Enclosure 3

WCAP-16097-NP, Revision 5, “Common Qualified Platform Topical Report”

(Non-Proprietary)

June 2020

Westinghouse Non-Proprietary Class 3

WCAP-16097-NP
Revision 5

June 2020

Common Qualified Platform Topical Report

Westinghouse

WCAP-16097-NP
Revision 5

Nuclear Safety Related Common Qualified Platform Topical Report

Matthew A. Shakun*
Licensing Engineering

June 2020

Reviewer: Christopher S. Phillips*
CE Plant Safety Systems

Brandon M. Taylor*
Standard Hardware and Common Q Platform

Warren R. Odess-Gillett*
Licensing Engineering

Richard M. Paese*
Licensing Engineering

Approved: Zachary S. Harper*, Manager
Licensing Engineering

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

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

REVISION HISTORY

RECORD OF CHANGES

Revision	Revision Made By	Description	Date
00	D.N. Menard	• See PRIME for revision history	5/2003
01	Matthew A. Shakun	• See PRIME for revision history	8/2010
02	Matthew A. Shakun	• See PRIME for revision history	3/2012
03	Matthew A. Shakun	• See PRIME for revision history	7/2012
03 Approved	Matthew A. Shakun	• See PRIME for revision history	2/2013
04	Matthew A. Shakun	• See PRIME for revision history	6/2019
04 Approved	Matthew A. Shakun	• See PRIME for revision history	1/2020
05	Matthew A. Shakun	The primary purpose of this revision is to: • Reflect the change in ownership of the AC160 components • Clarify how software loading is performed • Clarify how Safety HMI platform is protected during startup • Other technical clarifications See NA-SSPCE-20-0006-CQP-PR-NR for change evaluation. Note: The review performed by Richard M. Paese signifies the non-applicability of this topical report revision to the AP1000 project unless further AP1000 plant licensing action is taken.	6/2020

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT.)

TABLE OF CONTENTS (CONT.)

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS AND TRADEMARKS

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

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

LIST OF ACRONYMS AND TRADEMARKS (cont.)

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

LIST OF ACRONYMS AND TRADEMARKS (cont.)

SRAM	Static RAM
SVVP	Software Verification and Validation Plan
SW	Software
SWC	Surge Withstand Capability
SWT	Software Stall Timer
TCB	Task Control Block
TMI	Three Mile Island
V&V	Validation and Verification
WDT	Watchdog Timer
WWDT	Window Watchdog Timer
WYSIWYG	What You See Is What You Get

Advant® is a registered trademark of Westinghouse Electric Company LLC, its affiliates and/or its subsidiaries.

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

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

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

Common Q™ is a trademark or registered trademark of Westinghouse Electric Company LLC, its affiliates and/or its subsidiaries in the United States of America and may be registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited. Other names may be trademarks of their respective owners.

ANSYS and any and all ANSYS, Inc. brand, product, service and feature names, logos and slogans are registered trademarks or trademarks of ANSYS, Inc. or its subsidiaries in the United States or other countries.

Green Hills Software and INTEGRITY are trademarks or registered trademarks of Green Hills Software, Inc.

All other product and corporate names used in this document may be trademarks or registered trademarks of other companies, and are used only for explanation and to the owners’ benefit, without intent to infringe.

GLOSSARY OF TERMS

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

Term	Definition
Advant	The Common Q™ platform includes the Advant Controller 160 (AC160). It is used in applications that require high availability and redundancy.
Baseline Common Q™ Equipment	Baseline Common Q™ Equipment is the Common Q™ Equipment that was referenced in the NRC Safety Evaluation, dated February 24th, 2003.
MDAT	The data set used within multiprocessing applications between processors and global memory.

REFERENCES

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

2. “Quality Management System,” Westinghouse Electric Company LLC.

3. “Automation Level 3 Policies & Procedures,” Westinghouse Electric Company LLC.

4. “Westinghouse Management System Quality Procedures,” Westinghouse Electric Company LLC.

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

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

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

8. 3BDS 003 340R701, “System Software Extension Designer’s Guide”.

9. 3BDS 005 665R501, Rev. C, “Data Base Elements Advant Controller 160 Reference Manual”.

10. 3BDS 005 666R101, Rev. E, “PC Elements Advant® Controller 160 Version 1.3 Reference Manual”.

11. (Reference Deleted)

12. (Reference Deleted)

13. (Reference moved to Bibliography)

14. (Reference moved to Bibliography)

15. (Reference moved to Bibliography)

REFERENCES (cont.)

16. (Reference moved to Bibliography)

17. (Reference moved to Bibliography)

18. (Reference moved to Bibliography)

19. 3BDS 005 740R501, "S600 I/O Hardware, Advant Controller 160 Reference Manual" .

20. (Reference moved to Bibliography)

21. (Reference moved to Bibliography)

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

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

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

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

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

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

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

BIBLIOGRAPHY

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

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

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

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

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

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

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

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

9. "Green Hills Software Corporate and Product Overview", Green Hills Software, May 2015.

1 PURPOSE

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

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

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

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

2 SCOPE

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

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

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

This topical report is structured with a main body and several appendices. The main body includes the basic platform description and addresses all of the key issues described in the Standard Review Plan, NUREG-0800, Revision 7. 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 includes a failure mode and effects analysis for all shared services and assesses common mode failure mechanisms.

