant Protection System

4.4.3.1 Description

CENP's CENPD-396-P, Appendix 3, provides the functional requirements and conceptual design approach for upgrading an existing RPS and ESFAS through the implementation of a DPPS based upon Common Q components.

The Appendix 3 DPPS upgrading is mainly focused on its application to CENP's CE-designed plants. This DPPS upgrading is applicable to both the RPS and the PPS generations of CE plants. For both RPS and PPS plants, it is possible to upgrade only the RPS, or only the ESFAS, or both the RPS and the ESFAS. This appendix specifically addresses the most comprehensive case, namely that of replacing both the RPS and the ESFAS. Considerations involved in replacing a subset of this equipment (the RPS or the ESFAS only) are also discussed.

The proposed DPPS upgrading is limited to replacement of the equipment located in the PPS cabinet and the ESFAS auxiliary relay cabinets. Sensors and related signal conditioning equipment external to the PPS cabinet and final actuated devices (trip circuit breakers, ESF valves, pumps, and other equipment) are not to be altered by this DPPS upgrade and are addressed only as an interface.

The proposed DPPS comprises four redundant channels that perform the necessary bistable, coincidence, initiation logic and associated maintenance/test functions. The system includes four redundant remote control modules (RCM) located on the main control room panels, one for each channel. Plants have the option of retaining their existing RCM, or replacing the existing RCM with a standard Common Q flat-panel-display-based RCM. In RPS-generation plants, the RCM may be implemented in the RPS cabinet since there is no RCM feature in the current design.
Each redundant DPPS channel is composed of a bistable processor chassis and a local coincidence logic processor (LCLP) with four processor modules. Each bistable processor chassis contains two redundant bistable modules, each employing a separate central processing unit module. The bistable processor in each DPPS channel receives channelized process sensor analog inputs, discrete and analog signals from the ex-core detector system,

and discrete signals from the core protection calculator to perform all bistable comparisons for the RPS trips and the ESFAS actuations. In normal operation, a trip in either channel bistable is evaluated as a channel trip by the LCLPs. Each bistable processor module sends its bistable trip status to its associated LCLP in the same channel and to the other redundant RPS channels and both ESFAS trains' local coincident logic processors (LCLPs) by high speed data communications links. Each HSL utilizes fiber-optic modems and cables to provide electrical isolation between the redundant channels.

The bistable processor also receives and sends digital data from and to its extension chassis (via bus extension cable), the interface and test processor, and the maintenance and test panel (via the PLC internal network). Status is provided by data communication modules over the PLC internal AF100 network to the other processors (MTP and ITP) in the same cabinet assembly.

A reactor trip (RT) or an ESFAS initiation signal is generated whenever two out of the four redundant bistable channel trip conditions are sensed in the LCLP for a particular function. Four LCLPs in each channel redundantly perform the "full two-out-of-four" bistable channel comparison and control the opening of one set of reactor trip circuit breakers (RTCBs) by a selective arrangement of LCLP contact outputs.

The proposed DPPS design encompasses an additional level of "selective two-out-of-four" logic before each RTCB. The initiation logic that performs the RPS selective two-out-of-four logic is hardwired using the LCLP's digital output module initiation relay contacts. Whenever a trip condition occurs for an LCLP, its associated initiation relay contacts open. If a selective two-out-of-four LCLP trip condition is present, the corresponding interposing relays are deenergized, thus causing the two RT circuits (the "undervoltage trip coil" and the "shunt trip coil") for that channel to go to their respective "active states" (open state for the undervoltage trip coil and closed state for the shunt trip coil). Either condition will cause the RTCB to open. This initiation logic is the same for the four DPPS channels. An actual RT occurs when the appropriate combination of "open" RTCBs for channels A, B, C, and D is present (a "selective two-out-of-four" arrangement of the four RTCBs).

As in the RPS, each one of the two digital ESFAS (DESFAS) trains comprises four ESFAS LCLPs, located in each auxiliary relay cabinet, performing a full two-out-of-four channel comparison. The DESFAS actuation logic is similar to the RT initiation logic. Each digital output module contact operates an interposing relay, the contacts of which form the selective two-out-of-four logic arrangement. This same interposing relay is deenergized by both the DESFAS watchdog timer contact associated with the LCLP and by manual ESFAS actuation from the main control board. Two independent sets of manual actuation switches for each ESFAS function on the main control board open contacts in the affected trip legs in both ESFAS trains. The RPS and the ESFAS LCLP arrangement is subjected to continuous hardware monitoring and annunciation of failures to maximize system availability.

Bistable trip inputs to LCLPs may be bypassed (trip channel bypass) to perform maintenance and/or testing on instrument channel inputs, on a bistable processor, or to permit continued operation with a failed sensor channel. The trip channel bypass reduces the system logic to two-out-of-three coincidence. Each trip function may be bypassed individually, in only one channel at a time, from the MTP or the RCM in the affected channel. It is also possible to

bypass all bistable trip functions in a channel from any of the remaining three channels. The LCLP also receives the trip channel bypass status information in the other three redundant safety channels through the HSLs.

Consistent with existing RPS and PPS installations, the standard DPPS is composed of a four-bay (one for each redundant channel) cabinet assembly that will house the PLC equipment, the excore neutron flux monitoring system electronics chassis, maintenance and test equipment, internal power supplies, RPS and ESFAS initiation circuits, initiation relays, fiber-optic isolation devices, and other miscellaneous equipment.

Each cabinet assembly receives power from a different, separate, and isolated 120-Vac vital instrument bus. Multiple pairs of internal alternating current/direct current (ac/dc) power supply outputs are auctioneered to provide enhanced fault tolerance. The power supply will contain an ac/dc front end to which various dc-to-dc modules are connected, depending on the voltage requirements of the different DPPS cabinet components. Redundancy will be available for the processor power supplies using diode auctioneering, which provides bumpless transfer upon module failure, and separate auctioneered power supplies will also be used for the DPPS initiating circuitry and interposing relays. In the case of the DESFAS auxiliary relay cabinets, there are two 120-Vac vital bus power supplies per train. Within a train, power supply diode auctioneering will use one power supply from each vital bus, such that the loss of a vital bus will neither cause nor inhibit a DESFAS train actuation from within the DESFAS cabinet. Power supplies used to actuate the relays will be separate from those used in the LCLPs and the ITPs.

Monitoring, testing, and maintenance of the DPPS is provided using both the MTP and a separate ITP located in each DPPS channel and DESFAS train. The MTP is the primary local DPPS human-machine interface. It is used to monitor DPPS status, perform DPPS control functions, such as the insertion of bistable trip channel bypasses, and reset ESFAS initiation signals. System surveillance testing or maintenance can also be initiated and monitored using its display panel. The MTP also communicates with external systems through an ethernet link.

The ITP in each DPPS channel and DESFAS train performs continuous passive monitoring and either fully automatic, manually initiated automatic, or manually initiated testing of the associated channel. It provides the DPPS cross-channel feedback for test status monitoring and cross-channel comparisons. All four DPPS ITPs receive DESFAS status information from both DESFAS trains by one-way (broadcast mode) dedicated HSLs from the DESFAS ITP in each train. DPPS channel ITPs communicate with each other through a subordinate interchannel AF100 network. This network will be separate from the intrachannel AF100 network in each DPPS channel, and will not perform any Class 1E function. Connection of this AF100 ITP network between channels will be by fiber-optically isolated devices, such that no electrical fault within a DPPS channel may propagate to the processors or other circuitry in the other channels.

