Westinghouse Non-Proprietary Class 3

WCAP-16097-NP-A
Revision 3

February 2013

Common Qualified Platform Topical Report

Westinghouse

WCAP-16097-NP-A
Revision 3

Nuclear Safety Related

Common Qualified Platform Topical Report

Matthew A. Shakun*
Nuclear Automation Licensing

February 2013

Reviewer: Warren R. Odess-Gillett*
Nuclear Automation Licensing

Martin P. Ryan*
Nuclear Automation Licensing

Approved: Mark J. Stofko*, Manager
Nuclear Automation Licensing

*Electronically approved records are authenticated in the electronic document management system.

Westinghouse Electric Company LLC
1000 Westinghouse Drive
Cranberry Township, PA 16066

© 2013 Westinghouse Electric Company LLC
All Rights Reserved

NRC SAFETY EVALUATION – FEBRUARY 7, 2013

This section contains the following documents:

- NRC cover letter, "Final Safety Evaluations for Topical Report WCAP-16097, Revision 3, 'Common Qualified Platform Topical Report,' (TAC NO. ME5157) and WCAP-16096-P/NP, 'Software Program Manual for Common Q Systems' (TAC NO. ME5159)"

- "Safety Evaluation by the office of Nuclear Reactor Regulation Westinghouse Topical Report WCAP-16097-P, Revision 3 'Common Qualified Platform' TAC. NO. ME5157"

- LTR-NRC-12-7 NP-Enclosure, "Response to NRC Request for Additional Information on the Common Qualified Platform Topical Report (WCAP-16097-P, Rev. 1)," January 2012.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

February 7, 2013

J. A. Gresham, Manager
Regulatory Compliance
Westinghouse Electric Company
1000 Westinghouse Drive, Suite 428
Cranberry Township, PA 16066

SUBJECT: FINAL SAFETY EVALUATIONS FOR TOPICAL REPORT WCAP-16097, REVISION 3, "COMMON QUALIFIED PLATFORM TOPICAL REPORT," (TAC NO.ME5157) AND WCAP-16096-P/NP, "SOFTWARE PROGRAM MANUAL FOR COMMON Q SYSTEMS" (TAC NO. ME5159)

Dear Mr. Gresham:

By letter dated August 26, 2011 (Agencywide Documents Access and Management System (ADAMS) Accession Nos. ML103220240 and ML103220086), and supplemented by letters dated March 6, July 17, and July 20, 2012 (ADAMS Accession Nos. ML12207A513, ML12072A289, and ML12205A051), Westinghouse Electric Company (Westinghouse) submitted WCAP-16097, Revision 3, "Common Qualified Platform Topical Report," and WCAP-16096-P/NP, "Software Program Manual for Common Q Systems" to the U.S. Nuclear Regulatory Commission (NRC) staff for review. By letter dated January 7, 2013, an NRC draft safety evaluation (SE) regarding our approval of WCAP-16096 and WCAP-16097was provided for your review and comment.

By letter dated January 18, 2013, Westinghouse commented on the draft SEs. The NRC staff's disposition of Westinghouse comments on the draft SEs can be found at ADAMS Accession Nos. ML13029A012 for WCAP-1609 and ML13028A511 for WCAP-16096.

Based on its review of the information submitted by Westinghouse, the NRC staff finds the topical reports (TRs) acceptable for referencing subject to the limitations specified in the TRs and in the NRC SEs. The final SEs define the basis for our acceptance of the TR.

Our acceptance applies only to material provided in the subject TRs. We do not intend to repeat our review of the acceptable material described in the TRs. When the TRs appear as references in license applications, our review will ensure that the material presented applies to the specific plant involved. License amendment requests that deviate from these TRs will be subject to a plant-specific review in accordance with applicable review standards.

In accordance with the guidance provided on the NRC website, we request that Westinghouse publish accepted versions of each TR within three months of receipt of this letter. The accepted version shall incorporate this letter and the enclosed final SEs after the title page. Also, the accepted version must contain historical review information, including NRC requests for additional information (RAI) and your responses after the title page. The accepted version shall include an "-A" (designating accepted) following the TR identification symbol.

As an alternative to including the RAIs and RAI responses behind the title page, if changes to the TRs were provided to the NRC staff to support the resolution of RAI responses, and the NRC staff reviewed and approved those changes as described in the RAI responses, there are two ways that the accepted version can capture the RAIs:

1. The RAIs and RAI responses can be included as an Appendix to the accepted version.
2. The RAIs and RAI responses can be captured in the form of a table (inserted after the final SE) which summarizes the changes as shown in the approved version of the TR. The table should reference the specific RAIs and RAI responses which resulted in any changes, as shown in the accepted version of the TR.

If future changes to the NRC's regulatory requirements affect the acceptability of these TRs, Westinghouse and/or licensees referencing it will be expected to revise the TRs appropriately, or justify its continued applicability for subsequent referencing.

If you have any questions or need additional information, please feel free to contact the NRC project manager for these TRs, Joe Holonich. Mr. Holonich can be reached at 301-415-7297.

Sincerely,

Sher Bahadur, Deputy Director
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Project No. 280

Enclosure:
1. WCAP-16097 SE
2. WCAP-16096 SE

cc w/encl:
Stephanie Smith
Westinghouse Electric Company
5000 Ericsson Drive, Suite 517
Warrendale, PA 15086

TABLE OF CONTENTS FOR COMMON Q SAFETY EVALUATION

SUMMARY 1

1.0 INTRODUCTION 3

2.0 SYSTEM DESCRIPTION 4
2.1 Common Q System 4
2.2 Previously Developed Software 8
2.3 Application Software 9
2.4 Nuclear Applications 9

3.0 REVIEW CRITERIA AND METHOD OF REVIEW 10
3.1 Review Criteria 10
3.2 Method of Review 14

4.0 SYSTEM EVALUATION 15

4.1 Evaluation of the Common Q Design 15
4.1.1 AC160 PLC System 16
4.1.1.1 AC160 Hardware 16
4.1.1.1.1 PM646A Processor Module 16
4.1.1.1.2 Input/Output Subsystem 17
4.1.1.1.3 CI631 Communication Module and Global Memory 17
4.1.1.2 AC160 Software 18
4.1.1.2.1 AC160 System Base Software 18
4.1.1.2.2 Application Software 20
4.1.1.2.3 Software Tools 21
4.1.1.3 AC160 Self-Testing 22
4.1.1.3.1 PM646A Diagnostics 23
4.1.1.3.2 S600 Input / Output Module and CIM Diagnostics 23
4.1.1.3.3 High Speed Link Diagnostics 24
4.1.1.3.4 AF100 Diagnostics 24
4.1.1.3.5 Redundant AF100 Interface 24
4.1.1.3.6 Application Watchdog Counter 25
4.1.1.4 Throughput and Response Time 25
4.1.1.5 Hardware Interrupts In The AC160 26
4.1.1.6 Deterministic Performance 27
4.1.2 Flat-Panel Display System 29
4.1.3 Communication Subsystems 30
4.1.3.1 Advant Field Bus 100 30
4.1.3.2 High Speed Link (HSL) 32
4.1.3.3 External Communications 33
4.1.3.4 ISG 04 Evaluation 33
4.1.4 Power Supply 47
4.1.5 Watchdog Timer Functions 48
4.1.6 Defense-in-Depth and Diversity 48
4.1.7 Evaluation of New Custom Program Control Elements 50

4.2 Evaluation of the Commercial-Grade Dedication of the Common Q Platform .. 50
4.2.1 Vendor Surveys 53
4.2.1.1 Vendor Survey for AC160 PLC System 53
4.2.1.2 Vendor Survey for the FPDS 55
4.2.2 Seismic and Environmental Qualification 56
4.2.2.1 Environmental, Seismic and Electromagnetic Qualification of the AC160 56
4.2.2.1.1 Temperature and Humidity 58
4.2.2.1.2 Seismic Testing 58
4.2.2.1.3 Electromagnetic Interference and Radio Frequency Interference 59
4.2.2.2 Seismic and Environmental Qualification of Non-AC160 Hardware 60
4.3 Life Cycle Planning Process for Application Software 61
4.4 Common Q Applications 61
4.5 Common Q Platform Generic Change Process 61
4.6 Common Q Record of Changes Document 62

5.0 SUMMARY OF REGULATORY COMPLIANCE EVALUATIONS 62

6.0 PLANT-SPECIFIC ACTION ITEMS 67

7.0 GENERIC OPEN ITEMS 70

8.0 REFERENCES 72

LIST OF ACRONYMS 74
Table 1 - Common Q Qualified Components 79

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

WESTINGHOUSE TOPICAL REPORT WCAP-16097-P, REVISION 3

"COMMON QUALIFIED PLATFORM"

TAC. NO. ME5157

SUMMARY

The Common Qualified (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 from the standard Advant Control (AC)160 computer system developed by Asea Brown Boveri (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 Common Q platform consists of the following basic system elements:

- Advant Controller Processor Module
- Input and Output Modules
- Bus Communication Interface Modules
- Power Supply Modules
- Advant Fieldbus Communication Systems
- Flat-panel Display System (FPDS) (For Operator Module (OM) and Maintenance Test Panel (MTP))
- High Speed Link (HSL) Communication System

The AC160 software resides on flash Programmable Read Only Memory (PROM) in the processor module. This software consists of a real-time operating system, task scheduler, diagnostic functions, communication interfaces, and a plant specific application program. The application program is created using the ABB Master Programming Language (AMPL) Control Configuration (ACC) software development environment that includes a function block library for creating specific logic for the application.

Safety-related instrumentation & control (I&C) systems based on the application of Common Q platforms are designed to 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 NRC staff considered regulatory requirements, technical positions, guides, and standards in the Standard Review Plan (SRP), (NUREG-0800) Chapter 7, in the review of the Common Q platform design. Westinghouse Electric Company's (Westinghouse's), "Software Program Manual (SPM) for Common Q Systems," specifies plans for implementing a structured software life cycle process for application software and provides guidance for configuration management of commercial-grade hardware and previously developed software. Since the application software has not yet

ENCLOSURE 1

been developed, the NRC 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. Licensees using the

Common Q platform for plant-specific applications will be required to implement the application software in accordance with Westinghouse's SPM and any other application-specific requirements as determined by the safety-critical nature of the application.

In regard to the commercial dedication of the Common Q platform, including the previously developed software and tools, Westinghouse previously 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. In its original safety evaluation (SE) (Reference 3), the NRC staff previously found that the AC160 system planned for the Oskarshamn Modernization Project was the same as that used for the Common Q system, and the quality evaluation done for the Oskarshamn Modernization Project was determined to be applicable to the commercial grade dedication (CGD) of the Common Q system. To verify the validity of this safety conclusion in light of the changes made to the Common Q platform, the NRC conducted an audit of the Westinghouse CGD processes used for the Watts Bar PAMS application and determined that the Westinghouse CGD processes continue to provide an acceptable means of ensuring that NRC regulations are being met by components of the system that are commercially developed.

Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," identifies criteria for defense against common-mode and common cause failures. To defend against potential common-mode failures, the Staff considers high quality development processes for hardware and software, as well as defense-in-depth, and diversity to be key elements in a digital system design. Maintaining high quality processes increases the reliability of both individual components and complete systems. The staff has reviewed the CGD process of the Common Q platform and determined the level of quality established for the Common Q platform is sufficient for use in safety related I&C applications at nuclear power plants. The quality of the plant-specific Common Q system is dependent on proper implementation of the Westinghouse SPM and the resolution of plant-specific items identified in Section 6.0 of this SE.

In regard to diversity and defense-in-depth (D3), the NRC staff has established acceptance guidelines for D3 assessment and has identified four echelons of defense against common-mode failures:

1. control systems,
2. reactor trip system,
3. engineered safety feature actuation system, and
4. monitoring and indication system.

These guidelines are documented in BTP 7-19. The generic methodology proposed by Westinghouse follows the guidance in BTP 7-19. Applications which use the Common Q platform will require a plant-specific D3 assessment in order to determine if adequate diversity has been established for the safety functions performed by that system. See Plant Specific Action Item (PSAI) 6.11.

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 TR meet the plant license requirements. Because this TR is for a generic platform, licensees referencing this TR must describe in detail how they propose to use the Common Q design in plant-specific applications and must address all PSAI's listed in Section 6.0 of this SE.

1.0 INTRODUCTION

By letter dated September 20, 2010 (Reference 1), Westinghouse Electric Company, LLC (Westinghouse) submitted Revision 3 of TR WCAP-16097, "Common Qualified Platform Topical Report" (Reference 2) to the NRC for review and approval. This SE provides the results of the NRC staffs review of the Westinghouse TR, and other supporting documents.

Based on the information provided and the review conducted, the NRC staff concludes that the design of the revised Common Qualified (Common Q) platform satisfies the relevant NRC regulatory requirements for a generic system application and is acceptable for safety-related instrumentation and control (I&C) applications in nuclear power plants. However, plant specific application analyses must be performed to ensure the generic approval granted by this SE remains valid for a specific system or plant application utilizing the Common Q platform.

This TR had previously been submitted to the NRC by Combustion Engineering Nuclear Power (CENP) as document number CENPD-396-P, Revision 1. Two additional supplements were subsequently submitted to the NRC in order to close GOIs that had been identified in the original SE that was issued on August, 11, 2000. The following section discusses the review history regarding these submittals.

COMMON Q TR Licensing History

On June 5, 2000, Westinghouse (formerly Combustion Engineering Nuclear Power - CENP) submitted TR CENPD-396-P, Revision 1, "Common Qualified Platform," to the NRC for review, describing the design of the Common Q platform for safety-related I&C applications in nuclear power plants. The Common Q Platform TR contained four appendices, three of which contained system descriptions and a failure modes and effect analysis (FMEA).

Common Qualified Platform
Appendix 1 – Post Accident Monitoring System
Appendix 2 – Core Protection Calculator System
Appendix 3 – Plant Protection System
Appendix 4 – Integrated Solution

On August 11, 2000, the NRC staff issued a SE regarding the acceptability for referencing of TR No. CENPD-396, Revision 1, "Common Qualified Platform," which identified GOIs (Agencywide Documents Access and Management System (ADAMS) Accession No. ML003740165).

By letter dated May 11, 2001, Westinghouse submitted additional information to closeout four of the GOIs (GOIs 7.4, 7.7, 7.9, and 7.10). The NRC staff subsequently issued the first supplemental SE that addressed those four GOIs by letter dated June 22, 2001 (ADAMS Accession No. ML011690170).

By letter dated August 14, 2002, Westinghouse submitted supplemental information for review by the NRC staff to: (1) close five more GOIs from the review of the Common Q digital I&C platform, and (2) approve proposed changes to the Common Q TR CENPD-396-P, the SPM,

and Appendices 1 and 2. A remaining GOI (i.e., PSAI 6.10) stated that a licensee implementing any Common Q platform applications must prepare its plant-specific model for the design to be implemented and perform the FMEA for the application.

Subsequently, Westinghouse changed the Common Q TR document number from CENPD-396 to WCAP-16097 (ADAMS Accession No. ML031820482). The last approved version of the Common Qualified platform TR, both proprietary and non-proprietary versions were submitted by letter dated May 23, 2003, and are listed below.

WCAP-16097-P-A, Rev. 0	(ADAMS Accession No. ML031830507)
WCAP-16097-P-A, Appendix 1, Rev. 0	(ADAMS Accession No. ML031830507)
WCAP-16097-P-A, Appendix 2, Rev. 0	(ADAMS Accession No. ML031830889)
WCAP-16097-P-A, Appendix 3, Rev. 0	(ADAMS Accession No. ML031830895)
WCAP-16097-P-A, Appendix 4, Rev. 0	(ADAMS Accession No. ML031830904)
WCAP-16097-NP-A, Rev. 0	(ADAMS Accession No. ML031820484)
WCAP-16097-NP-A, Appendix 1, Rev. 0	(ADAMS Accession No. ML031820736)
WCAP-16097-NP-A, Appendix 2, Rev. 0	(ADAMS Accession No. ML031820738)
WCAP-16097-NP-A, Appendix 3, Rev. 0	(ADAMS Accession No. ML031820741)
WCAP-16097-NP-A, Appendix 4, Rev. 0	(ADAMS Accession No. ML031820743)

2.0 SYSTEM DESCRIPTION

The Common Q platform consists primarily of a set of digital hardware and software components from the standard AC160 system, a product developed by ABB Products in Europe. The standard AC160 is a system of PLC products currently used for control systems in several industries including the nuclear power industry. To complete the Common Q platform, Westinghouse combines a FPDS and other components with its set of AC160 system components. The FPDS consists of the flat-panel display module which has 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 SE briefly describes the revised Common Q application framework. This application framework includes the tools, techniques, restrictions, guidance, and methodologies used for the development of a Common Q platform based system.

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. To develop such an application, Westinghouse procures the hardware and Previously Developed Software (PDS) components that make up the Common Q platform from commercial-grade suppliers and dedicates them for use in nuclear power plants. The following discussion applies to equipment in each of the redundant divisions of safety I&C systems.

Advant Controller 160 (AC160)

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

- AC160 with PM646A processor module (PM)
- S600 input and output (S600 I/O) modules

- Bus communication interface (CI631) modules
- Power supply modules
- Advant Fieldbus 100 (AF100) Communication system
- FPDS (For Operator Module (OM) and Maintenance Test Panel (MTP))
- High Speed Link (HSL) Communication

Note: See Table 1 for a complete listing of approved hardware modules of the updated Common Q system platform.

An AC160 system has three types of hardware modules: processor modules (model PM646A), analog and digital I/O modules (S600 series), and a communication module (CI631). These hardware modules are designed to be mounted into 19-inch subracks. A typical AC160 configuration has one or two subracks and each of the subracks can accommodate up to 10 modules.

AC160 controllers can be configured with between one and six processor modules in an AC160 chassis, however, the number of PMs is limited to four for Common Q applications. This is PSAI 6.16. The number of PMs used varies from application to application and is determined by the processing power and speed required.

The AC160 processors are programmed in the AMPL. This programming language includes a range of programmable functions, including logic constructs, logic block interfaces to the AF100 network, global memory, I/O, and a HSL interface.

Each PM supports two high speed communication links (HSL) which are used to support data communications between redundant safety divisions for safety functions such as two-out-of-four voting. The HSL data links are electrically isolated using fiber optic cable.

The PM has a built in watchdog timer (WDT) module that is to be used in the Common Q systems. This internal WDT has a timing function that is used to monitor the processing system and detect inactivity. Depending on the specific system application, the WDT can be used to annunciate a failure, actuate a channel trip, or set output states to predefined conditions. Isolation is provided for those applications where the WDT is connected to external systems.

The AC160 uses the S600 I/O system of I/O modules. A range of I/O modules is included in the S600 series for analog and digital signals of various types. The specific I/O modules that are approved for use in Common Q platform based systems are listed in Table 1. These modules can be configured to support temperature measurement, pulse counting, rotational speed measurement, and other applications as needed.

The bus communication interface (CI631) module provides the interface with the redundant AF100 communication bus, which is described below with the other communication buses. The CI631 modules also have global memory, which the AC160 modules use to share process data with other stations on the AF100 bus within the division.

The Common Q 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 SE. This SE identifies the AC160 components that the NRC staff has approved for use in Class 1E applications in Table 1.

Power Supply

The Common Q power supply sub-system is based on a 19-inch rack or 24-inch panel assembly with plug-in or quick-disconnect modules. Various modules are available to accommodate different output voltages required for an application. The power supply is designed for use by the processor, loop transmitters, digital logic, relays, and reed switch position transmitter circuits.

Power supply redundancy is available for the Common Q system and can be implemented to meet safety application requirements. For configurations that utilize this feature, faults in one half of a redundant supply will not prevent the other half from maintaining system functionality. Redundant modules can be replaced while the power supply remains energized without disturbing the powered system. The power supply has overvoltage and over temperature protection, soft start, and a high power factor.

Data Communication

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

- the AF100 network communication system;
- HSL serial communication system; and
- external communication systems such as Ethernet.

The AF100 is used for transferring process data and messages within a single division (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 divisions in a multidivisional system. Fiber-optic modems and cables maintain isolation of redundant safety divisions.

The external communication system is used to transfer calculated data from the Common Q system to the external systems, such as a non-safety-related plant control system.

Flat Panel Display System (FPDS)

Westinghouse adds the FPDS to the AC160 system to form the Common Q platform. The FPDS consists of the flat-panel display with touch screen capability, a microprocessor-based single-board computer module, and communication interfaces for communication with the AC and other isolated external systems. These communications interfaces are circuit card modules that are installed into the single board computer. A typical FPDS Personal Computer (PC) node box has two of these communications interface modules installed. One module facilitates communications with the AC160 over the AF100 bus and another facilitates communications to a non-safety-related system such as a plant computer.

The FPDS is used for the OM in the main control room (MCR) and for the MTP in the AC160 equipment cabinet. The FPDS does not perform automatic safety functions. If the FPDS halts, the safety-critical applications in the AC160 controllers can continue to operate unimpeded. The FPDS can be used to support performance of safety critical actions by operators such as post accident monitoring or control of safety related components. Additional details about the

operating systems and the functions of the Common Q software are provided in Section 4.0 of this SE.

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 OM and for the MTP functions.

Operator Module (OM)

The OM is used in the MCR for operator functions such as changing certain system parameters or viewing safety system parameters.

In some applications, the OM could be used to perform safety critical functions. For these cases, an additional safety significance evaluation is required. See Section 4.1.2 of this SE for additional details on this requirement.

Maintenance Test Panel (MTP)

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 surveillance tests, change system setpoints, and display detailed system diagnostic messages. Each Common Q safety division is required to have both an OM and an MTP.

The MTP is also used for loading PM646A software via a serial port communications cable that is only connected to the processor when the safety division is out of service. When AC160 safety system software is to be loaded or altered, the software load enable (SLE) keyswitch is placed into the SLE position and the MTP is re-booted into a development mode. The safety application in the MTP is halted during these evolutions.

2.2 Previously Developed Software (PDS)

PDS is 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

PDS for the AC160

Run-time PDS

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 PM646A processor module. The operating system software executes the control modules of the application program, diagnostic routines, and communication interfaces.

The run-time PDS for the FPDS consists of a real-time operating system and the GUI system.

Development and Support Tool PDS

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.
Previously Developed Software for the Flat Panel Display 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.

2.3 Application Software

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

All software residing on safety system computers at run time must be qualified for its intended application. The software for the safety-related functions implemented in the Common Q platform will be produced under a quality assurance program. Westinghouse has submitted the Common Q SPM, WCAP-16096, "Software Program Manual for Common Q Systems" (Reference 6) for NRC staff review. The SPM describes the Westinghouse software development process, including hardware integration. In addition to performing the required safety functions, the Common Q application software is capable of performing automated diagnostics on the safety systems. Automated diagnostics can continuously test the

functionality of certain features of the application. 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 software (PDS) that is 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.

2.4 Nuclear Applications

A description of some proposed Common Q nuclear applications was previously provided in the original SE (Reference 3) and will not be repeated here because the changes made to the platform do not affect the application designs and the previously provided descriptions will remain valid.

AC160 Deterministic Performance

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. If the single processor load is maintained at less than 70 percent and the processor does not malfunction, then control module overruns will be avoided and all tasks can be guaranteed to be fully accomplished. 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. The licensee is required to review this analysis per PSAI 6.6 of this SE. 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 data 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.

3.0 REVIEW CRITERIA AND METHOD OF REVIEW

3.1 Review Criteria

The acceptance criteria used as the basis for this review are defined in NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants,” Rev. 5, dated March 2007. NUREG-0800, which is hereafter referred to as the Standard Review Plan (SRP), sets forth a method for reviewing compliance with applicable sections of Part 50 to Title 10 of the *Code of Federal Regulations* (10 CFR), “Domestic Licensing of Production and Utilization Facilities” and 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants.” Specifically, SRP Chapter 7, “Instrumentation and Controls,” addresses the requirements for I&C systems in nuclear power plants based on light-water reactor designs. The procedures for review of digital systems applied in this evaluation are principally contained within SRP Chapter 7 and are augmented and supplemented by Interim Staff Guidance (ISG).

The suitability of a digital platform for use in safety systems depends on the quality of its components; quality of the design process; and system implementation aspects such as real-time performance, independence, and online testability. Because this equipment is intended for use in safety systems and other safety-related applications, the submitted TR was evaluated in

accordance with the provisions of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” and IEEE Std 7-4.3.2 2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” based on the guidance contained in SRP Chapter 7, Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std 603,” and Appendix 7.1-D, “Guidance for Evaluation of the Application of IEEE Std 7-4.3.2,” which provide acceptance criteria for these two standards.

The following regulations and design criteria in 10 CFR Part 50 are applicable in whole or in part for general review of the suitability of this I&C platform for generic safety-related applications:

- 10 CFR 50.55a(a)(1), “Quality Standards for Systems Important to Safety,” requires that “Structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed”
- 10 CFR 50.55a(h), “Protection and safety systems,” approves the 1991 version of IEEE Std 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” for incorporation by reference, including the correction sheet dated January 30, 1995
- 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants”
  - General Design Criterion (GDC) 1, “Quality Standards and Records”
  - GDC 2, “Design Basis for Protection Against Natural Phenomena”
  - GDC 4, “Environmental and Dynamic Effects Design Basis”
  - GDC 13, “Instrumentation and Control”
  - GDC 19, “Control Room”
  - GDC 20, “Protection System Functions”
  - GDC 21, “Protection System Reliability and Testability”
  - GDC 22, “Protective System Independence”
  - GDC 23, “Protective System Failure Modes”
  - GDC 24, “Separation of Protection and Control”
  - GDC 25, “Protection System Requirements for Reactivity Control Malfunctions”

- 10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”

SRP Chapter 7, Table 7-1, identifies regulatory guides (RGs), and BTPs, which contain information, recommendations, and guidance and, in general, provide an acceptable basis to implement the above requirements for both hardware and software features of safety-related digital I&C systems. Based on the scope of the Common Q platform and the limitations of a platform-level review, the following guides and positions are determined to have relevance for consideration in this SE:

Regulatory Guides

- RG 1.22, "Periodic Testing of Protection System Actuation Functions"
- RG 1.53, Revision 2, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," which endorses IEEE Std 379-2000, “Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems”

- RG 1.75, Revision 3, "Physical Independence of Electrical Systems," which endorses IEEE Std 384-1992, "Criteria for Separation of Class 1E Equipment and Circuits"
- RG 1.89, Revision 1, “Qualification for Class 1E Equipment for Nuclear Power Plants”
- RG 1.97, Revision 4, "Instrumentation for Light-water-cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident"
- RG 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems," which endorses IEEE Std 338-1987, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems"
- RG 1.152, Revision 3, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 7-4.3.2-2003, “Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations”
- RG 1.153, Revision 1, "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"
- RG 1.168, Revision 1, “Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 1012-1998, “IEEE Standard for Software Verification and Validation Plans,” and IEEE Std 1028-1997, “IEEE Standard for Recommended Practices for Software Design Descriptions”
- RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 828-1990, “Software Configuration Management Plans,” and IEEE Std 1042-1987, “IEEE Guide to Software Management”
- RG 1.170, “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 829-1983, “Software Test Documentation”
- RG 1.171, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 1008-1987, “IEEE Standard for Software Unit Testing”
- RG 1.172, “Software Requirements Specification for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 830-1993, “Guide for Software Requirements Specification”
- RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Systems used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 1074-1995, “IEEE Std for Developing Software Life Cycle Processes”
- RG 1.180, Revision 1, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” which endorses IEEE Std 1050-1996, “IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations,” and specified test methods from MIL-STD-461E, “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,” and IEC 61000, “International Electrotechnical Commission Series of EMI/RFI Test Methods”

NRC Technical Reports (NUREG-Series Publications)

- NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition,” Chapter 7, “Instrumentation and Controls,” March 2007

Branch Technical Positions

- BTP 7-11, Revision 5, “Guidance on Application and Qualification of Isolation Devices”
- BTP 7-14, Revision 5, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems”
- BTP 7-17, Revision 5, “Guidance on Self-Test and Surveillance Test Provisions”
- BTP 7-18, Revision 5, “Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems”
- BTP 7-19, Revision 5, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems”
- BTP 7-21, Revision 5, “Guidance on Digital Computer Real-Time Performance”

Additional RGs: In addition to the RGs prescribed in Table 7-1 of the SRP, the following guides were determined to applicable to the Common Q platform SE.