3 CODES AND STANDARDS

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

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
1.	RG 1.22 BTP 7-8 BTP 7-17	USNRC Regulatory Guide – Periodic Testing of Protection System Actuation Functions (Safety Guide 22) The Common Q™ platform supports a safety application to conform to this RG, Branch Technical Position 7-8 and -17, and IEEE Std 338 as described below: A. Provisions are made to permit periodic testing of the complete Common Q™ system with the reactor shutdown or operating. B. Provisions for testing the Common Q™ platform are incorporated via the Maintenance and Test Panels (MTP) and/or Interface and Test Processors (ITP) located in each Common Q™ cabinet. Testing each cabinet is performed using its MTP. C. No provisions are made in the design of the Common Q™ platform at the system level to intentionally bypass an initiation or actuation signal that may be required during power operation (this does not include override functions that are part of the system). All trip channel bypasses are on a channel level to prevent an operator from inadvertently bypassing a trip function. D. Manual testing for a Common Q™ platform division is interlocked to prevent testing in more than one redundant division simultaneously. When a trip channel is bypassed for manual testing, the bypass is indicated in the main control room. E. Actuated devices which can not be tested during power operation, will be tested when the reactor is shut down. F. An additional level of Common Q™ platform testing is provided by the PLC hardware self-diagnostic tests.	00 02/1972
2.	RG 1.29	USNRC Regulatory Guide – Seismic Design Classification The Common Q™ platform equipment is designated as a system to be Seismic Category I. Those portions of the equipment whose continued function is not required are designated Seismic Category II and are designed so that the SSE will not cause a failure which will reduce the functioning of the Common Q™ platform safety function to an unacceptable level. The Licensee is responsible for the application of RG 1.29 in accordance with their licensing basis.	05 07/2016

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
3.	RG 1.47	USNRC Regulatory Guide – Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems The Common Q platform supports implementation of bypassed and inoperable status indication for safety system applications. The Licensee is responsible for the application of RG 1.47 in accordance with their licensing basis.	01 02/2010
4.	RG 1.53	USNRC Regulatory Guide – Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems Each system is designed so that credible single failures within the system shall not prevent proper protective action at the system level. See Sections 4 and 5 and the appendices of this report for system descriptions that implement these criteria. Single failures considered in the designs are addressed in the Failure Modes and Effects Analyses in the appendices. The Licensee is responsible for the application of RG 1.53 in accordance with their licensing basis.	02 11/2003
5.	RG 1.62	USNRC Regulatory Guide – Manual Initiation of Protective Actions A. RPS/ESFAS applications using the Common Q™ platform can be designed such that initiation functions and actuations can be initiated manually. B. Manual initiation of protective functions is provided at the system level. C. Manual Common Q™ initiation switches are remotely located in the main control room. Manual ESFAS switches are located locally on the ESFAS cabinets. D. The amount of equipment common to manual and automatic initiation paths is kept to a minimum. No credible single failure in the manual, automatic or common portions of the Common Q™ will prevent initiation of a protective action by manual or automatic means. E. Manual initiation requires a minimum of equipment consistent with the needs of A, B, C, and D above. The Licensee is responsible for the application of RG 1.62 in accordance with their licensing basis.	01 06/2010

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
6.	RG 1.75 BTP 7-11	USNRC Regulatory Guide – Physical Independence of Electric Systems The Common Q™ platform supports a safety application to conform to this RG and BTP 7-11 as described below: The Common Q™ PPS and CPC systems are composed of four redundant cabinet assemblies which provide physical mechanical and electrical separation. The independence and separation of redundant Class 1E circuits within and between the Common Q™ assemblies is accomplished primarily through the use of fiber optic technology and, as necessary, 6 inch separation, barriers or conduits. A further description of the application of these criteria is provided in Sections 4 and 5 of this report. The Licensee is responsible for the application of RG 1.75 in accordance with their licensing basis.	03 02/2005
7.	RG 1.89	USNRC Regulatory Guide – Qualification for Class 1E Equipment for Nuclear Power Plants The Common Q™ platform conforms to this RG and IEEE Std 323 as follows. The environmental qualification of this equipment is by an appropriate combination of type testing and analysis as described further in Section 7 of this report. The Licensee is responsible for the application of RG 1.89 in accordance with their licensing basis.	01 06/1984
8.	RG 1.97 BTP 7-10	Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident Guidance on Application of Regulatory Guide 1.97 The Common Q™ platform supports a safety application to conform to this RG. See Equipment Qualification RGs/Standards for disposition of Common Q Platform generic equipment qualification. The Licensee is responsible for the application of RG 1.97 in accordance with their licensing basis.	05 04/2019

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
9.	RG 1.100	USNRC Regulatory Guide – Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants The generic 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 7.3 for a further description of the seismic qualification efforts. The applicability of this revision applies to project specific equipment qualification when this revision is specified. The Licensee is responsible for the application of RG 1.100 in accordance with their licensing basis.	02 06/1988 03 09/2009
10.	RG 1.105 BTP 7-12	Setpoints for Safety-Related Instrumentation Guidance on Establishing and Maintaining Instrument Setpoints The instrument uncertainties calculation of the safety systems is in accordance with ISA-67.04. The instrument uncertainties for the CPC are factored in the Statistical Combination of Uncertainties (Reference 7). The Licensee is responsible for the application of RG 1.105 in accordance with their licensing basis.	03 12/1999
11.	RG 1.118 BTP 7-17	USNRC Regulatory Guide – Periodic Testing of Electric Power and Protection Systems The Common Q™ platform supports a safety application to conform to this RG, IEEE Std 338 and BTP 7-17 as described in the compliance statement for RG 1.22. The Licensee is responsible for the application of RG 1.118 in accordance with their licensing basis.	03 04/1995
12.	RG 1.152	USNRC Regulatory Guide – Criteria for Use of Computer Software in Safety Systems of Nuclear Power Plants The Common Q™ platform conforms to this RG by following IEEE Std 7-4.3.2, which provides methods acceptable for designing software, verifying software, implementing software, and validating computer systems in safety related systems. Refer to the Common Q™ Software Program Manual (SPM), Reference 5 and refer to Section 6 for a further description of the basic elements of the SPM. The Common Q platform Secure Development and Operational Environment (SDOE) plan is described in Common Q™ Software Program Manual (SPM), Reference 5. The Licensee is responsible for the application of RG 1.152 in accordance with their licensing basis.	03 07/2011

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
13.	RG 1.153	USNRC Regulatory Guide – Criteria for Safety Systems This Reg. Guide endorses IEEE Std 603-1991, which establishes minimum functional and design requirements for the power, instrumentation, and control portions of safety systems for nuclear power plants. See the response to IEEE 603-1991 for Common Q™ conformance.	01 06/1996
14.	RG 1.168	Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants The Common Q™ Validation and Verification plans conform to this RG as described in Section 6 of this report and in the Common Q™ SPM, Reference 5. The Licensee is responsible for the application of RG 1.168 in accordance with their licensing basis.	02 07/2013
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. The Licensee is responsible for the application of RG 1.169 in accordance with their licensing basis.	01 07/2013
16.	RG 1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants The Common Q™ design and implementation processes conform to this RG as described in the Common Q™ SPM. The Licensee is responsible for the application of RG 1.171 in accordance with their licensing basis.	01 07/2013
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. The Licensee is responsible for the application of RG 1.172 in accordance with their licensing basis.	01 07/2013
18.	RG 1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants The Common Q™ design and implementation processes conform to IEEE Std 1074-1995 as augmented by this RG, as described in the Common Q™ SPM for Common Q™ Systems, Reference 5. The Licensee is responsible for the application of RG 1.173 in accordance with their licensing basis.	01 07/2013

