ENCLOSURE 4

WCAP-16675–NP

Revision 5

"AP1000™ Protection and Safety Monitoring System Architecture Technical Report"

(Non-Proprietary)

Westinghouse Non-Proprietary Class 3

WCAP-16675-NP
Revision 5
APP-GW-GLR-147
Revision 2

November 2010

AP1000™ Protection and Safety Monitoring System Architecture Technical Report

WCAP-16675-NP
Revision 5
APP-GW-GLR-147
Revision 2

AP1000™ Protection and Safety Monitoring System Architecture Technical Report

Edward P. Schindhelm/Robert E. Single for*, Principal Engineer
Reactor Protection Systems I,
Nuclear Automation

November 2010

Reviewers: John G. Ewald*, I&C Lead Engineer
Electronic Systems Integration

Thomas P. Hayes*, AP1000 Consultant
Reactor Protection Systems I

Warren R. Odess-Gillett*, Fellow Engineer
Safety Systems Platform Configuration Management

Approved: John S. Strong*, Program Manager
NuStart/DOE Design Finalization

*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	Author	Description
1	Jennifer T. Drylie	For the detailed record of changes for Revision 1, please see the record copy of that revision.
2	Jennifer T. Drylie	For the detailed record of changes for Revision 2, please see the record copy of that revision.
3	Jennifer T. Drylie	WCAP-16675-NP, Rev. 3 is now co-numbered as APP-GW-GLR-147, Rev. 0. The non-proprietary version of WCAP-16675 is now assigned a unique AP1000™ document number. Class 3 DCP changes. List of Acronyms and Abbreviations – Added terms per RAI-SRP 7.1-ICE-25. Changed ITP from Integrated Test Processor to Interface and Test Processor. Definitions – Added "hardwired" per RAI-SRP7.1-ICE-24. Added "partial trip" per RAI-SRP7.2-ICE-06. Added "fault tolerant" per RAI-SRP7.2-ICE-03. References – Added WCAP-16674-P per QUES-TR89-N. Added IEEE-100 which defines "fault tolerant." Added WCAP-16097-NP for consistency with WCAP-16674. Reflected that references APP-PMS-J1-002 through APP-PMS-J1-012 were combined into APP-PMS-J1-001. Deleted References 4, 5, and 6, as they are included in Reference 3. References 9 through 19 are obsolete documents; replaced Reference 9 with the replacement document and deleted References 10 through 19. Corrected the revision date for References 23 and 24 per IR #09-355-M010. Section 2.1 – Added clarification related to the bypass of two or more divisions per QUES-TR89-D. Subsection 2.2.1 – Added clarification about the IR range per QUES-TR89-E. Subsection 2.2.3.2.2 – Specified that the ILP is Advant® Controller 160 (AC160) per OI-SRP-7.2-04. Subsection 2.2.6 – Added a description of MTP per RAI-SRP7.9-ICE-04. Subsection 2.2.6.1 – Added text indicating that bypass is handled administratively per QUES-TR89-M. Subsection 2.2.6.2 – Modified text related to software loading per CI-SRP-7.9-01. Section 3.1 – Added clarification regarding AF100 message transfer per CI-SRP-7.9-ICE-01 and CI-SRP-7.9-ICE-02. Subsection 3.2.5 – Editorial.

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Author	Description
3 (cont.)	Jennifer T. Drylie	Subsection 3.3.1 – Removed text relating to communication isolation and IEEE 7-4.3.2 from the third paragraph as it does not apply to discrete hardwired signals per OI-SRP7.9-ICE-02. Modified Figure 3-1 to show the 2nd form of Case D communication. Subsection 3.3.2 – Removed text relating to communication isolation and IEEE 7-4.3.2 from the third paragraph as it does not apply to discrete hardwired signals per OI-SRP7.9-ICE-02. Subsection 3.3.3 – Modified Figure 3-2 to clarify the gateway interface. Modified text for consistency with WCAP-16674. Subsection 3.3.4 – Added text to the first paragraph describing the electrical isolation of the dedicated switches in the RSR per CI-SRP7.9-ICE-03. Removed text relating to communication isolation and IEEE 7-4.3.2 from the third paragraph as it does not apply to discrete hardwired signals per OI-SRP7.9-ICE-02. Modified text for consistency with WCAP-16674. Subsection 3.3.5 – Editorial. Removed the term "manual" because the non-safety interface is both automatic and manual. Removed references to "state-based" and "system-based" priority logic and added text describing the resulting priority as implemented on AP1000 per QUES-TR88-D. Modified Figure 3-3 to better define the CIM/SRNC interface. Subsection 3.4.2 – Editorial. Modified text for consistency with WCAP-16674. Subsection 5.1.5 – Changed "non-software based" to "FPGA based" for the CIM description per QUES-TR89-GG. Subsection 5.2.4 – Editorial. Modified text for consistency with WCAP-16674. Section 6.3 – Editorial. Modified the calibration description to reflect the design. Subsection 6.4.1 – Modified the bypass description per RAI-SRP7.2-ICE-02. Modified the last paragraph per OI-SRP-7.5-ICE-02. Section 7 – Modified the proprietary markings per QUES-TR89-KK.