A variety of self-test diagnostic and supervisory functions are performed by the DPPS PLCs to continuously monitor their operation. Each of the PLC modules has its own self-diagnostic functions. While the application program is running, the self-diagnostic routines continue checking operation without delaying or influencing the execution. Each PLC processor (e.g., a bistable processor or an LCLP) is monitored by the use of background self-diagnostics for the processor and I/O module faults.

For Common Q applications, an external and independent watchdog timer is used in each LCLP module, both in the RPS and the ESFAS functions. This watchdog timer module will time out, opening the selective two-out-of-four leg with the failed module if a fatal fault is detected. Hardware watchdog timers are not used in the bistable processors; however, the bistable processor status is monitored by the LCLPs.

According to CENPD-396-P, Appendix 3, CENP's approach, the implementation of the DPPS will provide protection functions and ESF functions that are functionally identical to those implemented in the equipment that the DPPS is replacing. For PPS generation plants, the DPPS will accommodate the trip and pretrip contacts from the CPC auxiliary protective cabinets for the high local power density and low DNBR trips. For RPS generation plants, these trips do not exist, but they use analogous trips (high axial power distribution and thermal margin/low pressure) that will be accommodated by the DPPS into the bistable processor trip algorithms.

4.4.3.2 Specific Evaluation Criteria for DPPS

The replacement components described in Appendix 3 must provide functionality and safety that are at least equivalent to those of the equipment being replaced. The proposed design approach must satisfy the applicable requirements described in Sections 7.2 and 7.3 of the SRP.

The staff's review of Appendix 3 draws especially upon the guidance and criteria in the following codes and standards:

- RG 1.22, "Periodic Testing of Protection System Actuation Functions"
- RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"
- RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems" (endorses ANSI/IEEE Std 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems")
- RG 1.62, "Manual Initiation of Protection Actions"
- RG 1.75, "Physical Independence of Electrical Systems" (endorses IEEE Std 384-1992, "Criteria for Independence of Class 1E Equipment and Circuits")
- RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants" (endorses IEEE Std 7-4.3.2-1993, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations")
- RG 1.153, "Criteria for Power Instrumentation and Control Portions of Safety Systems," (endorses IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations")
- NUREG/CR 6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems"
- 10 CFR 50.34(f)
- 10 CFR 50.55a(a)(1)
- 10 CFR 50.55a(h)
- 10 CFR Part 50, Appendix A, GDC as follows:
    - GDC 1 – Quality Standards and Records
    - GDC 2 – Design Basis for Protection Against Natural Phenomena
    - GDC 4 – Environmental and Dynamic Effects Design Bases

GDC 13 – Instrumentation and Control
GDC 19 – Control Room
GDC 20 – Protection System Functions
GDC 21 – Protection System Reliability and Testability
GDC 22 – Protection System Independence
GDC 23 – Protection System Failure Modes
GDC 24 – Separation of Protection and Control Systems
GDC 25 – Protection System Requirements for Reactivity Control Malfunctions

- BTP HICB-17, "Guidance on Self-Test and Surveillance Test Provisions"
- BTP HICB-19, "Guidance on Evaluation for Defense-in-Depth and Diversity in Digital Computer-based Instrumentation and Control Systems"
- 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram"

4.4.3.3 DPPS Evaluation

The proposed DPPS implementation provides RPS and ESFAS functions that are functionally identical to those implemented in the equipment that the DPPS is replacing. The DPPS is designed to (1) monitor the same parameters and provide an equivalent plant status information, and actuate the same systems (RPS and ESFAS) subject to the same trip setpoints, (2) provide the same alarms, and (3) provide the same limiting signal (i.e., the CWP) to control systems as the existing design. Functional operation of individual trip functions and bypass functions (operating and trip channel) are unaffected by the DPPS upgrade. Also, the existing capabilities for each trip (audible and visual pretrip indication, bypasses, etc.) and trip function variations will be accommodated on a plant-specific basis. The measurement channels are unaffected by the DPPS upgrade, and existing inputs will be used. The use of bistables feeding two-out-of-four coincidence logic remains, although existing hardware performing these functions will be replaced with digital bistable processors and LCLPs performing the same functions. The existing RTCBs, their configuration, and their relationship to the control element drive mechanism control system will be unaffected by the DPPS upgrade. The existing subgroup relays providing contact inputs to the various ESF components, control circuits will most likely be replaced with new equivalent relays, although this is not a necessary requirement of the DPPS upgrade.

For PPS generation plants, the proposed DPPS is designed to accommodate the trip and pretrip contacts from the CPC auxiliary protective cabinets for the high local power density and low DNBR trips. For RPS generation plants, high axial power distribution and thermal margin/low pressure will be accommodated by the DPPS into the bistable processor trip algorithms.

The proposed DPPS implementation modifies the location where the full two-out-of-four coincidence for the ESFAS is processed, but this new configuration is functionally identical to the existing configuration. The proposed DPPS design implementation does not encompass new functionality features for the RPS and the ESFAS and, consequently, does not involve a new approach on the compliance of these systems with the functionality requirements and design basis of 10 CFR Part 50. The licensee will be required to verify that the new system provides the same functionality as the system that it is replacing on a plant-specific basis. This is plant-specific action item 6.8.

The DPPS channels must have a response time consistent with that of the existing PPS implementation. A licensee implementing a digital DPPS shall verify that the Common Q system response time accomplishes the specific time requirements for its plant with regard to the Chapter 15 accident analysis. This is plant-specific action item 6.6.

The DPPS is designed with either a single multi-bay cabinet or four completely separate cabinets. The cabinets are separated physically by the walls of the cabinets and are separated thermally with appropriate fire barriers between the cabinet bays. The cabinets are provided with forced air cooling, temperature sensors and a high temperature alarm and contain a minimum of flammable material. Associated components inside the DPPS cabinets are considered the same as Class 1E components.

Each channel is located in a separate bay and is independent of the redundant channels. Fiber-optic modems and cables are utilized for the cross-channel communication HSLs to maintain independence and isolation between channels. Mechanical and electrical separation is provided between RCMs of redundant channels. Fiber-optic isolation is used to ensure that an electrical fault in one channel will not propagate to another channel through the ITP cross-channel data link. Fiber-optic modems and cables are used for the communications between DESFAS ITPs and the ITPs of other DPPS channels.

Each DPPS cabinet assembly receives power from a separate and isolated 120-Vac vital instrument bus. Electrical power is not shared between channels, allowing for complete electrical separation and isolation.

The DPPS cabinet contains Class 1E and associated circuits that are separated and isolated in accordance with IEEE Std 384-1992, as supplemented by RG 1.75. On the basis of its review, the staff concludes that the DPPS design complies with the requirements of IEEE Std 603-1991 with regard to system independence and, therefore, satisfies the requirements of GDC 22.

Plant interfaces with existing equipment will retain design basis and licensing basis compliances with the DPPS upgrading. The DPPS signals for the plant annunciator system (PAS) are treated as associated circuits and are isolated at the PAS. The communication between DPPS channels and the plant monitoring system is accomplished by fiber-optic modem and cabling. Outputs from the redundant channels to nonsafety-related areas are isolated by fiber-optic data links.

On the basis of its review, the staff finds that the proposed DPPS design satisfies the requirements of IEEE Std 603-1991 for interactions of control and protection systems. Therefore, the staff finds that the proposed DPPS design satisfies the requirements of GDC 24.