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
19.	RG 1.180	Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems Rev. 0 of the RG endorses MIL-STD-461D and MIL-STD-462D. The baseline Common Q™ equipment is qualified in accordance with these MIL STDs as endorsed by RG 1.180, and EPRI TR 102323, and further described in Section 7.4 of this topical report. Rev. 1 of the RG endorses MIL-STD-461E and International Electrotechnical Commission (IEC) 61000 series of EMI/RFI test methods. New additions or enhancements to previously tested Common Q™ equipment are tested in accordance with these standards as augmented by RG 1.180, Rev. 01. The Licensee is responsible for the application of RG 1.180 in accordance with their licensing basis.	00 01/2000 01 10/2003
20.	IEEE Std 7-4.3.2	IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations See RG 1.152 conformance for more information.	2003
21.	ANSI/IEEE Std 279 BTP 7-17	"Criteria For Protection Systems For Nuclear Power Generating Stations" The Common Q™ platform supports safety system applications that need to conform to this standard. This standard has been replaced by IEEE-603-1991. The Licensee is responsible for the application of IEEE 279 or IEEE 603 in accordance with their licensing basis.	1971
22.	IEEE Std 323	IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Systems See RG 1.89 conformance for more information.	1983
23.	IEEE Std 338	IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems The Common Q™ platform supports a safety application to conform to this standard as augmented by RG 1.118. See RG 1.118 conformance for more information.	1987
24.	IEEE Std 344	IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations See RG 1.100 conformance for more information.	1987 2004

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
25.	IEEE Std 379	IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems See RG 1.53 conformance for more information.	2000 (Reaffirmed 2008)
26.	IEEE Std 383	IEEE Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations The Common Q™ conforms to this standard as below. The aging and flame retarding qualification requirements of this standard are invoked on the Common Q™ custom internal wiring and cabling. The Licensee is responsible for the application of IEEE 383 in accordance with their licensing basis.	2003
27.	IEEE Std 384 BTP 7-11	IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits The Common Q™ platform supports a safety application to conform to this standard as augmented by RG 1.75 and Branch Technical Position 7-11 as described in the RG 1.75 conformance.	1992
28.	IEEE Std 420	IEEE Standard for the Design and Qualification of Class 1E Control Board, Panels and Racks. The Common Q™ equipment supports a safety application to conform to this standard as augmented by and described in the compliance statements for the following IEEE Standards: -323, -338, -383, -384, and -603. The Licensee is responsible for the application of IEEE 420 in accordance with their licensing basis.	1982
29.	IEEE Std 494	IEEE Standard Method for identification of Documents Related to 1E Equipment. The Common Q™ documentation conforms to this standard by having the term “Nuclear Safety Related” applied on the face of each document and drawing.	1974 (Reaffirmed 1990)

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
30.	IEEE Std 603 BTP 7-1 BTP 7-2 BTP 7-3 BTP 7-6 BTP 7-8 BTP 7-9 BTP 7-11 BTP 7-12 BTP 7-13 BTP 7-14 BTP 7-17 BTP 7-19 BTP 7-21	IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations The Common Q™ platform supports a safety application to conform to this standard as augmented by RG 1.153, Rev. 01, 06/1996 and Branch Technical Positions 7-1, 2, 3, 6, 8, 9, 11, 12, 13, 14, 17, 19 and 21. The Licensee is responsible for the application of IEEE 279 or IEEE 603 in accordance with their licensing basis.	1991
31.	IEEE Std 627	IEEE Standard for Design Qualification of Safety System Equipment used in Nuclear Power Plants The Common Q™ platform qualification process conforms to this standard as described in Section 7 of this report and the conformance statements for IEEE Std 323 and RG 1.89. The Licensee is responsible for the application of IEEE 627 in accordance with their licensing basis.	1980 (Reaffirmed 1997)
32.	IEEE Std 730	IEEE Standard for Software Quality Assurance Plans The Common Q™ SPM (Reference 5) describes the design and implementation processes for Common Q applications. The Licensee is responsible for the application of IEEE 730 in accordance with their licensing basis.	1998
33.	IEEE Std 828	IEEE Standard for Software Configuration Management Plans See RG 1.169 conformance for more information.	2005
34.	IEEE Std 830	IEEE Recommended Practice for Software Requirements Specifications See RG 1.172 conformance for more information.	1998
35.	IEEE Std 1012	IEEE Standard for Software Verification and Validation Plans See RG 1.168 conformance for more information.	2004
36.	IEEE Std 1016	IEEE Recommended Practice for Software Design Descriptions The Common Q™ design documentation practices conform to this standard as described in the Common Q™ SPM, Reference 5. The Licensee is responsible for the application of IEEE 1016 in accordance with their licensing basis.	1998 (Reaffirmed 2009)