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Author	Description
4	Edward P. Schindhelm	Incorporated DCP, APP-GW-GEE-1213, Rev. 0. Change made to Section 3.3.4. Incorporated DCP, APP-GW-GEE-1258, Rev 0. Change made to Section 1.1. Deleted any reference to cyber security per RAI-SRP7.8-DAS-11 Rev 0. Class 3 DCP and editorial changes: • Updated Reference 9 to Rev. 1 and Reference 30 to Rev. 3. Deleted Reference 20. • Subsection 2.2.2 – Deleted setpoints. • Subsection 2.2.6.2 – Deleted "permanent." • Subsection 3.3.2 – Resolved CAPs IR#10-161-M010 by adding a discussion of PMS actuation of non-safety loads. • Figure 4-1 – 18" flat panel display (FPD) dimension was incorrect. Removed dimension. • Subsection 5.1.3.1 – Added typically. • Subsection 5.1.5 – Deleted sentence "Because of its…failure analysis." • Subsection 4.2 – Changed Reference 20 to Reference 9. • Deleted unused acronyms. • Editorial corrections made to List of Trademarks, List of Definitions, References, and body of text.
5	Edward P. Schindhelm	Class 3 DCP: • Added subsection 2.2.8. • Revision numbers for References 9, 28, and 32 updated.

FORWARD

The AP1000™ Protection and Safety Monitoring System (PMS) described in this document provides protection against unsafe reactor operation during steady-state and transient power operations. The PMS initiates selected protective functions to mitigate the consequences of design basis events. This document identifies the functional performance requirements and describes the PMS system. The PMS safety system is designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power.

The AP1000 Design Control Document (DCD) (Reference 1) was written to permit the use of either the Eagle protection system hardware described in the AP600 DCD or the Common Qualified (Common Q) Platform. This document describes the Common Q implementation of the AP1000 PMS. The Common Q Platform is described in WCAP-16097-NP-A, "Common Qualified Platform" (Reference 2), and WCAP-16097-P Appendix 4, "Common Qualified Platform Integrated Solution" (Reference 3). The Common Q Platform was accepted by the U.S. Nuclear Regulatory Commission (NRC) via the Safety Evaluation Reports in Reference 2.

Section 1 of this document summarizes the AP1000 PMS functional requirements, which received Design Certification, and are compatible with the Common Q hardware and software. Section 2 describes the Common Q architecture for the AP1000 PMS. Section 3 addresses the interfaces and communications between the safety system divisions and between the safety system and non-safety systems. Section 4 describes the Safety/Qualified Data Processing System (QDPS) display implementation. Section 5 is a brief description of the Common Q Platform that was described in more detail in References 2 and 3. Section 6 describes the maintenance, test and calibration features of the PMS implementation. Section 7 is the summary and conclusion.

The PMS architecture described in this report is the same as the PMS architecture described in WCAP-16438-P, "FMEA of AP1000 Protection and Safety Monitoring System" (Reference 21).

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

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.

1oo2	One-out-of-two
1oo3	One-out-of-three
2oo3	Two-out-of-three
2oo4	Two-out-of-four
AC	Alternating Current
AC160	Advant® Controller 160
ACC	AMPL Control Configuration
ADC	Analog-to-Digital Converter/Conversion
ADS	Automatic Depressurization System
AF100	Advant Fieldbus 100
AMPL	Advant Master Programming Language
AOI	Advant Ovation® Interface
ASCII	American National Standard Code for Information Interchange
BPL	Bistable Processor Logic
CDP	Cyclic Data Packet
CIM	Component Interface Module
Common Q	Common Qualified
CPU	Central Processing Unit
CVS	Chemical and Volume Control System
DAC	Digital-to-Analog Converter/Conversion
DAS	Diverse Actuation System
DB	Database
DC	Direct Current
DCD	Design Control Document
DDS	Data Display and Processing System
DVD-ROM	Digital Video Disc Read-only Memory
Enet	Ethernet
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FMEA	Failure Modes and Effects Analysis
FOM	Fiber-Optic Modem
FOR	Fiber-Optic Receiver
FOT	Fiber-Optic Transmitter
FPD	Flat Panel Display
FPDS	Flat Panel Display System
Func	Function
HDLC	High-Level Datalink Control
HSL	High Speed Link
I&C	Instrumentation and Control
I/E	Current-to-Voltage Isolator

LIST OF ACRONYMS AND ABBREVIATIONS (cont.)

I/O	Input/Output
ICP	Integrated Communications Processor
ILP	Integrated Logic Processor
IR	Intermediate Range
ITP	Interface and Test Processor
LCL	Local Coincidence Logic
LED	Light Emitting Diode
Maint	Maintenance
MCR	Main Control Room
MTC	Maintenance and Test Cabinet
MTP	Maintenance and Test Panel
NI	Nuclear Instrumentation
NIS	Nuclear Instrumentation Subsystem
NISPA	Nuclear Instrumentation Signal Processing Assembly
NooM	N-out-of-M
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
PC	Process Control
PDSP	Primary Dedicated Safety Panel
PLC	Programmable Logic Controller
PLS	Plant Control System (AP1000)
PM	Processor Module
PMS	Protection and Safety Monitoring System
PR	Power Range
PRHR	Passive Residual Heat Removal
PROM	Programmable Read Only Memory
QDPS	Qualified Data Processing System
Qual	Qualified
RCS	Reactor Coolant System
RNC	Remote Node Controller
ROM	Read Only Memory
RSR	Remote Shutdown Room
RT	Reactor Trip
RTCB	Reactor Trip Circuit Breaker
RTD	Resistance Temperature Detector
SDSP	Secondary Dedicated Safety Panel
SER	Safety Evaluation Report
SOE	Sequence of Events
SR	Source Range
SRAM	Static Random Access Memory
SRNC	Safety Remote Node Controller
ST	Shunt Trip
SVC	Squib Valve Controller
TFT	Thin-Film Transistor

LIST OF ACRONYMS AND ABBREVIATIONS (cont.)