- RG 1.100, Revision 3, “Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants,” which endorses IEEE Std 344-1987, “IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations”
- RG 1.209, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants,” which endorses IEEE Std 323-2003, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations”

Interim Staff Guidance

- DI&C-ISG-04, Revision 1, “Interim Staff Guidance on Highly-Integrated Control Rooms – Communications Issues (HICRc)”
- DI&C-ISG-02, Revision 2, “Interim Staff Guidance on Diversity and Defense-in-Depth Issues”

Industry Standards

- 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," as endorsed by RG 1.100 “Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants”

- 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 7-4.3.2-2003, “IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations” as endorsed by RG 1.152, “Criteria for Digital Computers in Safety Systems of Nuclear Power.”

The Common Q platform is based on existing commercial off-the-shelf (COTS) digital I&C components. As such, certain industry guidelines that address dedication and qualification processes are applicable. The NRC staff reviewed and accepted the following industry guidance documents based on conditions established in SEs. These positions were also determined to have relevance for consideration in this SE.

- Electric Power Research Institute (EPRI) TR-102323, “Guidelines for Electromagnetic Interference Testing in Power Plants” (ADAMS Legacy Library Accession No. 9412270127) as accepted by the NRC SE dated April 30, 1996 (ADAMS Legacy Library Accession No. 9605070359).
- EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” (ADAMS Legacy Library Accession No. 9610080308) as accepted by the NRC SE dated July 1997 (ADAMS Legacy Library Accession Nos. 9810150221, and 9810150223) (ADAMS Accession No.ML12205A284).
- EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants” (ADAMS Legacy Library Accession No. 9801130303) as accepted by the NRC SE dated July 30, 1998 (ADAMS Legacy Library Accession Nos. 9808120276 and 9808120281) (ADAMS Accession No. ML12205A265).

3.2 Method of 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 testability. The NRC 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 and 4.2 of this SE.

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 NRC staff issued a SE on TR-106439. The NRC staff determined that TR-106439 contains an acceptable method for dedicating commercial-grade digital equipment for nuclear power plant safety applications.

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 I&C systems in

nuclear power plants. EPRI TR-107330 was approved by the NRC staff on July 30, 1998. The NRC staff has applied the guidance in EPRI TR-106439 and TR-107330 in reviewing the Westinghouse program for the qualification of the Common Q hardware and software. Westinghouse 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, Westinghouse teams conduct reviews at the vendors' facilities to determine the quality of the vendors' activities. These reviews focus 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 Westinghouse review teams are documented in proprietary reports and records. The NRC staff reviewed Westinghouse's records and reports on CGD activities. The NRC staff's evaluations on the CGD activities are documented in Section 4.2 of this SE.

4.0 SYSTEM EVALUATION

This section details the NRC staff's evaluation of the Common Q platform. The evaluations include:

1) the Common Q design, and
2) the CGD of the Common Q platform.

Since hardware and software components rely upon each other to perform any function, the following discussion frequently does not contain all of the details that were reviewed in order for the NRC 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 is stated in Section 5.0. Where the information in Section 4.0 supports a safety conclusion, the conclusion is stated within that subsection.

During the course of this SE, the NRC staff identified several areas where additional information was required to support the conclusions of the SE. These Requests for Additional Information (RAIs) including the Westinghouse responses to them are documented in References 8, 9, and 16.

The NRC staff has identified one generic open item (GOI) that remains unresolved. Additional information will be needed to complete an evaluation of this aspect of the Common Q platform. This GOI is listed in Section 7.0. Items that will require plant-specific consideration are also identified throughout the evaluation and are summarized 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 NRC staff considered both the hardware and software components and their performance as a system.

The hardware components for the Common Q are listed in Table 1 of this SE:

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 categories:

- 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 categories 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 PM646A Processor Module

Westinghouse indicates in WCAP-16097 (Reference 2) that the PM646A is the processor module that will be used in the Common Q platform. The PM646A contains diagnostic capabilities over the previous versions of the PM. The NRC staff has evaluated the PM646A and has determined the findings in this SE apply only to the PM646A processor module and not to previous versions of the processor module.

The PM646A 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 (application processor), 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 (SRAM). At startup, the application and system software are copied from the nonvolatile memory into the SRAM, where it is executed.

- The memory 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 PM646A 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 SRAM for communications.

Each PM646A 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 interdivisional communications.

The processing section and the communication section of the PM646A communicate with each other through a dual-port random-access memory (DPRAM), which is housed in the PM646A module. Each section can access the contents of this DPRAM 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 PM646A to satisfy independence and separation requirements for safety systems.

4.1.1.1.2 Input/Output Subsystem

The AC160 PLC controller may contain up to 75 I/O modules. S600 I/O models that are qualified for use in nuclear safety applications are listed in Table 1 of this SE.

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 NRC staff's description of the automatic self-testing for the S600 I/O modules is found in Section 4.1.1.3.2 of this SE.

For some applications, the existing S600 I/O modules may already satisfy plant-specific requirements. In other cases, modules designed to meet the requirements of TR-107330 may not satisfy the plant-specific requirements. The NRC 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 executing 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.

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 4.1.3.1. The CI631 also houses global memory used for sharing intradivisional data among multiple PM646A 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 NRC staff's description of the automatic self-testing for the CI631 module is found in Section 4.1.1.3.2 of this SE.

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 PM646A processor module.

4.1.1.2.1 AC160 System Base Software

The PM646A 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 PM646A executes the safety-related application program. The communication section is the interface for the HSLs and it handles the serial communication with other safety divisions.

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.

PM646A Processing Section Tasks

The processing section of the PM646A 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 (also known as control modules) 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 WDT,
    - 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.

PM646A Communications Section Tasks

The communication section of the PM646A module handles the serial communication to other safety divisions. 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 task – 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 WDT thus preventing the WDT's timeout.
- Copy program – The copy program copies serial communication data from the application program to the communication section of the PM646A module.

- Transmission task – The transmission program updates the serial transmission buffer with application data copied by the copy program.
- Receiver task – The receiver program puts the serial communication data received from other safety divisions into a buffer to be read by the application program.
- Configuration task – The configuration program allocates the resources for serial communication data transfer.
- Debug task – The diagnostic program has two functions: (1) to output messages for software diagnostics and (2) to test the window WDT. After the test activates the relay, the window WDT is quickly retriggered before its relay contacts have a chance to open.
- Background task – The background program performs a CRC on the system flash PROM. The background program is monitored for completion within a specified timeout period.

Tasks associated with Saving Data to Flash PROM

One new feature being added to the Common Q software design is the capability of storing and retrieving application data such as system setpoints to the Flash PROM within the PM646A. This feature has been implemented in order to improve data access performance of the system and to reduce the systems reliance on the PC node box. With this revised design configuration, programs will now access configuration data from the Flash PROM content rather than access data from a PC node Box. To implement this feature, the following two tasks have been added to the Common Q system software functions:

1. A task is performed that enables applications to work on a mirror RAM copy of the FLASH PROM content instead of working directly on the FLASH PROM.

2. A task which performs actual writing to and supervision of Flash PROM has been added to the system platform.

Each of these tasks has been implemented by way of new custom PC Elements described in Section 4.1.7 of this SE. The NRC staff has reviewed the functional details of this new feature provided by Westinghouse and has concluded that there is no adverse impact on the ability of the Common Q system to perform its assigned safety functions. The NRC staff also concludes that the established level of deterministic behavior of the Common Q system as defined in Section 4.1.1.6 of this SE has not been compromised by the addition of this feature.

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 program control elements. The executable code for the standard set of logic blocks (i.e., program control elements) is part of the base software. In addition, custom Process Control (PC) elements can be created as an extension to the base software.. The programmer references the program control element library to create the specific logic for the application.

The application program is written in the AMPL and consists of a process control part and a database part.

Process Control

The process control part of a user application program describes the control algorithm and the control strategy. It contains the program 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 program control elements. Each executable unit can be given its own cycle time and its own execution conditions. Program control elements are the smallest building blocks in a process control program. The control module is made up of function calls to the program control element library. The program control element library is stored on system flash PROM.

Each AC160 processor has one process control program. Under the process control program is an executable control module. 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.

Database

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 AC160 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 (AS100 Edit),
- Function Chart Builder, and
- Bus Configuration Builder.

The tools use the AMPL. AMPL is based on function blocks, called program 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 program 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 (Reference 6).

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

4.1.1.3 AC160 Self-Testing

BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," indicates that digital computer-based I&C systems are prone to different kinds of failures than are traditional analog systems. BTP 7-17 states 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. Diagnostic functions monitor system operation and report any faults detected. 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 categories:

1. AC160 module 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. The collection and presenting diagnostic information to the plant staff is done at application design time.
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. This is PSAI 6.15.

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 built in WDT in the PM646A, ensure that the execution of each control module does not exceed its cycle time and that the AC160 system operates properly. The processor module was designed so that if it does not complete its operations within specified times or fails the self-diagnostics test, its operation is halted. If the processor module halts, the WDT times out.

The operation of the PM646A 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 WDT in the

process section times out. If the communication section detects that the process section is not operating, the communication section halts itself. This causes the WDT in the communication section to time out, signaling the failure. Additionally, the PM646A of one division is monitored by the PM646A of other divisions, which notify the operator if one division 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 PM646A 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 divisions. The automatic self-test software will be developed with the application software under the quality assurance and procedures specified in the SPM (Reference 6).

4.1.1.3.1 PM646A 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 PM646A 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 S600 Input / Output Module and Communications Interface Module Diagnostics

Diagnostics of the S600 modules I/O and the CI631 communication interface module are executed by interrogating all modules for errors. The S600 modules have self-contained diagnostics the results of which are reported to the PM646A base software diagnostics routine via a device status word. The CI631 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 PM646A 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 PM646A 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 bus mastership 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 PM646A.

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 PM646A 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

Application WDTs are no longer required for Common Q applications. The AC160 self testing functions described in Section 4.1.1.3 supersede the need for application WDT features. Therefore no evaluation of this function was performed by the NRC staff.

On the basis of the review in Section 4.1.1.3, the NRC staff concludes that the self-testing features of the AC160 system adequately support the self-test issues identified in BTP 7-17.

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. Westinghouse has stated that during the design phase of the specific Common Q application, a throughput calculation of the following will be performed:

1. The propagation delay of the input system;
2. The propagation delay of the HSL cross-division 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, Westinghouse will calculate and measure the actual execution time for all the executing tasks (control modules) created for a Common Q application in the PM646A. Westinghouse 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 overruns. The actual central processing unit (CPU) load depends on the configured cycle times for the application program. Westinghouse will then generate a timing diagram that shows the relationship of the tasks to each other. Westinghouse 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, a timing analysis will be performed 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 include system response time requirements for control actions initiated from the display. During operation of the Common Q application, the 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 7-21 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 7-4.3.2-2003) so that the entire system meets its timing requirements

- Timing requirements should be satisfied by design commitments

Westinghouse has committed to perform a system response and display response analyses in order to meet the response time requirements identified in BTP 7-21. Based on its review of the Common Q system architecture and Westinghouse's design commitments to perform throughput and response-time analyses, the NRC staff concludes that for the systems and components reviewed, the Common Q design satisfies the response time requirements

identified in BTP 7-21 and is, therefore, acceptable in this regard. When implementing a Common Q safety system the licensee must review Westinghouse'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 PSAI 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 affect 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 (WDT)

Every two seconds the processor diagnostics will test the window WDT. In so doing, it causes an interrupt from the window WDT. The ISR reads the window WDT registers and re-triggers the window WDT 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 Checker

The mirror RAM checker issues an interrupt when it detects an error in RAM. The RAM Checker is an Erasable Programmable Logic Device (EPLD). When a read command is issued from the processor, the RAM Checker will read the contents of both the work RAM and the mirror RAM. If they are different, then it issues an interrupt that will halt the processor. This

check 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 processor WDT 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 systems 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 PM646A's error log every time the control module is not executed within the cycle time. If this failure occurs four consecutive times, the PM646A system halts and the processor WDT times out. Westinghouse 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 PM646A, Westinghouse will require that at least one control module measure the whole system load condition. On the basis of this review, the NRC 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 are 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 division is indirectly monitored by other divisions and the operator is notified if the one division fails to send data or sends bad data.

On the basis of this review, the NRC staff finds that Westinghouse 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 WDT. This provision addresses any deadlocks.

The NRC staff concludes that the design features, the operation of the AC160 PLC system, and Westinghouse's commitments to perform timing analyses and tests provide sufficient confidence that the AC160 will operate deterministically to meet the recommendations in BTP 7-21 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. There are also communications interface cards installed into the single board computer to support communications with the AF100 bus and with external systems. Refer to Table 1 for a list of FPDS components reviewed for this SE. Westinghouse 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 PM646A 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 I/O and is used for transmission of data to non safety 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 non safety systems and its own operation does not adversely affect the operation of the safety-critical side.

The NRC 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 WDT. 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.

For instances where the FPDS is performing safety critical functions or where it is credited to initiate or control protective actions, an additional safety significance evaluation shall be performed to address the added reliance on the FPDS to accomplish the required safety functions. Such an application may require re-classification of the FPDS as Safety Critical. For example, if the OM is providing the only indication of a RG 1.97 Type A variable and thus being relied upon by the plant operator to initiate a required safety function, then the safety significance of the OM is elevated and the impacts of not having the necessary information available during the design basis event should be considered and addressed in this safety significance evaluation. This is PSAI 6.24.

On the basis of this review, the NRC staff concludes that the FPDS conforms to the requirements of IEEE Std. 603-1991 as augmented by RG 1.75,“ Criteria for Independence of Electrical Safety Systems,” related to separation between the FPDS and the AC160 PLC system components. See also Section 4.1.3.4 of this SE for an additional evaluation of the level of communications independence established between the FPDS and the AC160. The NRC staff concludes that the design features, the operation of the FPDS system, and Westinghouse’s commitments to perform integrated system tests provide sufficient confidence that the FPDS will operate as designed.

4.1.3 Communication Subsystems

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

- AF100 Network – Provides a communication path for intradivision communications and a separate AF100 bus can be used for interdivision communications in the DPPS;
- HSL Serial Communication – Provides a communication path for interdivision communication; and
- Ethernet or Serial External communications – Provides a path for communication between the Common Q platform and external computer systems.

4.1.3.1 Advant Fieldbus 100

The Common Q equipment connected to the AF100 bus may include the OM, the MTP, the ITP, and the AC160 processor chassis. Each of these devices requires a communications interface module to support communications on the AF100 bus. For the AC160 processor, the communications interface card is the CI631 and for the node boxes, the communications interface module is the CI527W. 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 divisions. 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: (1) process data transfer and (2) 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 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. Bus mastership 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. Bus master assignment is normally limited to the MTP node boxes within a safety system. These node boxes normally have direct connections to the AF100 bus and do not rely on fiber optic modems to maintain connectivity. Certain application restrictions have been identified in order to ensure continued safety functionality when a bus master node fails. These restrictions are listed in the “Application Restrictions for Generic Common Q Qualification” document (Reference 21). These application restrictions are intended to ensure that the AC160 will continue to perform the required safety functions when a failure of a FPDS node occurs.

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, Westinghouse will perform throughput analysis and response time analysis. Westinghouse 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, Westinghouse will determine the AF100 data set peripherals transfer cycle time from the AF100 network throughput analysis. Westinghouse 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 intradivision communications, and the AF100 communication system for one division is completely isolated from the AF100 system of other divisions. Therefore, a failure in the AF100 system in one division does not affect the AF100 communication systems in the other division(s).

On the basis of the AF100 bus utilization for intradivision communications within multi-division systems, and given that the AF100 bus does not possess the capability to interfere with the performance of the systems safety function by the AC160 safety processor, the NRC staff concludes that the AF100 communication system satisfies the requirements in IEEE Std 7-4.3.2-2003, Section 5.6, "Independence."

4.1.3.2 High Speed Link Serial Communication

The HSL is a serial RS-422 link that is used for exchanging data between the safety divisions. The data transmission cycle time and the amount of data transferred during a cycle are determined by application-specific design. Westinghouse stated that the timing analysis of the communication section is performed as part of the propagation delay analysis of the HSL cross division communication to assure that the multiple control modules in the system design are executing deterministically. After the configuration of the plant-specific process control program is determined, the data the PM646A 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 from which it wants. Therefore, the receive lines on the HSL ports can have different data. Additionally, the devices are also optically isolated from each other. The other divisions have the same HSL system. Therefore, a fatal fault in one link or one HSL division 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 program; the application program 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 a cyclic redundancy check (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 program, which takes appropriate action.

To ensure that safety systems meet the response time requirement, Westinghouse stated that it will perform throughput analysis and response time analysis. In addition, the Common Q SPM (Reference 6) Section 5.5.6 identifies integration and acceptance test activities to be performed

during the test phase of the software development process. These tests are intended to ensure that the developed system conforms to the established functional and performance requirements. System time response requirements are among these performance requirements. Common Q system timing requirements, including overall computer system response time are required to be documented as design requirements which must also undergo verification and validation. Westinghouse, therefore, performs response time tests to validate the design's compliance with both the system response and the display response requirements.

On the basis that the HSL is configured such that it sends and receives only unidirectional, time-based data across multiple divisions of a system and the transmit data is optically, and therefore electrically, isolated before being transmitted to other channels and given that the HSL transmits both the true and a binary inverse signal to its receiver thus allowing the verification of the originating signal from the initiating HSL, the NRC staff concludes that the HSL communications meet the requirements of Section 5.6 of IEEE Std 7-4.3.2-2003, for communication independence.

4.1.3.3 Ethernet or Serial External Communications

The FPDS single-board computer may have two separate hardware communication interfaces: an AF100 interface for communication with the Advant processors and an Ethernet or serial interface for communications to external systems such as a plant computer system over fiber optic cables. Each interface will have its own buffers and software for data communication.

AF100 Communications

The AF100 communications link is only used for inter-node data transfer within a single Common Q division. The communications interface module used within the FPDS single board computer is the CI527W.

Ethernet/Serial Communications

The microprocessor and the application codes on the single-board computer can move data from buffers on the AF100 interface card to buffers on the Ethernet/Serial interface. This design feature will eliminate propagation of any fault from nonsafety systems to the Common Q systems that perform safety functions. The NRC staff concludes that the external communication system meets the requirements of Section 5.6 of IEEE Std 7-4.3.2-2003, for communication independence.

4.1.3.4 Interim Staff Guide (ISG) 04 Evaluation

The NRC Task Working Group 4, "Highly Integrated Control Rooms-Communications Issues," developed interim NRC staff guidance on the review of communications issues applicable to digital safety systems. DI&C-ISG-04 contains NRC staff positions on three areas of interest: (1) Interdivisional Communications, (2) Command Prioritization, and (3) Multidivisional Control and Display Stations. Evaluation of a safety system against this guidance is an application-specific activity that requires an assessment of a full system design. Since the Common Q TR does not address specific applications or establish a definitive safety system design, the evaluation against this guidance is limited to consideration of the means provided within the platform to address issues related to interactions among safety divisions and between surveillance requirement (SR) equipment and equipment that is not SR. A full safety system

design, which is based on the Common Q platform, will require further evaluation against this guidance as a PSAI.

Section 5.6 of the Common Q platform topical report," Compliance to Interim Staff Guidance Highly Integrated Control Room – Communications (ISG #4-HICRC)," contains Westinghouse's positions on how the Common Q system (platform) design complies with the NRC staff guidance provided in DI&C-ISG-04, Revision 1 - Task Working Group No. 4, "Highly-integrated Control Rooms-Communications Issues."

DI&C-ISG-04, Staff Position 1 - Interdivisional Communications

Staff Position 1 of DI&C-ISG-04 provides guidance on the review of communications, which includes transmission of data and information among components in different electrical safety divisions (or channels) and communications between a safety division and equipment that is not SR. This ISG does not apply to communications within a single division or channel. This NRC staff position states that bidirectional communications among safety divisions and between safety and non-safety equipment may be acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems. It also states that systems which include communications among safety divisions and/or bidirectional communications between a safety division and non-safety equipment should adhere to the 20 points described below. The methods by which the Common Q platform either meets these points or provides an acceptable alternative method of complying with NRC regulations are discussed below.

Staff Position 1, Point 1

Staff Position 1, Point 1, states that a safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE Std 603. It is recognized that division voting logic must receive inputs from multiple safety divisions.

The shared data that is required for voting functions of a Common Q safety system are transferred between divisions of the system through the HSL communications interfaces. These interfaces are described in Section 4.1.3.2 of this SE. This voter function is not dependent on data from other divisions in that the voter will still be able to complete its safety function even if this HSL data is either faulty or not available. This is accomplished during application development by programming the voter to use data from other divisions only when it is available and valid, and by setting predetermined default outputs when the minimum required data for performing the coincidence voting function is not available.

The processor module is designed such that the processing section of the PM646A operates asynchronously from the communication section and all data is transferred through a dual ported RAM interface. The processing section of the PM646A is also continuously informed of the status of each communication interface so that it retains the ability to perform its safety function without reliance on data from outside of the PM646A.

The Common Q TR does not propose any reliance on interdivisional communications or input from any external systems to perform safety functions. Therefore, no channel is dependent upon any information or resource originating from outside its own safety division.

The NRC staff determined that the Common Q platform complies with the guidance provided by Staff Position 1, Point 1. However, if a plant application of the Common Q system invokes interdivisional communications, then the specific interconnections defined for the plant-specific safety application must be evaluated in a plant-specific review.

Staff Position 1, Point 2

Staff Position 1, Point 2, states that the safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.

The HSL communications interfaces that are used by the Common Q platform to transfer data between system divisions contain several barriers that are designed to protect safety channels from adverse influences caused by information or signals originating at the opposite side of the data link. These barriers include:

- Use of DPRAM
- Use of CRCs on all received data
- Continuous monitoring of communications link status
- Detection of communications link failure
- Data transfer restrictions

Since the HSL communications interfaces are safety related, the protection features provided by these barriers are implemented within the affected division.

The Common Q platform does not propose any direct communication interfaces between the PM646A and non safety related systems outside of the safety division. The platform does include provisions for a communications link between the FPDS and non safety related systems; however, the FPDS as described in Sections 2.0 and 4.1.2 of this SE is designed to perform a graphical user interface (GUI) function and does not initiate any required safety actions. In addition, the PM646A as described in Section 4.1.1.1.1 of this SE is designed to perform all system safety functions independently and without reliance on the FPDS. If the FPDS fails or halts, the AC160 continues to run without it. It is not required for the safety functions. Therefore the safety functions being performed by the Common Q system cannot be adversely influenced through this safety related to non safety related interface.

The NRC staff determined that the Common Q platform provides protection of the safety function and complies with the guidance provided by Staff Position 1, Point 2.

Staff Position 1, Point 3

Staff Position 1, Point 3, states that a safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the

safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (e.g., could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system.) Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.

The design features of the Common Q platform as described in the TR do not include communications from outside a single division that do not support the safety function. The Digital Plant Protection system annex of the Common Q TR describes two functions that use data from outside of the division. Those functions are coincidence voting, and surveillance testing support functions both of which support the primary safety function of the system. This however, does not preclude the implementation of such features during development of a plant specific design.

The NRC staff determined that the Common Q platform complies with the guidance provided by Staff Position 1, Point 3. However, the NRC staff recognizes that the Common Q platform provides allowances for implementation of system features that could affect compliance with this position. These cases would require plant-specific analysis to verify compliance with this staff position.

Staff Position 1, Point 4

Staff Position 1, Point 4, states that the communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be SR, and must be designed, qualified, fabricated, etc., in accordance with 10 CFR Part 50, Appendices A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure the safety function will be performed within the

timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.

As described in Section 4.1.1.1.1 of this SE, the Common Q platform communications are carried out by a communications processor that is separate from the processor that executes the safety functions of the system. The processing section and the communication section of the PM646A communicate with each other through a DPRAM. All data is transferred between these sections through this dual ported RAM interface. The processor module is designed such that the processing section of the PM646A operates asynchronously from the communication section. All components of this communications interface including the DPRAM, the processing section of the PM646A, and the communications section of the PM646A are safety related. CGD of the Common Q components is further addressed in Section 4.2 of this SE.

The PM646A includes design features to ensure that the safety function within the processing section of the processor always has access to the current data in the DPRAM. Should the processing section of the PM646A become unable to access data stored on the DPRAM, it would continue to operate. Performance of required safety functions of the system within the required timeframes would then depend on the application being written in a way that the system defaults to a safe state when the DPRAM data cannot be accessed.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and has determined that the Common Q platform complies with Staff Position 1, Point 4.

Staff Position 1, Point 5

Staff Position 1, Point 5, states that the cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor, assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.

A discussion of the Common Q throughput and response time is provided in Section 4.1.1.4 of this SE. The actual CPU load depends on the configured cycle times for the application program. To ensure that the Common Q system meets its application system response time requirements, the execution time for all of the systems tasks is calculated and measured during system development. This calculation includes terms to address the response time of the memory processing and associated circuits. Westinghouse has imposed a CPU load limit of 70 percent in order to avoid control module overruns which could adversely affect the deterministic behavior and response time of the system. In addition, the actual CPU load is monitored by the application program during operation which will provide an alarm if a specified maximum CPU load is exceeded.

Staff Position 1, Point 5, cannot be assessed for the Common Q platform and must be evaluated as an application specific review for a plant-specific application. When implementing a Common Q safety system the licensee must review Westinghouse'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 PSAI 6.6.

Staff Position 1, Point 6

Staff Position 1, Point 6, states that the safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.

Section 4.1.1.2.1 of this SE describes the interactions that take place between the processing and communication sections of the PM646A safety processor. While the processing section of the PM646A module executes the safety algorithms, the communication section controls HSL communications.

The processing section control program consists of several control modules which become prioritized operating system tasks when compiled. The tasks are scheduled by a task scheduler who controls task execution sequence. This is not event driven or controlled by interrupts from outside of the safety division. In addition, the processing section control program does not perform communication handshaking when accessing data from the DPRAM.
The communication section is an event-driven interrupt system, however, the criteria of DI&C-ISG-04 Position 6 only apply to the safety function processor which corresponds to the processing section of the PM646A.

The NRC staff review determined that communications protocols associated with the communications used by the Common Q platform include the use of communications handshaking, but this handshaking is done by the communications section of the PM646A. The safety function processor contained within the PM646A communicates externally using only the dual-ported memory, and this process does not use handshaking or interrupts. The NRC staff therefore determined that the Common Q platform complies with Staff Position 1, Point 6.

Staff Position 1, Point 7

Staff Position 1, Point 7, states that only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.

For the Common Q system, configuration data established by the application program is used to instantiate data sets which are used by the communications section of the PM646A. In this manner, these data sets are predefined and their format and sequence are pre-determined. The allocation of DPRAM is static and does not change during program execution.

The identification of unrecognized or faulty data or messages is performed by the communications section of the processor module, which flags the data as bad to ensure that the safety application will not use this information in the performance of its safety function. The

Common Q system also has provisions for identifying data as being updated even if it has not changed in value since the previous update.

Based upon the above discussion on the Common Q platform's use of predefined data sets with a pre-determined format via the respective communications processors, the NRC staff concludes that the Common Q platform complies with Staff Position 1, Point 7.

Staff Position 1, Point 8

Staff Position 1, Point 8, states that data exchanged between redundant safety divisions or between safety and non-safety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.

For the Common Q platform, all data that is exchanged between redundant safety divisions are processed through the DPRAM interface located between the processing and the communications sections of the processor module. Section 4.1.1.2.1 of this SE describes the interactions that take place within this interface.

Data exchanged between safety and non-safety systems only occurs at the external communications interface of the FPDS as described in Section 4.1.3.3 of this SE. Because the FPDS does not initiate any required safety actions and because the FPDS portion of the Common Q safety system is further isolated from the processing section of the processor module which does perform safety functions, this data cannot adversely affect the safety functions being performed by the Common Q system. The PC node box performs communications functions to support the interface to non safety systems and serves as an interposing processor for the pathway between the safety processor and non safety systems.

For the Common Q platform, all data exchanges between redundant safety divisions and data exchanged between the safety processor and non-safety systems are performed using interposing safety related communications processors.

- For communications between redundant safety divisions, this interposing processor is the communications processor in the communications section of the PM646A.

- For communications between the safety processor and non safety systems, the interposing processor is the PC node box processor in the FPDS.

The safety function processor (processing section of the PM646A) processes this data as defined by the control modules which are converted to system tasks controlled by the task scheduler. The NRC staff has determined that the data exchange within Common Q platform based systems complies with Staff Position 1, Point 8.

Staff Position 1, Point 9

Staff Position 1, Point 9, states that incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.