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
37.	IEEE Std 1028	IEEE Standard for Software Reviews and Audits The Common Q™ SPM, Reference 5, describes the software reviews and audits that will be performed per this standard. See RG 1.168 conformance for more information.	2008
38.	IEEE Std 1074	IEEE Std for Developing Software Life Cycle Processes See RG 1.173 conformance for more information.	2006
39.	ISA-S67.04.01	Setpoints For Nuclear Safety Related Instrumentation Used in Nuclear Power Plants For digital to digital replacements (i.e., CPC, Qualified Safety Parameter Display System (QSPDS), etc.) the replacement Common Q™ system will be as accurate or more accurate than the system it is replacing, and will use existing field interfaces and setpoints. For analog to digital Common Q™ replacements (i.e., RPS, PPS, etc.), an assessment shall be made on the impact of any applicable setpoint analyses by the replacement system. The Common Q™ platform supports a safety application to conform to this standard as augmented by RG 1.105. See RG 1.105 conformance for more information.	1994
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 7.4 of this topical report) include testing using the oscillatory SWC test wave as defined in Section 2.2 of this standard. (SWC testing was performed to IEC 801-5) The Licensee is responsible for the application of ANSI C37.90.1 in accordance with their licensing basis.	1989
41.	EPRI NP-5652 EPRI 3002002982	EPRI Guideline for Utilization of Commercial Grade Items in Nuclear Safety Related Applications EPRI Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications: Revision 1 to EPRI NP-5652 and TR-102260 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. Westinghouse's practices encompass all 4 of these processes as follows: Special tests and inspections are part of the Common Q™ qualification program that includes seismic, EMI/RFI and environmental testing of the commercial grade item (Section 7 of this report) Commercial-grade survey of supplier, source verification, and acceptable supplier/item performance record is part of the Hardware and Software Commercial Grade Dedication Processes described in Section 10.	1988 2014

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
42.	EPRI Topical Report TR-102323	EPRI Guidelines for Electromagnetic Interference Testing in Power Plants See RG 1.180 conformance for more information.	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 See RG 1.180 conformance for more information.	1993
45.	MIL-STD-462D	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment See RG 1.180 conformance for more information.	1993
46.	MIL-STD-461E	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment This standard supersedes MIL-STD-461D and MIL-STD-462D. See RG 1.180 conformance for more information.	1999
47.	IEC 61000 series	Electromagnetic Compatibility (EMC) See RG 1.180 conformance for more information.	
48.	BTP 7-14	Guidance on Software Reviews for Digital Computer-Based I&C Systems The Common Q™ program meets the intent of this BTP and is defined in the Common Q™ Software Program Manual.	
49.	BTP 7-18	Guidance on Use of Programmable Logic Controllers in Digital Computer-Based I&C Systems The Common Q™ program meets the intent of this BTP and is defined in the Common Q™ Software Program Manual and its Commercial Grade Dedication Program as described in Section 10.	
50.	BTP 7-19	Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems Defense-in-Depth and Diversity for specific systems are discussed in the Integrated Solution Appendix of this Topical Report.	
51.	BTP 7-21	Guidance on Digital Computer Real-Time Performance Common Q™ designs are described in more detail in follow-up appendices to this Topical Report and encompass the existing design parameters of the systems that are replaced.	

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
52.	EPRI TR-107330	Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants	1996
53.	NUREG-0737	Clarification of Three Mile Island (TMI) Action Plan Requirements All Common Q™ Post Accident Monitoring Systems shall meet these requirements.	1980
54.	NUREG-0800	Chapter 7 of the USNRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Rev. 7 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.	2016
55.	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
56.	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 (e.g., [ ]^{a,c}). Section 10.1 discusses the Software Commercial Grade Dedication process.	1996
57.	10 CFR 50 Appendix A	GDC 1: "Quality Standards and Records" The Common Q™ Quality Assurance procedures shall conform to these criteria. GDC 2: "Design Bases For Protection Against Natural Phenomena" GDC 4: "Environmental And Dynamic Effects Design Bases" Common Q™ hardware and software qualification procedures shall conform to these criteria. GDC 12: "Suppression Of Reactor Power Oscillations" The Common Q™ CPC implementation will still have the Local Power Density Trip function that addresses this criterion. GDC 13: "Instrumentation And Control" Common Q™ systems shall be designed and tested to meet this criterion.	

Ref. No.	Document No.	Title/Conformance	Revision No., Issue Date
57. (cont.)	10 CFR 50 Appendix A	GDC 19: “Control Room” A Control Room interface (Flat Panel Display System) is provided for each Common Q™ system. GDC 20: “Protection System Functions” Common Q™ systems responsible for the functions defined in this GDC shall be designed and tested to conform to this criterion. The Common Q™ Platform applications support the following GDCs: GDC 21: “Protection System Reliability and Testability” GDC 22: “Protection System Independence” GDC 23: “Protection System Failure Modes” GDC 24: “Separation of Protection and Control Systems” GDC 25: “Protection System Requirements For Reactivity Control Malfunctions” GDC 10: “Reactor Design” The Common Q™ DPPS and CPC applications support this criterion. See appendices for details. GDC 15: “Reactor Coolant System Design” The DPPS High Pressure Trip is an example of a Common Q™ application supporting this criterion. See DPPS appendix for details. GDC 16: “Containment Design” The DPPS is a Common Q™ application that supports this criterion. See DPPS appendix for details. GDC 28: “Reactivity Limits” Both the CPC and DPPS Common Q™ applications (e.g., Variable High Power Trip or High Linear Power Trip) support this criterion. GDC 29: “Protection Against Anticipated Operation Occurrences” Both the CPC and DPPS Common Q™ applications support this criterion. GDC 33: “Reactor Coolant Makeup” Both the DPPS and ESFAS Common Q™ applications support this criterion. Refer to the DPPS and ESFAS appendices for details.	

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

4 COMMON Q™ OVERVIEW

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

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

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

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

a,c

Figure 4-1 Simplified Block Diagram

4.1 ADVANT CONTROLLER 160 (AC160)

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

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

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

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

Each processor module supports two high speed communication links (HSL). The HSLs will be typically used in the broadcast mode to transmit data to other divisions of the safety system. These data links are electrically isolated using fiber optic cable. The HSL is discussed in Section 4.5 and subsection 5.2.4.2.

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

The processor module has a built in window watchdog timer module (WWDT) that is to be used in the Common Q™ systems. Depending on the specific system application, the WWDT can be used to annunciate a failure, actuate a divisional trip, or set output states to predefined conditions. For example, the WWDT 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 timers are discussed in subsections 5.2.1.2.1 and 5.2.1.3.

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

4.1.1 AC160 Software

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

- Application Builder

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

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

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

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

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

[ ]^{a,c}

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

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

4.1.2 Input and Output Cards

The Advant Controller 160 uses the S600 I/O system. A range of I/O modules is available, covering analog and digital signals of various types. In addition, there are modules for temperature measurement

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

and rotational speed measurement. The process signals are connected to the front of the I/O modules. S600 I/O modules that will be used in Common Q™ applications are discussed in subsection 5.2.1.1.3.