UPS	Uninterruptible Power Supply
UV	Undervoltage
V&V	Verification and Validation
WDT	Watchdog Timer

LIST OF TRADEMARKS

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

AP1000™ is a trademark of Westinghouse Electric Company LLC.

Intel® is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Ovation® is a registered trademark of Emerson Process Management.

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

Windows® is a registered trademark Microsoft Corporation in the United States and/or other countries.

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.

LIST OF DEFINITIONS

Actuated Equipment:

The assembly of prime movers and driven equipment used to accomplish a protective function (such as solenoids, shutdown rods, and valves) (Reference 1, Section 7.1).

Actuation Device:

A component that directly controls the motive power for actuated equipment (such as circuit breakers, relays, and pilot valves) (Reference 1, Section 7.1).

Channel:

An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined (Reference 7, Section 2).

Component-Level Actuation:

The actuation of a single actuation device (component) (Reference 1, Section 7.1).

Division:

The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components (IEEE Standard 603-1991 {Reference 7}, Section 2).

Fault Tolerant

Pertaining to a system or component that is able to continue normal operation despite the presence of faults (IEEE Standard 100-2000 {Reference 29}).

Hardwired

A dedicated (non-multiplexed) point-to-point connection between two devices via electrical wires or cables.

Partial Trip

The condition during which either redundant half of a protection channel is set to its tripped state. Partial trips are logically ORed into a single channel trip value at the local coincident logic (LCL) before being applied to its respective NooM channel vote.

LIST OF DEFINITIONS (cont.)

Protection and Safety Monitoring System:

The aggregate of electrical and mechanical equipment, which senses generating station conditions and generates the signals to actuate reactor trip and engineered safety features, and which provides the equipment necessary to monitor plant safety-related functions during and following designated events (Reference 1, Section 7.1).

Protective Function:

Any one of the functions necessary to mitigate the consequences of a design basis event. Protective functions are initiated by the Protection and Safety Monitoring System logic and will be accomplished by the trip and actuation subsystems. Examples of protective functions are reactor trip and engineered safety features (such as valve alignment and containment isolation) (Reference 1, Section 7.1).

Safety System:

The aggregate of electrical and mechanical equipment necessary to mitigate the consequences of design basis events (Reference 1, Section 7.1).

System-Level Actuation:

The actuation of a sufficient number of actuation devices to affect a protective function (Reference 1, Section 7.1).

REFERENCES

1. APP-GW-GL-700 (Non-Proprietary), Rev. 17, Chapter 7, "AP1000 Design Control Document," Westinghouse Electric Company LLC.

2. WCAP-16097-NP-A (Non-Proprietary), Rev. 0, "Common Qualified Platform Topical Report," Westinghouse Electric Company LLC. (This document is also referred to as CENPD-396-P-A, Revision 2.)

3. WCAP-16097-P-A, Appendix 4 (Proprietary), Rev. 0, "Common Qualified Platform Integrated Solution," Westinghouse Electric Company LLC. (This document is also referred to as CENPD-396-P, Appendix 4, Task-1067, Revision 2.)

4. Deleted.

5. Deleted.

6. Deleted.

7. IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc., 1991.

8. WCAP-15776 (Non-Proprietary), Rev. 0, "Safety Criteria for the AP1000 Instrument and Control Systems," Westinghouse Electric Company LLC.

9. APP-PMS-J1-001, Rev. 2, "AP1000 Protection and Safety Monitoring System Functional Requirements," Westinghouse Electric Company LLC.

10. Deleted.

11. Deleted.

12. Deleted.

13. Deleted.

14. Deleted.

15. Deleted.

16. Deleted.

17. Deleted.

REFERENCES (cont.)

18. Deleted.

19. Deleted.

20. Deleted.

21. WCAP-16438-P (Proprietary), Rev. 2, "FMEA of AP1000 Protection and Safety Monitoring System," Westinghouse Electric Company LLC.

22. Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," U.S. Nuclear Regulatory Commission, Revision 3, May 1983.

23. IEEE Standard 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc., 1993.

24. IEEE Standard 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuit," Institute of Electrical and Electronics Engineers, Inc., 1992.

25. IEEE Standard 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc., 1998.

26. NUREG-0800, Rev. 4, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, June 1997.

27. Regulatory Guide 1.62, "Manual Initiation of Protective Actions," U.S. Nuclear Regulatory Commission, October 1973.

28. WNA-PS-00016-GEN (Proprietary), Rev. 5, "Standard Acronyms and Definitions," Westinghouse Electric Company LLC.

29. IEEE Standard 100-2000, "IEEE 100 The Authoritative Dictionary of IEEE Standards Terms Seventh Edition," Institute of Electrical and Electronics Engineers, Inc, 2000.

30. WCAP-16674-P (Proprietary), Rev. 3, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," Westinghouse Electric Company LLC.