As described in Section 4.1.1.1.1 of this SE, the Common Q platform communications are carried out by a communications processor that is separate from the processor that executes the safety functions of the system. The processing section and the communication section of the PM646A communicate with each other through a DPRAM. The allocation of DPRAM memory is static in that it is stored in fixed predetermined locations within the PM646A memory map and these locations do not change during program execution. These memory locations are allocated and dedicated to support the communications interface functions of the processor module. Data in each direction (i.e., receive and transmit) is stored in separate DPRAM memory locations within the PM646A.

The NRC staff determined that the dual-ported memory usage within the Common Q platform complies with Staff Position 1, Point 9.

Staff Position 1, Point 10

Staff Position 1, Point 10, states that safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g., engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor/shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. “Hardwired logic” as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a “TRUE” or “1” at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.

On-line changes to Common Q safety system software are performed in two ways.

1. Changes to system setpoints are performed by a safety related application that runs in the MTP PC node box. A description of the MTP functions is provided in Section 2.1 of this SE.

   In order to prevent setpoint changes from being made while the safety division is in operation, a function enable key switch that provides a digital input signal to the MTP must be turned to send a permissive signal to the safety related photon application. Once this permissive signal is received, the operator is then presented with options on the MTP touch screen display for modifying safety system setpoints. This is not considered to be a hardwired interlock or a physical disconnection of the MTP because the function enable keyswitch signal is software based. This is a condition specifically stated as not acceptable in this ISG staff position, however, because the division of the safety system being altered is not operable during such evolutions, these changes are not considered to be performed in an on-line manner. In addition, the guidance criterion of DI&C-ISG-04 does not apply to communications within a single division. Because the MTP is in the same division as the safety processor that it is communicating with the DI&C-ISG-04 criteria do not apply for this communications segment. Therefore, the DI&C-ISG-04 guidance which calls for physical disconnect does not apply for setpoint changes made to the Common Q safety system.

   The MTP provides restrictions to prevent making changes in more than one division at a time. Each MTP can only be used to make setpoint changes in its associated safety division. There is at least one dedicated MTP in each safety division.

   Placement of the function enable key switch in the enable position causes a system alarm but does not inhibit operation of the remaining Common Q system in any way. Because of this, administrative controls must be put into place to ensure that changes to setpoints are only performed while the system is not being relied upon to perform its safety functions and the affected division of the Common Q safety system must be declared inoperable. This is PSAI 6.18.

   The NRC staff determined that the criteria of DI&C-ISG-04, Staff Position 1, Point 10 do not apply to the communications between the PM646A and the MTP PC Node box that are used to facilitate changes to system setpoints. Furthermore, the methods used to change Common Q system setpoints conform to the applicable criteria of DI&C-ISG-04, Staff Position 1, Point 10 as long as the provisions of PSAI 6.18 are satisfied.

2. Software changes are performed using a non safety related application development application that runs on a separate disk drive within the MTP PC node box.

   In order to prevent software changes from being made to the Common Q system while the safety division is in operation, a software load enable (SLE) key switch must be turned and the MTP must be re-booted into a Windows® based software development environment. In addition, a serial RS-232 communications cable which is not connected to the PM646A while the safety system is operable and performing its safety functions must be plugged into a serial port on the front of the processor module. When the Common Q system is placed into a software load configuration the application within the PM646A is halted and all system variables associated with the affected AC160 are flagged as invalid.

   Any changes made to AC160 software will also affect the CRC checksum value which is continually monitored by the safety application which will activate a system alarm. An alarm is also actuated when the SLE switch is turned to alert the operator of this situation.

The MTP provides restrictions from making software changes in more than one division at a time. Each MTP can only be used to change software in its associated AC160 safety division processor. There is at least one dedicated MTP in each safety division.

The staff determined that the method used to load or change Common Q system software does conform to the applicable criteria of DI&C-ISG-04, Staff Position 1, Point 10 because the Common Q system includes hard wired interlocks of the MTP that will be active during the software load process.

Staff Position 1, Point 11

Staff Position 1, Point 11, states that provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.

As discussed in DI&C-ISG-04 Position 1, Point 1, and in Sections 4.1.1.1, and 4.1.3 of this SE, the Common Q platform does not depend on interdivisional communications or external systems to perform its safety functions. The safety processor instruction sequence is described in Section 4.1.1.6 of this SE.

The Common Q TR does not propose any provision for sending or receiving software instructions from other divisions of the system or from NSR systems connected through the FPDS node boxes. The NRC staff determined that the Common Q platform complies with Staff Position 1, Point 11.

Staff Position 1, Point 12

Staff Position 1, Point 12, states that communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in non-safety equipment, do not constitute “single failures” as described in the single failure criterion of 10 CFR Part 50, Appendix A. This Section provides 12 examples of credible communication faults, but cautions that the possible communication faults are not limited to the list of 12.

For Common Q communications messages may be corrupted due to the following causes;

- Errors in communications processors,
- Errors introduced in buffer interfaces,
- Errors introduced in the transmission media, or
- Interference or electrical noise.

For interdivisional communications through the high speed data links, there are design features including the mirror RAM check (described in Section 4.1.1.5 of this SE) and the use of CRC’s (described in Section 4.1.3.2 of this SE) that provide added assurance that data corruption during transmission from the data source (another safety division) and the receiving safety processor will be identified and handled by the safety processor and will not adversely affect the

safety function of the system. The design and operation of the Common Q is intended to prevent communication faults from adversely affecting the application program or its ability to perform its assigned safety functions.

Westinghouse provided explanations for how the Common Q system would respond to each of the 12 faults listed in DI&C-ISG-04 Position 1, Point 12, within the Common Q TR Section 5.6.12. For each of these cases, specific design features of the Common Q system that have been evaluated by the NRC staff in this SE were credited for ensuring that the integrity of the safety functions would be maintained.

The NRC staff determined that communications faults, including the 12 examples contained in Staff Position 1, Point 12, will not adversely affect the performance of the required safety functions, and that the Common Q platform complies with Staff Position 1, Point 12.

Staff Position 1, Point 13

Staff Position 1, Point 13, states that vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely, or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.

Vital communications which are the subject of this point are performed through the HSL communications interface for the Common Q system. Provisions to ensure that data received over this interface is correct and correctly understood have been included in the Common Q platform design as follows:

- Use of CRC to verify integrity of received data (Section 4.1.3.2)
- Mirror RAM Checks (Section 4.1.1.5)
- I/O Flash Custom PC Element (Section 4.1.7)

Error correcting code is not utilized in Common Q systems. When errors are detected the systems are designed to flag data as failed and to enter into a state that would not compromise the safety functions of the system. The Common Q TR does not propose any interchannel/interdivisional communications or input from any external systems that would be required for performance of the system safety functions. Therefore, each safety processor is not dependent upon any information or resource originating from outside processor's own safety division to perform its assigned safety functions.

The NRC staff determined that the Common Q platform complies with Staff Position 1, Point 13.

Staff Position 1, Point 14

Staff Position 1, Point 14, states that vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement

of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.

The Common Q vital communications that pertain to this point are the HSL serial communications interfaces that are used for data exchange between different divisions of a Common Q system. Section 4.1.3.2 discusses the functions of the HSL. Transmission of data over the Common Q HSL is unidirectional and does not rely on acknowledgement from the receiving processor. The Common Q HSL communications is designed to achieve a logical point-to-point configuration. No equipment outside of the divisions of the sending and receiving processors is relied upon to establish communications between these safety processors.
The NRC staff determined that the Common Q platform complies with Staff Position 1, Point 14.

Staff Position 1, Point 15

Staff Position 1, Point 15, states that communications for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.

The evaluation of Common Q against Staff Position 1, Point 7, determined that a fixed data format of the data sets used by the PM646A was established. As a result, these data sets are predefined and their format and sequence are pre-determined.

As described in Section 4.1.3.2 of this SE, the data transmission cycle time and the amount of data transferred during a cycle is determined by application-specific design. The data transmitted and the frequency of transmission remains fixed for any given configuration while the system is operable. The Common Q system also has provisions for identifying data as being updated even if it has not changed in value since the previous update.

The NRC staff determined that the Common Q platform complies with Staff Position 1, Point 15.

Staff Position 1, Point 16

Staff Position 1, Point 16, states that network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 CFR Part 50, Appendix A, GDC 24, which states, “interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired” and (2) IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” (Source: NUREG/CR-6082, Section 3.4.3)).

The Common Q system does not utilize network based communications for the exchange of data between the safety processor within a division and other divisions of the Common Q system. Instead, as described in Section 4.1.3.2 of this SE the HSL which is a logical point to point communications interface is used for this purpose. The protocols used for the HSL interface include provisions for identifying a loss of connectivity. In addition, the processing section of the processor module functions independently from the communications section and is designed to accomplish all safety related function tasks independently of the communications processor. Even if the communications processor were to stall, there would be no loss of system safety functionality.

The NRC staff determined that the Common Q platform complies with Staff Position 1, Point 16.

Staff Position 1, Point 17

Staff Position 1, Point 17, states that pursuant to 10 CFR 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.

Vital communications for the Common Q system are performed over the HSL data communications interface. The components of this interface are the PM646A, a fiber optic modem and fiber optic cables that are routed between safety divisions. The fiber optic cabling provides electrical isolation between safety divisions as well as EMI/RFI protection for the remaining system components. The PM646A and the fiber optic modems are subject to environmental qualifications as discussed in Section 4.2.2 of this SE. The generic qualification of the Common Q system encompasses both the hardware and the software used in the system. The Common Q platform was qualified in accordance with the EPRI TR-102323 criteria. As noted in Section 4.2.2 of this SE, the qualification of the Common Q does not include the fiber optic cables used to connect the HSL fiber optic modems. Therefore, an application specific evaluation will be required for plant specific applications of a Common Q system that utilizes fiber optic cables to connect HSL's between safety divisions.

The NRC staff has determined that the Common Q platform meets the guidance provided by Staff Position 1, Point 17. However, as noted above, fiber optic cables used to implement the HSL communications interfaces for a system in safety applications will require application specific review and approval to verify these cables are qualified for the environment in which they will be used, in accordance with 10 CFR 50.49 as applicable.

Staff Position 1, Point 18

Staff Position 1, Point 18, states that provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

The proposed functionality for the Common Q platform includes:

- Cross divisional communications for the purpose of coincidence voting over the HSL communications interface.
- Communications to external non safety systems from a FPDS node box.

Neither of these functions is considered to be unneeded. These communications provisions are analyzed in a FMEA which is performed for each project that deploys the Common Q Platform. This is PSAI 6.10. The NRC staff determined that for the Common Q system, the requirement to perform failure modes and effects analyses for a plant specific application meets the intent of the guidance provided in Staff Position 1, Point 18.

Staff Position 1, Point 19

Staff Position 1, Point 19, states that the communications data rates be such that they will not exceed the capacity of a communications link or the ability of nodes to handle traffic, and that all links and nodes have sufficient capacity to support all functions. To do this, the applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions and that communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

As described in the discussion for DI&C-ISG-04 Staff Position 1, Point 6, above, the communication rates for the HSL interface are established and controlled by the control tasks that are running within the processing section of the processor module. In addition the volume of data transmitted through an HSL interface remains constant as the safety function processor performs its safety functions. Actual data transmission rates and data volume are application specific parameters which cannot be assessed in a generic platform perspective. Since these parameters are constant for a given application an initial confirmation that parameter limits are not exceeded should be performed once the true data rates have been identified. Implementation of Common Q platform safety system applications will require application specific review to verify conformance to the guidance of Staff Position 1, Point 19.

Staff Position 1, Point 20

Staff Position 1, Point 20, states that the safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.

A discussion of the Common Q throughput and response time is provided in Section 4.1.1.4 of this SE. To ensure that the Common Q system meets its application system response time requirements, the execution time for all of the systems tasks is calculated and measured during system development. This calculation includes terms to address the response time of the memory processing and associated circuits. Westinghouse has imposed a CPU load limit of 70 percent in order to avoid control module overruns which could adversely affect the deterministic behavior and response time of the system.

The Common Q system is also designed such that the processing section of the processor module does not depend on any of the data that originates outside of its division to perform its safety functions or to meet its time response requirements. Therefore, data errors and error rates will not affect the deterministic performance or response time of the safety function processor.

DI&C-ISG-04, Section 2 - Command Prioritization

Section 2 of DI&C-ISG-04 provides guidance applicable to a prioritization device or software function block, which receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device.

The design of field device interfaces and the determination of means for command prioritization were not provided in the Common Q TR. If a Common Q platform based design is used for the development of a command prioritization system then an additional evaluation of that system against the criteria of DI&C-ISG-04 Section 2 should be performed. Since the Common Q TR

does not address a specific application involving command prioritization, no evaluation against this staff position could be performed.

DI&C-ISG-04, Section 3 - Multidivisional Control and Display Stations

Section 3 of DI&C-ISG-04 provides guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division, and applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.

The design of multidivisional stations was not provided in the Common Q TR. If a Common Q platform based design is used for the development of a multidivisional station, then an additional evaluation of that system against the criteria of DI&C-ISG-04, Section 3, should be performed. Since the Common Q TR does not address a specific application involving a multidivisional control or display station, no evaluation against this staff position could be performed.

4.1.4 Power Supply

Westinghouse has designed and qualified a series of Common Q power supplies. Power supply qualification testing is addressed in the Summary Qualification Reports (Reference 15 and Reference 22). The design, manufacture, and CGD of the Common Q power supplies are part of the Westinghouse 10 CFR Part 50, Appendix B, and quality assurance program.

Westinghouse, is an Appendix B approved supplier, has designed, built, and qualified the supplemental Common Q hardware under its 10 CFR Part 50, Appendix B, quality assurance program, that includes the dedication of commercial-grade items in accordance with the guidance in the EPRI TRs TR-106439 and/or TR-107330. Westinghouse submitted the Summary Qualification Report to summarize the results of the Common Q supplemental hardware qualification program. The supplemental equipment consisted of the FPDS, the Common Q power supplies, the WDT function in the PM646A module, and miscellaneous support equipment. The objective of this supplemental program is to qualify this set of equipment to the same levels as the previously qualified AC160 portions of the Common Qualified platform. Because all of the Common Q components must operate together and interact with each other to prove performance during the qualification testing, Westinghouse performed the supplemental environmental, seismic, and EMC testing on the complete complement of Common Q components. The Addendum to Summary Qualification Testing for Common Q Applications (Reference 10) includes a table (Table 7-1) that identifies updated Common Q power supply components that were included as equipment under test and summarizes the results of the EMI/EMC tests. Therefore, Common Q components that were previously qualified before the initial SE was issued underwent qualification testing again with the supplemental Common Q hardware.

4.1.5 Watchdog Timer Functions

An external and independent hardware WDT module is no longer included in the Common Q system design.

Each of the two internal sections (processing section and communications section), of the processor module contains a microprocessor. Both of these microprocessors have an associated Window Watchdog Timer (WWDT). Each WWDT is a precision WDT that must be

triggered within a small window of time. If the WWDT is triggered earlier or later than this time window, then the timer output changes state.

When a change of state occurs on either of the two WWDTs, the WDT relay whose contacts are accessible from the processor front panel changes state. Depending on the specific system application, the WDT relay can be used to annunciate a failure, actuate a divisional trip, or set output states to predefined conditions. For example, the WDT relay may be used to control the power to the relays for the digital output module. Isolation is provided by means of a solid state relay that is connected at the output of the WDT circuit for those applications where the watchdog timer is configured to interface with external systems. Appendix A of the Common Q TR provides additional information on the watchdog timer configuration.

Additional watchdog timers are associated with the processing section of the PM646A known as stall timers. These stall timers are designed to force a CPU reset when activated. A CPU reset will in turn activate the watchdog timer output relay.

4.1.6 Defense-in-Depth and Diversity

The Staff Requirements Memorandum on SECY 93-087, dated July 21, 1993, describes the NRC position on diversity and defense-in-depth (D3) requirements to compensate for potential common-cause programming failure. This requires that the applicant assess the defense-in-depth and diversity of the proposed instrumentation and control system, and if a postulated common cause failure (CCF) 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 CCF, shall be required to perform either the same function or a different function.

Guidance on the evaluation of D3 is provided in BTP 7-19. In addition, NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” dated December 31, 1994, summarizes several D3 analyses performed after 1990 and presents a method for performing such analyses.

Additional guidance on evaluation of the need for D3, and acceptable methods for implementing the required D3 in DI&C system designs, is contained in “Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-02 Task Working Group #2: Diversity and Defense-in-Depth Issues.”

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 7-19 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 Westinghouse has applied in the design description for the integrated solution. Depending upon how many of its I&C systems a licensee elects to upgrade via Common Q technology, it may need to apply Point 4.

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 via Common Q technology. It discusses 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 7-19. 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 or design certification applicant. This is PSAI 6.11.

On the basis of its review, the NRC staff found that Westinghouse diversity and defense-in-depth assessment methodology is consistent with the NRC staff position stated in BTP 7-19. Applications correctly following this methodology for a plant-specific diversity and defense-in-depth assessment should be acceptable.

4.1.7 Evaluation of New Custom PC Elements

Westinghouse developed three new custom PC elements to enable the firmware to save data to flash PROM. These custom PC elements were developed in accordance with the requirements of the Common Q Software Program Manual (Reference 6).

Flash Initialization Custom PC Element

The Flash Initialization custom PC element provides a means for copying data from Flash PROM to the PM646A RAM.

I/O Flash Custom PC Element

The I/O FLASH Custom PC Element provides an application interface (read/write access) to the data stored in the PM646A RAM. This element also performs supervisory functions which

monitor changes to RAM data and initiate updates to the Flash PROM in order to keep the Flash data current.

Update Flash Custom PC Element

The Update FLASH Custom PC Element is used by the application to store modified data located in RAM back to the Flash PROM. The PM646A firmware ensures that no RAM write access takes place while the Flash PROM is being updated.

The staff has evaluated the functional details of the features provided by these custom PC elements and has concluded that there is no adverse impact on the ability of the Common Q system to perform its assigned safety functions. The staff also concludes that the established level of deterministic behavior of the Common Q system as defined in Section 4.1.1.6 of this SE has not been compromised by the addition of this memory exchange feature.

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

EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," provides detailed guidance for the evaluation of existing commercial computers and software to meet the provisions of IEEE Std. 7-4.3.2-2003, which was approved in Regulatory Guide 1.152, Revision 3.

The CGD guidance provided in EPRI TR-106439 involves identifying the critical characteristics of the commercial grade digital equipment based on the safety-related technical and quality requirements, selecting appropriate methods to verify the critical characteristics to enable dedication of the digital equipment, and maintaining the dedication basis over the service life of the equipment. The guidance adapts the methods established in EPRI NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications," to digital equipment and is consistent with the guidance contained in Generic Letter (GL) 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products," and GL 91-05, "Licensee Commercial-Grade Procurement and Dedication Programs."

EPRI TR-106439 identifies three categories of critical characteristics in terms of physical, performance, and dependability attributes. These characteristics correspond to the categories identified in Section 5.4.2.2 of IEEE Std. 7-4.3.2 2003, which are physical, performance, and development process characteristics. Determination of specific critical characteristics is accomplished by a critical design review that accounts for the requirements of the safety application and the potential hazards that could interfere with the safety function.

Verification of the critical characteristics is at the heart of the dedication process. EPRI TR-106439 adapts four acceptance methods defined in EPRI NP-5652 to establish an approach to verify the characteristics for digital equipment. The four methods are:

- Method 1 --- Special Tests and Inspections
- Method 2 --- Commercial Grade Survey of Supplier
- Method 3 --- Source Verification
- Method 4 --- Acceptable Supplier/Item Performance Record

EPRI TR-106439 states that verification of the critical characteristics for digital equipment will require the use of more than one of the methods since no one method will typically be sufficient by itself.

Westinghouse performs commercial grade dedication for the following Common Q software components:

1. The QNX operating system which is used for the Flat Panel Display system PC Node Boxes, and
2. The Advant Base System Software which is implemented in the AC160 controller.

Westinghouse performs commercial grade dedication for the following Common Q hardware components:

1. The Flat Panel Display System,
2. The AC160 Controller, and
3. The Module Power Supply System

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. Westinghouse is a third-party dedicator for the Common Q platform.

BTP 7-14 provides acceptance criteria for commercial-off-the-shelf software and software embedded in commercial-off-the-shelf components as follows:

“Commercial-off-the-shelf software and software embedded in commercial-off-the-shelf components, such as meters, circuit breakers, or alarm modules should be appropriately evaluated to confirm that required characteristics are met. EPRI TR TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," as approved by NRC’s SE dated July 17, 1997, describes an acceptable method for performing this evaluation.”

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.”

Westinghouse is an approved 10 CFR Part 50 Appendix B supplier. The staff does not attempt in this review to renew Westinghouse’s status as an approved 10 CFR Part 50 Appendix B supplier. However, during a visit to a Westinghouse facility on February 28, through March 4, 2010, the NRC staff performed an audit of Westinghouse’s documentation associated with the Watts Bar Unit two Post Accident Monitoring system commercial grade dedication activities (Reference 7). During this audit, the NRC staff examined the Westinghouse procedures being used for developing commercial dedication instructions as well as a recent Commercial Grade Dedication Survey report for the QNX operating system (Reference 13).

Chapter 10, “Commercial Grade Dedication Program,” of the TR refers to the guidance provided by IEEE Std 7-4.3.2-2003 and EPRI TR-106439 for the commercial-grade dedication of the Common Q platform. On the basis of the audit, the NRC staff determined that the procedures and processes in the documentation correspond to the requirements of IEEE STD 7-4.3.2-2003 and the guidance of EPRI TR-106439 and, therefore, provide an acceptable program for the dedication of commercial-grade items.

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. Westinghouse uses methods 1, 2, and 4 for the qualification of the Common Q platform.

The vendor survey applies to both the Previously Developed Software (PDS) and the hardware. The seismic and environmental qualification of the hardware also includes operation of the PDS and some test application 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 AC160 system software, and FPDS software. Two separate Westinghouse review teams perform surveys of the vendors for these two categories. Separate reports of the commercial-grade dedication effort are issued for each of these categories. 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. Both of these groups have been tested and the NRC staff has reviewed the test reports. The staff’s re-affirmation evaluation of Westinghouse’s dedication activities follows.

4.2.1 Vendor Surveys

4.2.1.1 Vendor Survey for AC160 PLC System

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 60880 1986, "Software for Computers in the Safety Systems of Nuclear Power Stations." IEC 60880 is referenced in IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

Westinghouse 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 Westinghouse 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

IEEE Std 7-4.3.2 2003 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 identify and correct tool induced flaws. Section 3.3.10 of the Common Q SPM states that:

> "*The inadvertent introduction of software hazards by project tools is mitigated by the proper use of techniques for software configuration management, software quality assurance, and IVV as described in this SPM*".

Section 4.19 of the SPM also states that;

> *"The tools, techniques and methodologies employed in this process shall provide means for software to be verifiable from each phase of the project to the next".*

This establishes compliance with the software tools criteria of Section 5.3.2 of IEEE Std 7-4.3.2-2003 because errors introduced into software by tools will be identified and corrected through the V&V and testing processes outlined in the Common Q SPM. Therefore, Westinghouse 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.

The AC160 products manufactured in Sweden that conform to the requirements of BA AUT-99-ADVANT-00 are supplied to Westinghouse. The individual modules and assemblies are subjected to an incoming receipt inspection by Westinghouse. Configuration information is maintained in a documentation database that contains the reference details, including the models, and revision levels of all Common Q system components.

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 are taken of the PCBs for all AC160 equipment. The digital images serve as a record of the actual assembly of each AC160 module used for safety

system applications. The digital images are 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 Westinghouse.

These requirements and processes establish a detailed configuration for the safety-related AC160 equipment. The traceability aspect of the configuration provides 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 are used for Common Q safety system development.

The staff has 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 NRC staff concludes that the AC160 PLC system meets the requirements set forth in BTP 7-18 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- 2003 as endorsed by RG 1.152 Revision 3 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.

The two products that are 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, and
- QNX photon application builder (PhAB).

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

Westinghouse did not dedicate the software development tools. IEEE Std 7-4.3.2- 2003 does not require that the software tools be dedicated if the V&V process will detect errors that the tools may introduce. The Westinghouse V&V procedures are specified in the SPM and have been evaluated in this SE. IEEE Std 7-4.3.2- 2003 requires that the tools be identified and placed under software configuration management control. Westinghouse configuration management is evaluated as part of the Common Q Software Program Manual (Reference 6) SE. On the basis of the above, the NRC staff concludes that it is acceptable that the PDS development tools from QSSL not be dedicated.

Westinghouse has committed to develop a technical manual for each of the Common Q systems. The Westinghouse audit team indicates that the application specific Common Q system technical manual will provide error diagnostic and troubleshooting information. The staff observes that SPM Section 10.6 specifies that Westinghouse will develop and provide a maintenance manual for each Common Q system as part of the User Documentation for the system. The staff concludes that the above provisions for a maintenance manual are acceptable.

On the basis of the review of the QNX CGDR, the NRC staff concludes that Westinghouse has acceptably dedicated the commercial-grade QNX, and Photon microGUI, 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 protection functions. For the qualification of the FPDS hardware, see Section 4.2.2.2.

4.2.2 Seismic and Environmental Qualification

An evaluation of the Common Q Seismic and Environmental qualifications was initially performed under the Common Q Safety Evaluation (Reference 3) as supplemented by Safety Evaluations (References 4 & 5). This evaluation addresses the baseline Common Q equipment as well as changes that have been made to the Common Q platform since these previous SE's were performed.

4.2.2.1 Environmental, Seismic and Electromagnetic Qualification of the AC160

This section is the NRC 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.

The following AC160 items were included in the initial tests:

- Processor 19-inch subrack
- Expansion 19-inch subrack
- PM645C processor module (Superseded by PM646A)
- PM646 processor module including its internal watchdog timer. (Superseded by PM646A)
- CI631 communication interface module
- Models of S600 I/O modules to include:
    - AI620

  - AI635 (Discontinued)
  - AI685
  - AO650
  - DI620
  - DO620 (Discontinued)
  - DO625
  - DO630
  - DP620
- TC630 fiber-optic modem
- TC514 fiber-optic modem
- OZDV 114 fiber-optic modem
- TC625 wire modem

The following additional items were subjected to seismic, environmental, and electromagnetic compatibility (EMC) testing in order to incorporate this equipment into the baseline Common Q platform.
PC Node Box/Flat Panel Display Equipment Under Test:

- PC Node Box
- 6.5 inch Flat Panel Display
- 12 inch Flat Panel Display
- 15 inch Flat Panel Display
- 19 inch Flat Panel Display

Power Supply/Input Line Filter

- 24Vdc/20A
- 24Vdc/10A
- 48Vdc/5A
- 12Vdc/15A
- Input Line Filter

Fiber Optic Modem

- Fiber Optic Modem OZDV 114B

Analog Input Module

- AI687
- AI688

Common Q platform equipment is qualified for a mild environment, such as a main control room and auxiliary electrical equipment rooms. Westinghouse and previously CENP performed the following tests: EMI/RFI testing, environmental testing, and seismic testing.

For these tests, CENP had initially 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 was configured to replicate the worst case hardware configuration that encompassed the intended applications of the Common Q platform equipment. For the other tests, the AC160 system was configured to represent the loading conditions for anticipated Common Q applications.

Subsequent to these initial tests, Westinghouse performed additional seismic, environmental, and EMC testing in order to qualify new equipment for inclusion into the Common Q platform. The results of this additional testing are summarized in the Addendum to Summary Qualification Report of Hardware Testing for Common Q Applications (Reference 10).

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 323-2003, "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

Westinghouse 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. See References 10, 14, 15 and 22 for additional information on tests performed on the original Common Q equipment. The tests showed that none of the AC160 modules failed to function as a result of the environmental conditions imposed by the tests. The environmental conditions imposed by these tests 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.

An addendum to the Summary Qualification Report of Hardware Testing for Common Q Applications was submitted by Westinghouse (Reference 10) to address new Common Q equipment that has been introduced to the platform since the previous evaluation was completed in 2000. The temperature conditions during these tests accounted for the expected heat rise in a cabinet where the test specimens would normally be installed. Because installed installation configurations can vary depending on the application specific design, it is imperative that a plant specific analysis be performed for each application to ensure that the design basis temperature (test temperature minus the IEEE Std 323-1983 margin requirement) of the Common Q equipment is not exceeded when installed in the cabinet. See PSAI 6.4. The analysis shall demonstrate, 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 7-1 of the TR.