The proposed DPPS design encompasses provisions to permit complete channel testing without affecting system operability by placing the channel in bypass. Additionally, the DPPS design incorporates component redundancy features within the channel that provide flexibility during online testing making it possible to perform automatic online testing of a channel without rendering the channel inoperable. The proposed DPPS design includes fully automatic, manual, or manually initiated automatic test capability for determining system operability. Manual testing is interlocked to prevent testing in more than one channel simultaneously. The scope of the testing capability includes sensor check, trip bistable check, CPC testing (as part

of the bistable processor passive testing), RPS local coincidence testing, RPS initiation logic testing, ESFAS coincidence logic testing, ESFAS initiation circuits testing, and bypass testing. Provisions are not included in the DPPS design to perform overall response time testing from input to output of the DPPS.

The failure modes and effect analysis demonstrates that the system maintains its capability of performing its protective functions when removing from service any component of the channel. The staff finds that the proposed DPPS design conforms to the guidelines for testing in RG 1.22, RG 1.118, and IEEE Std 338-1987. The staff finds that the DPPS design conforms to the requirements of IEEE Std 603-1991 for system reliability and testability and satisfies the criteria of GDC 21. A licensee implementing the DPPS design will need to define a formal methodology for overall response time testing. This is plant-specific item 6.12.

Trip and input channel bypass capability will be retained in the DPPS design, with a two-out-of-three logic on the remaining channels, thus maintaining the required coincidence of two channels for trip. The staff finds that this design meets the single-failure criterion of IEEE Std 603-1991 and is, therefore, acceptable.

The existing manual bypass and reset capability will be retained. Trip channel bypasses are manually initiated in each channel from the MTP or the RCM. In addition, the existing capability of automatically inserting and removing bypasses for some specific parameters, subject to permissive interlocks, will be also retained. All manually blocked or bypassed actuations are automatically removed when the permissive condition is no longer present. The trip channel bypass may be removed manually. A bypass error indication is initiated if more than one trip channel bypass is attempted for the same trip parameter. The control room operators control trip channel bypasses from the RCM. The staff finds that the proposed DPPS design satisfies bypass criteria of IEEE Std 603-1991 and is, therefore, acceptable.

Bypassing a channel actuates an alarm to indicate the channel is being bypassed. The channels under test or bypass conditions are indicated in the RCM and the MTP. The operating bypasses have visible and audible alarms as well as features that provide a permissive range at which they can be operated. The staff finds that the proposed DPPS design conforms to the criteria of RG 1.47 and IEEE Std 603-1991 for bypassed and inoperable status indications and it is, therefore, acceptable.

The DPPS implementation will retain the existing manual trip (RTS) and manual actuation (ESFAS) capability. A manual trip can be performed by depressing two sets of mechanical pushbutton switches on the main control board. The ESFAS manual actuation contact arrangement is similar to the existing system-level actuation. Two independent sets of manual actuation switches for each ESFAS function on the main control board open contacts in the affected trip legs in both ESFAS trains. Additionally, there are manual ESFAS initiation reset switches locally located on the DPPS cabinet and ESFAS manual actuation switches (train specific) locally located in the auxiliary relay cabinets. The amount of equipment common to manual and automatic initiation paths is kept to a minimum, such that no single failure will prevent initiation of a protective action by manual or automatic means. The staff finds that the DPPS design satisfies the requirements of IEEE Std 603-1991 and RG 1.62 for manual initiation of protective action and is, therefore, acceptable.

The proposed DPPS design provides the capability to manually change addressable constants, such as selected calibration values, pretrip and trip setpoints, and bypass permissives. This capability is subject to key switch control. Access to these items is indicated to the operator. The DPPS software (setpoints and code) is protected against unauthorized alterations by control of access to software media by the plant owner. Downloading revised DPPS channel software is subject to a hardware interlock. Access to the DPPS cabinet equipment for changing setpoints and channel bypass is administratively controlled by door key locks.

The proposed DPPS is designed to provide at least the same existing plant information. Indications are provided for all protective actions, including identification of channel trips. The operator has the means to monitor the overall RPS/ESFAS status, including certain inputs and intermediate calculated variables. The display modules are located in the main control room (the RCM) and locally at the DPPS cabinet (the MTP). The staff concludes that the proposed DPPS design satisfies the requirements of IEEE Std 603-1991 in this regard.

The proposed DPPS design automatically compares redundant analog input module outputs for agreement. Failures of I/O modules are detected by the use of background diagnostics. A defective input channel is indicated by observing the system status light. Components may be repaired or replaced by placing the affected channel in bypass. The staff concludes that this design satisfies the requirements of IEEE Std 603-1991 in this regard.

The staff reviewed the model and the FMEA prepared by CENP for the proposed DPPS design. The FMEA was prepared assuming that one set of the redundant channels is bypassed. The analysis concludes that the DPPS is capable of performing its protective functions for all the single failures considered in the design. The staff finds that the results of the FMEA, together with the qualification of the equipment against adverse environments, conform to the guidelines for applying the single failure criteria in IEEE Std 603-1991 and IEEE Std 379-1988, as endorsed by RG 1.53 and, therefore, the requirements of GDC 23. A similar approach may be used by a licensee implementing a DPPS design when preparing its specific model and the FMEA. This is plant-specific item 6.10.

The proposed DPPS is designed in accordance with CENP's quality assurance plan described in the SPM. The evaluation of this quality assurance plan is found in Section 4.3 of this SE.

The proposed DPPS design implementation uses application software that will be designed, developed, tested, and qualified in accordance with the Common Q SPM. The staff has reviewed the software development process in Section 4.3 of this SE.

The proposed DPPS design implementation uses hardware components that have been designed and qualified in accordance with the guidelines described in the topical report. The staff has reviewed these guidelines in Sections 4.1 and 4.2 of this SE.

The AC160 base software and the QNX operating system used in the DPPS have undergone a commercial-grade dedication program as described in the topical report. The staff has reviewed the commercial-grade dedication program in Section 4.2 of this SE.

The review of human factors considerations for a specific DPPS implementation is plant-specific action item 6.7.

CENPD-396-P, Appendix 3, includes a proposal for changes to the STS in connection with the implementation of a DPPS design. The changes to the STS are not approved (see Section 5.0). The staff finds the proposed TS changes to be consistent with the RPS and ESFAS upgrading proposed. Nonetheless, a licensee implementing a DPPS shall provide its specific proposal for changing the TS. The staff will review changes to the TS or plant procedures as a plant-specific action item (see plant-specific action item 6.9).

Defense-in-depth and diversity requirements for digital computer-based instrumentation and control (I&C) systems are stated in BTP HICB-19 and NUREG/CR-6303. The staff requirements memorandum on SECY-93-087 describes the staff's position on defense-in-depth and diversity. According to this position, the applicant or licensee will assess the defense-in-depth and diversity of the proposed I&C system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed. In performing the assessment, the applicant or licensee will analyze each postulated common-mode failure for each event that is evaluated in the accident analysis sections of the safety analysis report (SAR). The applicant or licensee will demonstrate adequate diversity within the design for each of these events (see plant-specific action item 6.11).

If a postulated common-mode failure will disable a safety function, a diverse means must be provided to perform either the same function or a different function that provides adequate protection. A set of displays and controls in the main control room enables operators to manually actuate systems performing critical safety functions and monitoring of parameters that support safety functions.

In addressing the staff position regarding I&C diversity, CENP states that in a case of replacement of all safety systems, it shall undertake an approach similar to the System 80+ approach for common-mode failures, which was found acceptable by the NRC, as stated in the System 80+ final SER.