31. WCAP-16096-NP-A (Non-Proprietary), Rev. 1A, "Software Program Manual for Common Q Systems," Westinghouse Electric Company LLC.

32. APP-PMS-J4-105, Rev. 2, "AP1000 Protection and Safety Monitoring System Component Functional Logic Specification," Westinghouse Company LLC.

1 AP1000 PMS FUNCTIONAL REQUIREMENTS

The Protection and Safety Monitoring System (PMS) performs the reactor trip (RT) functions, the engineered safety features (ESF) actuation functions, and the Qualified Data Processing System (QDPS) functions.

During normal operation, administrative procedures and plant control systems serve to maintain the reactor in a safe state, preventing damage to the three barriers (fuel clad, reactor coolant system, and reactor containment building) that prevent the spread of radioactive material to the environment. Accident conditions causing one or more of the barriers to be threatened can occur. The PMS monitors key plant parameters and automatically initiates various protective functions to prevent violation of any of the three barriers, or if violation of a barrier cannot be prevented, to maintain the integrity of the remaining barriers. This ensures that, given a design basis event, the site boundary radiation releases will be below U.S. Nuclear Regulatory Commission (NRC) limits. The system performs its functions by actuating a variety of equipment and by monitoring the plant process using a variety of sensors and operations performing calculations, comparisons, and logic based on those sensor inputs. The PMS functional requirement documents discuss the protective functions that are performed and the requirements these functions place on the equipment that performs them.

1.1 REACTOR TRIP FUNCTIONS

The PMS generates an automatic reactor trip for the following conditions:

1. Source Range High Neutron Flux Trip as described in APP-PMS-J1-001, "AP1000 Protection and Safety Monitoring System Functional Requirements" (Reference 9).

2. Intermediate Range High Neutron Flux Trip as described in Reference 9.

3. Power Range High Neutron Flux Trip (Low Setpoint) as described in Reference 9.

4. Power Range High Neutron Flux Trip (High Setpoint) as described in Reference 9.

5. Power Range High Positive Flux Rate Reactor Trip as described in Reference 9.

6. Over-temperature ΔT Reactor Trip as described in Reference 9.

7. Overpower ΔT Trip as described in Reference 9.

8. Reactor Trip on Low Pressurizer Pressure as described in Reference 9.

9. Reactor Trip on Low Reactor Coolant Flow as described in Reference 9.

10. Reactor Trip on Reactor Coolant Pump Underspeed as described in Reference 9.

11. Reactor Coolant Pump Bearing Water Temperature Trip as described in Reference 9.

12. Pressurizer High Pressure Reactor Trip as described in Reference 9.

13. Pressurizer High Water Level Reactor Trip as described in Reference 9.

14. Reactor Trip on Low Water Level in any Steam Generator as described in Reference 9.

15. High-2 Steam Generator Water Level in Any Steam Generator as described in Reference 9.

16. Automatic Depressurization Systems Actuation Reactor Trip as described in Reference 9.

17. Core Makeup Tank Actuation Reactor Trip as described in Reference 9.

18. Reactor Trip on Safeguards Actuation as described in Reference 9.

19. Manual Reactor Trip as described in Reference 9.

20. Passive Residual Heat Removal (PRHR) Actuation Reactor Trip as described in Reference 9.

1.2 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM FUNCTIONS

AP1000™ provides instrumentation and controls to sense accident situations and initiate engineered safety features (ESF). The occurrence of a limiting fault, such as a loss of coolant accident or a secondary system break, requires a reactor trip plus actuation of one or more of the engineered safety features. This combination of events prevents or mitigates damage to the core and reactor coolant system components, and provides containment integrity.

The PMS is actuated when safety system setpoints are reached for selected plant parameters. The selected combination of process parameter setpoint violations is indicative of primary or secondary system boundary challenges. Once the required logic combination is generated, the PMS equipment sends the signals to actuate appropriate ESF components.

The following is a list of the ESF system-level actuations initiated by the PMS:

1. Safeguards Actuation as described in Reference 9.

2. Containment Isolation as described in Reference 9.

3. In-Containment Refueling Water Storage Tank Injection as described in Reference 9.

4. Core Makeup Tank Injection as described in Reference 9.

5. Automatic Depressurization System Actuation (Stages 1-3 and Stage 4) as described in Reference 9.

6. Reactor Coolant Pump Trip as described in Reference 9.

7. Main Feedwater Isolation as described in Reference 9.

8. Passive Residual Heat Removal Actuation as described in Reference 9.

9. Turbine Trip as described in Reference 9.

10. Containment Recirculation as described in Reference 9.

11. Steam Line Isolation as described in Reference 9.

12. Steam Generator Blowdown System Isolation as described in Reference 9.

13. Passive Containment Cooling Actuation as described in Reference 9.

14. Startup Feedwater Isolation as described in Reference 9.

15. Boron Dilution Block as described in Reference 9.

16. Chemical and Volume Control System (CVS) Isolation as described in Reference 9.

17. Steam Dump Control as described in Reference 9.

18. Main Control Room Isolation as described in Reference 9.

19. Auxiliary Spray and Purification Line Isolation as described in Reference 9.

20. Containment Air Filtration Isolation as described in Reference 9.

21. Refueling Cavity Isolation as described in Reference 9.

22. CVS Letdown Isolation as described in Reference 9.

23. Pressurizer Heater Block as described in Reference 9.

24. Steam Generator Relief Isolation as described in Reference 9.

25. Normal Residual Heat Removal Containment Isolation as described in Reference 9.

26. Demineralized Water Transfer and Storage System Isolation as described in Reference 9.

27. Reactor Vessel Head Vent Valve Control (as described in Reference 32).

1.3 QUALIFIED DATA PROCESSING SYSTEM

The AP1000 processing and display function is performed by equipment that is part of the PMS, Plant Control System (PLS), and the Data Display and Processing System (DDS).