The NRC staff concludes that the referenced temperature qualification tests provide reasonable assurance that the Common Q equipment will operate properly within its specified environmental conditions. Additionally, the NRC staff concludes that for plant-specific Common Q systems, the licensee should validate that Westinghouse'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 PSAI 6.4.

4.2.2.1.2 Seismic Testing.

The test specimens were mounted to a tri-axial seismic simulator table and were subjected to a series of seismic simulation tests. The tests performed on the test specimens included resonance search tests and random multi-frequency tests. The random tri-axial multi-frequency tests, which simulate a series of earthquake environments, were performed in accordance with

IEEE Std 344-1987. Common Q equipment is designed to withstand the cumulative effects of a minimum of five operating basis earthquakes (OBE) and one safe shutdown earthquake (SSE) without loss of either safety function or physical integrity.

The PM646A processor module and the AI685 analog input module failed to perform satisfactorily at the SSE level. These modules are qualified to the OBE level defined in Figure 6-7 of Reference 15.

The addendum to the Summary Qualification Report of Hardware Testing for Common Q Applications (Reference 10) was submitted by Westinghouse to address new Common Q equipment that has been introduced to the platform since the previous evaluation was completed in 2000. Section 7.1 of this report describes the additional seismic testing performed to qualify the new Common Q components and provides a summary of the seismic test results. The test input was shown to meet all requirements specified in IEEE Std 344-1987.

Several installation limitations were identified in Section 9 of the Common Q Qualification Summary Report. Some of these restrictions apply to actions such as installation and maintenance activities that will be performed by the licensee. It is therefore necessary for the licensee to ensure adherence to these restrictions throughout the design, development, installation, operation, and maintenance phases of a Common Q project. This should be included in the analysis activity prescribed by PSAI 6.4.

On the basis of this review, the NRC staff concludes that the tested AC160 equipment is qualified to the triaxial seismic simulator table limits shown in either Figure 4-2, “Composite SSE Test Response Spectra (TRS), 1% Damping,” of Test Report 2008677-IC-TR560-10, Revision 00, “Seismic Qualification Report for Module Equipment Qualification for Common Q Applications,” (Reference 12) or Figures 6-1, 6-4, 6-5, and 6-7, “Test Series Test Response Spectra (TRS),” as delineated in Section 6.3.3 of the Summary Qualification Report of Hardware Testing for Common Q Applications,” (Reference 15) depending on which qualification test included the specific module being evaluated . Therefore, the NRC 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 cited above. Additionally, because the test specimen was configured using dummy modules to fill all the used rack slots, the licensee must verify that its Common Q system does not have any unfilled rack slots. This is PSAI 6.4.

4.2.2.1.3 Electromagnetic Interference and Radio Frequency Interference

EPRI submitted TR TR-102323, "Guideline for Electromagnetic Interference Testing in Power Plants," for staff review in 1994. The TR 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 NRC staff issued a SE 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.

Electromagnetic compatibility (EMC) tests and measurements have been performed on the AC160 portions of the Common Q platform equipment in accordance with EPRI TR-102323. The details of these tests and measurements are described in 2008677-IC-TR560-12, "EMI Qualification Test Report for Common Q Applications," (Reference 11). Four PM645C modules and one PM646 module were used for the initial test. These processor modules have been superseded by the PM646A.

Additional testing was performed to qualify the PM646A processor module and the results of this test are summarized in the Summary Qualification Report of Hardware Testing for Common Q applications (00000-ICE-37764 Revision 03) (Reference 15).

The test specimen hardware configuration was configured to simulate the worst case hardware configuration to encompass the expected applications of the equipment. The worst case hardware configuration was simulated by configuring the AC160 to the maximum load without going to a bus extension. This would allow the addition of up to another two AC160 racks. Westinghouse 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 were actively used.

Westinghouse performed four emission tests and seven susceptibility tests on the test specimen. Table 6-0 of reference 11 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, Westinghouse recorded some anomalies. Therefore, the NRC staff finds that the AC160 equipment did not meet the EMI susceptibility requirements of TR-102323. The NRC staff, however, accepts the EMI test results reported in reference 11, 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 a site specific 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 issue is addressed by PSAIs 6.4, 6.21, and 6.22.

Test results revealed that electric field emissions from the Common Q equipment exceeded specified limits when the High Speed Link (HSL) was connected to the test system. As a result the site specific analysis to be performed for an application based upon the Common Q platform that includes implementation of High Speed Links shall quantify the impact of higher electromagnetic emissions on operation of locally mounted equipment. This is PSAI 6.21.

Tests also revealed that AI685 modules configured for either RTD or Thermocouple inputs require installation of a metallic barrier to shield the module from the effects of radiated electric fields. This is PSAI 6.22.

4.2.2.2 Seismic and Environmental Qualification of Non-AC160 Hardware

Westinghouse has addressed the previously addressed GOI 7.6 regarding the seismic and environmental qualification for the FPDS, WDT, and Common Q Power Supply modules by performing environmental, seismic, and EMC testing on the complete complement of Common Q equipment. This testing included those components that had been previously qualified for the initial SE and the test results are documented in the Addendum to Summary Qualification Report of Hardware Testing for Common Q Applications (Reference 10).

The qualification of the Common Q platform did not include qualification of the fiber optic cables used to connect the HSL Fiber Optic Modems. It is expected that the qualification requirements for all cabling used for a Common Q system be evaluated under the cognizance of the licensees design control processes. Therefore, an application specific evaluation is required for plant specific applications of a Common Q system that utilizes fiber optic cables to connect HSL's between safety divisions.

4.3 Life Cycle Planning Process for Application Software

Westinghouse submitted WCAP-16096 (Formerly CE-CES-195-P), "Software Program Manual for Common Q Systems," (SPM) (Reference 6) for staff review. It specifies the life cycle planning process for application software. 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. The Common Q SPM is being evaluated by the NRC in conjunction with this SE and a separate SE will be issued for the Common Q SPM.

4.4 Common Q Applications

Westinghouse (formerly CENP) has previously submitted Appendices 1 through 4, which describe proposed design approaches for implementing the Common Q platform in various safety systems at nuclear power plants. These appendices provide additional information to support the NRC staff's review of the generic design details of the Common Q platform. The staff previously evaluated the content of the appendices in the original Common Q SE (Reference 3). Changes made to these appendices were also evaluated in the supplemental SE (Reference 5). Since no new changes have been submitted to these appendices, no further evaluation was performed for this SE.

4.5 Common Q Platform Generic Change Process

Per letter dated August 12, 2010 (Reference 17), Westinghouse submitted WCAP-17266 "Common Q Platform Generic Change Process (Reference 18) for NRC review and approval.

The Common Q generic change process defined by WCAP-17266 describes methods used by Westinghouse to screen, and evaluate proposed changes to Common Q components, software or processes defined within the Common Q Platform and Software Program Manual TRs subsequent to NRC review and approval. This process defines criteria to be used for the determination of whether the safety conclusions of the NRC SE remain valid following the proposed change or if the changes will require submittal to the NRC for evaluation and approval prior to implementation.

The staff has reviewed this document and acknowledges the benefits provided by implementation of a formal TR screening, evaluation, and change process however, the NRC is unable to perform a SE of the processes defined by this document or make any safety conclusions regarding these processes at this time. An NEI and NRC sponsored workshop has been proposed to evaluate the feasibility of adopting a generic TR Change Control Program. The applicant is encouraged to participate in the development of this program to provide Westinghouse's perspective for additional staff consideration.

The Common Q platform generic change process is included as a reference within this SE in order to provide future reviewers of Common Q applications that reference this SE with

information discussing how Westinghouse evaluates and documents changes to the Generic Common Q platform components, and processes defined within the Common Q TR. It is also beneficial for reviewers of Common Q applications to have access to the Westinghouse generic change process in order to interpret the information provided in the Record of Changes document discussed below.

4.6 Common Q Record of Changes Document

Per letter dated August 25,' 2010 (Reference 19), Westinghouse submitted WCAP-16097, Appendix 5, "Common Qualified Platform Record of Changes, "(Reference 20) for NRC review and approval.

The staff reviewed the Common Q Record of Changes (ROC) and confirmed that the changes to the Common Q platform hardware, software and processes defined within the Common Q Generic Platform TR are consistent with the revised TR evaluated by this SE. Furthermore, the NRC staff reviewed the information provided in the Tables within the ROC and determined that these tables provide valuable information that should be used during application specific reviews to determine acceptability of platform components (hardware, software, and process) that have been changed subsequent to the NRC review and approval of the TR's. PSAI 6.23 is therefore being included in this SE to provide direction for plant specific SEs to include a review of the current Common Q record of changes to assess the validity of previously derived safety conclusions in light of the changes made to the Common Q platform.

5.0 SUMMARY OF REGULATORY COMPLIANCE EVALUATIONS

This SE 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 GOI 7.8. Careful attention must also be given to the plant-specific items listed in Section 6.0 of this SE.

The General Design Criterion listed in Appendix A, 10 CFR Part 50, establish minimum requirements for the design of nuclear power plants. IEEE 603-1991 is 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 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.

Paragraph 50.55a(a)(1), Quality standards, ASME Codes and IEEE Standards, and alternatives for systems important to safety, is addressed by conformance with the codes and standards listed in the SRP. Westinghouse uses codes, standards and commercial-grade dedication in the development of the Common Q system that are either the same as or equivalent to the standards in the SRP. The staff has reviewed the revised list of referenced standards in the updated Common Q TR and has evaluated these against the standards referenced in the SRP. The staff concludes that the Common Q system is in conformance with this requirement.

Paragraph 50.55a(h) endorses IEEE Std 603-1991, which addresses both system-level design issues and quality criteria for qualifying devices. Westinghouse has addressed these issues in the Common Q TR. Subject to the limitations identified in this SE, the NRC staff finds that the Common Q system meets the criteria of IEEE Std 603-1991 and the supplemental standard

IEEE Std 7-4.3.2-2003. For the systems and components reviewed, the NRC staff concludes that the Common Q system is in compliance with this requirement.
Paragraph 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 (PSAI 6.14).

Paragraph 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 D3analysis to be performed by the licensee (see PSAI 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

SRP Chapter 7 Appendix 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 Std 7-4.3.2-2003 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 divisions or more than one of the two redundant ESFAS trains. These redundant divisions 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 Westinghouse 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 323-2003, "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 are listed in Table 1 below.

For the systems and components reviewed, the independence criteria of IEEE Std 603-1991 for the Common Q system is met through the redundancy and separation of the divisions. The communication between divisions 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 338-1987. 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 can be 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 delineated in the Common Q application appendices that were reviewed, the NRC 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 NRC staff conducted a review of the safety system descriptions in the TR 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 NRC 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 NRC 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 NRC staff concludes that Westinghouse has identified those systems and components consistent with the design bases for those systems. Therefore, the NRC 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 NRC 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 NRC 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 NRC 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 NRC staff concludes that a Common Q system conforms to the design bases requirements of IEEE Std 603-1991. On the basis of its review, the NRC 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 NRC 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 379-2000 as supplemented by RG 1.53. On the basis of this review, the NRC staff concludes that, for the systems and components reviewed, the Common Q system satisfies the requirement of IEEE Std 603-1991 with regard to system reliability and testability. Therefore, the NRC 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 NRC staff concludes that for the systems and components reviewed, the Common Q system satisfies the requirement of IEEE Std 603-1991 with regard to system independence. Therefore, the NRC staff concludes that the Common Q system satisfies the requirements of GDC 22.

On the basis of its review of the failure modes and effects analyses that CENP previously submitted in Appendices 1, 2, and 3, the NRC staff concludes that the proposed design approaches are consistent with the requirements of GDC 23. Therefore, the NRC 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 PSAI 6.10).

Based on its review of the interfaces between the Common Q safety systems and plant operating control systems, the NRC staff concludes that for the systems and components reviewed, the Common Q safety systems satisfy the requirements of IEEE Std 603-1991 with

regard to control and protection system interactions. Therefore, the NRC staff finds the Common Q safety systems satisfy the requirements of GDC 24.

On the basis of its review, the NRC 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 NRC staff finds that the Common Q RTS satisfies the requirements of GDC 25.

The NRC staff's conclusions are based upon the requirements of IEEE Std 603-1991 with respect to the design of the Common Q system. Therefore, the NRC 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 IEEE Std 603-1991.

On the basis of its review of the Westinghouse defense-in-depth and diversity analysis methodology, the NRC staff determined that this methodology provides a method by which the licensee could comply with the criteria for defense against common-mode failure in digital instrumentation and control systems. Adequate diversity and defense against common-mode failure must be provided to satisfy the requirements of GDC 21 and 22, and Item II.Q of the Staff Requirements Memorandum on SECY-93-087. The NRC 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 PSAI 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 NRC staff concludes that the AC160 PLC system satisfies BTP 7-18 and follows the guidance in EPRI TR-106439 and is, therefore, acceptable.

Based on its review, the NRC 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 Std 603-1991 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.

6.0 PLANT-SPECIFIC ACTION ITEMS

The following plant-specific actions must be performed by the licensee prior to placing a safety related system based on the Common Q platform into an operable status. If such a system is being installed under a license amendment, NRC approval for installation of the Common Q system would also be required.

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 ***This Plant-Specific Action Item has been resolved by supplemental SE dated June 22, 2001 (Reference 4).***

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. The licensee must also ensure that the plant specific common Q system configuration does not exceed the configuration used during platform qualification testing. See Sections 4.2.2.1.1, 4.2.2.1.2, and 4.2.2.1.3.

The Common Q test specimen was configured 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 Westinghouse software development process for application software, the NRC staff concludes that the Common Q software program manual 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 NRC staff or others to evaluate the quality of the design features upon which the safety determination will be based. When a license amendment process is used for implementation of a Common Q based safety system, the NRC 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 the 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 and 4.1.3.4 of this SE as well as Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3 of Reference 3 for additional information on this item.

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, 4.4.3.3, and 4.4.4.3.6 of Reference 3 for additional information on this item.

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 of Reference 3 for additional information on this item.

6.9 Modifications to plant procedures and/or TS due to the installation of a Common Q safety system will be reviewed by the NRC 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 of Reference 3 for additional information on this item.

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 Section 5.0 and 4.1.3.4 of this SE as well as Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3 of Reference 3 for additional information on this item.

6.11 A licensee implementing any Common Q application (i.e., PAMS, CPCS, or DPPS) shall demonstrate that the plant-specific Common Q application complies with the criteria for defense against common-mode failure in DI&C systems and meets the requirements of BTP 7-19. See Sections 4.1.6 of this SE as well as Sections 4.4.2.3, 4.4.3.3, and 4.4.4.3.3 of Reference 3 for additional information on this item.

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 of Reference 3 for additional information on this item.

6.13 The analysis of the capacity of the shared resources to accommodate the load increase due to sharing. Section 4.4.4.3.1 of Reference 3 for additional information on this item.

6.14 The licensee implementing Common Q applications 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.

6.15 During the Software development process, the licensee must specify plant specific requirements for system automatic self-testing features that are needed to ensure proper functioning of the Common Q application during operation. See Section 4.1.1.3.

6.16 A licensee implementing a Common Q DPPS shall ensure that no more than four processor modules are installed within a single AC160 controller. See Section 2.1.

6.17 A licensee implementing a Common Q DPPS must ensure that all hardware components used for system development are approved for use in nuclear safety system class 1E applications and are listed in Table 1. See Section 2.1 for a discussion of the hardware components of the Common Q platform.

6.18 The licensee implementing Common Q applications must ensure that administrative controls are put into place to ensure that changes to setpoints are only performed while the system is not being relied upon to perform its safety functions. The affected division of the Common Q safety system must be declared inoperable prior to implementation of setpoint changes. See Section 4.1.3.4.

6.19 A licensee implementing a specific application based upon the Common Q platform must ensure that the serial communications link between the MTP and the Processor

Module is disabled by means of a physical disconnection (i.e., cable is removed from the serial port at the front of the PM646A). Alternative means of disconnecting this serial communication link may be considered, however, any means of disabling this communication link which rely upon software logic would invalidate the DI&C-ISG-04 conformance safety conclusions in Section 4.1.3.4 Staff Position 1, Point 10 of this SE.

6.20 A licensee implementing an application based upon the Common Q platform that utilizes fiber optic cables to connect HSL's between safety divisions shall ensure that all plant specific environmental qualification requirements for this cabling are met. See Section 4.2.2.2.

6.21 A licensee implementing an application based upon the Common Q platform that includes implementation of HSL must perform a site specific analysis to quantify the impact of higher electromagnetic emissions on operation of locally mounted equipment. See Section 4.2.2.1.3.

6.22 A licensee implementing an application based upon the Common Q platform that uses AI685 modules configured for either RTD or Thermocouple input must ensure that the installation includes a metallic barrier in front of the module. See Section 4.2.2.1.3.

6.23 A licensee implementing an application based upon the Common Q platform should perform a review of the current Common Q Record of Changes document to assess the validity of previously derived safety conclusions if changes have been made to the Common Q platform hardware, software, or processes defined in the Common Q TR.

6.24 A licensee implementing an application based upon the Common Q platform that relies on the FPDS to perform safety critical functions shall perform an evaluation to address the added reliance on the FPDS to accomplish the required safety functions. The affects of not having the necessary information available on the FPDS during the design basis event should be considered and addressed in this evaluation.

6.25 A licensee implementing an application based upon the Common Q platform that relies upon the use of ITPs and the AF100 busses to provide separation between safety and non-safety signals must evaluate the plant-specific design against the independence criteria of IEEE 7-4.3.2-2003, Section 5.6.

7.0 GENERIC OPEN ITEMS

During the initial SE of the Common Q TR (Reference 3), the NRC staff identified 10 GOIs. Of these GOI's 9 have since been closed as a result of additional information provided by the vendor which was evaluated by the NRC staff in two supplemental SEs (Reference 5 and 6). On the basis of its review of the updated Westinghouse Common Q platform as well as supplemental information provided, the NRC staff determined the status of GOI's to be as follows:

7.1 ***This GOI has been resolved by supplemental SE dated February 24, 2003 (Reference 5).***

Westinghouse addressed this issue by developing and qualifying the analog input module AI685 which meets the guidance of EPRI TR 107330.

7.2 ***This GOI has been resolved by supplemental SE dated February 24, 2003 (Reference 5).***

Westinghouse addressed this issue by qualifying the Common Q power supply system components. Refer to Table 1 for a list of Common Q Power Supply components reviewed for this SE. Power supply qualification testing is addressed in the Summary Qualification Report (Reference 15).

7.3 ***This GOI has been resolved by supplemental SE dated February 24, 2003 (Reference 5).***

7.4 ***This GOI has been resolved by supplemental SE dated June 22, 2001 (Reference 4).***

7.5 ***This GOI has been resolved by supplemental SE dated February 24, 2003 (Reference 5).***

7.6 ***This GOI has been resolved by supplemental SE dated February 24, 2003 (Reference 5).***

7.7 ***This GOI has been resolved by supplemental SE dated June 22, 2001 (Reference 4).***

7.8 Westinghouse 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 ***This GOI has been resolved with regard to the acceptability of the design concept by supplemental SE dated June 22, 2001 (Reference 4). Evaluation of each forthcoming design against the independence requirements for safety systems will still need to be performed as prescribed in PSAI 6.25.***

7.10 ***This GOI has been resolved with regard to the acceptability of the design concept by supplemental SE dated June 22, 2001 (Reference 4). Evaluation of each forthcoming design against the independence requirements for safety systems will still need to be performed as prescribed in PSAI 6.25.***

7.11 Westinghouse has not yet conducted seismic and environmental qualification testing on the DI621 Digital Input module. The NRC staff's review of the I/O modules is discussed in Section 4.1.1.1.2.

8.0 REFERENCES

1. Submittal of WCAP-16097-P and WCAP-16097-NP, Revision 3, "Common Qualified Platform Topical Report" (Proprietary/Non-Proprietary) for Review and Approval, Agency wide Documents Access and Management System (ADAMS), Accession No. ML12207A513.

2. Common Qualified Platform TR WCAP-16097-P and WCAP-6097-NP Revision 3, ADAMS Accession Nos. ML12207A512/ML12207A510.

3. Safety Evaluation – Acceptance for Referencing of TR CENPD-396-P, Rev. 01, "Common Qualified Platform," and Appendices 1, 2, 3, AND 4, Rev. 01, ADAMS Accession No. ML003740165.

4. Safety Evaluation for the closeout of several of the Common Qualified Platform Category 1 Open Items related to Reports CENPD-396-P, Revision 1, and CE-CES-195, Revision 1, ADAMS Accession No. ML011690170.

5. Acceptance of the changes to TR CENPD-396-P, Rev. 01, "Common Qualified Platform," and closeout of category 2 open items. ADAMS Accession No. ML030550776.

6. Software Program Manual for Common Q Systems WCAP-16096-NP, Revision 4, ADAMS Accession No. ML12205A052.

7. Trip Report for the Audit of the Common Q Post Accident Monitoring (PAMS) System Used at Watts Bar Nuclear Plant, Unit 2, ADAMS Accession No. ML110691232.

8. Request for Additional Information, License TR (WCAP-160096) Software Program Manual for Common Q Systems, ADAMS Accession No. ML112490485.

9. Request for Additional Information, Licensing TR (WCAP-160097) Common Qualified Platform TR, ADAMS Accession No. ML112850828.

10. Addendum to Summary Qualification Report of Hardware Testing for Common Q Applications (WCAP-17415-P/NP Revision 0), ADAMS Accession Nos. ML11200A207/ML11200A206.

11. EMI Qualification Test Report for Module Equipment Qualification for Common Q Applications, 2008677-IC-TR560-12, ADAMS Accession No. ML003726316 (Proprietary Information. Not Publically Available).

12. Seismic Qualification Test Report for Module Equipment Qualification for Common Q Applications, 2008677-IC-TR560-10 Revision 00, ADAMS Accession No. ML003733106.

13. Commercial Grade Dedication Report for QNX Operating System, 00000-ICE-37722 Revision 00, ADAMS Accession No. ML003733136. (Proprietary Information. Not Publically Available).

14. Environmental Test Report for Module Equipment Qualification for Common Q Applications (2008677-IC-TR560-11 Revision 00). ADAMS Accession No. ML003733079 (Proprietary Information. Not Publically Available).

15. Summary Qualification Report of Hardware Testing for Common Q Applications (000000-ICE-37764 Revision 3), ADAMS Accession Nos. ML11320A144 (Proprietary Information. Not Publically Available).

16. Response to NRC Request for Additional Information on the Common Qualified Platform TR (WCAP-16097-P, Rev. 1), ADAMS Accession Nos. ML12034A210/ML12034A211.

17. Transmittal Letter for WCAP-17266-P/NP, “Common Q Platform Generic Change Process”, Revision 0, ADAMS Accession No. ML102290175.

18. Common Q Platform Generic Change Process (WCAP-17266-P/NP, Revision 0), ADAMS Accession Nos. ML102290177/ML102290176.

19. Transmittal Letter for WCAP-16097-P/NP, “Common Qualified Platform Record of Changes,” Revision 1, ADAMS Accession No. ML2115A213.

20. Common Qualified Platform Record of Changes (WCAP-16097-P/NP, Appendix 5), Revision 1, ADAMS Accession Nos. ML2115A215/ML2115A214.

21. WNA-DS-01070-GEN-P/PNP, Revision 6, “Application Restrictions for Generic Common Q Qualification,” ADAMS Accession Nos. ML11364A030/ML11364A029.

22. WCAP-16166-P Supplement 1-E06, Revision 0, “Equipment Qualification Report for AC160 Platform – Common Qualified (Common Q) Power Supply,” ADAMS Accession No. ML12283A004

Attachments

Table 1 Common Q System Qualified Components:
List of Acronyms

Principal Contributor: R. Stattel

Date: February 7, 2013

9.0 LIST OF ACRONYMS

ABB	Asea Brown Boveri
AC160	Advant Controller 160
ACC	AMPL Control Configuration
AF100	Advant Fieldbus 100
AISC	Application Specific Integrated Circuit
ALWR	Advanced Light Water Reactor
AMPL	ABB Master Programming Language
API	Application Programming Interface
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transients Without Scram
BIOB	Backplane I/O Bus
BTP	Branch Technical Position
CE	Combustion Engineering
CENP	Combustion Engineering Nuclear Power
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
COTS	Commercial-Off-The-Shelf
CPC	Core Protection Calculator
CPCS	Core Protection Calculator System
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CS	Communication Section
CWP	CEA Withdrawal Prohibit
D3	Diversity and Defense-in-Depth
DB	Database
DBE	Design Basis Event

DESFAS	Digital ESFAS
DI	Digital Input
DLCE	Design Life Cycle Evaluation
DNBR	Departure from Nucleate Boiling Ratio
DPPS	Digital Plant Protection System
DPRAM	Dual Port Random Access Memory
DSP	Data Set Peripheral
EMC	Electromagnetic Compatibility
EPRI	Electric Power Research Institute
EPLD	Erasable Programmable Logic Device
ESF	Engineered Safety Features
ESFAS	Engineered Safeguards Features Actuation System
FAT	Factory Acceptance Test
FCB	Function Chart Builder
FE	Function Enable
FMEA	Failure Modes and Effect Analysis
FOM	Fiber Optic Modem
FPD	Flat Panel Display
FPDS	Flat-Panel Display System
FSAR	Final Safety Analysis Report
GDC	General Design Criteria
GUI	Graphical User Interface
HDD	Hard Disk Drive
HDLC	High Level Data Link Control
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
IPC	Interprocess Communication
ISR	Interrupt Service Routine
ITP	Interface and Test Processor
LC	Loop Controller

LCLP	Local Coincidence Logic Processor
LED	Light Emitting Diode
LPD	Local Power Density
MCR	Main Control Room
MTBF	Mean Time Between Failures
MTP	Maintenance and Test Panel
NEI	Nuclear Energy Institute
NSSS	Nuclear Steam Supply System
OM	Operator Module
OBE	Operational Basic Earthquake
PAMS	Post-accident Monitoring System
PAS	Plant Annunciator System
PC	Program Control or Personal Computer
PCB	Printed Circuit Board
PCE	Program Control Element
PDS	Previously Developed Software
PIT	Precision Interval Timer
PLC	Programmable Logic Controller
PM	Processor Module
PPS	Plant Protection System
PROM	Programmable Read-only Memory
PS	Processing Section
QA	Quality Assurance
QSPDS	Qualified Safety Parameter Display System
QSSL	QNX Software Systems Limited
RAM	Random Access Memory
RCM	Remote Control Module
RCP	Reactor Coolant Pump
RFI	Radio Frequency Interference
RG	Regulatory Guide
RPS	Reactor Protection System
RSP	Remote Shutdown Panel
RSPT	Reed Switch Position Transmitter
RTC	Real Time Clock
RTD	Resistance Temperature Detector

RTS	Reactor Trip System
RTCB	Reactor Trip Circuit Breaker
RVLMS	Reactor Vessel Level Monitoring System
SAR	Safety Analysis Report
SBC	Single Board Computer
SCADA	Supervisory Control and Data Acquisition
SCMP	Software Configuration Management Plan
SCR	Software Change Request
SDM	Service Data Manager
SDP	Service Data Protocol
SE	Safety Evaluation
SLE	Software Load Enable
SMM	Subcooled Margin Monitor
SPM	Software Program Manual
SQAP	Software Quality Assurance Plan
SRAM	Static RAM
SRP	Standard Review Plan
SSP	Software Safety Plan
STS	Standard Technical Specifications
SVVP	Software Verification and Validation Plan
SW	Software
SWC	Surge Withstand Capability
TCB	Task Control Block
TMI	Three Mile Island
TS	Technical Specification(s)
TSTF	Technical Specification Task Force
V&V	Verification and Validation
WDT	Watchdog Timer

Advant® is a registered trademark of ABB Process Automation Corporation.

QNX® and Photon® are registered trademarks of QNX Software Systems GmBH & Co. KG (“QSSKG”, formerly “QSSL”) and are used under license by QSS.

Unix® is a registered trademark of The Open Group in the US and other countries.

Windows® is a registered trademark of Microsoft group of companies.