In Appendix 3 of CENPD-396-P, CENP identifies some diversity features included in the proposed DPPS design. These diversity features encompass: bistable processor and analog input signal diversity, CPCs functional diversity, PPS process instrumentation functional diversity, and algorithm software diversity relative to the execution sequence of the bistable functions. The staff believes that these features provide design enhancements on system diversity, but they do not provide complete protection against common-mode failures.

The staff's position is that a licensee applying for a DPPS upgrade shall carry out the plant-specific defense-in-depth and diversity analysis in order to demonstrate compliance with the requirements of BTP HICB-19 and NUREG/CR-6303. In performing this analysis an approach similar to that used for the System 80+ is acceptable to the NRC staff.

On the basis of the above review, the staff concludes that the design approach to be used for the replacement of existing RPS, ESFAS and PPS functions with the Common Q platform as set forth in Appendix 3 is acceptable, subject to the satisfactory resolution of the generic open items, the satisfactory implementation of the plant-specific items, and conditions set forth in this safety evaluation.

4.4.4 Appendix 4 – Integrated Solution

4.4.4.1 Description

Appendix 4 describes the implementation of the Common Q for a configuration where the licensee replaces more that one of the systems described in Appendices 1, 2, and 3, that is, PAMS, CPCS, and PPS (PPS includes RPS and ESFAS). Appendix 4 describes the sharing of some of the Common Q resources, such as display panels and communications buses, when two or more of the above systems are installed in the plant.

In addition to the integration of safety systems described above, Appendix 4 also includes a high-level description of the optional integration of the Common Q replacements with digital nonsafety reactor control systems. The described nonsafety portions are implemented using ABB technology that is diverse from that used in the Common Q. The information on the integration with the nonsafety control systems is presented at the conceptual level. Design details will be the subject of future submittals. Two of the reasons given by CENP for including the description of the nonsafety control system in Appendix 4 are (1) to discuss the interfaces to the safety systems, and (2) to indicate the conceptual implementation of the diversity of components in such a nonsafety control system as a credible backup to a postulated common mode failure in the safety systems.

Many of the high-level descriptions of the nonsafety systems are presented by CENP as design concepts with examples of the technology in which they might be implemented. CENP has stated that the purpose of Appendix 4 is to obtain the staff's evaluation of particular aspects, especially concepts, of an integrated control system solution using ABB technology. For cases where the design is still in the conceptual stages, CENP seeks the staff's review of the concepts as an acceptable approach for an integrated I&C replacement using the Common Q platform.

Many of the high-level descriptions of the nonsafety portions of the control systems described in Appendix 4 are essentially the same as those that are described in Section 7 of the CENP standard design, "CESSAR System 80+," which CENP submitted to the staff for certification on March 30, 1989. The staff issued NUREG-1462, "Final Safety Evaluation Report Related to the Certification of the System 80+ Design," in August 1994. Where applicable, the staff will incorporate evaluations from NUREG-1462.

4.4.4.2 Specific Evaluation Criteria for the Integrated Solution

The functional requirements for the integrated solution remain the same as for each system that is being replaced. The replacement components described in Appendix 4 must provide functionality and safety that is at least equivalent to that of the equipment being replaced.

The staff's review of Appendix 4 is based on the assumption that the Common Q platform and its implementation into the PAMS, CPCS, and DPPS have been found to be acceptable for use in the safety systems in nuclear power generating stations. The degrees and conditions of that acceptability are treated in other sections in this safety evaluation.

The standards and evaluation criteria for the integrated solution encompass all those criteria that applied to the appendices for PAMS, CPCS, and DPPS. The staff considers the following standards and criteria to be particularly significant for the review of the integrated solution:

- 10 CFR 50.62 (anticipated transients without scram [ATWS])
- GDC 24, "Separation of Protection and Control Systems"
- RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"
- RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," (endorses ANSI/IEEE Std 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems")
- RG 1.62, "Manual Initiation of Protection Actions"
- RG 1.75, "Physical Independence of Electrical Systems," (endorses IEEE Std 384, "Criteria for Separation of Class 1E Equipment and Circuits")
- BTP HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems"

The integrated solution employs digital computers in nonsafety systems that are important to safety. The SRP includes the following supplemental guidance for computer-based systems important to safety that is significant for the review of the integrated solution:

- 10 CFR 50 Appendix R, Section III.G.1.b (remote cold shutdown)
- 10 CFR 50 Appendix R, Section III.L.1 (alternate or dedicated shutdown)

4.4.4.3 Integrated Solution Evaluation

CENP has included in Appendix 4, Section A4.3.4 which is entitled, “NRC Scope of Review.” CENP states therein that, "The purpose of this appendix is to obtain the NRC’s approval of particular aspects of an integrated control system solution using ABB technology." CENP then provides a summary discussion of design for the integrated solution, emphasizing the following six concepts:

1. Integration of shared services
2. ESFAS level 3 loop controllers
3. Defense-in-depth and diversity
4. Interface between safety and nonsafety channels
5. Multichannel operator station control
6. Independence of main control room and remote shutdown panel

In Appendix 4, "Integrated Solution," CENP describes the implementation of the Common Q in I&C replacements where more than one of the systems described in Appendices 1, 2, and 3 are to be replaced. The conditions and limits of acceptability for each system are found in the staff’s evaluations of those appendices in preceding sections of this safety evaluation. Integrated solution concepts that the staff finds in this section of this safety evaluation to be acceptable are subject to those conditions and limitations.

The integrated solution may be installed with or without an upgrade of the plant’s nonsafety control system. Both cases are described. Appendix 4 discusses an upgrade in which nonsafety control functions are replaced with computer technology that is diverse from that used in the Common Q platform.

CENP describes how the Common Q Integrated Solution will interface across fiber-optic links with the following plant functions:

- Data processing system;
- Main control room;
- Remote shutdown panel; and
- Workstations in plant offices.

The staff has organized the following six sections of the safety evaluation for the integrated solution under the six concepts that are listed above.

4.4.4.3.1 Integration of Shared HMI Resources Within a Safety Channel

When any one of the safety systems (PPS (i.e., ESFAS and/or RPS), PAMS, CPCS) is replaced separately, each channel of the safety system requires:

- an OM that is located in the MCR;
- a MTP that is located in the safety cabinet;
- an AF100 bus for in-channel communications and, in some instances;
- an ITP located in the safety cabinet.

That potentially requires up to four sets, i.e., one set per channel, of the above resources for the replacement systems. However, when two or more of the replacement safety systems (PPS, ESFAS, RPS, PAMS, CPCS) are installed in a plant, each of the safety channels still requires only one set of the above resources. This is because one set of resources can be shared within a safety channel for all of the installed replacement systems. Each set of shared resources is still dedicated to its own safety channel.

CENP describes in the topical report how that each of the shared resources has the capability of performing the required functions without overloading the system. CENP and/or the licensee will write application software as required for Common Q I&C replacements. For the case of shared resources, that software will be designed to satisfy the HMI requirements for shared resources. The quality assurance and V&V processes for the development of application software are specified in the topical report and the SPM and must be applied by the teams developing the application software.

