CENPD-396-NP
REVISION 01

COMMON QUALIFIED PLATFORM

MAY 2000

CE NUCLEAR POWER LLC

Legal Notice

THIS REPORT WAS PREPARED AS AN ACCOUNT OF WORK PERFORMED BY CE NUCLEAR POWER LLC. NEITHER CE NUCLEAR POWER LLC NOR ANY PERSON ACTING ON ITS BEHALF:

- MAKES ANY WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED INCLUDING THE WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY, WITH RESPECT TO THE ACCURACY, COMPLETENESS, OR USEFULNESS OF THE INFORMATION CONTAINED IN THIS REPORT, OR THAT THE USE OF ANY INFORMATION, APPARATUS, METHOD OR PROCESS DISCLOSED IN THIS REPORT MAY NOT INFRINGE PRIVATELY OWNED RIGHTS; OR

- ASSUMES ANY LIABILITIES WITH RESPECT TO THE USE OF, OR FOR DAMAGES RESULTING FROM THE USE OF, ANY INFORMATION, APPARATUS, METHOD OR PROCESS DISCLOSED IN THIS REPORT.

Westinghouse Electric Company

CE Nuclear Power LLC

Windsor, Connecticut 06095

COMMON QUALIFIED PLATFORM

TOPICAL REPORT

CENPD-396-NP, Rev. 01

May 2000

TABLE OF CONTENTS

1. Purpose

The purpose of this report is to describe a nuclear safety related I&C platform designed by CE Nuclear Power. 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, Core Protection Calculator Systems, Reactor Protection Systems, Plant Protection Systems, 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. One solution also allows obsolescence management for the next 20 years.

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.

CE Nuclear Power's licensing experience includes CPCs at eleven plants and other digital I & C safety related systems such as the Advanced Light Water Reactor (ALWR) design and System 80^+, for both the Reactor Protection System functions and for the Engineered Safety Features functions. System 80^+ received NRC licensing approval in 1994 for these digital safety systems. The system 80^+ licensing process has addressed the key issues of:

- An environmental, seismic, and electromagnetic interference (EMI) testing and qualification program for digital I&C systems that is acceptable to the NRC
- A commercial grade dedication process for computer hardware and software that is acceptable to the NRC
- A verification and validation (V&V) process for computer software that is acceptable to the NRC
- A design and defense in depth evaluation process that addresses the NRC's concerns with respect to the potential for a common mode failure related to software and that meets current industry standards and licensing guidelines

In response to current utility needs, Common Q products will 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 4. 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. References

3.1 ABB PPC Document No. GKW F 310 708, "Advant Power Reliability and Availability, Reliability Data Sheet, Advant Controller 160 Including S600 I/O"

3.2 ABB Combustion Engineering Nuclear Operations Quality Assurance Manual for Service Related Activities, QAM-100, Fourth Edition

3.3 ABB Combustion Engineering Nuclear Operations Quality Procedure Manual, QPM-101

3.4 ABB Combustion Engineering Nuclear Power Instrumentation, Controls and Electrical Equipment Quality Assurance Program Description, QAM-400

3.5 CE Nuclear Power Document CE-CES-195-P, Software Program Manual For Common Q Systems, Revision 01

3.6 CENPD-255-A, Class 1E Qualification – Qualification of Class 1E Electrical Equipment, Revision 3, October 1985.

3.7 CEN-356(V)-P, Revision 01-P, Modified Statistical Combination of Uncertainties, July, 1987

3.8 ABB Advant Document 3BDS 003 340 B, "AC110 System Software Extension"

3.9 ABB Advant Document 3BDS 005 556R1, "Data Base Elements Advant Controller 160 Reference Manual"

3.10 ABB Advant Document 3BDS 005 557R1, "PC Elements Advant Controller 160 Reference Manual"

3.11 ABB Advant Document 3BDS 014 721 R101, "Advant Controller 160 Product Guide"

3.12 ABB Advant Document 3BDS 005 555R1, "Advant Controller 160 Version 1.2 User's Guide"

3.13 ABB Advant Document 3BSE 000 506R0201, "Advant Fieldbus 100 User's Guide"

3.14 ABB Advant Document 3BSE 009 626R0201, "AMPL Configuration, Advant Controller 100 Series Reference Manual"

3.15 ABB Memo DPPS-97-011, April 17, 1997, Richard M. Manazir, "Minutes of Meeting in Mannheim with ABB Industrietechnik AG, February 17-28, 1997"