Table 1 Common Q System Qualified Components

Item	*Component*	*Product Revision* *(Up to this revision reviewed for this SE)*	*Description*
AC160 Hardware Modules			
1	AI620	A	S600 Analog Input Module
2	AI685	G	S600 Analog Input Module
3	AI687	C	S600 Analog Input Module
4	AI688	A	S600 Analog Input Module
5	AO610	A	S600 Analog Output Module
6	AO650	A	S600 Analog Output Module
7	CI527W	C	Communications Interface Module
8	CI631	F	Communications Interface Module
9	DI620	A	S600 Digital Input Module
10	DO620	C	S600 Digital Output Module
11	DO625	A	S600 Digital Output Module
12	DO630	A	S600 Digital Output Module
13	DP620	A	S600 Pulse Counter Module
14	PM646A	T	Advant Controller 160 (AC160) Processor Module
15	TC514V2	B	AF100 Fiber-optic Modem
PC Node Box			
16	TL-WEST-002	A	PC Node Box
17	TL-WEST-003-001	C	PC Node Box
18	TL-WEST-003-003	C	PC Node Box
19	Kontron BIOS	3.1	BIOS
20	SUN-WSN-001	L	PC Node Box – 2 TCP/IP
21	SUN-WSN-003	F	PC Node Box – 2 UDP TX
22	SUN-WSN-004	F	PC Node Box – 2 UDP RX

Item	***Component***	***Product Revision*** ***(Up to this revision reviewed for this SE)***	***Description***
23	SUN-WSN-005	F	PC Node Box – 1 TCP/IP 1 UDP TX
24	SUN-WSN-006	F	PC Node Box – 1 TCP/IP 1 UDP RX
25	VERSALOGIC BIOS	VS-SUNCOR1, Rev. 1 Release 1.00	BIOS
Flat Panel Displays			
26	AVT-12 FPRM/TS-WES	1	12.1” Flat Panel Display
27	AVT-15 FPRM/TS-WES	1	15.0” Flat Panel Display
28	AVT-18 FPRM/TS-WES	1	18.0” Flat Panel Display
29	AVT-18FPRM-CAP-S-W	0	18.0” Flat Panel Display
30	TFS-18RM-CAP-WES	D	18.0” Flat Panel Display
31	SUN-WSD-006	K	6.5” Flat Panel Display
32	SUN-WSD-012	J	12.1” Flat Panel Display
33	SUN-WSD-015	M	15.0” Flat Panel Display
34	SUN-WSD-019	L	19.0” Flat Panel Display
Fiber Optic Modems			
35	OZDV Fiber Optic Modem A	0404	HSL Fiber Optic Modem
36	OZDV Fiber Optic Modem B	0000	HSL Fiber Optic Modem
Common Q Power Supply			
37	W12-FM	Rev. 5	AC Line Filter Module
38	W1-FEM	Rev. 7	Front-End Module
39	W1-24	Rev. 7	MAXI Module (24Vdc)
40	W1-0524	Rev. 5	Dual MINI Module (5/24Vdc)
41	W1-1500	Rev. 5	Dual MINI Module (15Vdc)
42	W1-282824	Rev. 8	Triple MICRO Module
43	W1-363624	Rev. 1	Triple MICRO Module
QUINT Power Supply			
44	QUINT-PS/1AC/24DC/20/WH	0	24 VDC, 20 Amp
45	QUINT-PS/1AC/24DC/10/WH	0	24 VDC, 10 Amp

Item	***Component***	***Product Revision*** ***(Up to this revision reviewed for this SE)***	***Description***
46	QUINT-PS/1AC/48DC/5/WH	0	48 VDC, 5 Amp
47	QUINT-PS/1AC/12DC/15/WH	0	12 VDC, 15 Amp
Software Modules			
48	AC160 Base Software	1.3/9	Base Software
49	ACC Tool	1.7/1	Tool
50	QNX 4.25G OperatingSystem	Rev. 4	Operating System

Note: *The Common Qualified Platform Record of Changes (Reference 20) defines the revision level and the basis for modules that have changed since the last Safety Evaluation Report.*

Response to NRC Request for Additional Information on the Common Qualified Platform Topical Report (WCAP-16097-P, Rev. 1)

January 2012

Westinghouse Electric Company LLC
1000 Westinghouse Drive
Cranberry Township, PA 16066

©2012 Westinghouse Electric Company LLC
All Rights Reserved

1. The AC160 S600 I/O modules listed below are described in Section 5.2.1.1.3 of the topical report (TR) but are not listed as AC160 Hardware Modules in Table 11-1 of the TR. Since Table 11-1 shows components to the common Q platform that are qualified for use per document 2C48361, it is unclear why these non-approved modules are being described.

S600 Input / Output Modules		
4	AI630	RTD / Resistance Input
5	AI635	Thermocouple Input
6	DI621	Digital Input
7	DO610	Digital Output

Please provide an explanation for why these modules are being described in the Common Q TR or why they are not listed as approved common Q platform components. The U.S. Nuclear Regulatory Commission (NRC) staff would like to know if it is Westinghouse Electric Company's (Westinghouse) intent to have these modules included as approved common Q platform components.

Westinghouse Response:
The modules listed in the table above have been superseded by other modules, or they are no longer being used. Therefore, Revision 2 of the Topical Report will remove those modules from subsection 5.2.1.1.3.

2. Use of the terms "Channel" and "Division" throughout the TR is not consistent with industry accepted terminology. For example, throughout the TR, the term channel is used to denote redundant implementations of safety applications; however, Section 5.6 of the TR contains a discussion of AF100 configurations that cross division boundaries. This section also discusses the use of High Speed Link (HSL) links to cross divisional boundaries. It appears that the terms are being used in a synonymous manner. These terms are not defined in the Glossary of the TR. The following definitions are provided in IEEE Std 7-4.3.2 2010.

> ***channel***: *An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined. (IEEE Std 603-2009)*
>
> ***division***: *The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.*

It is important for the purposes of this safety evaluation for the NRC staff to understand the intended context for these terms as they are applied in the TR. Please provide definitions for these terms relative to how they are used in the TR.

Westinghouse Response:
Revision 1 of the Topical Report was reviewed, and the use of "channel" and "division" are now used consistent with IEEE Std. 603 for Revision 2.

3. I/O Modules

   In Section 5.2.1.1.3 of the TR, the following statement is made in regard to the replacement capabilities of I/O modules:

   > *"All I/O modules may be replaced electrically, not necessarily system wise, while the system is powered (and typically in test mode)."*

   The NRC staff requires clarification of what is meant by the terminology "system wise." Please explain this terminology and provide information regarding any limitations that would need to be imposed on system operability when I/O modules are to be replaced.

   Westinghouse Response:
   The term "system wise" refers to the ability to replace an I/O module in a particular system without having to bypass a channel/division. This restriction has been defined in WNA-DS-01070-GEN, "Application Restrictions for Generic Common Q Qualification". Restriction H48 states:

a,c

   Westinghouse submitted documents, WNA-DS-01070-GEN-P and NP on the docket under transmittal letter, LTR-NRC-11-67.

4. Please provide additional information regarding the various watchdog timer (WDT) functions that are described in Sections 4.1, 5.2.4, 5.2.1.2.1 and 5.4.4. Specifically, the staff requests clarification in regard to the following WDT functions of the common Q platform.

   a. Since there does not seem to be a separate WDT module included in the common Q platform any longer, it is not clear why a separate module is being described. Please provide a description of the WDT module if it is to be included as a common Q platform component or clarify what is being referred to in Section 5.2.

      Westinghouse Response:
      The description of the watchdog timer was supplemented with additional information and moved to subsection 5.2.1.3. A figure will be added that provides a configuration of the

watchdog timer. Table 5-1 will be added to provide a summary of the watchdog timer arrangement. This information has been provided in Appendix A.

Accordingly, WDT will be removed from Section 5.2, since it is not considered a separate building block of the Common Q Platform.

b. Since the WDT is built into the processor module it is unclear to the staff how it would be connected to external systems as described in Section 4.1. Please provide an explanation and/or specific example of how a system would be configured to utilize this function. This explanation should include a description of how signal isolation between systems is achieved.

Westinghouse Response:
The figure that will be added in 5.2.1.3 (provided in Appendix A) depicts a normally closed relay. This relay can be used to initiate a fail-safe state (e.g., Reactor Trip).

c. Section 5.2.1.2.1 on page 5-13 implies that there are two different watchdog functions being performed by the system; however, only one watchdog function (other than the application watchdog function) is described within the TR in Section 5.2.4, "Watchdog Timer".

Westinghouse Response:
The two watchdog functions described in subsection 5.2.1.2.1 refer to the [ ][a,c] Subsection 5.2.1.3 will provide a further description of the watchdogs in the PM646A. See Appendix A.

d. Please provide a description of the functions performed by the "WD-Timer of the uP58360" which is also referred to as the "processor watchdog" within the TR.

Westinghouse Response:
Subsection 5.2.1.3 will provide a description of the functions performed by Watchdog timer of the uP68360. See Appendix A.

e. Does the updated common Q system retain the capability for an Application Watchdog Timer to be implemented? Section 5.4.4 of the TR was revised to eliminate previous requirements for application WDTs and explanations were added to justify this change. It is not clear to the staff whether these application WDTs will be retained as a feature of the common Q system or if this feature is being eliminated from the common Q system altogether. As revised, Section 5.4.4 no longer provides any description of the application WDT function or provisions for when it is to be implemented. Please provide an explanation of this feature including a discussion of when it would be implemented, or state that application WDTs are no longer required for common Q systems if this is the case.

Westinghouse Response:
The application watchdog function was never a platform function. It was a requirement on the project-specific application software to implement logic heartbeats. This requirement is not required as justified in Section 5.4.4.

To eliminate confusion, "hardware watchdog" was changed to "hardware watchdog function" in subsection 5.4.4.

5. The staff's approach to this safety evaluation update is to determine if the previously established safety conclusions are impacted by revisions made to the TR and changes made to the common Q platform components. As such, any restrictions imposed by previous SE's are not being revised or evaluated. Please identify if there are any restrictions or previous SE conclusions that Westinghouse intends for the staff to re-evaluate as a part of this SE effort.

   Westinghouse Response:
   There are no restrictions or conclusions in the previous SER that Westinghouse would like the staff to re-evaluate.

Appendix A –Watchdog Timer

[

]a,c

The watchdog timer relay is a form C relay, whose contacts are accessible from the processor front panel. Depending on the specific system application, the watchdog timer can be used to annunciate a failure, actuate a divisional trip, or set output states to predefined conditions. For example, the watchdog timer relay may be used to control the power to the relays for the digital output module. Isolation is provided for those applications where the watchdog timer is connected to external systems.

a,c

Table 1	**Processor Module WDT Arrangement Watchdog Timer Summary**		

a,c

Figure 1 Watchdog Timer Configuration

REVISION HISTORY

RECORD OF CHANGES

Revision	Revision Made By	Description	Date
00	D.N. Menard	This is the original issue of this document. This document was previously released as CENPD-396-P. It is being prepared to create the accepted version in accordance with the USNRC Safety Evaluation dated February 24, 2003. The previously released document CENPD-396-P, Revision 1 has been modified as follows: • A document titled, "Changes to the Westinghouse Common Qualified Platform Topical Report, CENPD-396-P, Rev. 01" was provided to the NRC via LTR-NRC-02-41, dated August 14, 2002. The changes identified in that document have been incorporated into this revision. • The Reference to the Software Program Manual has been updated. • Minor changes were made to clarify some of the technical descriptions. • Correction of typographical errors. • Minor document format changes were made. • In accordance with established NRC procedures, this accepted version of the Common Q Topical Report includes the original Safety Evaluation, two supplemental Safety Evaluations and associated cover letters that were issued by the NRC. • References to the ABB Quality Assurance Manual and procedures were replaced with the Westinghouse Quality Management System and its implementing procedures.	5/2003
01	Matthew A. Shakun	• Added "or an equivalent mechanism" to conformance clause for RG 1.47 in Section 3, "Codes And Standards." • Changed 'automatic' tests to 'surveillance' tests. • Added updated standards and indicated which applied to baseline Common Q equipment or new/enhanced modules.	8/2010

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Revision Made By	Description	Date
01 (cont.)	Matthew A. Shakun	• Changed pointer from "IEEE 7-4.3.2 Annex G" to "IEEE 7-4.3.2 Annex E" in subsection 5.2.5.3, "External Communications" and subsection 5.3.2, "Flat Panel Display System" for communication independence. • Added subsection 4.3.3.1, "Manual Component-Level Control." This information was derived from WCAP-16674-P. • Changed TCP/IP to UDP/IP in subsection 5.3.2.1, "Datalink To External Systems." Also, deleted paragraph that said it was alright to lose the FPDS. • Added description of new Analog Input cards, AI687 and AI688, to subsection 5.2.1.1.3, "Input/Output Subsystem." • Changed HSL delay time in subsection 5.3.1.3, "High Speed Link Communications" from 4 ms to 20 ms. • Changed reference from ANSI C to Standard C. • Reworded some requirements that contained errors to be more consistent with Westinghouse's internal policy and procedures. • Updated Section 6, "Software Quality," to include new sections (Software Test Plan, Secure Development and Operational Environment Plan) that were added to the updated revision of the SPM. • Added description of Flash capabilities for PM646A in Processor Section Software Description, in subsection 5.2.1.2.1. • Added Section 5.6, "Compliance to Interim Staff Guidance Highly Integrated Control Room – Communications (ISG #4-HICRc)." • Deleted "One solution also allows obsolescence management for the next 20 years" from Section 1, "Purpose." • Deleted second paragraph from Section 2, "Scope," which talked about CE Nuclear's experience. • Deleted ITP (Interface Test Processor) from Section 4.4, "AF100 Communication."	8/2010

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Revision Made By	Description	Date
01 (cont.)	Matthew A. Shakun	• Deleted Note from subsection 5.2.1.1.1, "PM646A Processor Module." • Deleted "Bus Extender CI615" from subsection 5.2.1.1.3, "Input/Output Subsystem." • Deleted "Common Q applications are not expected to require any options to the base software" from subsection 5.2.1.2.1, "Base Software." • Changed "has a 16 year" to "has more than 16 years" in subsection 5.2.2.2.1, "Operating System." • Reworded Manually Initiated Tests in subsection 5.2.2.3.2 to change functionality of the ITP. • Added requirement to Loading/Changing Setpoints in subsection 5.2.2.3.2. • Deleted "on-demand data that is initiated from the Flat Panel Display Systems" from subsection 5.3.1.4, "AF100 Communications." • Reworded examples of Message Transfer in subsection 5.3.1.4.2, "Message Transfer." • Added operation nodes "configured to be bus master that are" attached to subsection 5.3.1.4.3, "Bus Master." • Changed "ITP" to "MTP" in subsection 5.4.3.2, " [ ]a,c." • Deleted "also reviewing the actual" from subsection 6.3.2, "Verification." • Deleted clause that says the design team can develop test procedures from subsection 6.3.3, "Validation." • Updated Section 10, "Commercial Grade Dedication Program," to be consistent with Westinghouse Policies and Procedures. • Changed Section 11 from "Future Documentation" to "Common Q Platform Components". • Added Section 12 "Future Platform Changes." This section references WCAP-17266-P, which discusses modifications to the Common Q Platform.	8/2010

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Revision Made By	Description	Date
01 (cont.)	Matthew A. Shakun	• Added clause to Section 4.1, "Advant Controller 160 (AC160)" that there is an application requirement that only allows an upper limit of four PM646As. • Updated Section 4.2, "Power Supply" and subsection 5.2.3, "Power Supply," to include a 24" panel assembly and to add quick disconnect modules. • Updated subsection 5.2.1.1, "AC160 Hardware Description," to say that subracks are designed for "front or" rear mounting. Also changed the number of allowed communication modules from 18 to 19. • Changed "can" to "could" in the subrack portion of subsection 5.2.1.1.1, "PM646A Processor Module." • Removed first paragraph of subsection 5.2.1.1.3, "Input/Output Subsystem," because that information was identical to Section 4.2, "Power Supply." • Added "electrically not necessarily system wise" to subsection 5.2.1.1.3, "Input/Output Subsystem." • Added "approximately" to Calibration of Analog Input and Outputs of subsection 5.2.1.1.3, "Input/Output Subsystem." • Changed title of subsection 5.2.2.1 to "Flat Panel Display System Hardware Description." • Updated subsection 5.2.3, "Power Supply," by removing "the modules will be similar in design to and based on prior power supply components and design." Changed "bumpless" to "load," "overtemperature" to "under-voltage," "hold up" to "ride through," and "10 ms" to "40 ms." Also, changed to "adversely" affect. • Changed "for a minimum of 3000 cycles, simulating" to "depending on its planned application to simulate" in Section 7.1, "Component Cycling and Burn-in." • Deleted "The EMI and environmental test shall be performed prior to the seismic test" from subsection 7.3.1, "Seismic Qualification Requirements."	8/2010

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Revision Made By	Description	Date
01 (cont.)	Matthew A. Shakun	• Updated Section 7.4, "Electromagnetic Interference (EMI) Testing," to differentiate the testing between baseline equipment and new equipment. New equipment now conforms to the requirements of RG 1.180 Rev. 01. • Added "through October of 1998" to the AC160 operating history portion of subsection 8.3.1, "AC160 Design Evolution." • Specified the HSL Fiber Optic Modems as OZDV 114A/OZDV 114B in subsection 5.2.1.1.2 PM646A High Speed Link Communication Interface • Added "through the CI527W" and "through the TC514" in Section 5.3.2 Flat Panel Display System. • Added description of the AO610 to subsection 5.2.1.1.3 Input/Output Subsystem • Added that "the displays are available in multiple sizes" to subsection 5.2.2.1.2 Flat Panel Display • Changed "AC160 tool AC160ILO" to "same tool for installing the base software" in subsection 5.2.1.2.3 Software Tools. • Deleted DI622, DI635, and DI636 from 5.2.1.1.3 Input/Output Subsystem. • First time used acronyms were defined in the body of the text. • Added Appendix 5, Record of Changes to the Common Q Platform. • Minor document editorial and format changes were made.	8/2010
02	Matthew A. Shakun	Revision 1 was modified to incorporate the following changes, which were necessary to respond to the NRC's Request for Additional Information: • RAI #1: AI630, AI635, and DO610 have been superseded by other modules, or are no longer being used. Therefore, these modules have been removed from subsection 5.2.1.1.3. DI621 was added to table 11-1. • RAI #2: "Channel" was replaced with "division" where applicable.	3/2012

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Revision Made By	Description	Date
02 (cont.)	Matthew A. Shakun	• RAI #4: a. The description of the watchdog timer was supplemented with additional information and moved to subsection 5.2.1.3. Figure 5-13 was added to provide a configuration of the watchdog timer. Table 5-1 was added to provide a summary of the watchdog timer arrangement. Accordingly, the watchdog timer module was removed from Section 5.2, since it is not considered a separate building block of the Common Q Platform. b. Figure 5-13 was added to subsection 5.2.1.3. This figure depicts a normally closed relay. This relay can be used to initiate a fail-safe state (e.g., Reactor Trip). c. Subsection 5.2.1.3 provides a description of the functions performed by the Watchdog timer. d. Subsection 5.2.1.3 provides a description of the functions performed by the Watchdog timer. e. "Hardware watchdog" was changed to "hardware watchdog function" in subsection 5.4.4. Revision 1 was modified to implement the following changes that were documented in Westinghouse's Corrective Action Process: • CAPs IR 10-313-M034: The "serial RS 422 link" was changed to a "serial RS 485 link" in Section 4.5, subsection 5.2.1.1.1, and subsection 5.2.1.1.2. This description is consistent with the AC160 for Westinghouse User's Guide (3BDS 005 663R501) • CAPs IR 11-024-M013: The cited Regulatory Guides and IEEE Standards were evaluated against the current regulatory requirements. This evaluation determined that the wrong year of some RG and IEEE standards were being referenced. The following corrections were made: RG 1.62, Rev. 1 (2010) was added. RG 1.75, Rev. 2 (1978) was removed. RG 1.100, Rev. 2 (1998) was changed to RG 1.100, Rev. 2 (1988). RG 1.152, Rev. 1 (1996) and Rev. 2 (2006) were	

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Revision Made By	Description	Date
		changed to RG 1.152, Rev. 3 (2011). RG 1.153, Rev. 0 (1985) was removed. RG 1.168, Rev. 0 (1997) was removed. IEEE Std. 730.1-1989 was changed to 1998. IEEE Std. 828-1990 was changed to 2005. IEEE Std. 830-1993 was changed to 1998. IEEE Std. 1012-1986 was removed. IEEE Std. 1016-1987 was changed to 1998. IEEE Std. 1028-1988 was removed. IEEE Std. 1074-1994 was changed to 1997. In some instances, this Topical Report references later versions of IEEE standards than endorsed by Regulatory Guides. IEEE Std. 323-1983 is being referenced since it was in the NRC-approved Topical Report. IEEE Std. 830-1998 and IEEE Std. 1074-1997 are being referenced since they were in the NRC-approved SPM (WCAP-16096-NP-A, Rev. 1A). IEEE Std. 828-2005 is being referenced after an evaluation between 2005 and 1998 (version referenced in NRC-approved SPM) determined that no requirements were omitted in the later version. • CAPs IR 11-091-M026: Section 10.1 was modified to include firmware to the scope of the Software Commercial Grade Dedication Process. The following was added: "Firmware for new AC160 S600 modules." Revision 1 was modified to incorporate the following additional changes: • "Software Installation Plan" was added to Section 6. • The following sentence was deleted from Section 10.1 because it confused readers to believe that Commercially dedicated equipment do not get IV&V: "Since the hardware and software is already developed, the formal Verification and Validation (V&V) activities cannot be performed on existing vendor equipment." • Table 7-2 was updated to be consistent with the environmental profile depicted in Figure 7-4. • Table 11-1 was updated to remove [ ]a,c since it not a component of the Common Q Platform. It was also updated to fix a typo	

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Revision Made By	Description	Date
		with [ ]a,c. • Since WCAP-17266-P was already submitted to the NRC, Section 12 was updated to remove the following sentence: "This document will be submitted to the NRC for review." • References that were only used for background information to prepare the topical report and are not explicitly cited were moved to the bibliography. • Minor editing and formatting changes were also made.	
03	Matthew A. Shakun	Revision 2 was modified to incorporate the following changes: Subsection 5.3.1.4.3, Bus Master, was updated to describe how the bus master is configured: [ ]a,c • The following text, which was in the NRC-approved version was added back to subsection 5.3.2.1, Datalink To External Systems: "There are two communication interfaces in the Flat Panel Display System which are isolated from each other (i.e., two separate interface cards). Should a failure in communications to a non-safety system occur causing the Flat Panel Display System to halt, the safety-critical applications in the AC160 controllers can continue to operate unimpeded. It is possible that the Flat Panel Display System has control of the AF100 bus master at the time it ceases to operate. As discussed in previous sections, the bus master can be assumed by another node if it fails, so the AF100 network can continue to operate without the Flat Panel Display in operation." • Updated References and Bibliography	7/2012

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Revision Made By	Description	Date
03 Approved	Matthew A. Shakun	Revised to issue the NRC accepted version. Reference 5 was changed to the NRC-approved SPM, WCAP-16096-P-A, Revision 4. IEEE Std. 1074-1997 was changed to IEEE Std. 1074-1995 to be consistent with the SPM. The description of the HSL serial link was clarified to "RS-422 at the physical layer" in Section 4.5. Subsections 5.2.1.1.1 and 5.2.1.1.2 were updated to remove the call out of a specific RS standard. RG 1.152, Revision 2 was changed to RG 1.152, Revision 3 in Section 10.1 Power Supply Module, [ ]^{a,c}, was removed from Table 11-1 since it is not considered a component of the Common Q Platform. Digital Input Module, [ ]^{a,c}, was removed from Table 11-1 and subsection 5.2.1.1.3 since it is still pending equipment qualification. "Common Q" was changed to "Common Q™" throughout the document. Note: This change has not been marked by a change bar.	See EDMS

TABLE OF CONTENTS

REVISION HISTORY ii
LIST OF TABLES xiv
LIST OF FIGURES xv
LIST OF ACRONYMS AND TRADEMARKS xvii
GLOSSARY OF TERMS xx
REFERENCES xxi
BIBLIOGRAPHY xxiii
1 PURPOSE 1-1
2 SCOPE 2-1
3 CODES AND STANDARDS 3-1
4 COMMON Q™ OVERVIEW 4-1
4.1 ADVANT CONTROLLER 160 (AC160) 4-3
4.1.1 AC160 Software 4-3
4.1.2 Input and Output Cards 4-4
4.1.3 Interface and Test Processor (ITP) 4-5
4.2 POWER SUPPLY 4-5
4.3 FLAT PANEL DISPLAY SYSTEM (FPDS) 4-5
4.3.1 Flat Panel Display System Software 4-6
4.3.2 Maintenance and Test Panel (MTP) 4-6
4.3.3 Operator's Module 4-6
4.4 AF100 COMMUNICATION 4-7
4.5 HIGH SPEED LINK (HSL) COMMUNICATION 4-7
5 COMMON Q™ PLATFORM 5-1
5.1 FUNCTIONAL REQUIREMENTS 5-1
5.2 SYSTEM DESCRIPTION (BUILDING BLOCKS) 5-1
5.2.1 Advant Controller 5-1
5.2.2 Flat Panel Display System 5-27
5.2.3 Power Supply 5-33
5.2.4 Communication Subsystems 5-34
5.3 DETERMINISTIC PERFORMANCE 5-35
5.3.1 AC160 Deterministic Performance 5-35
5.3.2 Flat Panel Display System 5-42
5.4 SYSTEM DIAGNOSTICS 5-42
5.4.1 AC160 Diagnostics 5-42
5.4.2 Flat Panel Display Diagnostics 5-44
5.4.3 Surveillance Testing 5-44
5.4.4 Application Watchdog 5-45
5.5 SYSTEM INTERFACES 5-45

TABLE OF CONTENTS (cont.)

5.6 COMPLIANCE TO INTERIM STAFF GUIDANCE HIGHLY INTEGRATED CONTROL ROOM – COMMUNICATIONS (ISG #4-HICRC) 5-49
5.6.1 ISG-4 Position 1 5-49
5.6.2 ISG-4 Position 2 5-50
5.6.3 ISG-4 Position 3 5-51
5.6.4 ISG-4 Position 4 5-52
5.6.5 ISG-4 Position 5 5-54
5.6.6 ISG-4 Position 6 5-54
5.6.7 ISG-4 Position 7 5-54
5.6.8 ISG-4 Position 8 5-55
5.6.9 ISG-4 Position 9 5-55
5.6.10 ISG-4 Position 10 5-56
5.6.11 ISG-4 Position 11 5-57
5.6.12 ISG-4 Position 12 5-57
5.6.13 ISG-4 Position 13 5-59
5.6.14 ISG-4 Position 14 5-60
5.6.15 ISG-4 Position 15 5-60
5.6.16 ISG-4 Position 16 5-61
5.6.17 ISG-4 Position 17 5-61
5.6.18 ISG-4 Position 18 5-61
5.6.19 ISG-4 Position 19 5-62
5.6.20 ISG-4 Position 20 5-62
6 SOFTWARE QUALITY 6-1
6.1 SOFTWARE QUALITY ASSURANCE 6-2
6.2 SOFTWARE CONFIGURATION MANAGEMENT 6-3
6.2.1 [ ]a,c 6-3
6.2.2 Previously Developed Software 6-5
6.3 SOFTWARE VERIFICATION AND VALIDATION 6-6
6.3.1 [ ]a,c 6-6
6.3.2 [ ]a,c 6-7
6.3.3 [ ]a,c 6-8
6.4 OPERATION AND MAINTENANCE 6-9
7 EQUIPMENT QUALIFICATION 7-1
7.1 COMPONENT CYCLING AND BURN-IN 7-3
7.2 ENVIRONMENTAL TESTING 7-3
7.3 SEISMIC TESTING 7-8
7.3.1 [ ]a,c 7-8
7.4 ELECTROMAGNETIC INTERFERENCE (EMI) TESTING 7-8
8 EQUIPMENT RELIABILITY 8-1
8.1 FAILURE MODE AND EFFECTS ANALYSIS (FMEA) 8-1
8.2 MEAN TIME BETWEEN FAILURES (MTBF) ANALYSIS 8-4
8.3 OPERATING HISTORY 8-4

TABLE OF CONTENTS (cont.)