The staff has reviewed the sharing of the same AF100 bus, ITP, MTP, and the OM among the PAMS, CPCS, RPS, ESFAS, and PPS in each safety channel as presented in Appendix 4 for the integrated configuration. The staff finds that the sharing of these resources does not reduce their capacity to perform their intended functions as described in the topical report and Appendices 1, 2, and 3. Therefore, the staff concludes that the proposed design approach of sharing these display and communications resources is acceptable. However, the final acceptability of the sharing of these resources will be determined during the plant-specific applications. The analysis of the capacity of the shared resources to accommodate the load increase due to sharing is plant-specific action item 6.13.

4.4.4.3.2 ESFAS Component Control Level Loop Controllers

CENP proposes to replace the hardwired relay logic (in the auxiliary relay cabinets) currently in use in the ESFAS safety trains with loop controllers (LCs) serviced by a dedicated redundant AF100 communications bus. The Appendix 3 Common Q ESFAS replacement is interfaced directly to matrix relays from digital output modules for ESFAS actuation. For the integrated solution upgrade, these matrix relays and digital contact output modules can be replaced with a redundant AF100 bus interface with LCs that will then control the ESFAS initiation.

The LCs will be diverse from the digital components used in the Common Q platform. The LCs will be simple programmable logic controllers that will send signals to switchgear in motor control centers and electrical distribution panels that control plant components. LCs provide both control and data acquisition. The software in the LCs typically requires less than 6 kilobytes of memory and is completely deterministic (i.e., repetitive and noninterrupt driven).

The demand signals from the ESFAS LCLP will be transmitted over the in-channel dual redundant AF100 bus to dedicated LCs that are distributed throughout the plant to provide component control. The LCs will perform the same two-out-of-four coincidence logic that was before accomplished by the matrix relays, and interface directly to control the safety components. In addition to the LCs executing ESFAS logic, they will also read in and process input functions such as manual on/off switches, process interlocks, high torque interlocks for motor operated valves, and thermal overloads.

When existing PPS functions are replaced as described in Appendix 3, that is, without using the LCs to replace the matrix relays, the automated testing can only go as far as to verify that the S600 digital output modules are responding according to the automated test signal. The matrix relays and the interposing relays that initiate ESFAS systems still require manual testing. The integrated solution full-scale configuration advances the automated testing further downstream toward the controlled component. With LCs replacing the ESFAS matrix relays, the two-out-of-four coincidence function can be tested automatically.

A control signal from each manual actuation switch is directed to an LC at the lowest level in the digital control path. Under normal conditions in the Integrated Solution, the LCs provide signals to plant components in response to digital signals received through the ESFAS communication network. The dedicated manual signals actuate plant components by overriding the input data received from the failed ESFAS network interface. CENP needs to provide in future submittals the design information for the LCs to support their diversity from the Common Q components. This is Generic Open Item 7.8.

The LCs used in safety applications will have to meet the requirements of Appendix B or be dedicated under 10 CFR Part 21. CENP shall address this requirement in a future submittal for the staff's review. Also, the diverse, nonsafety LC component controllers when installed for control systems must be demonstrated in a future submittal to be free from common mode failure with the LCs in the safety channels. This design is similar to that proposed and approved in the System 80+. The staff finds that the concept of using LCs to replace the safety component actuation relays may prove to be acceptable. This will be the subject of a future CENP submittal (see Generic Open Item 7.8).

4.4.4.3.3 Defense-in-Depth and Diversity

D-in-D&D is evaluated in Section 4.1.6

4.4.4.3.4 Interface Between Safety and Nonsafety Channels

In the integrated configuration four ITPs and five AF100 buses provide the interface between the safety channels and the nonsafety control system. In addition to electrically isolating the safety channels from the nonsafety control system, the ITP provides data communication buffering of the nonsafety control signals. Signals generated from the safety side that are transmitted to the nonsafety control system will be for monitoring purposes only. Any safety signals required for control by the diverse nonsafety control systems will be split at the analog sensor and fed to both the safety and nonsafety data acquisition systems. This communication path provides data acquisition for the plant data processing system and the nonsafety plant control stations. The ITP will pass control signals over the separate safety in-channel AF100 bus to the LCs for component control. Should the ESFAS require control, the nonsafety control signals will be overridden by the ITP.

This same interface is used for transmission of selective automation signals from the nonsafety control system to the safety system. For instance, the pressurizer level signal is a nonsafety signal typically used to control charging pumps which are safety-related. The charging pumps serve two purposes. They perform normal control of pressurizer level and they are also actuated by safety injection signals to supplement the emergency core cooling system. During normal operation, the pressurizer level signal is transmitted from the nonsafety side via the ITP and AF100 to the safety channel LCs where the charging pumps are normally controlled. The nonsafety pressurizer level control system may be sending demand signals to the LCs to turn off the charging pumps while at the same time a safety injection signal is received by the LCs from the ESFAS channels to start the charging pumps. At the LCs, the ESFAS demand signals have priority over the nonsafety control signals. The existing interlocks and controls that prioritize the control of the safety channel components must be implemented in the application programming of the ITPs and LCs.

The staff has reviewed the above approach of using the ITPs and the AF100 buses as described in Appendices 3 and 4 to provide separation of safety and nonsafety signals and finds that there is not sufficient detail in Appendix 4 to permit an evaluation of the design approach 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 Generic Open Item 7.9.

4.4.4.3.5 Multichannel Operator Station Control

To control a safety channel component for control purposes only, the operator selects the correct manual release switch for the channel to be controlled. There is a set of four manual release switches, one for each of the safety channels, at each operator station. These are push buttons that are hardwired to the safety systems' ITPs. Each release switch arms a specific safety channel allowing the operator to manually control safety components in that channel as long as a manual demand signal is transmitted before a timeout expires (e.g., one minute) or the operator arms a different safety channel. This unburdens the operator from having to constantly rearm the safety channel for each manual maneuver such as lining up a set of valves. The ITP will also prevent multiple components being armed at the same time. The ITP will then pass the control signal over the separate safety in-channel AF100 bus to the

LC for component control. Should the ESFAS require control, the nonsafety control signal will be overridden. In addition to electrically isolating the safety system from the nonsafety control system, the ITP provides data communication buffering of the nonsafety control signals.

In the event of the common mode failure of the AC160 PLCs in all safety channels and trains, the operator would turn to the set of displays and controls in the main control room that are provided to comply with the requirements of Point 4 of BTP HICB-19.

These features provide the continued capability for the integrated solution to provide the operators with control of the safety channel components for alignment of valves and motors through the use of the nonsafety control devices while providing that the ESFAS demands will be met when required. The evaluation of the design approach requires detail beyond the scope of the present submittals. Therefore, the staff could not establish the acceptability of the proposed design approach for manually controlling safety-related components at this time. This is Generic Open Item 4.4.4.3.5.

4.4.4.3.6 Main Control Room and Remote Shutdown Panel

In the event that the MCR becomes uninhabitable, a manual transfer of control from the MCR to the remote shutdown panel (RSP) takes place. When this transfer occurs, a relay disconnects the MCR control from the safety channels. For the case of the hardwired connection between the D-in-D&D Point 4 manual actuation switches and the LCs, there is no transfer, but relay contacts disconnect these devices from the LCs. This disconnect provides protection against inadvertent actuation from the uninhabited MCR of components in the safety trains.

All the connections between the MCR and the RSP to the safety channel are isolated using fiber-optics to ensure that a fire in the MCR or RSP does not propagate to multiple channels.

The staff finds the above provisions for independence of MCR and RSP to be conceptually correct. However, there is not sufficient information for the staff to complete its evaluation of the manual transfer of control. This will be the subject of a future submittal.