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

4.1.3 Interface and Test Processor (ITP)

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

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

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

4.2 POWER SUPPLY

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

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

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

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

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

4.3 FLAT PANEL DISPLAY SYSTEM (FPDS)

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

[

]a,c

4.3.1 Flat Panel Display System Software

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

[

]a,c

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

4.3.2 Maintenance and Test Panel (MTP)

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

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

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

4.3.3 Operator's Module

The Operator's Module uses the same Common Q™ flat panel display system. The Operator's Module will be used for operator functions such as changing setpoints, viewing control rod positions, or displaying RG 1.97 variables (including Type A variables). Non-volatile memory, such as a solid state disc, is used for operator setpoints or other applications where warm system starts using updated constants is needed.

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

4.3.3.1 Manual Component-Level Control

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

4.4 AF100 COMMUNICATION

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

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

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

The message transfer services are implemented to enable stations on the Advant Fieldbus to send and receive messages. Message transfer is not performed cyclically, but only when one (or more) of the attached communication interfaces have something to send. Message transfer does not influence process data transfer in any way. Process data transfer remains deterministic since a certain amount of the Advant Fieldbus bandwidth is reserved for message transfer.

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

4.5 HIGH SPEED LINK (HSL) COMMUNICATION

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

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

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

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

5 COMMON Q™ PLATFORM

5.1 FUNCTIONAL REQUIREMENTS

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

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

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

5.2 SYSTEM DESCRIPTION (BUILDING BLOCKS)

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

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

5.2.1 Advant Controller

Advant Controller 160 is used in applications that require high availability and redundancy.

5.2.1.1 AC160 Hardware Description

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

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

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

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

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

By using redundant communication interfaces to Advant Fieldbus and to I/O extension bus, redundant power supply modules and redundant external power, the availability of the Advant Controller 160 can be increased as needed to achieve high reliability and availability. When operated in the redundant mode, failure of one of the redundant items does not interfere with the continued operation of the other. Redundant I/O modules can be replaced during operation of the system without impact.

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

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

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

5.2.1.1.1 PM646A Processor Module

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

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

a,c

Figure 5-1 AC160 Hardware

Processor Module

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

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

- The PM646A processor module consists of two hardware sections, the processing section with microprocessor and memory for the application program and the communication section with a separate microprocessor and memory for the communication signal exchange to other controllers.
- A Motorola MC68360 processor (application processor), 1 Mbyte nonvolatile memory (Flash PROM) for the user built application and 2 Mbytes of nonvolatile memory (Flash PROM) for the system software and 2 Mbytes of Static RAM (SRAM). At startup, the application software is copied from the nonvolatile memory into the SRAM memory where it is executed, whereas the system software is executed out of the nonvolatile memory.
- 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 512 Kbytes SRAM is provided for communications.

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

Subrack

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

The bus connector links the controller subrack to an optional extension subrack via a bus cable. The 10-position extension subrack extends the number of I/O modules of a station. The individual module address is given by its position in the subrack.

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

Diagnostic Functions

Advant Controller 160 performs a variety of diagnostic and supervision functions to continuously monitor the correct operation of the whole system. Each of the modules has diagnostic functions. The CPU module monitors the system as a whole by collecting all the diagnostic information and checking the consistency of the hardware configuration and the application software.

The supervision functions are subdivided into the following groups:

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

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

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

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

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

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

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

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

a,c

Figure 5-2 PM646A Processor Module

5.2.1.1.2 PM646A High Speed Link Communication Interface

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

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

5.2.1.1.3 Input/Output Subsystem

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

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

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

Analog Input Modules

[

]^{a,c}

Analog Output Modules

[ ]^{a,c}

[

]^{a,c}

Digital Input Modules

[

]^{a,c}

Digital Output Modules

[

]^{a,c}

Pulse Counting Module

[

]^{a,c}

Status of I/O Signals

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

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

Unused Supervised Inputs

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

Calibration of Analog Input and Outputs

During the course of manufacture, all measurement and output ranges of analog I/O modules are calibrated at an ambient temperature of approximately 25°C. Normally, the modules need no further calibration. If the accuracy is outside the specified limits (e.g., due to component failure), the module must be replaced. There are no calibration adjustments.

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

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

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

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

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

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

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

5.2.1.2 AC160 Software Description

The Advant Controller 160 Software consists of a real-time operating system [ ]^{a,c}, AC160 task scheduler, diagnostic functions, communication interfaces, and user application programs, all of which reside on flash PROM in the PM646A processor module. Refer to subsection 5.4.1 for a description of diagnostic functions, and subsection 5.2.4 for a description of the communications.

5.2.1.2.1 Base Software

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

a,c

Figure 5-3 Base Software Identification

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

[ ]^{a,c} Real Time Operating System

[

]^{a,c}

AC160 Kernel

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

[

]^{a,c}

a,c

Figure 5-4 Basic Functional Architecture PM646

[

]^{a,c}

[

]^{a,c}

a,c

Figure 5-5 [ ]^{a,c}

[

]^{a,c}

[

]^{a,c}

a,c

Figure 5-6 [ ]^{a,c}

[

]a,c

[

]a,c

[

]^{a,c}

[

]a,c

a,c

Figure 5-7 [ ]^{a,c}

[ ]^{a,c}

[

]^{a,c}

a,c

Figure 5-8 [ ]^{a,c}

[

]^{a,c}

[

]^{a,c}

a,c

Figure 5-9 [ ]^{a,c}

[

]^{a,c}

[

]^{a,c}

a,c

Figure 5-10 [ ]^{a,c}

[

]^{a,c}

[

]^{a,c}

a,c

Figure 5-11 [ ]^{a,c}

[

]^{a,c}

Function Block Library

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

[

]^{a,c}

5.2.1.2.2 Application Software

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

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

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

PC Part

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

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

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

[

]^{a,c}

[

]^{a,c}

a,c

Figure 5-12 [ ]^{a,c}

[

]^{a,c}

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

Database Part

The DB part in an Advant Controller 160 contains the DB elements which are used to configure the controller. DB elements in an Advant Controller 160 system describe the following items:

- The hardware configuration of the AC160 system: processor module, I/O modules, and communication interfaces (e.g., HSL and AF100)
- Common data elements (e.g., global data)
- Connection between the hardware and the common data elements (e.g., Data Set Peripheral [DSP] for AF100 communication and DB elements for the HSL)

5.2.1.2.3 Software Tools

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

For further description see References 9 and 10.