8.3.1 [ ][a,c] 8-4
9 DEFENSE-IN-DEPTH AND DIVERSITY 9-1
10 COMMERCIAL GRADE DEDICATION PROGRAM 10-1
10.1 SCOPE 10-1
10.2 SOFTWARE ASSESSMENT PROCESS FOR SOFTWARE COMMERCIAL GRADE DEDICATION 10-2
10.2.1 [ ][a,c] 10-2
10.2.2 [ ][a,c] 10-6
10.2.3 [ ][a,c] 10-6
10.2.4 [ ][a,c] 10-6
10.3 SOFTWARE COMMERCIAL DEDICATION 10-6
10.4 HARDWARE COMMERCIAL DEDICATION 10-7
10.5 CONFIGURATION MANAGEMENT 10-8
11 COMMON Q™ PLATFORM COMPONENTS 11-1
12 FUTURE PLATFORM CHANGES 12-1
13 CONCLUSIONS 13-1
APPENDIX A LIST OF APPENDICES A-1

LIST OF TABLES

Table 5-1 Processor Module WDT Arrangement Watchdog Timer Summary 5-27

Table 7-1 Cabinet Environmental Design Requirements 7-4

Table 7-2 Common Q™ Equipment Environmental Design Requirements 7-4

Table 8-1 [ ][a,c] 8-4

Table 8-2 [ ][a,c] 8-7

Table 11-1 [ ][a,c] 11-1

LIST OF FIGURES

Figure 4-1 Simplified Block Diagram 4-2
Figure 5-1 AC160 Hardware 5-3
Figure 5-2 PM646A Processor Module 5-6
Figure 5-3 Base Software Identification 5-10
Figure 5-4 Basic Functional Architecture PM646 5-11
Figure 5-5 [ ]a,c 5-12
Figure 5-6 [ ]a,c 5-13
Figure 5-7 [ ]a,c 5-17
Figure 5-8 [ ]a,c 5-18
Figure 5-9 [ ]a,c 5-19
Figure 5-10 [ ]a,c 5-20
Figure 5-11 [ ]a,c 5-21
Figure 5-12 [ ]a,c 5-23
Figure 5-13 Watchdog Timer Configuration 5-26
Figure 5-14 Operating System 5-29
Figure 5-15 OS Graphical User Interface 5-30
Figure 5-16 [ ]a,c 5-31
Figure 5-17 AC160 Application Program Execution Period 5-36
Figure 5-18 AC160 Hardware 5-38
Figure 5-19 [ ]a,c 5-40
Figure 5-20 [ ]a,c 5-48
Figure 5-21 PM646A Architecture 5-50
Figure 5-22 HSL Communication 5-51
Figure 5-23 [ ]a,c 5-53
Figure 6-1 [ ]a,c 6-5
Figure 7-1 [ ]a,c 7-1
Figure 7–2 [ ]a,c 7-2
Figure 7-3 Original Environmental Test Profile 7-6
Figure 7-4 Modified Environmental Test Profile 7-7

LIST OF FIGURES (cont.)

Figure 8-1 ABB Product Migration 8-5

LIST OF ACRONYMS AND TRADEMARKS

Acronyms used in the document are defined in WNA-PS-00016-GEN, "Standard Acronyms and Definitions" (Reference 28), or included below to ensure unambiguous understanding of their use within this document.

AC	Alternating Current
AC160	Advant® Controller 160
ACC	AMPL Control Configuration
AISC	Application Specific Integrated Circuit
AMPL	ABB Master Programming Language
API	Application Programming Interface
BIOB	Backplane I/O Bus
CDI	Commercial Dedication Instruction
CDP	Cyclic Data Packets
CEA	Control Element Assembly
CEO	Cognizant Engineering Organization
COTS	Commercial-Off-The-Shelf
CPC	Core Protection Calculator
CPCS	Core Protection Calculator System
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CS	Communication Section
DB	Database
DBE	Design Basis Event
DC	Direct Current
DI	Digital Input
DNBR	Departure from Nucleate Boiling Ratio
DPM	Dual Ported Memory
DSP	Data Set Peripheral
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPLD	Erasable Programmable Logic Device
EPRI	Electric Power Research Institute
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FAT	Factory Acceptance Test
FCB	Function Chart Builder
FE	Function Enable
FMEA	Failure Modes and Effects Analysis
FOM	Fiber Optic Modem
FPD	Flat Panel Display
FPDS	Flat Panel Display System
FSAR	Final Safety Analysis Report
GUI	Graphical User Interface
HDD	Hard Disk Drive

LIST OF ACRONYMS AND TRADEMARKS (cont.)

HDLC	High Level Data Link Control
HMI	Human-Machine Interface
HSL	High Speed Link
I&C	Instrumentation and Control
I/O	Input/Output
IEC	International Electrotechnical Commission
IPC	Interprocess Communication
ISR	Interrupt Service Routine
ITP	Interface and Test Processor
LED	Light Emitting Diode
LPD	Local Power Density
MTBF	Mean Time Between Failures
MTP	Maintenance and Test Panel
NRC	Nuclear Regulatory Commission
OM	Operator's Module
OBE	Operational Basic Earthquake
PAMS	Post Accident Monitoring System
PC	Process Control
PIT	Precision Interval Timer
PLC	Programmable Logic Controller
PM	Processor Module
PPS	Plant Protection System
PROM	Programmable Read Only Memory
PS	Processing Section
PVC	Polyvinyl Chloride
QSPDS	Qualified Safety Parameter Display System (predecessor to Common Q™ PAMS)
RAM	Random Access Memory
RFI	Radio Frequency Interference
RPS	Reactor Protection System
RSPT	Reed Switch Position Transmitters
RTC	Real Time Clock
RTD	Resistance Temperature Detector
SBC	Single Board Computer
SCADA	Supervisory Control and Data Acquisition
SCM	Software Configuration Management
SCR	Software Change Request
SDM	Service Data Manager
SDP	Service Data Protocol
SLE	Software Load Enable
SPM	Software Program Manual
SQAP	Software Quality Assurance Plan
SRAM	Static RAM
SVVP	Software Verification and Validation Plan

LIST OF ACRONYMS AND TRADEMARKS (cont.)

SW	Software
SWC	Surge Withstand Capability
TCB	Task Control Block
TMI	Three Mile Island
V&V	Validation and Verification
WDT	Watchdog Timer
WWDT	Window Watchdog Timer

Advant® is a registered trademark of ABB Process Automation Corporation.

QNX® and Photon® are registered trademarks of QNX Software Systems GmBH & Co. KG ("QSSKG", formerly "QSSL") and are used under license by QSS.

Unix® is a registered trademark of The Open Group in the US and other countries.

Windows® is a registered trademark of Microsoft group of companies.

GLOSSARY OF TERMS

Standard terms used in the document are defined in WNA-PS-00016-GEN, "Standard Acronyms and Definitions" (Reference 28), or included below to ensure unambiguous understanding of their use within this document.

Term	Definition
Advant	Advant is a registered trademark of ABB Process Automation Corp. The Common Q™ platform includes the Advant Controller 160 (AC160). The AC160 is part of the ABB Advant Power system. It is used in applications that require high availability and redundancy.
Baseline Common Q™ Equipment	Baseline Common Q™ Equipment is the Common Q™ Equipment that was referenced in the NRC Safety Evaluation, dated February 24th, 2003.

REFERENCES

1. GKW F 310 708, "Advant Power Reliability and Availability, Reliability Data Sheet, Advant Controller 160 Including S600 I/O," ABB PPC.

2. "Quality Management System," Westinghouse Electric Company LLC.

3. "Nuclear Automation Level 3 Policies & Procedures," Westinghouse Electric Company LLC.

4. "Westinghouse Level II Policies & Procedures," Westinghouse Electric Company LLC.

5. WCAP-16096-P-A, Rev. 4, "Software Program Manual for Common Q™ Systems," Westinghouse Electric Company LLC.

6. CENPD-255-A, Rev. 3, "Class 1E Qualification – Qualification of Class 1E Electrical Equipment," Nuclear Power Systems Combustion Engineering, Inc.

7. CEN-356(V)-P, Rev. 01-P, "Modified Statistical Combination of Uncertainties," Nuclear Power Systems Combustion Engineering, Inc.

8. 3BDS 003 340R701, "AC110 System Software Extension," ABB Process Automation Corporation.

9. 3BDS 005 665R501, Rev. B, "Data Base Elements Advant Controller 160 Reference Manual," ABB Process Automation Corporation.

10. 3BDS 005 666R101, Rev. C, "PC Elements Advant® Controller 160 Version 1.3 Reference Manual," ABB Process Automation Corporation.

11. (Reference Deleted)

12. 3BDS 005 663R501, Rev. A, "Advant Controller 160 for Westinghouse Version 1.3 User's Guide," ABB Process Automation Corporation.

13. (Reference moved to Bibliography)

14. (Reference moved to Bibliography)

15. (Reference moved to Bibliography)

REFERENCES (cont.)

16. (Reference moved to Bibliography)

17. (Reference moved to Bibliography)

18. (Reference moved to Bibliography)

19. 3BDS 005 740R401, "S600 I/O Hardware, Advant Controller 160 Reference Manual," ABB Process Automation Corporation.

20. (Reference moved to Bibliography)

21. (Reference moved to Bibliography)

22. MOD 97 – 1250, "Oskarshamn 1 – Project Mod Evaluation of Collected Operating Experience for Advant Controller 110," ABB Atom.

23. GKW F 310 291, Rev. 0, "Survey of Operational Experience with Software Advant Controller AC160," ABB Power Plant Controls.

24. "TÜV Product Service GmbH, Automation, Software and Electronics – IQSE Technical Report Of Software Approval (Proven In Use Demonstration) No. 960113399b/e March 4, 1998," Revision 1.0.

25. NUREG-1462, "Final Safety Evaluation Report Related to the Certification of the System 80+ Design," Volume 1.

26. WCAP-8587-(NP), Rev. 6-A, "Methodology for Qualifying Westinghouse WRD Supplied NSSS Safety Related Electrical Equipment," Westinghouse Electric Company LLC.

27. WCAP-17266-P, Rev. 0, "Common Q Platform Generic Change Process," Westinghouse Electric Company LLC.

28. WNA-PS-00016-GEN, "Standard Acronyms and Definitions," Westinghouse Electric Company LLC.

BIBLIOGRAPHY

1. 3BSE 000 506R801, "Advant Fieldbus 100 User's Guide," ABB Process Automation Corporation.

2. 3BSE 009 626R501, "AMPL Configuration, Advant Controller 100 Series Reference Manual," ABB Process Automation Corporation.

3. DPPS-97-011, "Minutes of Meeting in Mannheim with ABB Industrietechnik AG, February 17-28, 1997," ABB Process Automation Corporation, April 17, 1997.

4. "QNX Operating System – System Architecture for QNX 4.24," 2nd Edition, October 1997.

5. "QNX Photon microGUI™ Programmers Guide," 2nd Edition, December 1996.

6. "QNX Watcom Compiler & Tools User's Guide," First Edition, July 1996.

7. GKWF 700 894, Rev. 2, "Requirements Specification for ACC Tool for use in RPS Applications of BU Nuclear," ABB Process Automation Corporation.

8. GKWF 700 891, Rev. 2, "Requirements Specification for Advant Controller 160 AC160 SW-Version 1.3 and Controller HW PM646A for use in RPS applications for BU Nuclear," ABB Process Automation Corporation.

1 PURPOSE

The purpose of this report is to describe a nuclear safety related I&C platform designed by Westinghouse Electric Company. One common platform is being designed with a modular structure where various components can be applied to solve most utility needs for nuclear safety related applications, including component replacements and complete system upgrades. The platform is referred to as Common Qualified Platform; or, simply as "Common Q™."

The Common Q™ platform is applicable to Post Accident Monitoring Systems (PAMS), Core Protection Calculator Systems (CPCS), Reactor Protection Systems (RPS), Plant Protection Systems (PPS), Engineered Safeguards Systems and other nuclear safety related applications. Applying one solution to all safety system applications will significantly reduce utility operation and maintenance costs, including technical support and spare parts.

The goal of this report is to seek review and approval from the U.S. Nuclear Regulatory Commission for the use of the Common Q™ Platform for nuclear safety-related systems.

Brackets in this document indicate proprietary information. The bracket denoting the end of a proprietary segment of this report may appear one or more pages following the bracket denoting the start of the proprietary segment. As a result care should be exercised in determining what information in this report is proprietary.

2 SCOPE

The scope of this report includes the hardware and software associated with the Common Q™ platform. The Common Q™ platform described herein encompasses design, qualification, reliability, and commercial grade dedication.

Common Q™ products can be used to replace obsolete components in Post Accident Monitoring Systems (PAMS) and Core Protection Calculator Systems (CPCS). Post Accident Monitoring Systems include Subcooled Margin Monitoring, Heated Junction Thermocouple Monitoring, Inadequate Core Cooling Monitoring and Qualified Safety Parameter Display systems. It is expected that these systems can be upgraded under 10 CFR 50.59 as a "digital to digital" upgrade, followed by a migration path that extends the Common Q™ application to replace Plant Protection Systems and Reactor Protection Systems through licensing amendments.

As Common Q™ components are added to update and replace analog I&C systems, full licensing review and approval by the NRC will be required. Where Common Q™ is implemented in CPC Plants, open loop PPS functions can be accommodated to validate system protective functions.

This topical report is structured with a main body and several appendices. The main body includes the basic platform description and addresses all of the key issues described in the Standard Review Plan, NUREG-0800, Revision 5. Each appendix describes one system in a stand-alone environment. In other words, separate appendices will be prepared for the Post Accident Monitoring Systems, Core Protection Calculator System, Reactor Protection System, Plant Protection System and Engineered Safety Features System Actuation System. The information in the appendices include system configuration, failure mode and effects analysis, 10CFR50.59 assessment for digital to digital replacements, and other system specific information. The last appendix describes all systems in a fully integrated configuration. This appendix will also include a failure mode and effects analysis for all shared services and will assess common mode failure mechanisms.

3 CODES AND STANDARDS

This section identifies compliance to the codes and standards applicable for the COMMON Q™ designs.

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
1.	RG 1.22 BTP 7-8 BTP 7-17	USNRC Regulatory Guide – Periodic Testing of Protection System Actuation Functions (Safety Guide 22) The COMMON Q™ platform conforms to this RG, Branch Technical Position 7-8 and -17, and IEEE Std 338 as described below: A. Provisions are made to permit periodic testing of the complete COMMON Q™ system with the reactor shutdown or operating. B. Provisions for testing the COMMON Q™ platform are incorporated via the Maintenance and Test Panels (MTP) and/or Interface and Test Processors (ITP) located in each COMMON Q™ cabinet. Testing each cabinet is performed using its MTP. C. No provisions are made in the design of the COMMON Q™ platform at the system level to intentionally bypass an initiation or actuation signal that may be required during power operation (this does not include override functions that are part of the system). All trip channel bypasses are on a channel level to prevent an operator from inadvertently bypassing a trip function. D. Manual testing for a COMMON Q™ platform division is interlocked to prevent testing in more than one redundant division simultaneously. When a trip channel is bypassed for manual testing, the bypass is indicated in the main control room. E. Actuated devices which can not be tested during power operation, will be tested when the reactor is shut down. F. An additional level of COMMON Q™ platform testing is provided by the PLC hardware self-diagnostic tests.	00 02/1972
2.	RG 1.29	USNRC Regulatory Guide – Seismic Design Classification The COMMON Q™ platform equipment is designated as a system to be Seismic Category I. Those portions of the equipment whose continued function is not required are designated Seismic Category II and are designed so that the SSE will not cause a failure which will reduce the functioning of the COMMON Q™ platform safety function to an unacceptable level. The applicability of this revision applies to baseline Common Q™ equipment. The applicability of this revision applies to new or enhanced modules/components.	03 09/1978 04 03/2007

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
3.	RG 1.47	USNRC Regulatory Guide – Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems Annunciator outputs or an equivalent mechanism are provided to indicate the bypassing of COMMON Q™ platform operating or trip channel bypasses where applicable. The applicability of this revision applies to baseline Common Q™ equipment. The applicability of this revision applies to new or enhanced modules/components.	00 05/1973 01 02/2010
4.	RG 1.53	USNRC Regulatory Guide – Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems Each system is designed so that credible single failures within the system shall not prevent proper protective action at the system level. See Sections 4 and 5 and the appendices of this report for system descriptions that implement these criteria. Single failures considered in the designs are addressed in the Failure Modes and Effects Analyses in the appendices. The applicability of this revision applies to baseline Common Q™ equipment. The applicability of this revision applies to new or enhanced modules/components.	00 06/1973 02 11/2003
5.	RG 1.62	USNRC Regulatory Guide – Manual Initiation of Protective Actions A. The COMMON Q™ RPS/ESFAS initiation functions and actuations can be manually initiated. B. Manual initiation of protective functions is provided at the system level. C. Manual COMMON Q™ initiation switches are remotely located in the main control room. Manual ESFAS switches are located locally on the ESFAS cabinets. D. The amount of equipment common to manual and automatic initiation paths is kept to a minimum. No credible single failure in the manual, automatic or common portions of the COMMON Q™ will prevent initiation of a protective action by manual or automatic means. E. Manual initiation requires a minimum of equipment consistent with the needs of A, B, C, and D above. The applicability of this revision applies to new or enhanced modules/components.	00 10/1973 01 06/2010
6.	RG 1.75 BTP 7-11	USNRC Regulatory Guide – Physical Independence of Electric Systems The COMMON Q™ platform conforms to this RG and BTP 7-11 as described in the IEEE Std 384 compliance statement below in Section 3.	03 02/2005

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
7.	RG 1.89	USNRC Regulatory Guide – Qualification for Class 1E Equipment for Nuclear Power Plants The COMMON Q™ conforms to this RG and IEEE Std 323 as follows. The environmental qualification of this equipment is by an appropriate combination of type testing and analysis as described further in Section 7 of this report.	01 06/1984
8.	RG 1.97 BTP 7-10	Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident Guidance on Application of Regulatory Guide 1.97 The Post Accident Monitoring Systems deployed using the baseline Common Q™ Platform shall conform to these requirements. The applicability of this revision applies to new or enhanced modules/components.	03 05/1983 04 06/2006
9.	RG 1.100	USNRC Regulatory Guide – Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants The seismic qualification of the baseline COMMON Q™ equipment is in accordance with this RG and IEEE Std 344 as described below. The adequacy of the design is verified by a combination of testing and/or analysis for the performance of its safety functions during and after the equipment is subjected to the forces resulting from one SSE preceded by a number of DBEs. Refer to Section 7.3 for a further description of the seismic qualification efforts. The applicability of this revision applies to new or enhanced modules/components.	02 06/1988 03 09/2009
10.	RG 1.105 BTP 7-12	Setpoints for Safety-Related Instrumentation Guidance on Establishing and Maintaining Instrument Setpoints The instrument uncertainties calculation of the safety systems is in accordance with ISA-67.04. The instrument uncertainties for the CPC are factored in the Statistical Combination of Uncertainties (Reference 7).	03 12/1999
11.	RG 1.118 BTP 7-17	USNRC Regulatory Guide – Periodic Testing of Electric Power and Protection Systems The baseline Common Q™ conforms to this RG, IEEE Std 338 and 7-17 as described in the compliance statement for RG 1.22, Reference 1.0. The applicability of this revision applies to new or enhanced modules/components.	02 06/1978 03 04/1995

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
12.	RG 1.152	USNRC Regulatory Guide – Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants The Common Q™ conforms to this RG by following IEEE-ANS Std 7-4.3.2, which provides methods acceptable for designing software, verifying software, implementing software, and validating computer systems in safety related systems. Refer to the Common Q™ Software Program Manual (SPM), Reference 5 and refer to Section 6 for a further description of the basic elements of the SPM.	03 07/2011
13.	RG 1.153 BTP 7-17	USNRC Regulatory Guide – Criteria for Safety Systems This Reg. Guide endorses IEEE Std 603-1991, which establishes minimum functional and design requirements for the power, instrumentation, and control portions of safety systems for nuclear power plants. See the response to IEEE 603-1991 for Common Q™ conformance. NUREG-800, BTP 7-17 references this Reg. Guide as acceptance criteria.	01 06/1996
14.	RG 1.168	Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants The Common Q™ Validation and Verification plans conform to this RG as described in Section 6 of this report and in the Common Q™ SPM, Reference 5.	01 02/2004
15.	RG 1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants The Common Q™ design and implementation processes conform to this RG as described in the Common Q™ SPM.	00 09/1997
16.	RG 1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants The Common Q™ design and implementation processes conform to this RG as described in the Common Q™ SPM.	00 09/1997
17.	RG 1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants The Common Q™ design documentation practices conform to this RG as described in the Common Q™ SPM.	00 09/1997
18.	RG 1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants The Common Q™ design and implementation processes conform to IEEE Std 1074-1995 as augmented by this RG, as described in the Common Q™ SPM for Common Q™ Systems, Reference 5.	00 09/1997

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
19.	RG 1.180	Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems This RG revision endorses MIL-STD-461D and MIL-STD-462D for baseline Common Q™ equipment. This RG revision endorses MIL-STD-461E and International Electrotechnical Commission (IEC) 61000 series of EMI/RFI test methods for new/enhanced Common Q™ equipment.	00 01/2000 01 10/2003
20.	IEEE Std 7-4.3.2	IEEE Standard Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations	2003
21.	ANSI/IEEE Std 279 BTP 7-17	"Criteria For Protection Systems For Nuclear Power Generating Stations" The Common Q™ protection systems shall be designed and tested to conform to this standard. This standard has been replaced by IEEE-603-1991.	1971
22.	IEEE Std 323	IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Systems	1983
23.	IEEE Std 338	IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems The Common Q™ conforms to this standard as augmented by RG 1.118.	1987
24.	IEEE Std 344	IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations The baseline Common Q™ conforms to this standard as augmented by RG 1.100. The applicability of this revision applies to new or enhanced modules/components.	1987 2004
25.	IEEE Std 379	IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems The baseline Common Q™ conforms to this standard as augmented by RG 1.53 and described in the conformance statement for RG 1.53, Reference 4.0. A further description of the application of these criteria is provided in Sections 4 and 5 of this report. The applicability of this revision applies to new or enhanced modules/components.	1994 2000 (Reaffirmed 2008)

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
26.	IEEE Std 383	IEEE Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations The Common Q™ conforms to this standard as below. The aging and flame retarding qualification requirements of this standard are invoked on the Common Q™ custom internal wiring and cabling.	1974
27.	IEEE Std 384 BTP 7-11	IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits The Common Q™ platform conforms to this standard as augmented by RG 1.75 and Branch Technical Position 7-11 as described below. The Common Q™ PPS and CPC systems are composed of four redundant cabinet assemblies which provide physical mechanical and electrical separation. The independence and separation of redundant Class 1E circuits within and between the Common Q™ assemblies is accomplished primarily through the use of fiber optic technology and, as necessary, 6 inch separation, barriers or conduits. A further description of the application of these criteria is provided in Sections 4 and 5 of this report.	1992
28.	IEEE Std 420	IEEE Standard for the Design and Qualification of Class 1E Control Board, Panels and Racks. The Common Q™ equipment conforms to this standard as augmented by and described in the compliance statements for the following IEEE Standards: -323 (), -338 (4.0), -383 (4.0), -384 (4.0), and –603 (4.0).	1982
29.	IEEE Std 494	IEEE Standard Method for identification of Documents Related to 1E Equipment. The Common Q™ documentation conforms to this standard by having the term “Nuclear Safety Related” applied on the face of each document and drawing.	1974 (Reaffirmed 1990)
30.	IEEE Std 603 BTP 7-3 BTP 7-5 BTP 7-9 BTP 7-10 BTP 7-11 BTP 7-12 BTP 7-17 BTP 7-18 BTP 7-19 BTP 7-21	IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations The Common Q™ conforms to this standard as augmented by RG 1.153, Rev. 01, 06/1996 and Branch Technical Positions 7-3, 5, 9-12, 17-19 and 21.	1991

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
31.	IEEE Std 627	IEEE Standard for Design Qualification of Safety System Equipment used in Nuclear Power Plants The Common Q™ qualification process conforms to this standard as described in Section 7 of this report and the conformance statements for IEEE Std 323 and RG 1.89.	1980 (Reaffirmed 1997)
32.	IEEE Std 730.1	IEEE Standard for Software Quality Assurance Plans The Common Q™ design and implementation processes conform to this standard as described in Section 6 of this report and the Common Q™ SPM, Reference 5.	1998
33.	IEEE Std 828	IEEE Standard for Software Configuration Management Plans The Common Q™ design and implementation processes conform to this standard, augmented by RG 1.169, and as described in Section 6 of this report and the Common Q™ SPM, Reference 5.	2005
34.	IEEE Std 830	IEEE Recommended Practice for Software Requirements Specifications The Common Q™ design documentation practices conform to this standard, augmented by RG 1.172, and as described in the Common Q™ SPM, Reference 5.	1998
35.	IEEE Std 1012	IEEE Standard for Software Verification and Validation Plans The Common Q™ Validation and Verification plans conform to this standard, augmented by RG 1.168, and as described in Section 6 of this report and in the Common Q™ SPM, Reference 5.	1998
36.	IEEE Std 1016	IEEE Recommended Practice for Software Design Descriptions The Common Q™ design documentation practices conform to this standard as described in the Common Q™ SPM, Reference 5.	1998
37.	IEEE Std 1028	IEEE Standard for Software Reviews and Audits The Common Q™ SPM, Reference 5, describes the software reviews and audits that will be performed per this standard.	1997
38.	IEEE Std 1042	IEEE Guide To Software Configuration Management The Common Q™ SPM, Reference 5, includes the SCMP for Common Q™ systems, and uses this standard as a guide.	1987 (Reaffirmed 1993)
39.	IEEE Std 1074	IEEE Std for Developing Software Life Cycle Processes See response to Reg. Guide RG 1.173, Ref. 4.18.	1995

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
40.	ISA-S67.04.01	Setpoints For Nuclear Safety Related Instrumentation Used in Nuclear Power Plants For digital to digital replacements (i.e., CPC, Qualified Safety Parameter Display System (QSPDS), etc.) the replacement Common Q™ system will be as accurate or more accurate than the system it is replacing, and will use existing field interfaces and setpoints. For analog to digital Common Q™ replacements (i.e., RPS, PPS, etc.), an assessment shall be made on the impact of any applicable setpoint analyses by the replacement system. The Common Q™ conforms to this standard as augmented by RG 1.105.	1994
41.	ANSI C37.90.1	IEEE Standard Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems. The Common Q™ EMI/RFI qualification plans (described in Section 7.3 of this topical report) include testing using the oscillatory SWC test wave as defined in Section 2.2 of this standard. (SWC testing was performed to IEC 801-5)	1989
42.	EPRI NP-5652	EPRI Guideline for Utilization of Commercial Grade Items in Nuclear Safety Related Applications This guideline discusses four methods for use in commercial grade dedication: (1) special tests and inspections, (2) commercial-grade survey of supplier, (3) source verification, and (4) acceptable supplier/item performance record. CE Nuclear Power's practices encompass all 4 of these processes as follows: Special tests and inspections are part of the Common Q™ qualification program that includes seismic, EMI/RFI and environmental testing of the commercial grade item (Section 7 of this report) Commercial-grade survey of supplier, source verification, and acceptable supplier/item performance record is part of the Hardware and Software Commercial Grade Dedication Processes described in Section 10.	1988
43.	EPRI Topical Report TR-102323	EPRI Guidelines for Electromagnetic Interference Testing in Power Plants The baseline Common Q™ equipment conforms to this standard as described in Section 7.3 of this topical report. Susceptibility and emissions of the equipment are determined for both conducted and radiated signals.	1997
44.	EPRI Topical Report TR-106439	EPRI Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications The Common Q™ Commercial Grade Dedication Program for its building blocks shall follow the guidelines outlined in this report.	1996

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
45.	MIL-STD-461D	Military Standard Electromagnetic Interference Characteristics Requirements for Equipment The baseline Common Q™ equipment is qualified in accordance with this MIL STD as augmented by EPRI TR-102323, and further described in Section 7.3 of this topical report.	1993
46.	MIL-STD-462D	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment The baseline Common Q™ equipment is qualified in accordance with this MIL STD as augmented by EPRI TR-102323, and further described in Section 7.3 of this topical report.	1993
47.	MIL-STD-461E	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment This standard supersedes MIL-STD-461D and MIL-STD-462D. New additions or enhancements to previously tested Common Q™ equipment are tested in accordance with this standard as augmented by RG 1.180, Rev. 01.	1999
48.	IEC 61000 series	Electromagnetic Compatibility (EMC) New additions or enhancements to the baseline Common Q™ equipment are tested in accordance with this standard as augmented by RG 1.180, Rev. 01.	
49.	BTP 7-14	Guidance on Software Reviews for Digital Computer-Based I&C Systems The Common Q™ program meets the intent of this BTP and is defined in the Common Q™ Software Program Manual.	
50.	BTP 7-18	Guidance on Use of Programmable Logic Controllers in Digital Computer-Based I&C Systems The Common Q™ program meets the intent of this BTP and is defined in the Common Q™ Software Program Manual and its Commercial Grade Dedication Program as described in Section 10.	
51.	BTP 7-19	Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems Defense-in-Depth and Diversity for specific systems are discussed in the Integrated Solution Appendix of this Topical Report.	
52.	BTP 7-21	Guidance on Digital Computer Real-Time Performance Common Q™ designs will be described in more detail in follow-up appendices to this Topical Report and will encompass the existing design parameters of the systems that are replaced.	