The PMS provides signal conditioning, communications, and display functions for Regulatory Guide 1.97 (Reference 22), Category 1 variables and for Category 2 variables that are energized from the Class 1E direct current (DC) uninterruptible power supply system. The PLS and the DDS provide signal conditioning, communications, and display functions for Category 3 variables and for Category 2 variables that are energized from the non-Class 1E DC uninterruptible power system. The DDS also provides an alternate display of the variables, which are displayed by the PMS. Electrical separation of the DDS and the PMS is maintained through the use of isolation devices in the interconnections between the two systems.

The portion of the PMS that is dedicated to providing the safety-related display function is referred to as the Qualified Data Processing Subsystem (QDPS). The QDPS provides safety-related display of selected parameters in the control room. The QDPS consists of a redundant configuration of sensors, QDPS hardware, and qualified displays.

The QDPS performs the following functions:

- Provides safety-related data processing and display.
- Provides the operator with sufficient operational data to safely shut the plant down in the event of a failure of the other display systems.
- Provides qualified and nonqualified data to the Real-Time Data Network for use by other systems in the plant.
- Processes data for main control room (MCR) display, and to meet Regulatory Guide 1.97 (Reference 22) requirements.
- Provides data to the MCR, the remote shutdown workstation, the plant computer, other non-safety-related devices, and nonqualified emergency response facilities.

1.4 COMPONENT CONTROL FUNCTIONS

Control of individual safety-related components that perform Class 1E functions is provided. Component control consists of the following functions:

1. Resolution of multiple demands for a given component from various systems
2. Application of manual component demands
3. Performance of the component protection logic (torque limit, anti-pump latch, etc.)
4. Reporting of component status to the plant information system
5. Local component control

The inputs required for control of individual components are:

1. System-level actuation commands from the reactor trip and ESF actuation logic.
2. System-level actuation commands from the fixed-position switches in the MCR and remote shutdown room (RSR).

3. Individual safety component control commands from the non-safety PLS for component actuations with no onerous consequences (for test, maintenance, restoration and non-credited actuations).

4. Individual safety component control commands from the safety displays in the MCR for component actuations with onerous consequences.

5. Component feedback signals from the individual safety components.

The outputs to individual components consist of hardwired control signals to open or close a valve solenoid, motor-operated valve, or circuit breaker.

2 AP1000 PROTECTION AND SAFETY MONITORING SYSTEM DESCRIPTION

The PMS provides detection of off-nominal conditions and actuation of appropriate safety-related functions necessary to achieve and maintain the plant in a safe shutdown condition. The PMS controls safety-related components in the plant that are operated from the MCR or remote shutdown workstation.

In addition, the PMS provides the equipment necessary to monitor the plant's safety-related functions during and following an accident as required by Regulatory Guide 1.97 (Reference 22).

2.1 PMS ARCHITECTURE FOUR-DIVISION OVERVIEW

The AP1000 PMS consists of four redundant divisions, designated A, B, C, and D, as depicted on Figure 2-1. The PMS performs the necessary safety-related signal acquisition, calculations, setpoint comparison, coincidence logic, reactor trip/ESF actuation functions, and component control functions to achieve and maintain the plant in a safe shutdown condition. The PMS also contains maintenance and test functions to verify proper operation of the system. The PMS includes four redundant safety displays, one for each division, located on the Primary Dedicated Safety Panel (PDSP) in the MCR. Four redundant divisions are provided to satisfy single failure criteria and improve plant availability.

[

]^{a,c}

References 2 and 3 describe the Common Qualified (Common Q) hardware platform, which comprises the PMS configuration for the AP1000. The Common Q Platform, described in References 2 and 3, was accepted by the NRC via the Safety Evaluation Reports in Reference 2.

a,c

Figure 2-1 AP1000 PMS Architecture Four-Division Overview

The Instrumentation and Control (I&C) equipment performing reactor trip and ESF actuation functions, their related sensors, and the reactor trip switchgear are, for the most part, four-way redundant. This redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting to a two-out-of-three (2oo3) logic from a two-out-of-four (2oo4) logic.

Four redundant measurements, using four separate sensors, are made for each variable used for reactor trip. One measurement is processed by each division. Analog signals are converted to digital form by analog-to-digital converters (ADCs) within the division's BPL. Signal conditioning is applied to selected inputs following the conversion to digital form. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a parameter is generated if the channel's measurement exceeds its predetermined or calculated limit. Processing of variables for reactor trip is identical in each of the four redundant divisions of the protection system. [

]^{a,c} The LCL in each division is capable of generating a reactor trip signal if two or more of the redundant channels for a single variable are in the partial trip state.

The reactor trip signal from each of the four divisions of the PMS is sent to that division's reactor trip circuit breakers (RTCBs).