4.4.4.4 General Observations Regarding Appendix 4

CENP indicates that Appendix 4 is to describe the implementation of the Common Q platform when a plant installs multiple digital upgrades using the Common Q platform. CENP has not intended that Appendix 4 in its present form should contain sufficient information to permit the staff to evaluate any multiple upgrade. CENP indicates that the details of the designs will be described in future submittals.

The staff's findings with regard to the six concepts on which CENP requested the staff's focus are presented in the subsections above. These six design concepts do not represent all of the concepts that will need to be included in CENP's future submittals.

5.0 SUMMARY OF REGULATORY COMPLIANCE EVALUATIONS

This safety evaluation discusses the acceptability of the Common Q platform for use as a digital I&C replacement for existing safety-related systems in nuclear power plants. Each of the

findings or conclusions summarized below may be subject to the satisfactory resolution of generic open items named in the foregoing sections in this SE. Careful attention must also be given to the plant-specific items.

GDC listed in Appendix A, 10 CFR Part 50, establish minimum requirements for the design of nuclear power plants. IEEE 603 is also incorporated in 10 CFR Part 50, 50.55a(h). The Regulatory Guides and the endorsed industry codes and standards listed in Table 7-1 of the SRP are the guidelines used as the basis for this evaluation. Three Mile Island (TMI) Action Plan requirements for I&C systems are also identified in Table 7-1 of the SRP. This section of this SE discusses the acceptability of the Common Q system as it applies to these regulatory requirements.

Section 50.55a(a)(1), quality standards for systems important to safety, is addressed by conformance with the codes and standards listed in the SRP. Common Q also uses codes, standards and commercial-grade dedication in the development of the Common Q system that are the same as or equivalent to the standards in the SRP and, therefore, in conformance with this requirement.

Section 50.55a(h) endorses IEEE Std 603, which addresses both system-level design issues and quality criteria for qualifying devices. CENP has addressed these issues in the Common Q topical report. Subject to the limitations of this safety evaluation, the staff finds that the Common Q system meets the criteria of IEEE Std 603 and the supplemental standard IEEE Std 7-4.3.2-1996. For the systems and components reviewed, the staff concludes that the Common Q system is in compliance with this requirement.

Section 50.34(f)(2) specifies TMI action items that the licensees must address. These have generally been addressed by the licensees before and separate from the I&C systems and components to be replaced by the Common Q. The licensee must ascertain as a plant-specific item that the implementation of the Common Q does not render invalid any of the previously accomplished TMI action items (see plant-specific action item 6.14).

Section 50.62 specifies requirements for reduction of risk from ATWS. Appendix 4, "Integrated Solution," mentions the possibility of implementing the ATWS in the nonsafety control system configuration. The analysis of the compliance with 10 CFR 50.62 for diversity between a digital ATWS and a Common Q RTS shall be covered by the plant-specific D-in-D&D analysis to be performed by the licensee (see plant-specific action item 6.11).

Appendix A, 10 CFR Part 50, General Design Criteria. The following GDCs are applicable for this review:

- GDC 1 – Quality Standards and Records
- GDC 2 – Design Basis for Protection Against Natural Phenomena
- GDC 4 – Environmental and Missile Design Bases
- GDC 12 – Suppression of Reactor Oscillations
- GDC 13 – Instrumentation and Control
- GDC 19 – Control Room
- GDC 20 – Protection System Functions
- GDC 21 – Protection System Reliability and Testability
- GDC 22 – Protection System Independence
- GDC 23 – Protection System Failure Modes
- GDC 24 – Separation of Protection and Control Systems
- GDC 25 – Protection System Requirements For Reactivity Control Malfunctions

The following regulatory guides are applicable to this review:

- RG 1.22, "Periodic Testing of Protection System Actuation Functions"
- RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"
- RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems" (endorses ANSI/IEEE Std 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems")
- RG 1.62, "Manual Initiation of Protection Actions"
- RG 1.75, "Physical Independence of Electrical Systems" (endorses IEEE Std 384, "Criteria for Separation of Class 1E Equipment and Circuits")
- RG 1.97, "Instrumentation for Light-water-cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident"

- RG 1.118, "Periodic Testing of Electric Power and Protection Systems," (endorses IEEE Std 338, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems")
- RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants" (endorses IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations")
- RG 1.153, "Criteria for Power Instrumentation and Control Portions of Safety Systems," (endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations")
- RG 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (endorses ANSI/IEEE Std 1012, "IEEE Standard for Software Verification and Validation Plans," and IEEE Std 1028, "IEEE Standard for Software Reviews and Audits")
- RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (endorses IEEE Std 828, "IEEE Standard for Software Configuration Management Plans," and ANSI/IEEE Std 1042, "IEEE Guide to Software Configuration Management")
- RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (endorses IEEE Std 829, "IEEE Standard for Software Test Documentation")
- RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (endorses ANSI/IEEE Std 1008, "IEEE Standard for Software Unit Testing")
- RG 1.172, "Software Requirements Specification for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (endorses IEEE Std 830, "IEEE Recommended Practice for Software Requirements Specifications")
- RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (endorses IEEE Std 1074, "IEEE Standard for Developing Software Life Cycle Processes")

SRP Section 7.1-C provides guidance for evaluation of conformance to IEEE Std 603-1991, which provides criteria for I&C systems in general. Reference is made to IEEE-7-4.3.2 for hardware and software issues of digital computers.

To conform to requirements of IEEE Std 603-1991, the Common Q digital upgrade CPCS, PPS and ESFAS are designed so that any single failure in these systems will not prevent proper protective action at the system level. No single failure will defeat more than one of the four redundant CPCS/PPS channels or more than one of the two redundant ESFAS trains. These redundant channels and trains are electrically isolated and physically separated. Qualified isolation devices have been tested to ensure functional operability when subject to physical damage, short circuits, open circuits, or the application of credible fault voltages on the device output terminals. These provisions are for immunity to single failures and for independence.

The completion of protective action requirement of IEEE Std 603-1991 has been satisfied. Once initiated with the Common Q system, the RPS and ESF actuations proceed to completion. Return to normal operation requires deliberate operator action to reset the reactor trip breakers. The breakers cannot be reset while a reactor trip signal is present in the safety system. ESF actuations proceed to completion unless deliberate operator action is taken to terminate the

function. The design approach to be implemented is consistent with plant-specific functional logic to enable system-level protective actions to proceed to completion.

The quality criterion is satisfied with the CENP quality assurance program that meets the requirements of 10 CFR Part 50, Appendix B or by the dedication of commercial-grade digital hardware and software components through procedures that conform to the guidance in EPRI TR-106439 and EPRI TR-107330.

The AC160 system components that will be used in the Common Q have been environmentally and seismically qualified to ensure that they are capable of performing their designated functions while exposed to normal, abnormal, test, accident and post-accident environmental conditions. The type testing was performed in accordance with ANSI/IEEE Std 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," and EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants." The AC160 system components that have been qualified include:

- Processor 19-inch subrack
- Expansion 19-inch subrack
- PM645C processor module
- PM646 processor module
- CI631 communication interface module
- Eight models of S600 I/O modules to include:
    - AI620
    - AI635
    - AO650
    - DI620
    - DO620
    - DO625
    - DO630
    - DP620
- TC630 fiber-optic modem
- TC514 fiber-optic modem
- OZDV 114 fiber-optic modem
- TC625 wire modem

CENP has not conducted environmental qualification testing on the remaining Common Q components. The items not yet qualified are:

- FPDS
- WDT
- Power supply modules
- Components introduced in Appendix 4

For the systems and components reviewed, the independence criteria in the Common Q system is met through the redundancy and separation of the channels. The communication between channels is via fiber-optic cable.