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

Type Circuits

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

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

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

Custom PC Elements

Custom PC elements appear as standard PC elements with input and output terminals when inserted in a control program. They are developed outside of the ACC development environment and then added to the library of PC elements. Once in the library, the custom PC element is available for the programmer to use in a control program.

The custom PC element is developed using the system software extension option for the AC160 that allows custom PC elements to be added to the controller. The tools used to develop the custom PC element include a C compiler (MCC68K) and linker (LNK68K) from Mentor Graphics Microtec division. The linker generates a Motorola S-Record image file for the PC element. This image file is downloaded to the AC160 processor module’s flash PROM using the same tool for installing the base software. Reference 8 describes the methodology for creating these elements.

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

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

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

5.2.1.3 Watchdog Timers

[

]^{a,c}

5.2.1.3.1 [ ]^{a,c}

[

]^{a,c}

5.2.1.3.2 [ ]^{a,c}

[

]^{a,c}

[

]^{a,c}

5.2.1.3.3 [ ]^{a,c}

[

]^{a,c}

5.2.1.3.4 [ ]^{a,c}

[

]^{a,c}

5.2.1.3.5 Window Watchdog Timer Relay

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

a,c

Figure 5-13 Watchdog Timer Configuration

Table 5-1 Processor Module WDT Arrangement Watchdog Timer Summary

a,c

5.2.2 Flat Panel Display System

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

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

5.2.2.1 Flat Panel Display System Hardware Description

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

5.2.2.1.1 Single Board Computer

The single board computer is based on [ ]^{a,c}. There is an interface to the Advant AF100 communication bus so data can be communicated with the Advant processors. Other standard interfaces such as Ethernet and serial links are available for communications to external systems over fiber optic cables. The most typical external system that the FPDS will interface to is the Plant Computer. Typical Plant Computer interfaces are Ethernet or serial data link. Non-volatile memory, such as a solid state disc, is used for operator setpoints or other applications where warm system starts using updated constants is needed.

5.2.2.1.2 Flat Panel Display

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

5.2.2.2 Flat Panel Display Software Description

There are two qualified FPDS operating systems: [ ]^{a,c} Each FPDS (e.g., MTP, OM) will use one of these operating systems. The software used for the FPDS is described in the following sections.

5.2.2.2.1 [ ]^{a,c} Operating System

[

]^{a,c}

a,c

Figure 5-14 [ ]^{a,c} Operating System

[

]^{a,c}

a,c

[

]^{a,c}

[

]^{a,c}

5.2.2.2.2 [ ]^{a,c} Graphical User Interface

[

]^{a,c}

a,c

Figure 5-15 [ ]^{a,c} OS Graphical User Interface

[

]^{a,c}

[

]a,c

a,c

Figure 5-16 [ ]a,c

[

]a,c

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

5.2.2.2.3 [ ]a,c Software Tools

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

C Application Programming Tools

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

Display Building Tools

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

5.2.2.2.4 [ ]^{a,c} Operating System

[ ]^{a,c}

a,c

Figure 5-17 [ ]^{a,c} Operating System [Bibliography 9]

[

]^{a,c}

5.2.2.2.5 [ ]^{a,c} Graphical User Interface

[

]^{a,c}

[

]a,c

5.2.2.2.6 Software Tools

There are two areas of programming for the Flat Panel Display: application programs written in C or C++ and displays built using SCADE Display.

C and C++Application Programming Tools

The [ ]a,c supports the development of application programs in Standard C or C++. It includes a full functional development environment. The Multi IDE includes a series of tools to assist with proper development including a built in code analyzer to support coding standards. Additionally the use of a Green Hills Probe enables low level debugging and verification of code coverage during testing and development.

Display Building Tools

[

]a,c

a,c

Figure 5-18 [ ]^{a,c} Graphical User Interface Creation Process

5.2.2.3 Flat Panel Display System Applications

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

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

5.2.2.3.1 Operator's Module

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

5.2.2.3.2 Maintenance and Test Panel (MTP)

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

The MTP shall provide the following functions:

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

- The means for loading and changing setpoints/calibration factors

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

Manually Initiated Tests

The MTP provides the means for the operator to bypass a channel and initiate surveillance tests. These initiations shall be transmitted to the AC160 processor through the AF100 network. The results of the test are transmitted back to the MTP for display. The MTP shall also display any anomalies detected by the ITP from its passive testing (monitoring system operation without injecting test signals).

Loading/Changing Setpoints

The operator can load either a batch set of setpoints or can change an individual setpoint. In either case validation procedures shall be executed that will ensure data integrity. When setpoints are changed, they are transmitted over the AF100 network to the AC160. The AC160 shall transmit these changes back to the MTP for verification. The MTP software then shall compare the setpoints received from the AC160 with those stored on the MTP or entered by the operator. Any deviations shall be displayed and alarmed on the MTP. The operator can then reload the setpoints if there are any discrepancies. [

]^{a,c}

Data Link Interface To External Systems

There shall be a software program that transmits predefined data packets over a data link to an external system. The AC160 processors shall transmit data over the AF100 network at predefined intervals to the

MTP. The data link interface program in the MTP shall read this data off the AF100 network, format a data link packet, and transmit it to the external system.

5.2.3 Power Supply

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

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

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

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

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

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

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

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

5.2.4 Communication Subsystems

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

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

5.2.4.1 Advant Field Bus 100 (AF100)

The AF100 network is used for intradivisional communications. Advant Fieldbus 100 is a high performance fieldbus, which is used for communication between Advant Controllers and the Flat Panel Display System. The AC160 controllers and the Flat Panel Display System can be connected as nodes on the AF100 network.