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

3.17 QNX Photon microGUI™ Programmers Guide, 2nd Edition, December 1996

3.18 QNX Watcom Compiler & Tools User's Guide, First Edition, July 1996

3.19 S600 I/O Hardware, Advant Controller 160 Reference Manual, 3BDS 005 558R1

3.20 ABB Advant Document GKWF 700 894, "Requirements Specification for ACC Tool for use in RPS Applications of BU Nuclear, Revision 0

3.21 ABB Advant Document GKWF 700 891, " Requirements Specification for AC160 SW-Version 1.3 and Controller HW PM646 for use in RPS Applications for BU Nuclear" , Revision 1

3.22 ABB Atom, AB Report MOD 97 – 1250, "Oskarshamn 1 - Project Mod Evaluation of Collected Operating Experience for Advant Controller 110

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

3.24 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

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

4. Codes And Standards

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

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
1.	RG 1.22 BTP HICB-8 BTP HICB-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 HICB-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	00 02/1972

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		are on a channel level to prevent an operator from inadvertently bypassing a trip function. D. Manual testing for a COMMON Q platform channel is interlocked to prevent testing in more than one redundant channel 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.	
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.	03 09/1978
3.	RG 1.47	USNRC Regulatory Guide – Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems	00 05/1973

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		Annunciator outputs are provided to indicate the bypassing of COMMON Q platform operating or trip channel bypasses where applicable.	
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 5 and 6 and the appendices of this report for system descriptions that implement these criterion. Single failures considered in the designs are addressed in the Failure Modes and Effects Analyses in the appendices.	00 06/1973
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	00 10/1973

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		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.	
6.	RG 1.75 BTP HICB-11	USNRC Regulatory Guide - Physical Independence of Electric Systems The COMMON Q platform conforms to this RG and BTP HICB-11 as described in the IEEE Std 384 compliance statement below in Section 4.26.	02 09/1978
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 8.0 of this report.	01 06/1984
8.	RG 1.97 BTP HICB-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	03 05/1983

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		The Post Accident Monitoring Systems deployed using the Common Q Platform shall conform to these requirements.	
9.	RG 1.100	USNRC Regulatory Guide – Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants The seismic qualification of the 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 8.3 for a further description of the seismic qualification efforts.	02 06/1988
10.	DG 1045	Proposed Revision 3 to Reg. Guide 1.105, "Instrument Spans and Setpoints"	
	BTP HICB-12	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 No.	Document No.	Title/Conformance	Revision No., Issue Date
		(Reference 3.7).	
11.	RG 1.118 BTP HICB-17	USNRC Regulatory Guide - Periodic Testing of Electric Power and Protection Systems The Common Q conforms to this RG, IEEE Std 338 and HICB-17 as described in the compliance statement for RG 1.22, Reference 4.1.	02 06/1978
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 3.5 and refer to Section 7.0 for a further description of the basic elements of the SPM.	01 11/1996
13.	RG 1.153 BTP HICB-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,	1996

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		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 HICB-17 references this Reg. Guide as acceptance criteria.	
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 7 of this report and in the Common Q SPM, Reference 3.5.	1997
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.	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	

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		implementation processes conform to this RG as described in the Common Q SPM.	
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.	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 3.5.	1997
19.	IEEE Std 7-4.3.2	IEEE Standard Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations The Common Q conforms to this standard as augmented by RG 1.152 and described in the conformance statement for RG 1.152, Reference 4.12.	1993