The capability for test and calibration has been demonstrated in compliance with RG 1.22, RG 1.118 and IEEE 338. The capability exists to permit testing during power operation. The design does not require disconnecting wires, installing jumpers, or making other similar modifications to the installed equipment.

Access to the hardware is controlled via the front and rear cabinet doors which are normally locked. Door positions are monitored with an alarm to the operator if any door is opened.

The human factors considerations will be evaluated on a plant-specific basis and, therefore, are not included in this review.

For the systems and components reviewed, the Common Q meets the automatic and manual control requirements. Failure of the automatic controls does not interfere with the manual controls.

For the systems and components reviewed, the staff concludes that the design of the Common Q safety systems are acceptable and meet the relevant requirements of GDC 1, 2, 4, 13, 19-25, and 29, and 10 CFR 50.55a(a)(1) and 50.55a(h).

The staff conducted a review of the safety system descriptions in the topical report for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. For the systems and components reviewed, the staff concludes that the applicant adequately identified the guidelines applicable to these systems. Based upon the review of the Common Q and safety system design approaches for conformance to the guidelines, the staff concludes that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The review included the identification of those systems and components for the safety systems designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. On the basis of this review, the staff concludes that the CENP has identified those systems and components consistent with the design bases for those systems. Therefore, the staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

Based on the review of the CPCS design, the staff concludes that the CPCS high LPD channel trips to the PPS conform to the applicable requirements of GDC 12, "Suppression of Reactor Power Oscillations."

Based on the review of safety system status information, manual initiation capabilities, and provisions to support safe shutdown for the systems and components reviewed, the staff concludes that information is provided to monitor the safety systems over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for manual initiation of reactor trip. The Common Q safety systems appropriately support actions to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Therefore, the staff finds that the Common Q system designs satisfy the requirements of GDC 13 and 19.

Based on the review of system functions, for the systems and components reviewed, the staff concludes that a Common Q system conforms to the design bases requirements of IEEE Std 603. On the basis of its review, the staff concludes that the Common Q RTS includes the provision to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown consistent with the accident analysis presented in Chapter 15 of the SAR of the plants. Therefore, the staff finds that the RTS satisfies the requirements of GDC 20. Licensee evaluation of plant-specific accident analyses is required.

The Common Q system conforms to the guidelines for periodic testing in RG 1.22 and RG 1.118. The bypassed and inoperable status indication conforms to the guidelines of RG 1.47. The safety systems conform to the guidelines on the application of the single-failure criterion in ANSI/IEEE Std 379 as supplemented by RG 1.53. On the basis of this review, the staff concludes that, for the systems and components reviewed, the Common Q system satisfies the requirement of IEEE Std 603 with regard to system reliability and testability. Therefore, the staff finds that the Common Q system satisfies the requirements of GDC 21.

The Common Q system conforms to the guidelines in RG 1.75 for protection system independence for Common Q installed items. Implementing the Common Q will not adversely affect a plant's existing compliance with RG 1.75 On the basis of its review, the staff concludes that for the systems and components reviewed, the Common Q system satisfies the requirement of IEEE Std 603 with regard to system independence. Therefore, the staff concludes that the Common Q system satisfies the requirements of GDC 22.

On the basis of its review of the three failure modes and effects analyses that CENP submitted in Appendices 1, 2, and 3, the staff concludes that CENP's proposed design approaches are consistent with the requirements of GDC 23. Therefore, the staff finds that for the systems and components reviewed, the proposed application design approaches to be implemented with the Common Q system will satisfy the requirements of GDC 23. Plant-specific FMEAs will be required for any implementation of the Common Q system (see plant-specific action item 6.10).

Based on its review of the interfaces between the Common Q safety systems and plant operating control systems, the staff concludes that for the systems and components reviewed, the Common Q safety systems satisfy the requirements of IEEE Std 603 with regard to control and protection system interactions. Therefore, the staff finds the Common Q safety systems satisfy the requirements of GDC 24.

On the basis of its review, the staff concludes that for the systems and components reviewed, the Common Q RTS satisfies protection system requirements for malfunctions of the reactivity control system such as accidental withdrawal of control rods. Therefore, the staff finds that the Common Q RTS satisfies the requirements of GDC 25.

The staff's conclusions are based upon the requirements of ANSI/IEEE Std 603 with respect to the design of the Common Q system. Therefore, the staff finds that for the systems and components reviewed, the Common Q system satisfies the requirement of 10 CFR 50.55a(h) with regard to ANSI/IEEE Std 603.

On the basis of its review of the CENP defense-in-depth and diversity analysis methodology, the staff concludes that this methodology provides an acceptable method by which the licensee

may comply with the criteria for defense against common-mode failure in digital instrumentation and control systems. Therefore, the staff finds that for the systems and components reviewed, adequate diversity and defense against common-mode failure will be provided to satisfy these requirements of GDC 21 and 22, and Item II.Q of the Staff Requirements Memorandum on SECY-93-087. The staff requires, however, that each licensee ensure that the plant-specific application complies with the criteria for defense against common-mode failures in digital instrumentation and control systems (see plant-specific action 6.11).

On the basis of its review of the reports of the dedication of commercial-grade AC160 PLC hardware and software for use in nuclear safety systems, the staff concludes that the AC160 PLC system satisfies BTP HICB-18 and follows the guidance in EPRI TR-106439 and is, therefore, acceptable.

On the basis of the review of CENP's software development process for application software, the staff concludes that the SPM specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the staff or others to evaluate the quality of the design features upon which the safety determination will be based. The staff, therefore, concludes that the software development plan for new software for Common Q safety systems meets the guidance of RG 1.152 and that the special characteristics of computer systems have been adequately addressed. Based on its review, the staff finds, therefore, that the Common Q safety systems satisfy the requirements of GDC 1 and 21.

Based on its review, the staff concludes that, for the systems and components reviewed, the Common Q system meets the requirements of 10 CFR Part 50, Appendix A, General Design Criteria 1, 2, 4, 12, 13, 19, 20, 21, 22, 23, 24, and 25, and IEEE Standard 603 for the design of safety-related reactor protection systems, engineered safety features systems, and other plant systems, and the guidelines of RG 1.152 and supporting industry standards for the design of digital systems and is, therefore, acceptable.

The procedure to change STS is to submit proposed STS modifications to the Nuclear Energy Institute (NEI) Technical Specifications Task Force (TSTF). The changes are reviewed by TSTF for consistency in STS usage and convention, as well as technical accuracy, and are then submitted to NRC Technical Specifications Branch for review and approval. Since the STS changes were not submitted via the NEI TSTF, the proposed changes in Appendices 2 and 3 are not approved. Appendices 2 and 3 do, however, provide a technical basis for the TSTF submittal to the NRC.

6.0 PLANT-SPECIFIC ACTION ITEMS

The following plant-specific actions must be performed by an applicant when requesting NRC approval for installation of a Common Q system:

6.1 Each licensee implementing a specific application based upon the Common Q platform must assess the suitability of the S600 I/O modules to be used in the design against its plant-specific input/output requirements. See Section 4.1.1.1.2.

6.2 A hardware user interface that replicates existing plant capabilities for an application may be chosen by a licensee as an alternative to the FPDS. The review of the implementation of such a hardware user interface would be a plant-specific action item. See Section 4.1.2.