Each division controls two RTCBs. The reactor is tripped when two or more actuation divisions output a reactor trip signal opening their breakers. This automatic trip demand signal initiates the following two actions. It de-energizes the undervoltage (UV) trip attachments on the RTCBs, and it energizes the shunt trip (ST) devices on the RTCBs. Either action causes the breakers to trip. Opening the appropriate trip breakers by two divisions removes power to the rod drive mechanism coils, allowing the rods to fall into the core. This rapid negative reactivity insertion causes the reactor to shut down.

Bypass of a protection channel that generates a reactor trip signal and bypass of a reactor trip actuation division is permitted because the single failure criterion is met even when one channel or division is bypassed. Bypassing two or more redundant channels or divisions is not allowed and is handled via the design.

2.2 PMS ARCHITECTURE 1 DIVISION DETAIL

Figure 2-2 is a block diagram illustrating one division of the PMS subsystems for the Common Q architecture. Each division of the PMS contains the following major subsystems:
[

]^{a,c}

[

]a,c

The PMS subsystems contain the necessary equipment to perform the following functions:
[

]a,c

2.2.1 Nuclear Instrumentation Subsystem

[

]a,c

In each division, the neutron flux is monitored with three detector ranges: Source Range (SR), Intermediate Range (IR), and Power Range (PR). The signals derived from these detectors provide an indication of reactor power from 10E-8 percent to 200 percent. The processed signals are used to provide nuclear startup and overpower protection. The IR is capable of measuring reactor power to 200 percent for PAMs purposes only.

a,c

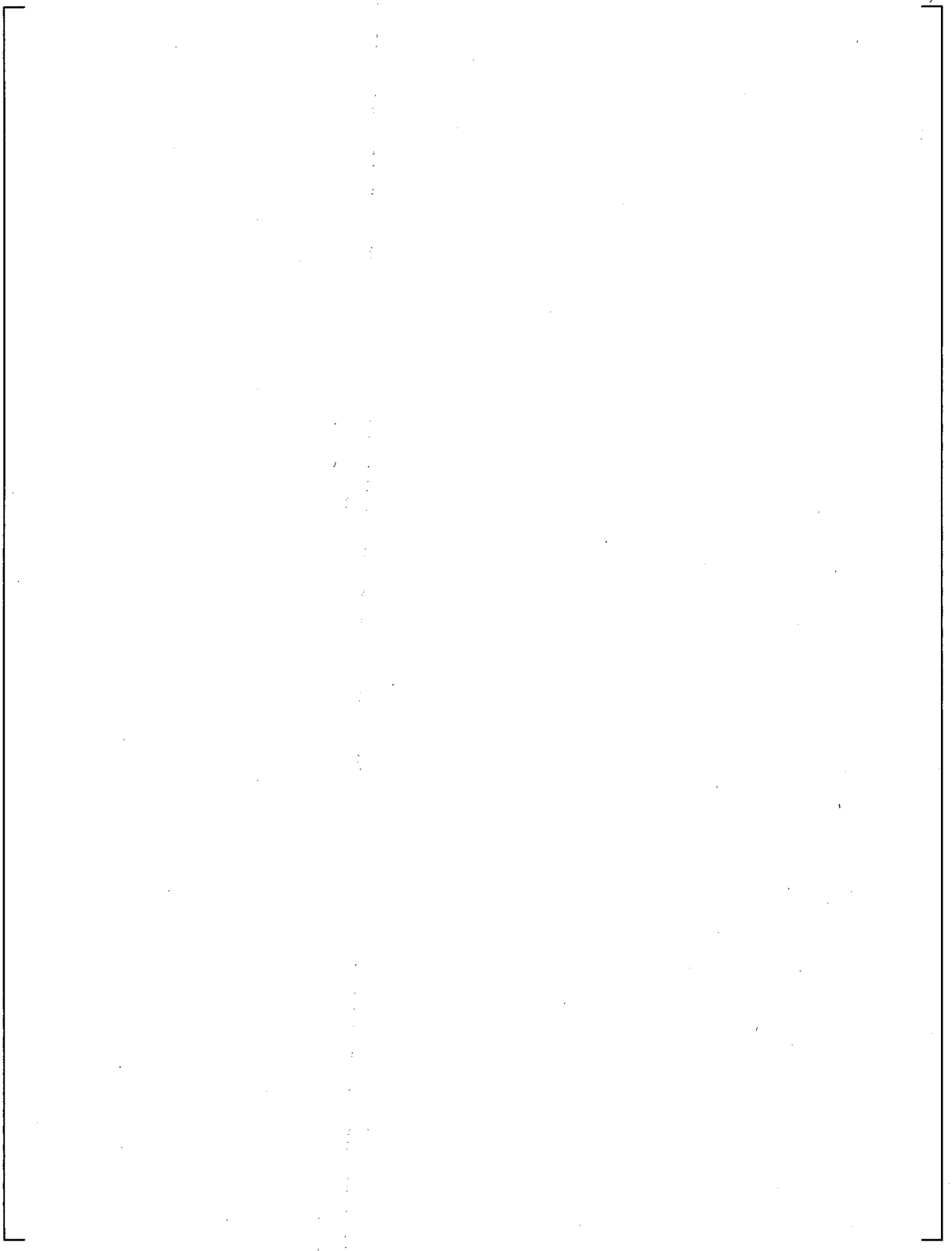

Figure 2-2 PMS Architecture 1 Division Detail

Three types of neutron detectors are used to monitor the leakage neutron flux from a complete shutdown condition to 120 percent of full power. Detector types for these three ranges are:

- SR – BF3 proportional counter
- IR – fission chamber
- PR – uncompensated ion chamber

The SR channel covers six decades of leakage neutron flux. The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with shutdown reactivity. This generally is greater than two counts per second. The IR channel covers eight decades. Detectors and instrumentation are chosen to provide overlap between the higher portion of the SR and the lower portion of the IR channels. The PR covers approximately two decades of the total instrument range. This is a linear range that overlaps the higher portion of the IR. The neutron detectors are installed in tubes located around the reactor vessel in the primary shield. The NI subsystem consists of the following hardware:

- SR detector, IR detector, and PR upper and lower detectors
- SR and IR preamplifiers
- NI system cabinet
- Field wiring, junction boxes, and containment penetrations

[

]^{a,c}

2.2.1.1 Neutron Detectors

2.2.1.1.1 Source Range Detector

The SR detector is used for startup and operation at very low reactor powers. High-voltage power to the SR detector is removed when the reactor is operating above the P10 permissive.

2.2.1.1.2 Intermediate Range Detector

The IR detector overlaps the operating range of the SR and PR channels.

2.2.1.1.3 Power Range Detector

The PR detectors provide the most accurate indication of reactor power over the range of 0.5 percent to 120 percent power. The PR channel is calibrated periodically at the current operating power level against calorimetric power.

2.2.1.2 Preamplifiers

2.2.1.2.1 Source Range Preamplifier

The SR preamplifier is located on a wall outside containment and receives the signal from the SR detector. The low-level signal is amplified and transmitted to the NI subsystem by the SR preamplifier. The SR preamplifier receives its operating power from the NI cabinet power supply. The SR preamplifier transmits its output signal to the NI cabinet by multi-conductor cable. The SR preamplifier contains embedded test circuitry that can be remotely activated from the MTP.

2.2.1.2.2 Intermediate Range Preamplifier

The IR preamplifier is located on a wall outside containment and receives the signal from the IR detector. The low-level signal is amplified and transmitted to the NI subsystem by the IR preamplifier. The IR preamplifier receives its operating power from the NI cabinet power supply. The IR preamplifier transmits its output signal to the NI cabinet by fiber-optic cables. The IR preamplifier contains embedded test circuitry that can be remotely activated from the MTP.

2.2.1.3 Nuclear Instrumentation Cabinet

[

]^{a,c} The SR high-voltage power supply can be de-energized to prevent damage to the SR detector when reactor power exceeds the upper limit of the SR detector.

NI signal processing and algorithms are performed by redundant Common Q subracks in the BPL cabinet. The Common Q hardware is described in References 2 and 3.

The NI power supply receives vital bus power and generates various DC voltages for use within the NI cabinet.

2.2.2 Bistable Processor Logic Subsystem

The PMS subsystems require data from field sensors and manual inputs (such as system-level blocks and resets) from the MCR to perform the protective function calculations. The results of the calculations drive the corresponding partial trip inputs of the reactor trip and ESF coincidence logic.

[

]^{a,c} The description provided below illustrates the operation of one of the four identical divisions.

[

]^{a,c}

The following description of the BPL subsystem applies equally to BPL-A1 and its redundant counterpart BPL-A2.