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
20.	ANSI/IEEE Std 279 BTP HICB-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
21.	IEEE Std 323	IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Systems The Common Q conforms to this standard as augmented by RG 1.89 and described in the conformance statement for RG 1.89, Reference 4.7.	1983
22.	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 1.22 and described in the conformance statement for RG 1.22, Reference 4.1.	1987
23.	IEEE Std 344	IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations The Common Q conforms to this	1987

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		standard as augmented by RG 1.100 and described in the conformance statement for RG 1.100, Reference 4.9.	
24.	IEEE Std 379	IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems The Common Q conforms to this standard as augmented by RG 1.53 and described in the conformance statement for RG 1.53, Reference 4.4 A further description of the application of these criterion is provided in Sections 5 and 6 of this report.	1994
25.	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
26.	IEEE Std 384 BTP HICB-11	IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits The Common Q platform conforms to this standard as augmented by	1992

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		RG 1.75 and Branch Technical Position HICB-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 criterion is provided in Sections 5 and 6 of this report.	
27.	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 (4.22), -383 (4.25), -384 (4.26), and –603 (4.29).	1982
28.	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”	1974

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		applied on the face of each document and drawing.	
29.	IEEE Std 603 BTP HICB-3 BTP HICB-5 BTP HICB-9 BTP HICB-10 BTP HICB-11 BTP HICB-12 BTP HICB-17 BTP HICB-18 BTP HICB-19 BTP HICB-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 00, 12/1985 and Branch Technical Positions HICB-3, 5, 9-12, 17-19 and 21.	1991
30.	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 8 of this report and the conformance statements for IEEE Std 323 and RG 1.89.	1980
31.	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 7 of this report and the Common Q SPM, Reference 3.5.	1989

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
32.	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 7 of this report and the Common Q SPM, Reference 3.5.	1990
33.	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 3.5.	1993
34.	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 7 of this report and in the Common Q SPM, Reference 3.5.	1986
35.	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 3.5.	1987

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
36.	IEEE Std 1028	IEEE Standard for Software Reviews and Audits The Common Q SPM, Reference 3.5, describes the software reviews and audits that will be performed per this standard.	1988
37.	IEEE Std 1042	IEEE Guide To Software Configuration Management The Common Q SPM, Reference 3.5, includes the SCMP for Common Q systems, and uses this standard as a guide.	1987
38.	IEEE Std 1074	IEEE Std for Developing Software Life Cycle Processes See response to Reg. Guide RG 1.173, Ref. 4.18.	1995
39.	ISA-S67.04	Setpoints For Nuclear Safety Related Instrumentation Used in Nuclear Power Plants For digital to digital replacements (i.e., CPC, 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	1994

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		analyses by the replacement system.	
40.	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 8.3 of this topical report) include testing using the oscillatory SWC test wave as defined in Section 2.2 of this standard.	1989
41.	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 8 of this report) Commercial-grade survey of supplier, source verification, and acceptable supplier/item performance record is	1988

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		part of the Hardware and Software Commercial Grade Dedication Processes described in Section 11 and in Reference 3.4, QOP 401.	
42.	EPRI Topical Report TR-102323	EPRI Guidelines for Electromagnetic Interference Testing in Power Plants The Common Q equipment conforms to this standard as described in Section 8.3 of this topical report. Susceptibility and emissions of the equipment are determined for both conducted and radiated signals.	1997
43.	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
44.	MIL-STD-461D	Military Standard Electromagnetic Interference Characteristics Requirements for Equipment The Common Q equipment is qualified in accordance with this Mil Std as augmented by EPRI TR-102323, Reference 4.42 and further described in Section 8.3 of this	1993