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
53.	EPRI TR-107330	Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants	1996
54.	NUREG-0737	Clarification of Three Mile Island (TMI) Action Plan Requirements All Common Q™ Post Accident Monitoring Systems shall meet these requirements.	1980
55.	NUREG-0800	Chapter 7 of the USNRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Rev. 5 The NRC will use this NUREG as the basis for their review of this topical report. Refer to the conformance statements for each Branch Technical Position listed herein.	2007
56.	NUREG/CR-6303	"Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" The Nuplex 80+ certification includes a methodology for analyzing the defense against a common mode failure. The methodology is similar to this NUREG. The Integrated Solution Appendix describes how this methodology would be applied to Common Q™.	1994
57.	NUREG/CR-6421	A Proposed Acceptance Process For Commercial-Off-The-Shelf (COTS) Software in Reactor Applications This NUREG shall be used as guidance when developing the Software Commercial Grade Dedication Plan for the Common Q™ COTS software (i.e., [ ]^{a,c} and ABB Advant®). Section 10.1 discusses the Software Commercial Grade Dedication process.	1996
58.	10 CFR 50 Appendix A	GDC 1: "Quality Standards and Records" The Common Q™ Quality Assurance procedures shall conform to these criteria. GDC 2: "Design Bases For Protection Against Natural Phenomena" GDC 4: "Environmental And Dynamic Effects Design Bases" Common Q™ hardware and software qualification procedures shall conform to these criteria. GDC 12: "Suppression Of Reactor Power Oscillations" The Common Q™ CPC implementation will still have the Local Power Density Trip function that addresses this criterion. GDC 13: "Instrumentation And Control" Common Q™ systems shall be designed and tested to meet this criterion.	

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
58. (cont.)	10 CFR 50 Appendix A	GDC 19: "Control Room" A Control Room interface (Flat Panel Display System) is provided for each Common Q™ system. GDC 20: "Protection System Functions" Common Q™ systems responsible for the functions defined in this GDC shall be designed and tested to conform to this criterion. The Common Q™ Platform applications support the following GDCs: 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" GDC 10: "Reactor Design" The Common Q™ DPPS and CPC applications support this criterion. See appendices for details. GDC 15: "Reactor Coolant System Design" The DPPS High Pressure Trip is an example of a Common Q™ application supporting this criterion. See DPPS appendix for details. GDC 16: "Containment Design" The DPPS is a Common Q™ application that supports this criterion. See DPPS appendix for details. GDC 28: "Reactivity Limits" Both the CPC and DPPS Common Q™ applications (e.g., Variable High Power Trip or High Linear Power Trip) support this criterion. GDC 29: "Protection Against Anticipated Operation Occurrences" Both the CPC and DPPS Common Q™ applications support this criterion. GDC 33: "Reactor Coolant Makeup" Both the DPPS and ESFAS Common Q™ applications support this criterion. Refer to the DPPS and ESFAS appendices for details.	

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
58. (cont.)	10 CFR 50 Appendix A	GDC 34: "Residual Heat Removal" Common Q™ applications detailed in the appendices are not applicable to this criterion. GDC 35: "Emergency Core Cooling" The DPPS and ESFAS Common Q™ applications support this criterion. GDC 38: "Containment Heat Removal" The Common Q™ PPS application supports this criterion. Refer to the DPPS appendix for details. GDC 41: "Containment Atmosphere Cleanup" GDC 44: "Cooling Water" The Common Q™ PAMS application supports these criteria by displaying relevant variables. Refer to the PAMS appendix for details.	

4 COMMON Q™ OVERVIEW

This section of the topical report gives a general overview of the Common Q™ system components. More details are provided in Section 5. Application of the Common Q™ to specific systems is given in the appendices.

Common Q™ by definition is Class 1E, therefore all of its building blocks are Class 1E. The Common Q™ platform consists of the following major building blocks which can be used to design a specific safety system:

- Advant Controller 160 (AC160) with PM646A Processor Module (also used for Interface and Test Processor – ITP in figure)
- Input and Output Cards
- Power Supply
- Flat Panel Display System (for Operators Module (OM) and Maintenance/Test Panel (MTP) shown in figure)
- Advant Fieldbus (AF100) Communication
- High Speed Link (HSL) Communication

Figure 4-1 is a generic representation of how the building blocks are configured for a safety system.

a,c

Figure 4-1 Simplified Block Diagram

4.1 ADVANT CONTROLLER 160 (AC160)

The AC160 is used for executing the protection algorithms for the Common Q™ applications.

ABB's Advant Controller 160 (AC160) is a high performance modular controller with multiprocessing capability for logic control. The processor module (PM) used in the Common Q™ applications is the PM646A.

AC160 is fully modular with modules mounted in 19" subracks. A typical Common Q™ configuration consists of processor module(s), input/output (I/O) modules and communication modules contained in one or two subracks. Each rack can accommodate up to 10 modules.

To provide scalability in performance and reliability, up to six processor modules could be used concurrently in one controller. Presently the Common Q™ Applications require an upper limit of four PM646As. Any applications of more than four PM646As will be evaluated for compliance with Section 7 requirements when needed. The processor modules within an AC160 controller share data with each other using the global memory resident on the AF100 Communication Interface (model CI631, twisted pair).

Each processor module supports two high speed communication links (HSL). The HSLs will be typically used in the broadcast mode to transmit data to other divisions of the safety system. These data links are electrically isolated using fiber optic cable. The HSL is discussed in Section 4.5 and subsection 5.2.5.2.

The processors are programmed in the ABB Master Programming Language (AMPL). In addition to the logic constructs, this language provides logic block interfaces to the AF100 network, global memory, I/O and the HSL. AMPL is discussed in subsection 5.2.1.2.

The processor module has a built in watchdog timer module that is to be used in the Common Q™ systems. Depending on the specific system application, the watchdog timer can be used to annunciate a failure, actuate a divisional trip, or set output states to predefined conditions. For example, the watchdog timer may be used to control the power to the relays on the digital output module. Isolation is provided for those applications where the watchdog timer is connected to external systems. The Watchdog Timer is discussed in subsection 5.2.4.

Fiber optic modems that have gone through a commercial grade dedication process will be used for electrical isolation from other safety divisions and non-safety systems.

4.1.1 AC160 Software

Software programming is done on a x86-based Personal Computer using the ABB AMPL Control Configuration (ACC) software development environment. The target code is generated and downloaded to the AC160 controller via the Personal Computer serial port. The AC160 software development environment is called ABB Master Programming Language (AMPL) Control Configuration (ACC). The ACC product consists of the following utilities:

- Application Builder

- Online Builder[1]
- Function Chart Builder
- Bus Configuration Builder

The tools use the ABB Master Programming Language (AMPL). AMPL is based on a library of predefined function blocks, called Process Control (PC) elements, and database elements, called DB elements. The PC elements and DB elements are combined into programs that form a complete control function. In addition to the base PC and DB libraries, there are optional libraries that can be configured to expand the PC and DB element set. Refer to subsection 5.2.1.2 for more information on the AC160 software.

The Advant Controller 160 (AC160) software consists of a real-time operating system [ ]a,c, task scheduler, diagnostic functions, communication interfaces, and user application programs, all of which reside on flash programmable read only memory (PROM) in the PM646A processor module. Refer to subsection 5.2.1.2 for a more detailed description of the AC160 software.

The application program in an AC160 coexists with the other AC160 system software programs such as the diagnostic routines and communication interfaces. The task scheduler schedules the execution of all these different entities.

[

]a,c Data is acquired over the I/O backplane (BIOB), the AF100 communication interface and the high speed link (HSL) interface. The AC160 base software resides in the AC 160 Central Processing Unit (CPU) module flash PROM (non-volatile memory).

[

]a,c

Creation of the application program (PCPGM) utilizes the ACC software development environment that includes a function block library (PC element library). The programmer references the PC element library to create specific logic for the application. Refer to subsection 5.2.1.2.2 for a description on how the software is developed.

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

4.1.2 Input and Output Cards

The Advant Controller 160 uses the S600 I/O system. A range of I/O modules is available, covering analog and digital signals of various types. In addition, there are modules for temperature measurement and rotational speed measurement. The process signals are connected to the front of the I/O modules. S600 I/O modules that will be used in Common Q™ applications are discussed in subsection 5.2.1.1.3.

1. Only applicable to the AC400 series controllers which are not part of Common Q™.

The system software in the Advant Controller 160 automatically checks that all I/O modules are operating correctly at system startup and by the application interfacing with the module. Reactions to errors are application specific and are discussed in the applicable appendices.

4.1.3 Interface and Test Processor (ITP)

In addition to the AC160 executing the protection algorithms for Common Q™ applications, some Common Q™ configurations (PPS and RPS) have another AC160 controller used for on-line testing.

The ITP is an independent AC160 chassis that is nuclear safety related and whose software is classified as Important To Safety (Safety Related)[2]. Refer to Reference 5 for a discussion on software classification. It communicates with the MTP and the other AC160 chassis in the division (executing protection algorithms) by way of a redundant AF100 network. The ITP is connected to optically isolated data links that allow all the ITPs in a multi-divisional system to communicate to one another. The fiber optic data links provide isolation and the ITP provides communication buffering to protect against external divisional faults.

The ITP is a testing system which performs continuous passive monitoring of expected outputs based on current inputs, and manually initiated automatic active testing. The ITP man-machine interface is the MTP. The combination of the ITP and MTP enhances maintenance and surveillance testing. Cross divisional data is compared in the ITP for consistency. The status of the other divisions is checked before any divisional test is initiated.

4.2 POWER SUPPLY

The power supply is based on a 19" rack or 24" panel assembly with plug-in or quick disconnect modules. Various modules are available to accommodate different output voltages.

The power supply will be designed for use by the processor, loop transmitters, digital logic, relays, and reed switch position transmitter circuits. Separate power supply modules will be used for these different functions where appropriate.

Redundancy will be available. Faults in one half of a redundant supply will not affect the other from operating normally. Redundant modules can be replaced while the power supply remains energized without disturbing the powered system.

The power supply will have features such as overvoltage and overtemperature protection, soft start, and high power factor.

4.3 FLAT PANEL DISPLAY SYSTEM (FPDS)

The flat panel display system consists of the flat panel display with touch screen capability, a single board computer, and standard communication interfaces for communication to the Advant Controller and isolated external systems.

2. The AC160 executing the Protection Algorithms has software classified as Protection (Safety Grade).

[

]a,c

4.3.1 Flat Panel Display System Software

The flat panel display is used for the Operator's Module and the Maintenance and Test Panel. The software classification for the FPD is application specific and in accordance with Reference 5.

[

]a,c

There are two types of programming for the flat panel display: application programs written in C and displays built using a display builder.

4.3.2 Maintenance and Test Panel (MTP)

The Maintenance and Test Panel is a flat panel display system.

The MTP will be used for maintenance and test functions in each Common Q™ system division. The MTP provides the means for the operator or technician to bypass a channel, initiate surveillance tests, and display detailed system diagnostic messages.

The MTP interfaces to the AC160 via the redundant Advant AF100 communication bus. The MTP also has non-volatile memory, such as a solid state disc, used for storing maintenance information to support warm system starts using technician updated data.

4.3.3 Operator's Module

The Operator's Module uses the same Common Q™ flat panel display system. The Operator's Module will be used for operator functions such as changing setpoints or viewing control rod positions. Non-volatile memory, such as a solid state disc, is used for operator setpoints or other applications where warm system starts using updated constants is needed.

For some systems such as the QSPDS, the functions of the Operator's Module and the MTP may be combined (see the appropriate appendix for details).

4.3.3.1 Manual Component-Level Control

Another function of the Operator's Module is to perform manual component-level control of safety components for maintenance and test purposes. This manual component control will not be credited as a safety function but rather as a means to manipulate an individual component to support maintenance and testing.

4.4 AF100 COMMUNICATION

The Advant Fieldbus 100 (AF100) is a high performance bus, which will be used for intradivisional communications.

The Operator's Module, the MTP, and the AC160 processor chassis are connected to the intradivisional bus.

The Advant Fieldbus 100 supports two different kinds of communication: process data and message transfer. Process Data transfer is managed through Cyclic Data Packets (CDPs). Each CDP is configured on the communication interface for a certain signal identity, cycle time, size and direction. Process data is always transferred cyclically on the Advant Fieldbus.

The message transfer services are implemented to enable stations on the Advant Fieldbus to send and receive messages. 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 amount of the Advant Fieldbus bandwidth is reserved for message transfer.

The Advant Fieldbus is deterministic and supports power up and power down of equipment on the bus.

4.5 HIGH SPEED LINK (HSL) COMMUNICATION

Each PM646A module actually contains both an application processor and a dedicated HSL communications processor. Depending on the system configuration requirements, one PM646A module may perform both application and communication processing.

The HSL will be used to transmit broadcast data to other divisions in a multi-divisional system. The HSL is a serial RS 422 link at the physical layer using High Level Data Link Control (HDLC) protocol with a 3.1 Mbits/second transfer rate. Each PM646A has one independent transmit link (output to two ports) and two independent receive links. The transmit data is optically isolated and transmitted to the other divisions. Receive links on multiple PM646As are used to receive data from each of the other divisions.

The data links are true broadcast only and meet the communication isolation requirements of IEEE 7-4.3.2.

Multiple HSLs may be used to provide redundancy for the interdivisional communication.

5 COMMON Q™ PLATFORM

5.1 FUNCTIONAL REQUIREMENTS

Functional Requirements for each application of the Common Q™ platform is discussed in application specific appendices to this topical report. The following applications shall be defined in the appendices:

- Core Protection Calculator (CPC)
- Reactor Protection System (RPS)
- Plant Protection System (PPS)
- Post Accident Monitoring Systems (PAMS)
- Engineered Safety Features Actuation System (ESFAS)

The specific appendix for each of the above systems will be submitted independently of the base topical report. Additional applications of the Common Q™ building blocks may also be submitted in additional specific appendices.

5.2 SYSTEM DESCRIPTION (BUILDING BLOCKS)

The Common Q™ Platform is based on the idea of using a consistent set of qualified building blocks that can be used for any safety system application. The building blocks are:

1. Advant Controller
2. Flat Panel Display
3. Power Supply
4. Communication Subsystems

5.2.1 Advant Controller

Advant Controller 160 is part of the ABB Advant Power family. It is used in applications that require high availability and redundancy.

5.2.1.1 AC160 Hardware Description

The Advant Controller 160 (AC160) consists of a number of hardware modules that can be configured in a chassis. These hardware modules fall into the general categories of processor, inputs and outputs, and communications.

ABB's Advant Controller 160 is a high performance modular controller for logic control with multiprocessing. Advant Controller 160 and its S600 I/O can be used stand-alone or it can communicate with other controllers.

The controller is specifically designed for high speed PLC type applications, but it also brings considerable problem solving power to all analog signal handling and arithmetic applications. Advant Controller 160 covers a wide range of programmable functions such as logic and sequence control, analog data handling, arithmetic, and pulse counting.

Advant Controller 160 is fully modular with modules mounted in 19" subracks. The subracks are designed for front or rear mounting. A minimal Advant Controller 160 configuration consists of one or two subracks containing the processor module, up to 19 I/O and communication modules, and a 24 VDC power supply.

In order to extend the number of I/O modules, up to 7 I/O stations may be connected to the controller, each consisting of up to two subracks.

By using redundant communication interfaces to Advant Fieldbus and to I/O extension bus, redundant power supply modules and redundant external power, the availability of the Advant Controller 160 can be increased as needed to achieve high reliability and availability. When operated in the redundant mode, failure of one of the redundant items does not interfere with the continued operation of the other. Redundant modules can be replaced during operation of the system.

To provide scalability in performance and reliability, up to six processor modules can be used concurrently in one controller. By adding one or more processor modules, the performance of the controller can be easily extended to meet the requirements of any specific application.

The processors share data with each other using the global memory contained in the AF100 Communication Interface (CI631).

Advant Controller 160 is designed to operate in demanding environments. A hardened enclosure assists in protecting the printed circuit boards from mechanical and electrostatic damage.

5.2.1.1.1 PM646A Processor Module

The hardware for Advant Controller 160 consists of processor modules, communication modules, I/O modules and process connectors, subracks, and power supplies.

The subracks are designed for wall mounting or mounting in cabinets. Normally they are mounted in cabinets. The modules are housed in a sheet steel enclosure, which assists in protecting the circuit boards. The enclosure has openings at the top and bottom for air convection. AC160 Hardware is shown in Figure 5-1.

a,c

Figure 5-1 AC160 Hardware

Processor Module

Although five different types of processor modules are available for Advant Controller 160, only the PM646A is intended to be used. The AC160 can be configured with PM646A modules running redundantly in a hot-standby/automatic failover mode or with PM646A modules running asynchronously.

The PM646A features important for Common Q™ Applications are the following:

- The PM646A processor module consists of two hardware sections, the processing section with microprocessor and memory for the application program and the communication section with a separate microprocessor and memory for the communication signal exchange to other controllers.

- A Motorola MC68360 processor (application processor), 1 Mbyte 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 Static RAM (SRAM). At startup, the application and system software are copied from the nonvolatile memory into the SRAM memory where it is executed.

- The memory 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.

- An RS-232-C port dedicated for connection of Advant Station 100 Series Engineering Stations (used for system maintenance and programming).

- A second Motorola MC68360 processor for HSL communications, with an extra 512 Kbytes nonvolatile memory (Flash PROM) for the system software and an extra 2 Mbytes SRAM is provided for communications.

- All PM646A processor modules contain two serial data link ports (high speed serial links) for signal and data exchange between processor modules for application and system purposes called Link 1 and Link 2.

Subrack

The 10-position controller subrack is the primary subrack of the Advant Controller 160. It provides dedicated positions for processor modules, communication, and bus extender modules. There is a two-digit thumbwheel switch for setting the station address. The individual module address is given by its position in the subrack.

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. The individual module address is given by its position in the subrack.

Up to seven additional subrack pairs (I/O stations) could be connected if additional I/O requirements apply.

Diagnostic Functions

Advant Controller 160 performs a variety of diagnostic and supervision functions to continuously monitor the correct operation of the whole system. Each of the modules has diagnostic functions. The CPU module 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 supervision functions are subdivided into the following groups:

- Problem detection
- Signaling the nature of the problem
- Automatic reaction to problems

Each module is equipped with two light emitting diode (LED) indicators, FAULT and RUN. During normal operation, the green RUN LED is lit on all modules. The red FAULT LED lights only if a problem occurs on the module. The status of the modules and of the I/O signals is also indicated by the associated DB (database) elements in the application program.

Missing modules are also signaled by the function supervising the configuration on the associated (DB) elements. The PC (process control/application) program can process the status signals on the DB elements in the same way as other signals. This feature provides the capability to include error-handling routines in application programs. Severe problems (e.g., component errors) in the processor module stop the processor module. These errors also switch an internal watchdog timer relay in the processor module. For Common Q™ applications, this relay is used to provide alarm, and in some applications, conservative failure responses of the affected division.

The diagnostic function displays an error code on the front of the CPU module to facilitate fault tracing.

The CPU checks the consistency of the module configuration specified by the DB elements and the actual configuration of the modules. This check is performed each time a module is switched on before it is switched to RUN. If the module installed does not correspond to the type of module specified by the

module DB element, then the module is not switched to RUN and the error is indicated on the associated divisional DB elements.

The following indicators are on the front of the PM646A processor module:

- The green LED, RUN1, indicates that the processing section of the PM646A is operational.
- The green LED, RUN2, indicates that the communication section of the PM646A is operational.
- The red LED, FAULT, indicates a severe fault and normally the processor module must be replaced.
- The diagnostic display indicates the processor module operating mode:
  - P- = startup
  - P1 = normal operation
  - P3 = stop after initialization
  - P4 = CPU is not running an application
  - P5 = loading application program from PROM
  - P6 = engineering station is connected
  - PL = waiting for download of system software
  - PU = loading system software option (enabling options)
  - xx = error code (If a two digit number (xx) is visible, the system has stopped and the number represents an error code).

The PM646A processor module is shown in Figure 5-2.

a,c

Figure 5-2 PM646A Processor Module

5.2.1.1.2 PM646A High Speed Link Communication Interface

The PM646A processor module contains two high-speed communication links (Link 1 and Link 2) provided for signal exchange. The HSLs are serial data link channels with HDLC protocol with a speed of 3.1 MBaud on each channel. The HSLs are used in the broadcast mode and function to transmit data to other divisions of the safety system. The data links are isolated using fiber optic modems, OZDV 114A/OZDV 114B.

Each link transmits the same data, i.e., there is only one transmit data table available to the application program. However, the data can be sent to two different locations. The receivers of each HSL are independent and can receive different data independently.

5.2.1.1.3 Input/Output Subsystem

The controller may contain up to 75 I/O modules. The maximum number of I/O signals for an Advant Controller 160 is 1500. The actual CPU load depends on the configured cycle times for the application program. Function element execution times are documented in Reference 12.

All I/O modules may be replaced electrically, not necessarily system wise, while the system is powered (and typically in test mode). Removing the front connector disconnects the process signals. A newly inserted module is automatically put into operation if the system identifies the module as being of the correct type and without faults.

The following module types are listed to show the variety of modules available. The specifications for any module used in a specific application will be reviewed before inclusion into the design for that system.

Analog Input Modules

[

]a,c

Analog Output Modules

[ ]a,c

[
]a,c

Digital Input Modules

[ ]a,c

Digital Output Modules

[

]a,c

Pulse Counting Module

[
]a,c

Status of I/O Signals

A yellow LED for each signal connected to the process indicates the status of the digital signals (DI, DO):

- Digital input signals: The signal status LED is located in the input signal path, i.e., it directly indicates input current.
- Digital output signals: The signal status LED indicates the output signal status.
- Checks the process voltage supply and fuses for process signals. Fuses or circuit breakers are the most frequent cause of missing process signals.

Unused Supervised Inputs

Unused analog inputs must be terminated appropriately in order to avoid error detection and signaling by the processor modules. The signals must also be set to OFF/Inactive in the database. Inactive signal values are not updated in the database.

Calibration of Analog Input and Outputs

During the course of manufacture, all measurement and output ranges of analog I/O modules are calibrated at an ambient temperature of approximately 25°C. Normally, the modules need no further

calibration. If the accuracy is outside the specified limits (e.g., due to component failure), the module must be replaced. There are no calibration adjustments.

The analog modules are designed in such a way that component aging has little affect on specified accuracy. This is the result of:

- Use of high quality, low drift components. For example, the analog circuits do not include any potentiometers (which are often the cause of drift problems).

- Use of self calibration techniques in modules of high specified accuracy (high end modules). The self calibration techniques are based on high precision resistors and on voltage sources with extremely low drift due to temperature and aging.

The system software in the Advant Controller 160 automatically checks that all I/O modules are operating correctly. In the event of a defective or missing module (e.g., during replacement), the module and associated signals are flagged at the "ERR" terminal of the data base elements. The signal value (VALUE) is not updated as long as the error persists. Common Q™ applications shall monitor the ERR terminal for each DB element.

The I/O module runs a self-testing routine following power-up and during operation. Provided, no serious defect is detected, the red LED (FAULT) extinguishes. The system software checks that:

- The module is in the correct position
- The module is of the right type
- The module is not defective
- The process connector is in place

If all these points are in order, the green LED (RUN) lights, the error flag on the data base element is reset, and the module switches to the operating mode.

5.2.1.2 AC160 Software Description

The Advant Controller 160 Software consists of a real-time operating system [ ][a,c], AC160 task scheduler, diagnostic functions, communication interfaces, and user application programs, all of which reside on flash PROM in the PM646A processor module. Refer to subsection 5.4.1 for a description of diagnostic functions, and subsection 5.3.1.2-4 for a description of the communications.

5.2.1.2.1 Base Software

Processor system software consists of the standard AC 160 system software products developed by ABB Automation Products, GmbH[ ][a,c]. The system software [ ][a,c] executes the control units of the application program, diagnostics routines and communication interfaces to the I/O backplane (BIOB), the AF100 Communication Interface and the High Speed Link (HSL) interface. The AC160 base software resides in the AC 160 CPU module flash PROM (non-volatile memory). This software is under configuration control and its version is identified in the manner shown in Figure 5-3.

a,c

Figure 5-3 Base Software Identification

There are software options available in the Base Software that add functionality to the PLC which can be enabled or disabled.

[ ]a,c Real Time Operating System

[

]a,c

AC160 Kernel

The application program and its control modules in an AC160 coexist with the other AC160 system software programs such as the diagnostic routines and communication interfaces. The AC160 task scheduler schedules the execution of all these different entities based on predefined priorities, the assigned cycle time of the control modules and their entry in the cycle time table. The cycle time table is used to assign priorities to control modules with the same cycle time.

[

]a,c

a,c

Figure 5-4 Basic Functional Architecture PM646

[

]a,c

a,c

Figure 5-5 [ ]a,c

[

]a,c

[

]a,c

a,c

Figure 5-6 [ ]a,c

[

]a,c

[

]a,c

[

]a,c

[

]a,c

[

]a,c

a,c

Figure 5-7 [ ]a,c

[

]a,c

a,c

Figure 5-8 [ ]a,c

[

]a,c

a,c

Figure 5-9 [ ]a,c

[

]a,c

a,c

Figure 5-10 [ ]a,c

[

]a,c

[

]a,c

a,c

Figure 5-11 [ ]a,c

[

]a,c

Function Block Library

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

]a,c

5.2.1.2.2 Application Software

Creation of the application program (PCPGM and CONTRM) utilizes the ACC software development environment that includes a function block library (PC element library). The programmer references the PC element library to create specific logic for the application.

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

The software for each application of Common Q™ is described in the Appendices to this topical report.

PC Part

The PC part of a user application program describes the control algorithm and the control strategy. It contains the PC elements (logic blocks), their interconnections and the connections to the DB elements. A PC program can be divided into several executable units (control modules-CONTRMs), each consisting of PC elements. Each executable unit can be given its own cycle time and its own execution conditions. PC elements are the smallest "building blocks" in a PC program.

There is a PCPGM PC element that is required for each PM646A application program. It has a separate cycle time than the CONTRMs. It represents the transfer rate of data between the PM646A and the CI631 AF100 Communication Interface.

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 (BIOB) from the I/O modules.

[

]a,c

[

]a,c

a,c

Figure 5-12 [ ]a,c

[

]a,c

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

Database Part

The DB part in an Advant Controller 160 contains the DB elements which are used to configure the controller. DB elements in an Advant Controller 160 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)
- Connection between the hardware and the common data elements (e.g., Data Set Peripheral [DSP] for AF100 communication and DB elements for the HSL)

5.2.1.2.3 Software Tools

Software programming is done on an x86-based PC and then the target code is generated and downloaded to the AC160 controller via the PC serial port. The AC160 software development environment is called ACC which is a product of ABB Automation Products, GmbH. The ACC product consists of the following utilities: Application Builder, AS100 Edit, Function Chart Builder and Bus Configuration Builder. The tools use the ABB Master Programming Language (AMPL). AMPL is based on function blocks, called PC elements, which are combined with each other into programs which form a complete control function.

For further description see References 9 and 10.

These tools can be used for on-line programming of the controller. However, for safety-related Common Q™ applications, this capability will be controlled administratively with additional password protection.

Type Circuits

ACC supports the development of type circuits. A type circuit is a logic block composed of PC elements that can be used many times in a control program. The same tool (Function Chart Builder) is used for both type circuit and control program development. Once a type circuit is developed it can be used in a control program just like any other PC element.

Although the type circuit appears as a single block, each PC element in the type circuit becomes part of the application program, much like a macro represents a set of language instructions. Therefore, the purpose of type circuits is to increase readability of the control program and to provide configuration control for a set of code, and not for performance enhancement or memory conservation.

The type circuit is considered a module and therefore must undergo documented module tests when used in protection class software as described in the Software Program Manual (Reference 5).

Custom PC Elements

Custom PC elements appear as standard PC 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 PC elements. Once in the library, the custom PC element is available for the programmer to use in a control program.