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

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

5.2.4.2 High Speed Link (HSL)

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

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

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

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

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

5.2.4.3 External Communications

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

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

5.3 DETERMINISTIC PERFORMANCE

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

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

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

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

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

5.3.1 AC160 Deterministic Performance

5.3.1.1 AC160 Application Program Execution Period

[

]^{a,c}

[

]a,c

a,c

Figure 5-19 AC160 Application Program Execution Period

[

]a,c

5.3.1.2 Access to the AC160 Backplane

[

]a,c

a,c

Figure 5-20 AC160 Hardware

[

]^{a,c}

[

]^{a,c}

5.3.1.3 High Speed Link Communications

[

]^{a,c}

5.3.1.4 AF100 Communications

[

]^{a,c}

[

]^{a,c}

5.3.1.4.1 Process Data Transfer

[

]^{a,c}

a,c

Figure 5-21 [ ]^{a,c}

[

]^{a,c}

5.3.1.4.2 Message Transfer

[

]^{a,c}

[

]^{a,c}

5.3.1.4.3 Bus Master

[

]^{a,c}

5.3.2 Flat Panel Display System

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

5.3.2.1 Datalink To External Systems

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

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

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

5.4 SYSTEM DIAGNOSTICS

5.4.1 AC160 Diagnostics

5.4.1.1 Processor

One component of the AC160 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 WWDT, 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 AC160 database element when referenced within an application program.

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

[

]^{a,c}

[

]a,c

5.4.1.2 I/O

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

5.4.1.3 High Speed Link

High Speed Link (HSL) diagnostics are executed to detect physical layer failures and failures of the communication link to another PM646A processor module. The physical layer of the HDLC protocol is secured through a cyclic redundancy check (CRC). The HSL sends the true and inverse values of the data and the PM646A HSL receiver compares them and marks the HSL data as failed if they do not match. Also if more than 3 out of 100 consecutive telegrams are disturbed, the system declares the link to be failed. If a CRC error is detected, the data associated with that CRC is ignored (i.e., DPM is not updated), the PS application is notified of the CRC error. Automatic recovery is guaranteed when 100 telegrams are received without error. A keep-alive signal is transmitted over the HSL every 25 milliseconds, if an application program has requested no transmission within this time. When a PM646A processor module has not received a keep alive signal or data for 250 milliseconds, the HSL is considered failed. All detected errors are reported to the application program.

5.4.1.4 AF100

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

The AF100 communication interface, CI631, monitors the validity of the data sets it is suppose to receive. If no data has been received for four cycles for the data set (i.e., 4 X CYCLETIM designation for the data set) or when the communication interface has failed, the database element for the data set will be flagged as failed. The control module programming will constantly monitor the database element flag and perform the appropriate error processing.

5.4.1.4.1 AF100 Interface (CI631)

The AC160 CI631 configuration provides on-line surveillance of this card to ensure that it is in operational condition. The CI module contains self-diagnostics, and the PM646A application program monitors the CI631 database element error terminal for any detected failures.

This information 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.

5.4.2 [ ]^{a,c} Flat Panel Display Diagnostics

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

5.4.3 [ ]^{a,c} Flat Panel Display Diagnostics

[

]^{a,c}

5.4.4 Surveillance Testing

[

]^{a,c}

5.4.4.1 Passive Testing

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

5.4.4.2 [ ]^{a,c}

[

]^{a,c}

5.4.5 Application Watchdog

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

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

5.5 SYSTEM INTERFACES

The following example (see Figure 5-22) is used to illustrate the use of Common Q™ building blocks to design a system. The example chosen is a possible implementation of the Core Protection Calculator System (refer to the CPCS Appendix for the official CPCS Common Q™ configuration).

Overview

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

CPC Processor

[

]^{a,c}

[

]a,c

[

]^{a,c}

a,c

Figure 5-22 [ ]^{a,c}

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

The purpose of this section is to address compliance to the twenty communication criteria established in Interim Staff Guidance Highly Integrated Control Room- Communications (DI&C-ISG-04) for the communication technologies of the Common Q™ platform.

]^{a,c}

5.6.1 ISG-4 Position 1

ISG-4, Position 1 states:

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

Compliance

[

]^{a,c}

a,c

Figure 5-23 PM646A Architecture

5.6.2 ISG-4 Position 2

ISG-4, Position 2 states:

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

Compliance

[

]^{a,c}

a,c

Figure 5-24 HSL Communication

[

]^{a,c}

5.6.3 ISG-4 Position 3

ISG-4, Position 3 states:

> *"A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that*

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

Compliance

[

]^{a,c}

5.6.4 ISG-4 Position 4

ISG-4, Position 4 states:

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

Compliance

[

]^{a,c}

a,c

Figure 5-25 [ ]^{a,c}

[

]^{a,c}

5.6.5 ISG-4 Position 5

ISG-4, Position 5 states:

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

Compliance

[

]a,c

5.6.6 ISG-4 Position 6

ISG-4, Position 6 states:

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

Compliance

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

5.6.7 ISG-4 Position 7

ISG-4, Position 7 states:

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

Compliance

[

]a,c

5.6.8 ISG-4 Position 8

ISG-4, Position 8 states:

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

Compliance

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

5.6.9 ISG-4 Position 9

ISG-4, Position 9 states:

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

Compliance

[

]a,c

5.6.10 ISG-4 Position 10

ISG-4, Position 10 states:

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

Compliance

[

]^{a,c}

[

]^{a,c}

5.6.11 ISG-4 Position 11

ISG-4, Position 11 states:

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

Compliance

[ ]^{a,c}

5.6.12 ISG-4 Position 12

ISG-4, Position 12 states:

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

Compliance

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

  [

  ]a,c

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

  [

  ]a,c

- Messages may be sent in the incorrect sequence.

  [

  ]a,c

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

  [

  ]a,c

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

  [

  ]a,c

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

  [

  ]a,c

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

  [ ]^{a,c}

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

  [ ]^{a,c}

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

  [ ]^{a,c}

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

  [ ]^{a,c}

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

  [ ]^{a,c}

- Message headers or addresses may be corrupted.