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		topical report.	
45.	MIL-STD-462D	Military Standard Electromagnetic Interference Characteristics, Measurement of The Common Q equipment is qualified in accordance with this MIL STD as augmented by EPRI TR-102323, Reference 4.42 and further described in Section 8.3 of this topical report.	1993
46.	BTP HICB-14	Guidance on SW 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.	
47.	BTP HICB-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 11.	
48.	BTP HICB-19	Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems Defense-in-Depth and Diversity for	

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		specific systems are discussed in the Integrated Solution Appendix of this Topical Report.	
49.	BTP HICB-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.	
50.	EPRI TR-107330	Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants The appendices in this topical report shall contain a conformance matrix indicating how the Common Q platform complies with this specification.	1998
51.	NUREG-0737	Clarification of TMI Action Plan Requirements All Common Q Post Accident Monitoring Systems shall meet these requirements.	1980
52.	NUREG-0800	Chapter 7 of the USNRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Rev 4	1997

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		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.	
53.	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
54.	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., [ ] and ABB Advant). Section 11.1 discusses the Software Commercial Grade Dedication process.	1996
55.	10 CFR 50 Appendix A	GDC 1: "Quality Standards and Records" The Common Q Quality Assurance	

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		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.	
		GDC 19: "Control Room" A Control Room interface (Flat Panel Display System) is provided for each Common Q system.	

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		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"	

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		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.	

Reference No.	Document No.	Title/Conformance	Revision No., Issue Date
		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.	

5. 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 6. 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 PM646 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 5 is a generic representation of how the building blocks are configured for a safety system.

[

]

ITP: Interface and Test Processor WDT: Watchdog Timer FOM: Fiber Optic Modem

Figure 5

5.1 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 used in the Common Q applications is the PM646.

AC160 is fully modular with modules mounted in 19" subracks. A typical Common Q configuration consists of processor module(s), 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 can be used concurrently in one controller. 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 channels of the safety system. These data links are electrically isolated using fiber optic cable. The HSL is discussed in Sections 5.5 and 6.2.5.2.

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 Section 6.2.1.2.

Although the processor module has a built in watchdog timer module, an independent external watchdog timer 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 channel 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 module is discussed in Section 6.2.4.

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

5.1.1 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 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 Section 6.2.1.2 for more information on the AC160 software.

The Advant Controller 160 software consists of a real-time operating system [ ], task scheduler, diagnostic functions, communication interfaces, and user application programs, all of which reside on flash PROM in the PM646 processor module. Refer to Section 6.2.1.2 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.

[

] 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 CPU module flash PROM (non-volatile memory).

[

]

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 Section 6.2.1.2.2 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.

[1] Only applicable to the AC400 series controllers which are not part of Common Q

5.1.2 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 Section 6.2.1.1.3.

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.

5.1.3 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 3.5 for a discussion on software classification. It communicates with the MTP and the other AC160 chassis in the channel (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-channel system to communicate to one another. The fiber optic data links provide isolation and the ITP provides communication buffering to protect against external channel 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 channel data is compared in the ITP for consistency. The status of the other channels is checked before any channel test is initiated.

5.2 Power Supply

The power supply is based on a 19" rack assembly with plug-in 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.

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

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

5.3 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.

[

]

5.3.1 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 3.5.

[

]

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

5.3.2 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 channel. The MTP provides the means for the operator or technician to bypass a channel, initiate automatic 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.

5.3.3 Operators 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).

5.4 AF100 Communication

The Advant Fieldbus 100 (AF100) is a high performance bus, which will be used for intrachannel communications and, for ITP to ITP interchannel communications. Interchannel communications will be on a separate, isolated AF100 bus. Each bus will be fully redundant.

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

5.5 High Speed Link (HSL) Communication

Each PM646 module actually contains both an application processor and a dedicated HSL communications processor. Depending on the system configuration requirements, one PM646 module may perform both application and communication processing.

The HSL will be used to transmit broadcast data to other channels in a multi-channel system. The HSL is a serial RS 422 link using High Level Data Link Control (HDLC) protocol with a 3.1 Mbits/second transfer rate. Each PM646 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 channels. Receive links on multiple PM646s are used to receive data from each of the other channels.