The custom PC element is developed using the system software extension option for the AC 160 that allows custom PC elements to be added to the controller. The tools used to develop the custom PC element include a C compiler (MCC68K) and linker (LNK68K) from Mentor Graphics Microtec division. The linker generates a Motorola S-Record image file for the PC element. This image file is downloaded to

the AC160 processor module's flash PROM using the same tool for installing the base software. Reference 8 describes the methodology for creating these elements.

The design process for a custom PC element requires the programmer to define the inputs and outputs of the module prior to coding the algorithms. This enforces a methodical design approach to building software modules.

Unlike a type circuit, which is a cluster of PC elements, a custom PC element increases the performance of the execution of a program because it is only one PC element. Therefore, sophisticated logic that would require many PC elements can be encapsulated into a single custom PC element.

The custom PC element shall be classified as a module and therefore undergo documented module tests as described in Section 6 for protection class software and the Software Program Manual (Reference 5).

5.2.1.3 Watchdog Timer

[

]a,c

The watchdog timer relay is a form C relay, whose contacts are accessible from the processor front panel. Depending on the specific system application, the watchdog timer can be used to annunciate a failure, actuate a divisional trip, or set output states to predefined conditions. For example, the watchdog timer relay may be used to control the power to the relays on the digital output module. Isolation is provided for those applications where the watchdog timer is connected to external systems.

a,c

Figure 5-13 Watchdog Timer Configuration

Table 5-1 Processor Module WDT Arrangement Watchdog Timer Summary a,c

5.2.2 Flat Panel Display System

The Flat Panel Display System consists of an x86 Single Board Computer for display and communication programs and a Flat Panel VGA interface for displays.

The flat panel display will be used for the operator display and, maintenance/test functions. This would include displaying real-time process data, entering setpoint data, starting surveillance tests, providing the interface for manual component control, and displaying system status.

5.2.2.1 Flat Panel Display System Hardware Description

The flat panel display system consists of the flat panel display with touch screen capability, a single board computer, and standard communication interfaces for communication to the Advant processor and other systems.

5.2.2.1.1 Single Board Computer

The single board computer is based on [ ]a,c. There is an interface to the Advant AF100 communication bus so data can be communicated with the Advant 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 to is the Plant Computer. Typical Plant Computer interfaces are Ethernet or serial data link. Non-volatile memory, such as a solid state disc, is used for operator setpoints or other applications where warm system starts using updated constants is needed.

5.2.2.1.2 Flat Panel Display

The flat panel display is a color TFT display that is readable under high ambient light conditions. The display has touch screen capability. The displays are available in multiple sizes.

5.2.2.2 Flat Panel Display Software Description

The software used for the Flat Panel Display is described in the following sections.

5.2.2.2.1 Operating System

[

]a,c

a,c

Figure 5-14 Operating System

[

]a,c

a,c

[

]a,c

[

]a,c

5.2.2.2.2 Graphical User Interface

[

]a,c

a,c

Figure 5-15 OS Graphical User Interface

[

]a,c

[

]a,c

a,c

Figure 5-16 [ ]a,c

[

]a,c

Each Common Q™ system will have specific Human-Machine Interface (HMI) response time requirements. The acceptance tests for a specific Common Q™ application will validate the drawing API performance.

5.2.2.2.3 Software Tools

There are two areas of programming for the Flat Panel Display: application programs written in C and displays built using a display builder.

C Application Programming Tools

The [ ][a,c] enforces the development of application programs in Standard C. Any text editor can be used for creating and editing the source code. All application programs for the Flat Panel Display shall be written in Standard C.

Display Building Tools

The [ ][a,c] supports the development of HMI displays for the Flat Panel Display. It contains a symbol library and a visual display building tool that allows the creation of graphical displays. The visual display building tool, [ ][a,c] for the runtime implementation of the display. [
][a,c]

5.2.2.3 Flat Panel Display System Applications

The Flat Panel Display System will be used for two subsystems for the Common Q™ Platform:

- The Operator's Module (OM)
- The Maintenance and Test Panel (MTP)

5.2.2.3.1 Operator's Module

The Operator's Module (OM) software shall reside on the Single Board Computer (SBC) of the Flat Panel Display. It will consist of one or more software programs (units) written in Standard C [
][a,c]. The OM is a control room device that allows operators to monitor the system division.

5.2.2.3.2 Maintenance and Test Panel (MTP)

The Maintenance and Test Panel (MTP) is also a Flat Panel Display System application. It too shall have software units custom written in Standard C and units generated by [ ][a,c] software. This software will perform maintenance and test functions for the Common Q™ Platform.

The MTP shall provide the following functions:

- The means for the operator to bypass the channel and initiate diagnostic tests on the system, and display the results

- The means for loading and changing setpoints

- The data link interface (serial or network) to external systems

Manually Initiated Tests

The MTP provides the means for the operator to bypass a channel and initiate surveillance tests. These initiations shall be transmitted to the AC160 processor through the AF100 network. The results of the test

are transmitted back to the MTP for display. The MTP shall also display any anomalies detected by the ITP from its passive testing (monitoring system operation without injecting test signals).

Loading/Changing Setpoints

The operator can load either a batch set of setpoints or can change an individual setpoint. In either case validation procedures shall be executed that will ensure data integrity. When setpoints are changed, they are transmitted over the AF100 network to the AC 160. The AC 160 shall transmit these changes back to the MTP for verification. The MTP software then shall compare the setpoints received from the AC 160 with those stored on the MTP or entered by the operator. Any deviations shall be displayed and alarmed on the MTP. The operator can then reload the setpoints if there are any discrepancies. [

]a,c

Data Link Interface To External Systems

There shall be a software program that transmits predefined data packets over a data link to an external system. The AC160 processors shall transmit data over the AF100 network at predefined intervals to the MTP. The data link interface program in the MTP shall read this data off the AF100 network, format a data link packet, and transmit it to the external system.

5.2.3 Power Supply

The power supply is based on a 19" rack or 24" panel assembly with plug-in or quick disconnect modules. Various modules are available to accommodate the different output voltages anticipated.

The power supply will be designed for use by the processor, loop transmitters, digital logic, relays, and reed switch position transmitter circuits. Separate power supply modules may be used for these different functions.

Redundancy will be available using diode auctioneering which provides load transfer upon module failure. Faults in one half of a redundant supply will not adversely affect the other from operating normally. Redundant modules can be replaced while the power supply remains energized without disturbing the powered system.

The power supply will have overvoltage and undervoltage protection. Undervoltage and overvoltage will be indicated.

The power supply will be configured so that it is not near its maximum loading to extend its life. Supplemental cooling will be provided if needed to also extend the life of components.

Sufficient ride through time (approximately 10 milliseconds) will be provided to allow momentary loss of external power due to bus transfer.

Soft start will be provided so that external sources powered by inverters will not be adversely affected.

The use of Polyvinyl Chloride (PVC) will be minimized.

5.2.4 Communication Subsystems

There are three types of communications that will be used in the Common Q™ Platform:

- AF100 network communications for intradivisional communications
- HSL serial communications for interdivisional communication
- External communications

5.2.4.1 Advant Field Bus 100 (AF100)

The AF100 network is used for intradivisional communications. Advant Fieldbus 100 is a high performance fieldbus, which is used for communication between Advant Controllers and the Flat Panel Display System. The AC 160 controllers and the Flat Panel Display System can be connected as nodes on the AF100 network.

The Advant Fieldbus 100 supports two different kinds of communication: process data and message transfer. Process data is dynamic data used to monitor and control a process, while message transfer is used for parameters, program loading and for diagnostic purposes.

For a description of the deterministic characteristics of the AF100 communications refer to subsection 5.3.1.4.

5.2.4.2 High Speed Link (HSL)

Data communications between PM646A processor modules from one Common Q™ redundant division to another is referred to as planned data exchange. Several PM646A processor modules can communicate with one another via its high speed serial links (HSL). Within the PM646A processor module construction are two printed circuit boards:

1. The processor module itself which contains the flashed base software, and

2. A communication module that performs the HSL communications between PM646A processor modules.

Each PM646A processor module has two high speed serial links (HSL). Each HSL consists of two half duplex serial communication lines. Therefore the PM646A processor module uses four HSL channels: two transmit and two receive channels. The transmit data is the same on both links because it is sent out in parallel.

For a more detailed discussion of the HSL operation, refer to the subsection 5.3.1.3, High Speed Link Communications.

5.2.4.3 External Communications

External communications are communications between the Common Q™ platform and external computer systems. The Flat Panel Display system is the interface component between the Common Q™ Platform and these external systems. The interface to external systems can be either serial or Ethernet.

The purpose of external communications is to send calculated data from the Common Q™ system to the external system. Because of the hardware separation between the two communication paths in the Flat Panel Display System (i.e., separate Ethernet/serial interface card and AF100 interface card) and software separation (i.e., separate buffers for each interface), the propagation of fatal errors to the safety algorithms in the AC160 due to communication faults from non-safety systems interacting with the Common Q™ system is avoided. The Flat Panel Display System meets the requirements of IEEE 7-4.3.2 Annex E for communication independence.

5.3 DETERMINISTIC PERFORMANCE

This section describes how the Common Q™ Platform is designed to guarantee deterministic performance. The AC160 subsystem design requires deterministic operation for the following reasons:

- It will execute Class 1E protection or monitoring algorithms.
- It will interface to the PPS/RPS or Reactor Trip System and to the Annunciator System.

Refer to subsection 5.4.1.1 for a description of verification checks performed on the downloaded software.

Because the Flat Panel Display System is used for HMI input and output and is used for transmission of data to non-safety monitoring systems, the design requires less determinism in its operation, but the design must ensure that errors or failures in its hardware and software components are isolated from the AC160-based subsystems.

The following subsections describe how these goals are achieved in the design of these two building blocks.

5.3.1 AC160 Deterministic Performance

5.3.1.1 AC160 Application Program Execution Period

[

]a,c

[

]a,c

a,c

Figure 5-17 AC160 Application Program Execution Period

[

]a,c

5.3.1.2 Access to the AC160 Backplane

[

]a,c

a,c

Figure 5-18 AC160 Hardware

[

]a,c

5.3.1.3 High Speed Link Communications

[

]a,c

5.3.1.4 AF100 Communications

[

]a,c

[

]a,c

5.3.1.4.1 Process Data Transfer

[

]a,c

a,c

Figure 5-19 [ ]a,c

[

]a,c

5.3.1.4.2 Message Transfer

[

]a,c

5.3.1.4.3 Bus Master

[

]a,c

5.3.2 Flat Panel Display System

The Flat Panel Display System interfaces to the protection algorithms executing in the AC160 subsystem portions of Common Q™ by way of the AF100 network, and it interfaces to non-safety systems by an optically isolated datalink. The Flat Panel Display System must ensure the integrity of its interface to the safety-critical side and ensure that its interface to non-safety systems and its own operation does not adversely effect the operation of the safety-critical side. The Flat Panel Display System meets the requirements of IEEE 7-4.3.2 Annex E for communication independence.

5.3.2.1 Datalink To External Systems

The datalink connecting the Flat Panel Display System to external systems can be either a serial or Ethernet datalink. In the case of a serial link, the communication shall be unidirectional broadcast.

The Ethernet datalink protocol is unidirectional protocol (UDP)/IP, thus isolating the non-safety system from the Flat Panel Display System of faults associated with the communication.

There are two communication interfaces in the Flat Panel Display System which are isolated from each other (i.e., two separate interface cards). Should a failure in communications to a non-safety system occur causing the Flat Panel Display System to halt, the safety-critical applications in the AC160 controllers can continue to operate unimpeded. It is possible that the Flat Panel Display System has control of the AF100 bus master at the time it ceases to operate. As discussed in previous sections, the bus master can be assumed by another node if it fails, so the AF100 network can continue to operate without the Flat Panel Display in operation.

5.4 SYSTEM DIAGNOSTICS

5.4.1 AC160 Diagnostics

5.4.1.1 Processor

One component of the AC 160 base software is the internal diagnostics that are executed continuously during controller operation. Diagnostic functions monitor system operation and report any faults detected. The monitoring functions include an internal watchdog, bus supervision and memory checking. 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 AC 160 database element when referenced within an application program.

During system start-up, the hardware of the PM646A processor module is tested. The following tests are performed:
[

]a,c

[

]a,c

5.4.1.2 I/O

Diagnostics of I/O and communication modules are executed by interrogating all modules for errors. The S600 modules have self-contained diagnostics the results of which are reported to the PM646A base software diagnostics routine via a device status word. Refer to Reference 19 for a description of the I/O module diagnostics.

5.4.1.3 High Speed Link

High Speed Link (HSL) diagnostics are executed to detect physical layer failures and failures of the communication link to another PM646A processor module. The physical layer of the HDLC protocol is secured through a cyclic redundancy check (CRC). If three (3) bad CRCs occur consecutively, the HSL will be marked failed. A keep-alive signal is transmitted over the HSL every 25 milliseconds if an application program has requested no transmission. When a PM646A processor module has not received data for 250 milliseconds, the HSL is considered failed. All detected errors are reported to the application program.

5.4.1.4 AF100

The AF100 uses bus mastership to continuously monitor the status of the nodes on the bus. For a description of the operation of the bus master, refer to subsection 5.3.1.4.3.

The AF100 communication interface, CI631, monitors the validity of the data sets it is suppose to receive. If no data has been received for four cycles for the data set (i.e., 4 X CYCLETIM designation for the data set) or when the communication interface has 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.

5.4.1.4.1 AF100 Interface (CI631)

The AC160 CI631 configuration provides on-line surveillance of this card to ensure that it is in operational condition. The CI module contains self-diagnostics, and reports any errors to the application in the PM646A.

This error report can be used for alarm or screen indication to direct technicians to the specific AC160 node that has the CI 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 PM is able to reboot the CI, the CI will return to service and there will be no red light.

5.4.2 Flat Panel Display Diagnostics

Each application program interface (API) call [ ]^{a,c} provides a status. The application program will have an error handler to appropriately dispatch the error when it occurs. The Appendices will address the disposition of errors.

5.4.3 Surveillance Testing

[

]^{a,c}

[

]a,c

5.4.3.1 Passive Testing

Passive testing requires the AC160 processors to periodically transmit sufficient data to the ITP so that it can validate the correct operation of the processors and compare its divisional data with corresponding data from other divisions (via other ITPs). Any deviations or errors are transmitted to the MTP for display and alarm.

5.4.3.2 [ ]a,c

[

]a,c

5.4.4 Application Watchdog

The design of the Common Q™ platform includes a hardware watchdog function within the processor module to override the activation outputs of the safety system should the processor halt. The AC160 internal diagnostics that monitor the activation and execution of each application task eliminates the need for application level software watchdog counters. Application level watchdog timers do not need to be implemented for HSL and AF100 communications either because the AC160 internal diagnostics include "keep-alive" monitoring of these communication interfaces and the data that they transmit and receive. The Appendices will address the disposition of errors.

For the operator or technician, a blinking heartbeat symbol on the Flat Panel Display shall provide indication that the display system is in operation.

5.5 SYSTEM INTERFACES

The following example (see Figure 5-20) is used to illustrate the use of Common Q™ building blocks to design a system. The example chosen is a possible implementation of the Core Protection Calculator System (refer to the CPCS Appendix for the official CPCS Common Q™ configuration).

Overview

The Core Protection Calculator System (CPCS) is composed of four divisions. Each CPCS division contains a processor to read field inputs, share Control Element Assembly (CEA) position signals (RSPTs), perform Departure from Nucleate Boiling Ratio (DNBR) and Local Power Density (LPD) calculations, and provide a trip output (digital output) for 2/4 logic in the RPS. For each division, there is a CPCS Operator's Module in the control room and a local display for maintenance and test.

CPC Processor

[

]a,c

[

]a,c

a,c

Figure 5-20 [ ][a,c]

5.6 COMPLIANCE TO INTERIM STAFF GUIDANCE HIGHLY INTEGRATED CONTROL ROOM – COMMUNICATIONS (ISG #4-HICRC)

The purpose of this section is to address compliance to the twenty communication criteria established in Interim Staff Guidance Highly Integrated Control Room- Communications (ISG #4-HICRc) for the communication technologies of the Common Q™ platform. [

]a,c

5.6.1 ISG-4 Position 1

ISG-4, Position 1 states:

> *"A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division voting logic must receive inputs from multiple safety divisions."*

Compliance

[

]a,c

a,c

Figure 5-21 PM646A Architecture

5.6.2 ISG-4 Position 2

ISG-4, Position 2 states:

> *"The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division."*

Compliance

[

]a,c

a,c

Figure 5-22 HSL Communication

[

]a,c

5.6.3 ISG-4 Position 3

ISG-4, Position 3 states:

> *"A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of*

readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration."

Compliance

[

]a,c

5.6.4 ISG-4 Position 4

ISG-4, Position 4 states:

"The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory."

Compliance

[

]a,c

a,c

Figure 5-23 [ ]a,c

[

]a,c

5.6.5 ISG-4 Position 5

ISG-4, Position 5 states:

> *"The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed."*

Compliance

[

]a,c

5.6.6 ISG-4 Position 6

ISG-4, Position 6 states:

> *"The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division."*

Compliance

As described in the criteria above and in subsection 5.2.1.2.1 the operation of the PM646A PS and CS fulfill this criteria.

5.6.7 ISG-4 Position 7

ISG-4, Position 7 states:

> *"Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior."*

Compliance

[

]a,c

5.6.8 ISG-4 Position 8

ISG-4, Position 8 states:

> *"Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions."*

Compliance

As described in the criteria above and in subsection 5.2.1.2.1 the operation of the PM646A PS and CS fulfill this criteria.

5.6.9 ISG-4 Position 9

ISG-4, Position 9 states:

> *"Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device."*

Compliance

[

]a,c

5.6.10 ISG-4 Position 10

ISG-4, Position 10 states:

> *"Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g., engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor/ shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes."*

Compliance

[

]a,c

[

]a,c

5.6.11 ISG-4 Position 11

ISG-4, Position 11 states:

> *"Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence."*

Compliance

[ ]a,c

5.6.12 ISG-4 Position 12

ISG-4, Position 12 states:

> *"Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:*

Compliance

- Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.

  [

  ]a,c

[

]a,c

- Messages may be repeated at an incorrect point in time.

[

]a,c

- Messages may be sent in the incorrect sequence.

[

]a,c

- Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.

[

]a,c

- Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.

[

]a,c

- Messages may be inserted into the communication medium from unexpected or unknown sources.

[

]a,c

- Messages may be sent to the wrong destination, which could treat the message as a valid message.

[

]a,c

- Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.

  [ ]a,c

- Messages may contain data that is outside the expected range.

  [ ]a,c

- Messages may appear valid, but data may be placed in incorrect locations within the message.

  [ ]a,c

- Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).

  [ ]a,c

- Message headers or addresses may be corrupted.

  [ ]a,c

5.6.13 ISG-4 Position 13

ISG-4, Position 13 states:

> *"Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting*

methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor."

Compliance

[

]a,c

5.6.14 ISG-4 Position 14

ISG-4, Position 14 states:

"Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified."

Compliance

[

]a,c

5.6.15 ISG-4 Position 15

ISG-4, Position 15 states:

"Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not."

Compliance

[

]a,c

5.6.16 ISG-4 Position 16

ISG-4, Position 16 states:

> *"Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 CFR. Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)"*

Compliance

[

]a,c

5.6.17 ISG-4 Position 17

ISG-4, Position 17 states:

> *"Pursuant to 10 C.F.R. § 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified."*

Compliance

[

]a,c

5.6.18 ISG-4 Position 18

ISG-4, Position 18 states:

> *"Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication."*

Compliance

The HSL communication has been qualified for use in safety applications. A Failure Modes and Effect Analysis (FMEA) is performed for each project that deploys the Common Q™ Platform. This FMEA includes the HSL communication.

5.6.19 ISG-4 Position 19

ISG-4, Position 19 states:

> *"If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing."*

Compliance

[

]a,c

5.6.20 ISG-4 Position 20

ISG-4, Position 20 states:

> *"The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing."*

Compliance

[

]a,c

6 SOFTWARE QUALITY

Computer software is essential to the design and operation of a Common Q™ System. [

]a,c

[

]a,c

6.1 SOFTWARE QUALITY ASSURANCE

[

]a,c

[

]a,c

6.2 SOFTWARE CONFIGURATION MANAGEMENT

[

]a,c

6.2.1 [ ]a,c

[

]a,c

[

]a,c

a,c

Figure 6-1 [ ]a,c

6.2.2 Previously Developed Software

[

]a,c

[

]a,c

6.3 SOFTWARE VERIFICATION AND VALIDATION

[

]a,c

6.3.1 [ ]a,c

[

]a,c

[

]a,c

6.3.2 [ ]a,c

[

]a,c

[

]a,c

6.3.3 [ ]a,c

[

]a,c

6.3.3.1 [ ]a,c

[

]a,c

[

]a,c

6.3.3.2 [ ]a,c

[

]a,c

6.3.3.3 [ ]a,c

[

]a,c

6.3.3.4 [ ]a,c

[

]a,c

6.4 OPERATION AND MAINTENANCE

[

]a,c

7 EQUIPMENT QUALIFICATION

The qualification program plan for the Common Q™ Platform equipment will be implemented using a combination of type-test and/or analyses. Where type testing is the qualification method, it will be performed on non-deliverable equipment. The planned Common Q™ Platform overall qualification phases are depicted in Figure 7-1. The Common Q™ Platform equipment qualification program shall subject the equipment to Component Cycling, EMI/RFI testing, environmental testing, and seismic testing.

a,c

Figure 7-1 [ ]a,c

A qualification plan will be issued defining the details associated with each phase of the qualification test. Figure 7-2 shows an overview of a typical qualification test timeline for the Common Q™ equipment.

a,c

Figure 7–2 [ ][a,c]

[

]a,c

7.1 COMPONENT CYCLING AND BURN-IN

Electromechanical aging (component cycling) could be a factor for some of the equipment and the appropriate test specimens will be aged depending on its planned application to simulate an end of life condition. The component cycling test will be the first qualification test performed.

An electrical burn-in test will be conducted on the equipment prior to testing to alleviate any infant mortality that may exist. The details of this burn in test will be defined in the qualification test plan.

7.2 ENVIRONMENTAL TESTING

The Common Q™ equipment will be qualified based on the assumption that the equipment will be installed in a mild environment. The mild environment is an environment expected as a result of normal and abnormal in service conditions where seismic is the only design basis event (DBE) of consequence.

The Common Q™ equipment environmental qualification will be demonstrated by a combination of type testing and analysis. The environmental qualification will be performed to satisfy the technical requirements of IEEE 323 as supplemented by RG 1.89, CENPD-255-A (Reference 6) and WCAP 8587 (Reference 26).

The expected room abnormal temperature and humidity parameters, where the Common Q™ cabinets will be installed are tabulated in Table 7-1. These environmental parameters envelope the expected room abnormal environment identified in CENPD-255-A (Reference 6) and WCAP 8587 (Reference 26).

The environmental qualification parameters for Common Q™ equipment installed in a cabinet, corresponding to the room ambient environment identified in Table 7-1, are tabulated in Table 7-2 and shown in Figure 7-4. These temperature and humidity parameters envelope requirements specified in Figure 7-3 and margin to satisfy the intent of IEEE 323-1983 (Reference 25 in Section 4).

As noted in IEEE 323-1983 Section 6.2.3 margin may be applied, if needed, in a number of ways, including increasing the test temperature range and repeating test cycles. The test margin is required to address reasonable uncertainties in demonstrating satisfactory performance and normal variations in commercial production to ensure that the equipment will perform under abnormal conditions specified. [

]a,c

The Common Q™ equipment will be subjected to abnormal environmental testing to meet the qualification requirements specified in Table 7-2 and shown in Figure 7-4. An evaluation will be performed for each application, if needed, to ensure that the design basis temperature of the Common Q™ equipment is not exceeded when installed in the cabinet. The evaluation, based on the data, will demonstrate that the equipment temperature specifications are not exceeded within the cabinet/enclosure when the cabinet/enclosure is subjected to the environmental conditions specified in Table 7-1.

a,c

Table 7-1 Cabinet Environmental Design Requirements

a,c

Table 7-2 Common Q™ Equipment Environmental Design Requirements

Table 7-2 (cont.) Common Q™ Equipment Environmental Design Requirements

a,c

a,c

Figure 7-3 Original Environmental Test Profile

a,c

Figure 7-4 Modified Environmental Test Profile

7.3 SEISMIC TESTING

[

]a,c

7.3.1 [ ]a,c

[

]a,c

7.4 ELECTROMAGNETIC INTERFERENCE (EMI) TESTING

The baseline Common Q™ equipment will be qualified in accordance with MIL Std 461D, MIL Std 462D, and as augmented by EPRI TR-102323. Susceptibility and emissions testing of the equipment will be performed for both conducted and radiated signals. The tests will be performed on each system in various modes of operation such that successful completion of the test demonstrates that the safety system function has not been compromised and the equipment performs within its design specifications.

The basis for selecting the specific tests, test methods, test levels and susceptibility criterion for the baseline equipment will be based on the EPRI TR-102323 guidelines.

Any new additions to the baseline equipment, whether they are new modules/devices or enhancements to existing modules/devices will be tested consistent with the requirements of RG 1.180, Rev. 01. No regression EMI testing will be performed; rather the requirements as defined in RG 1.180, Rev. 01 will be followed.

If the tests show that susceptibilities exist in the range of interest, then the following assessments shall be performed:

1. Further evaluations of test data and analyses shall be performed which determine that the susceptibilities pose no hazard to the safe operation of the equipment.

2. If necessary, a site survey shall be required to verify the actual environment at the equipment location does not exceed the susceptibility level.

3. If necessary, restrictions on the specific use of the equipment will be defined.

8 EQUIPMENT RELIABILITY

[

]a,c

8.1 FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

[

]a,c

[

]a,c

[

]a,c

8.2 MEAN TIME BETWEEN FAILURES (MTBF) ANALYSIS

[

]a,c

Table 8-1 [ ]a,c		

a,c

8.3 OPERATING HISTORY

[

]a,c

8.3.1 [ ]a,c

[

]a,c

[

]a,c

a,c

Figure 8-1 ABB Product Migration

[

]a,c

[

]a,c

a,c

[

]a,c

Table 8-2 [ ][a,c] a,c

Table 8-2 [ ][a,c] a,c

Table 8-2 [ ][a,c] a,c

Table 8-2 [ ][a,c] a,c

[

]a,c

9 DEFENSE-IN-DEPTH AND DIVERSITY

The Common Q™ building blocks form a basis that can be used in the design of safety systems. The defense-in-depth strategy is described in the Integrated Solution Appendix.

10 COMMERCIAL GRADE DEDICATION PROGRAM

10.1 SCOPE

[

]a,c

[

]a,c

10.2 SOFTWARE ASSESSMENT PROCESS FOR SOFTWARE COMMERCIAL GRADE DEDICATION

[

]a,c

10.2.1 [ ]a,c

[

]a,c

10.2.1.1 [ ]a,c

[

]a,c

[

]a,c

10.2.1.2 [ ]a,c

[

]a,c

10.2.1.3 [ ]a,c

[

]a,c

[

]a,c

10.2.1.4 [ ]a,c

[

]a,c

10.2.1.5 [ ]a,c

[

]a,c

10.2.1.6 [ ]a,c

[

]a,c

10.2.1.7 [ ]a,c

[

]a,c

10.2.1.8 [ ]a,c

[

]a,c

10.2.2 [ ]a,c

[

]a,c

10.2.3 [ ]a,c

[

]a,c

10.2.4 [ ]a,c

[

]a,c

10.3 SOFTWARE COMMERCIAL DEDICATION

[

]a,c

[

]a,c

10.4 HARDWARE COMMERCIAL DEDICATION

[

]a,c

[

]a,c

10.5 CONFIGURATION MANAGEMENT

[

]a,c

11 COMMON Q™ PLATFORM COMPONENTS

[ ]a,,c

Table 11-1 [ ]a,c a,c

Table 11-1 [ ][a,c] a,c

12 FUTURE PLATFORM CHANGES

[

]a,c

13 CONCLUSIONS

[

]a,c

APPENDIX A
LIST OF APPENDICES

The following appendices describe specific implementations of Common Q™ technology.

1. Common Qualified Platform Post Accident Monitoring Systems
2. Common Qualified Platform Core Protection Calculator System
3. Common Qualified Platform Digital Plant Protection System
4. Common Qualified Platform Integrated Solution

The following appendix lists the evolutionary changes to the Common Q™ Platform since the original qualification.

5. Common Qualified Platform Record of Changes