  [ ]^{a,c}

5.6.13 ISG-4 Position 13

ISG-4, Position 13 states:

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

Compliance

[

]^{a,c}

5.6.14 ISG-4 Position 14

ISG-4, Position 14 states:

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

Compliance

[

]^{a,c}

5.6.15 ISG-4 Position 15

ISG-4, Position 15 states:

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

Compliance

[

]^{a,c}

5.6.16 ISG-4 Position 16

ISG-4, Position 16 states:

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

Compliance

[

]^{a,c}

5.6.17 ISG-4 Position 17

ISG-4, Position 17 states:

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

Compliance

[

]^{a,c}

5.6.18 ISG-4 Position 18

ISG-4, Position 18 states:

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

Compliance

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

5.6.19 ISG-4 Position 19

ISG-4, Position 19 states:

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

Compliance

[

]^{a,c}

5.6.20 ISG-4 Position 20

ISG-4, Position 20 states:

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

Compliance

[

]^{a,c}

6 SOFTWARE QUALITY

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

]^{a,c}

[

]^{a,c}

6.1 SOFTWARE QUALITY ASSURANCE

[

]^{a,c}

6.2 SOFTWARE CONFIGURATION MANAGEMENT

[

]^{a,c}

6.2.1 [ ]^{a,c}

[

]^{a,c}

a,c

Figure 6-1 [ ]^{a,c}

6.2.2 Previously Developed Software

[ ]^{a,c}

[

]^{a,c}

6.3 SOFTWARE VERIFICATION AND VALIDATION

[

]^{a,c}

6.3.1 [ ]^{a,c}

[

]^{a,c}

6.3.2 [ ]^{a,c}

[

]^{a,c}

[

]^{a,c}

6.3.3 [ ]^{a,c}

[

]^{a,c}

6.3.3.1 [ ]^{a,c}

[

]^{a,c}

6.3.3.2 [ ]^{a,c}

[

]^{a,c}

6.3.3.3 [ ]^{a,c}

[

]^{a,c}

6.3.3.4 [ ]^{a,c}

[

]^{a,c}

6.4 OPERATION AND MAINTENANCE

[

]a,c

7 EQUIPMENT QUALIFICATION

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

a,c

Figure 7-1 [ ]^{a,c}

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

a,c

Figure 7–2 [ ]^{a,c}

[

]a,c

7.1 COMPONENT CYCLING AND BURN-IN

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

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

7.2 ENVIRONMENTAL TESTING

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

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

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

The environmental qualification parameters for Common Q™ equipment installed in a cabinet, corresponding to the room ambient environment identified in Table 7-1, are tabulated in Table 7-2 and shown in Figure 7-4. These temperature and humidity parameters envelope requirements specified in Figure 7-3 and margin to satisfy the intent of IEEE 323-1983 (Reference 22 in Table 3).

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

]^{a,c}

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

a,c

Table 7-1 Cabinet Environmental Design Requirements

a,c

Table 7-2 Common Q™ Equipment Environmental Design Requirements

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

a,c

a,c

Figure 7-3 Original Environmental Test Profile

a,c

Figure 7-4 Modified Environmental Test Profile

7.3 SEISMIC TESTING

[

]a,c

7.3.1 [ ]a,c

[

]a,c

7.4 ELECTROMAGNETIC INTERFERENCE (EMI) TESTING

The baseline Common Q™ equipment is qualified in accordance with MIL Std 461D and MIL Std 462D as endorsed by RG 1.180, and EPRI TR-102323. Susceptibility and emissions testing of the equipment is performed for both conducted and radiated signals. The tests are performed on each system in various modes of operation such that successful completion of the test demonstrates that the safety system function has not been compromised and the equipment performs within its design specifications.

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

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

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

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

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

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

8 EQUIPMENT RELIABILITY

[

]a,c

8.1 FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

[

]a,c

[

]^{a,c}

[

]a,c

8.2 MEAN TIME BETWEEN FAILURES (MTBF) ANALYSIS

[

]^{a,c}

a,c

Table 8-1 [ ]^{a,c}

8.3 OPERATING HISTORY

[

]^{a,c}

8.3.1 [ ]^{a,c}

[

]^{a,c}

a,c

Figure 8-1 AC160 Nuclear Product Migration

[

]^{a,c}

[

]^{a,c}

a,c

[

]^{a,c}

Table 8-2 [ ]^{a,c}

a,c

Table 8-2 [ ]^{a,c}

a,c

Table 8-2 [ ]a,c

a,c

Table 8-2 [ ]^{a,c}

a,c

[

]^{a,c}

9 DEFENSE-IN-DEPTH AND DIVERSITY

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

10 COMMERCIAL GRADE DEDICATION PROGRAM

10.1 SCOPE

[

]^{a,c}

[

]^{a,c}

10.2 SOFTWARE ASSESSMENT PROCESS FOR SOFTWARE COMMERCIAL GRADE DEDICATION

[

]^{a,c}

10.2.1 [ ]^{a,c}

[ ]^{a,c}

10.2.1.1 [ ]^{a,c}

[ ]^{a,c}

10.2.1.2 [ ]^{a,c}

[ ]^{a,c}

10.2.1.3 [ ]^{a,c}

[ ]^{a,c}

[

]^{a,c}

10.2.1.4 [ ]^{a,c}

[

]^{a,c}

[

]^{a,c}

10.2.1.5 [ ]^{a,c}

[

]^{a,c}

10.2.1.6 [ ]^{a,c}

[

]^{a,c}

10.2.1.7 [ ]^{a,c}

[

]^{a,c}

10.2.1.8 [ ]^{a,c}

[ ]^{a,c}

10.2.2 [ ]^{a,c}

[ ]^{a,c}

10.2.3 [ ]^{a,c}

[ ]^{a,c}

10.2.4 [ ]^{a,c}

[ ]^{a,c}

10.3 SOFTWARE COMMERCIAL DEDICATION

[

]^{a,c}

10.4 HARDWARE COMMERCIAL DEDICATION

[

]^{a,c}

[

]^{a,c}

10.5 CONFIGURATION MANAGEMENT

[

]^{a,c}

11 COMMON Q™ PLATFORM COMPONENTS

[ ]^{a,c}

Table 11-1 [ ]^{a,c}

a,c

Table 11-1 [ ]^{a,c}

a,c

Table 11-1 [ ]^{a,c}

12 FUTURE PLATFORM CHANGES

[

]a,c

13 CONCLUSIONS

[

]^{a,c}

APPENDIX A
LIST OF APPENDICES

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

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

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

5. Common Qualified Platform Record of Changes