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 interchannel communication.

6. Common Q Platform

6.1 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.

6.2 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. Watchdog Timer Module
5. Communication Subsystems

6.2.1 Advant Controller

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

6.2.1.1 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 rear mounting. A minimal Advant Controller 160 configuration consists of one or two subracks containing the processor module, a power supply module and up to 18 I/O and communication modules.

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 interface modules 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.

6.2.1.1.1 PM646 Processor Module

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

The subracks and cable duct 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.

[

]

Processor Module

Although four different types of processor modules are available for Advant Controller 160, only the PM646 is intended to be used. The AC160 can be configured with PM646 modules running redundantly in a hot-standby/automatic failover mode or with PM646 modules running asynchronously.

[

]

The PM646 features important for Common Q Applications are the following:

- The PM646 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 PM646 processor modules contain two RS-422 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) can 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 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 relay in the processor module. For Common Q applications, stopping the processor will also cause an external and independent watchdog timer to timeout.

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 channel DB elements.

[

]

The following indicators are on the front of the PM646 processor module:

- The green LED, RUN1, indicates that the processing section of the PM646 is operational.
- The green LED, RUN2, indicates that the communication section of the PM646 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).

6.2.1.1.2 PM646 High Speed Link Communication Interface

The PM646 processor module contains two high-speed communication links (Link 1 and Link 2) provided for signal exchange. The HSLs are serial RS-422 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 channels of the safety system. The data links are isolated using fiber optic modems.

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.

6.2.1.1.3 Input/Output Subsystem

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, pulse counting, position measurement and rotational speed measurement applications. The process signals are connected to the front of the I/O modules.

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 3.12.

All I/O modules may be replaced 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

[

]

Analog Output Modules

[

]

Digital Input Modules

[

]

Digital Output Modules

[

]

Pulse Counting Module

[

]

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 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.

Bus extender CI615

In addition to its function as a bus extension, the bus extender module CI615 installed in the basic station (i.e., the station with the processor modules) contains the communication and bus cable supervision functions.

- The green LED (RUN) indicates that the bus extender is operational.
- The red LED (FAULT) indicates a severe fault and normally the bus extender module must be replaced.
- The green LED (TRANSFER) indicates, by flashing, data read and write via the extension bus.

If the green LED (TRANSFER) on a CI610 does not light, all outputs on the I/O station are set to "0".

6.2.1.2 AC160 Software Description

The Advant Controller 160 Software consists of a real-time operating system [ ], AC160 task scheduler, diagnostic functions, communication interfaces, and user application programs, all of which reside on flash PROM in the PM646 processor module. Refer to section 6.4.1 for a description of diagnostic functions, and sections 6.3.1.2-4 for a description of the communications.

6.2.1.2.1 Base Software

Processor system software consists of the standard AC 160 system software products developed by ABB Automation Products, GmbH[

]. The system software [ ] 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 6.2.1.2-2.

[

]

Figure 6.2.1.2-2 Base Software Identification

There are software options available in the Base Software that add functionality to the PLC which can be enabled or disabled. Common Q applications are not expected to require any options to the base software.

6.2.1.2.1.1 [ ] Real Time Operating System

[

]

6.2.1.2.1.2 AC160 Kernel

[

6.2.1.2.1.2.1 Processor Section Software Description

[illegible]

6.2.1.2.1.2.2 Communication Section Software Description

]

6.2.1.2.1.3 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. [

]

6.2.1.2.2 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.

6.2.1.2.2.1 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 PM646 application program. It has a separate cycle time than the CONTRMs. It represents the transfer rate of data between the PM646 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.

[

]

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

6.2.1.2.2.2 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 Advant Controller 160 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)

6.2.1.2.3 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 3.9 and 3.10.

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.

6.2.1.2.3.1 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 3.5).

6.2.1.2.3.2 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 AC160 tool AC160ILO. Reference 3.8 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 7 for *protection* class software and the Software Program Manual (Reference 3.5).