6.3 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.

6.4 Each licensee implementing a Common Q application must verify that its plant environmental data (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the Common Q equipment is to be installed are enveloped by the environment considered for the Common Q qualification testing, and that the specific equipment configuration to be installed is similar to that of the Common Q equipment used for the tests. See Sections 4.2.2.1.1, 4.2.2.1.2, and 4.2.2.1.3.

CENP configured the Common Q test specimen for seismic testing using dummy modules to fill all the used rack slots. As part of the verification of its plant-specific equipment configuration the licensee must check that it does not have any unfilled rack slots. See Section 4.2.2.1.2.

6.5 On the basis of its review of the CENP's software development process for application software, the staff concludes that the SPM specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the staff or others to evaluate the quality of the design features upon which the safety determination will be based. The staff will review the implementation of the life cycle process and the software life cycle process design outputs for specific applications on a plant-specific basis. See Section 4.3.2.

6.6 When implementing a Common Q safety system (i.e., PAMS, CPCS, or DPPS), the licensee must review CENP's timing analysis and validation tests for that Common Q system in order to verify that it satisfies its plant-specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the safety analysis report. See Sections 4.1.1.4, 4.4.1.3, 4.4.2.3, and 4.4.3.3.

6.7 The OM and the MTP provide the human machine interface for the Common Q platform. Both the OM and the MTP will include display and diagnostic capabilities unavailable in the existing analog safety systems. The Common Q design provides means for access control to software and hardware such as key switch control, control to software media, and door key locks. The human factors considerations for specific applications of the Common Q platform will be evaluated on a plant-specific basis. See Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3, and 4.4.4.3.6.

6.8 If the licensee installs a Common Q PAMS, CPCS or DPPS, the licensee must verify on a plant-specific basis that the new system provides the same functionality as the system

that is being replaced, and meets the functionality requirement applicable to those systems. See Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3.

6.9 Modifications to plant procedures and/or TS due to the installation of a Common Q safety system will be reviewed by the staff on a plant-specific basis. Each licensee installing a Common Q safety system shall submit its plant-specific request for license amendment with attendant justification. See Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3.

6.10 A licensee implementing any Common Q application (i.e., PAMS, CPCS, or DPPS) must prepare its plant-specific model for the design to be implemented and perform the FMEA for that application. See Sections 4.4.1.3, 4.4.2.3, 4.4.3.3, and 5.0.

6.11 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 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.

6.12 A licensee implementing a Common Q DPPS shall define a formal methodology for overall response time testing. See Section 4.4.3.3.

6.13 The analysis of the capacity of the shared resources to accommodate the load increase due to sharing. See Section 4.4.4.3.1.

6.14 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.

7.0 GENERIC OPEN ITEMS

On the basis of its review of the CENP's Common Q platform, the staff has identified the following generic open items:

7.1 CENP has committed to develop a new I/O module or re-design some of those already considered for use in the Common Q platform in order to meet the performance requirements of EPRI TR-107330. The staff's review of the design and qualification of the new or re-designed I/O module is discussed in Section 4.1.1.1.2.

7.2 CENP has not yet finalized the selection of the Common Q power supplies. The staff's review of the design and commercial-grade dedication of the power supplies is discussed in Section 4.1.4.

7.3 CENP has not submitted information on the design or dedication of the hardware watchdog timer and it has not yet been subjected to testing for environmental qualification. The staff's review of the design and commercial-grade dedication of the hardware watchdog timer is discussed in Section 4.1.5.

7.4 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.

7.5 CENP will perform additional EMC tests and measurements on the PM646. The staff's review of the PM646 testing is discussed in Section 4.2.2.1.3.

7.6 CENP has not yet conducted seismic and environmental qualification testing on the non-AC160 hardware components. Items not yet tested include the FPDS, watchdog timer and power supply modules. The staff's review of the FPDS, watchdog timer and power supply modules qualification testing is discussed in Section 4.2.2.2.

7.7 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.

7.8 CENP needs to provide in future submittals the design information for the loop controllers to support their diversity from the Common Q components. This is discussed in Section 4.4.4.3.2.

7.9 The staff has reviewed the approach for the integrated solution of using the ITPs and the AF100 buses to provide separation of safety and nonsafety 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.

7.10 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.

Attachment: List of Acronyms

Principal Contributor: K. Mortensen

Date: August 11, 2000

LIST OF ACRONYMS

ABB	Asea Brown Boveri
AC160	Advant Controller 160
AF100	Advant Fieldbus 100
ALWR	Advanced Light Water Reactor
AMPL	ABB Master Programming Language
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transients Without Scram
BTP	Branch Technical Position
CE	Combustion Engineering
CEA	Control Element Assembly
CEAC	Control Element Assembly Calculator
CEAPD	CEA Position Display
CENP	CE Nuclear Power (Westinghouse)
CEO	Cognizant Engineering Organization
CETMS	Core Exit Thermocouple Monitoring System
CGD	Commercial-Grade Dedication
Common Q	Common Qualified
CPCS	Core Protection Calculator System
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CWP	CEA Withdrawal Prohibit
D-in-D&D	Defense in Depth and Diversity
DESFAS	Digital ESFAS
DLCE	Design Life Cycle Evaluation
DNBR	Departure from Nucleate Boiling Ratio
DPPS	Digital Plant Protection System
EMC	Electromagnetic Compatibility
EPRI	Electric Power Research Institute
ESF	Engineered Safety Features
ESFAS	Engineered Safeguards Features Actuation System
FMEA	Failure Modes and Effect Analysis
FPDS	Flat-Panel Display System
GDC	General Design Criteria
GUI	Graphical User Interface
HJTC	Heated Junction Thermocouple
HMI	Human Machine Interface
HSL	High Speed Link
I/O	Input/Output
I&C	Instrumentation and Control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISR	Interrupt Service Routine
ITP	Interface and Test Processor
LC	Loop Controller
LCLP	Local Coincidence Logic Processor
LPD	Local Power Density
MCR	Main Control Room

MTP	Maintenance and Test Panel
NEI	Nuclear Energy Institute
NSSS	Nuclear Steam Supply System
OM	Operator's Module
PAMS	Post-accident Monitoring System
PAS	Plant Annunciator System
PCB	Printed Circuit Board
PCE	Program Control Element
PDS	Previously-developed Software
PLC	Programmable Logic Controller
PM645C/PM646	Processor Module 645C or 646
PPS	Plant Protection System
PROM	Programmable Read-only Memory
QA	Quality Assurance
QSPDS	Qualified Safety Parameter Display System
QSSL	QNX Software Systems Limited
RCM	Remote Control Module
RG	Regulatory Guide
RPS	Reactor Protection System
RSP	Remote Shutdown Panel
RSPT	Reed Switch Position Transmitter
RCP	Reactor Coolant Pump
RTS	Reactor Trip System
RTCB	Reactor Trip Circuit Breaker
RVLMS	Reactor Vessel Level Monitoring System
SAR	Safety Analysis Report
SCMP	Software Configuration Management Plan
SE	Safety Evaluation
SMM	Subcooled Margin Monitor
SPM	Software Program Manual
SQAP	Software Quality Assurance Plan
SRP	Standard Review Plan
SSP	Software Safety Plan
STS	Standard Technical Specifications
SVVP	Software Verification and Validation Plan
TS	Technical Specification(s)
TSTF	Technical Specification Task Force
V&V	Verification and Validation
WTM	Watchdog Timer Module