6.2.2 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, and displaying system status.

6.2.2.1 Flat Panel Display 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.

6.2.2.1.1 Single Board Computer

The single board computer is based on [ ]. 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.

6.2.2.1.2 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.

6.2.2.2 Flat Panel Display Software Description

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

6.2.2.2.1 Operating System

[

]

6.2.2.2.2 Graphical User Interface

[

]

Each Common Q system will have specific HMI response time requirements. The acceptance tests for a specific Common Q application will validate the drawing API performance.

6.2.2.2.3 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.

6.2.2.2.3.1 C Application Programming Tools

The [ ] enforces the development of application programs in ANSI C (ANSI X3.159-1989, "American National Standard for Information Systems – Programming Language 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 ANSI C.

6.2.2.2.3.2 Display Building Tools

The [ ] 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, [ ] for the runtime implementation of the display. [ ]

6.2.2.3 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)

6.2.2.3.1 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 ANSI C [ ]. The OM is a control room device that allows operators to monitor the system channel.

6.2.2.3.2 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 ANSI C and units generated by [ ] 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

6.2.2.3.2.1 Manually Initiated Automatic Tests

The MTP provides the means for the operator to bypass a channel and initiate automatic tests (tests controlled by the system). These initiations shall be transmitted to the Interface and Test Processor (ITP – an AC160 processor in the Common Q platform) through the AF100 network. The ITP shall transmit the results of the test 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).

6.2.2.3.2.2 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.

6.2.2.3.2.3 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.

6.2.3 Power Supply

The power supply is based on a 19" rack assembly with plug modules. Various modules are available to accommodate the different output voltages anticipated. The modules will be similar in design to and based on prior power supply components and design.

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 bumpless transfer upon module failure. 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 overvoltage and overtemperature 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 hold up time (approximately 40 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 PVC will be minimized.

6.2.4 Watchdog Timer Module

An external and independent watchdog timer module is used to monitor the activity of the processing system. The watchdog timer module has a separate timing circuit and detects the lack of activity. Depending on the specific system application, the watchdog timer can be used to annunciate a failure, actuate a channel 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.

6.2.5 Communication Subsystems

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

- AF100 network communications for intrachannel communications
- HSL (High Speed Link) serial communications for interchannel communication,
- External communications.

6.2.5.1 Advant Field Bus 100 (AF100)

The AF100 network is used for intrachannel 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 Section 6.3.1.4.

6.2.5.2 High Speed Link (HSL)

Data communications between PM646 processor modules from one Common Q redundant channel to another is referred to as planned data exchange. Several PM646 processor modules can communicate with one another via its high speed serial links (HSL). Within the PM646 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 PM646 processor modules.

Each PM646 processor module has two high speed serial links (HSL). Each HSL consists of two half duplex serial communication lines. Therefore the PM646 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 Section 6.3.1.3, High Speed Link Communications.

6.2.5.3 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 are avoided. The Flat Panel Display System meets the requirements of IEEE 7-4.3.2 Annex G for communication independence.

6.3 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 Section 6.4.1.1 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.

6.3.1 AC160 Deterministic Performance

6.3.1.1 AC160 Application Program Execution Period

[

]

6.3.1.2 Access to the AC160 Backplane

[

]

6.3.1.3 High Speed Link Communications

[

]

6.3.1.4 AF100 Communications

[

]

6.3.1.4.1 Process Data Transfer

[

]

6.3.1.4.2 Message Transfer

[

]

6.3.1.4.3 Bus Master

[

]

6.3.2 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 G for communication independence.

6.3.2.1 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 may use an interactive protocol like TCP/IP where, on the physical layer, acknowledgments from the non-safety system occur. Having this interaction with a non-safety system occur at the Flat Panel Display System isolates the protection algorithms running in the AC160 nodes from 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 will be assumed by another node if it fails, so the AF100 network can continue to operate without the Flat Panel Display in operation.

6.4 System Diagnostics

6.4.1 AC160 Diagnostics

6.4.1.1 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 PM646 processor module is tested. The following tests are performed:[

]

6.4.1.2 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 PM646 base software diagnostics routine via a device status word. Refer to Reference 3.19 for a description of the I/O module diagnostics.

6.4.1.3 High Speed Link

High Speed Link (HSL) diagnostics are executed to detect physical layer failures and failures of the communication link to another PM646 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 PM646 processor module has not received data for 150 milliseconds, the HSL is considered failed. All detected errors are reported to the application program.

6.4.1.4 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 Section 6.3.1.4.3.

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.

6.4.1.4.1 Redundant AF100 Interface (CI631)

The AC160 redundant CI631 configuration provides on-line surveillance of these cards to ensure that they are in operational condition in case a failover is required. The primary and secondary CI modules contain self-diagnostics, and report any errors to the application in the PM646.

If the primary fails, there will be an automatic switchover to the secondary module. When this occurs the new primary module will report an error to the application that the original primary has failed. This error report can be used for alarm or screen indication to direct technicians to the specific AC160 node that has the 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 (as the standby) and there will be no red light.

The automatic failover can be periodically tested as follows:

1 – The technician verifies that CI 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 CI module (indicated by the LED light on front plate), and verifies the switchover of the other CI from backup to primary (same LED indication)

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

Upon detection of any error that would jeopardize the operation of the AC160 controller, the primary CI631 enters the passive state. [ ], and the processor modules will thus become aware of the situation. Using an engineering workstation to interrogate the error buffer, the diagnostics information can be obtained to find the cause of the problem.

In case of a forced switchover due to a CI631 failure, any ongoing service data (non-deterministic Message Transfer) communication will be aborted and restarted with the new primary CI631. If restarting from scratch is not possible, the communication with the originator of the service data message will be aborted, and the originator can then retry the transfer.

6.4.2 Flat Panel Display Diagnostics

Each application program interface (API) call [ ] 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.

6.4.3 Automatic Testing

[

6.4.3.1 Passive Testing

6.4.3.2 Active Testing

]

6.4.4 Application Watchdog

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

6.5 System Interfaces

The following example (see Figure 6.5-1) 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 channels. Each CPCS channel contains a processor to read field inputs, share CEA position signals (RSPTs), perform DNBR and LPD calculations, and provide a trip output (digital output) for 2/4 logic in the RPS. For each channel, there is a CPCS Operator's Module in the control room and a local display for maintenance and test.

CPC Processor

[

]

7. Software Quality

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

]

7.1 Software Quality Assurance

[

]

7.2 Software Configuration Management

[

7.2.1 Software Development Process

]

Figure 7.2-1

Software Development Environment

[

]

7.2.2 Previously Developed Software

[

]

7.3 Software Verification and Validation

[

|

7.3.1 V&V Plan

7.3.2 Verification

7.3.3 Validation

7.3.3.1 Module Testing

7.3.3.2 Unit Testing

7.3.3.3 Integration Testing

7.3.3.4 System Testing

]

7.4 Operation and Maintenance

[

]

8. 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 8-1. The Common Q Platform equipment qualification program shall subject the equipment to Component Cycling, EMI/RFI testing, environmental testing, and seismic testing.

FIGURE 8-1 PLANNED COMMON Q QUALIFICATION PHASES

A qualification plan will be issued defining the details associated with each phase of the qualification test. Figure 8-2 shows an overview of a typical qualification test timeline for the Common Q equipment.

[

]

Figure 8-2 Typical Qualification Test Program

[

]

8.1 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 for a minimum of 3000 cycles, simulating 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.

8.2 Environmental Testing

[

]

Table 8.2-1 Cabinet Environmental Design Requirements

[

] Notes:

(1) At or above 80°F, the moisture content is that which produces 90% RH at 80°F (dewpoint of 77°F).

(2) Outside normal range

Table 8.2-2 Common Q Equipment Environmental Design Requirements

[

] Notes:

(1) At or above 80°F, the moisture content is that which produces 90% RH at 80°F (dewpoint of 77°F).

(2) Outside normal range

[

]

Figure 8-3 Environmental Test Profile

8.3 Seismic Testing

[

8.3.1 Seismic Qualification Requirements

]

8.4 Electromagnetic Interference (EMI) Testing

The 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 will be based on the EPRI TR-102323 guidelines.

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.

EMI testing will be successfully completed before environmental and seismic qualification testing is performed.

9. Equipment Reliability

[

9.1 Failure Mode and Effects Analysis (FMEA)

]

9.2 Mean Time Between Failures (MTBF) Analysis

[

]

9.3 Operating History

[

9.3.1 AC160 Design Evolution

]

[

]

10. 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.

11. Commercial Grade Dedication Program

11.1 Scope

[

11.2 Procedure

11.2.1 Review Plan

11.2.1.2 Functional Requirements:

11.2.1.3 Design Requirements:

11.2.1.4 Software Development:

11.2.1.5 Hardware - Software Integration:

11.2.1.6 Validation (Testing):

11.2.1.7 User Documentation:

11.2.1.8 Maintenance:

11.2.2 Schedule

11.2.3 Review Performance

11.2.4 Review Report

11.3 Configuration Management

]

12. Future Documentation

The following table lists future documents that will be developed by Westinghouse or the licensee and either held for audit or submitted to the NRC in support of review of the nuclear plant's license amendment.

In addition, the following table indicates how future implementations of Common Q applications can be accommodated by submittals of generic appendices.

Future Common Q Documentation				
Document Description	**Submitted for SER revision**	**Held by Westing-house for Audit**	**Held by Licensee for Audit**	**Submitted with License Amendment (or via separate Topical)**
Evaluation of Product Software Change(s) - ongoing qualification		X		
Evaluation of Product Hardware Change(s) - ongoing qualification		X		
CPC 50.59 Evaluation			X	
PAMS 50.59 Evaluation			X	
Supplemental Qual Plan (Flat Panel, P/S, New AI, AF100/PC I/F,)		X		
Supplemental Qual Report		X		
Supplemental CGD Report, QA agreement, Product Ref Manauals, User Manuals, etc		X		
Training Plan per BTP HICB-14				X
Plant Specific Defense in Depth and Diversity Coping Analysis - plant-wide, bounding case				X
Plant Specific Defense in Depth and Diversity Coping Confirmation Evaluation - phased upgrade specific			X	
Generic Implementation Project Plan		X		
Generic Design Documentation for System Applications		X		
Generic Software V&V Reports for System Applications		X		
Generic HSI Design & HFE Evaluation		X		
Project Specific Project Plan			X	
Project Specific Design Documentation for System Applications			X	
Project Specific Software V&V Reports for System Applications			X	
Project Specific HSI Design & HFE Evaluation			X	
New Common Q Generic Application (eg. Diesel Sequencer) Appendix	X			
New Common Q Plant Specific Application (eg. Widget Controller) - digital to digital upgrade			X	
New Common Q Plant Specific Application (eg. Widget Controller) - analog to digital upgrade				X
Project Specific Qualfication Applicability Evaluation			X	
System Hardware Commercial Grade Dedication Report			X	
Tech Spec Change Requests (reference SER)				X
FSAR Revision, 50.59 (reference SER)			X	
FSAR Revision, analog to digital upgrade (reference SER)				X
Loop Controller - Remote I/O - Qual Plan & Reports, CGD reports, Manuals, etc.	X			

13. Conclusions

[

]

APPENDICES

The following appendices describe specific implementations of Common Q technology.

1. Post Accident Monitoring System (PAMS)
2. Core Protection Calculator (CPC) System
3. Plant Protection System (PPS)
4. Engineered Safety Features Actuation System (ESFAS)