[

]^{a,c}

a,c

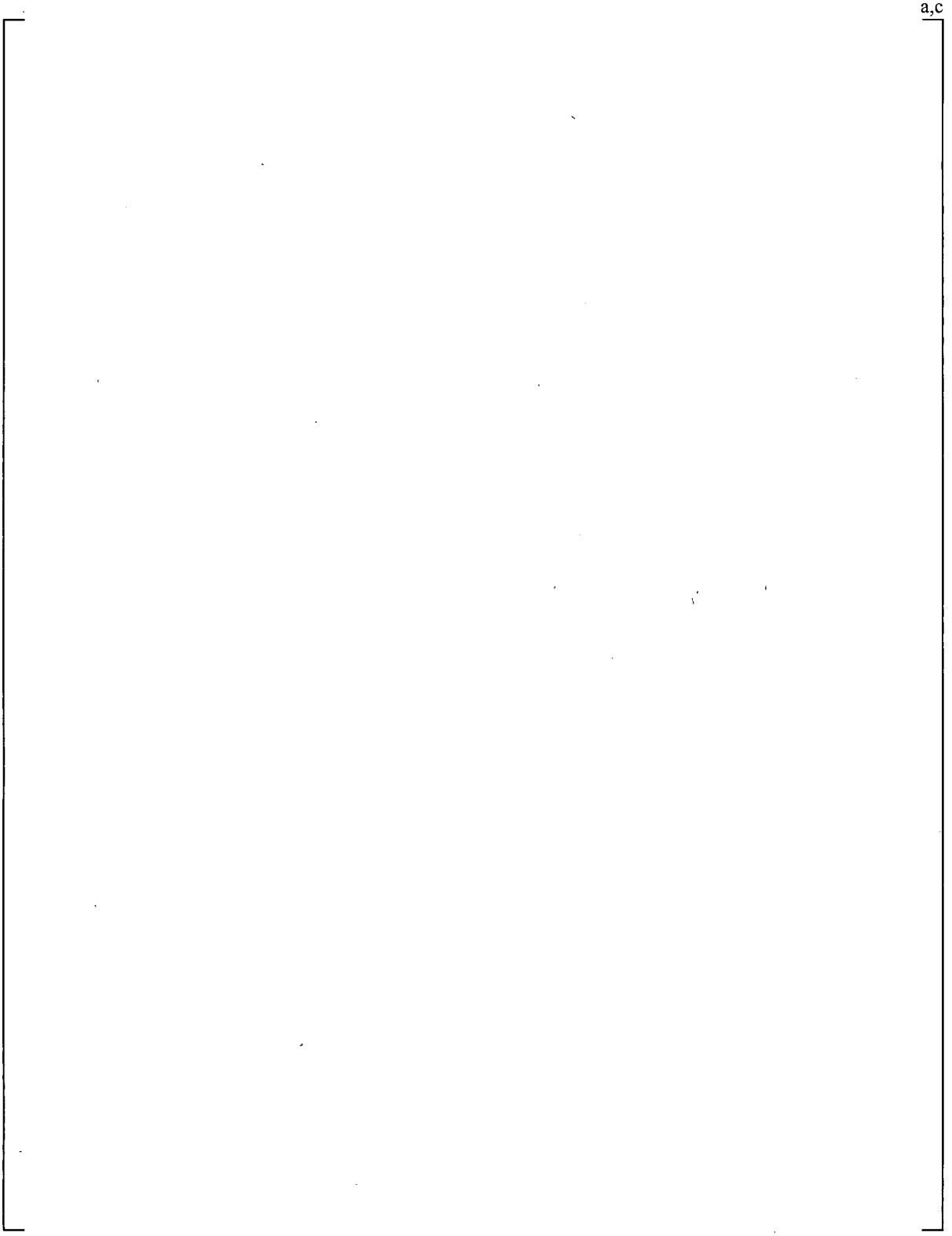

Figure 2-3 Division Redundancy

2.2.2.1 BPL Analog Inputs

The BPL subsystem interfaces with the process signals that measure the plant process parameters necessary to generate a reactor trip or ESF actuation and with the interlock signals from the ex-core nuclear instrumentation. Analog input modules acquire the analog process signal information. Process signals are generally 4 to 20 mA or 0 to 10 VDC, and are obtained from the channel-specific process transmitters. Other inputs include SR, IR, and PR nuclear instrumentation power level signals and resistance temperature detector (RTD) inputs for temperature measurement.

2.2.2.2 BPL Digital Inputs

Digital input modules acquire the digital signals from the NI subsystems.

2.2.2.3 BPL Processing Module

The BPL processor modules perform all pressure, temperature, level, flow, and NI algorithms and compare the results to predefined limits. A partial reactor trip or ESF actuation signal is generated if the setpoint is reached. [

]^{a,c}

2.2.2.4 BPL Analog Outputs

[

]^{a,c}

2.2.2.5 BPL Digital Outputs

[

]^{a,c}

2.2.2.6 BPL Communication

[

]^{a,c}

2.2.2.7 BPL Cross-Division Communication

[

]^{a,c}

[

]a,c

2.2.3 Local Coincidence Logic Subsystem

[

]a,c

The LCL subsystem acts to initiate a reactor trip or ESF actuation when a pre-determined condition in 2oo4 independent safety divisions reaches a partial trip or partial actuation state. The LCL also provides for the bypass of trip or actuation functions to accommodate periodic tests and maintenance. The LCL subsystem performs two primary functions:

1. The reactor trip coincidence logic performs the logic to combine the partial trip signals from the BPL subsystems and generates a fault tolerant trip output signal to the reactor trip switchgear and initiation logic.

2. The ESF coincidence logic performs the logic to combine the partial actuation signals from the BPL subsystems along with automatic and manual permissives, blocks, and resets to generate a fault tolerant actuation output signal to the ILP subsystems.

[

]a,c

2.2.3.1 Reactor Trip Coincidence Logic

[

]a,c

[

]a,c De-energizing the associated RTCB UV coil or energizing the RTCB ST coil forces the associated RTCB to open.

[

]a,c

2.2.3.1.1 Reactor Trip Switchgear Interface and Initiation Logic

[

]a,c

[

]a,c

2.2.3.1.2 Reactor Trip Circuit Breakers

The RTCBs are used to initiate reactor shutdown. The RTCBs connect the electrical motive power, supplied from motor generator sets, to the rod control system. The rod control system holds the control rods in position as long as electrical power is available. When the PMS senses that established limits for safe operation of the plant have been, or are about to be, exceeded, a command is generated to de-energize the UV trip device and energize the ST device in the RTCBs. This opens the breakers, disconnecting the power to the rod control system. When power is removed, the control rods drop by gravity into the reactor core, initiating the shutdown process.

[

]a,c

2.2.3.1.3 Manual Reactor Trip

A manual reactor trip is an entirely hardware based function that is initiated from the MCR by redundant momentary switches. The switches directly interrupt the power from the voting logic, actuating the UV and ST attachments in all four divisions. Figure 2-3 illustrates a simplified version of the implementation of the manual reactor trip function.

2.2.3.1.4 Availability

[

]^{a,c}

2.2.3.2 Engineered Safety Features Coincidence Logic

The ESF subsystem performs two primary functions:

1. The ESF coincidence logic function performs system-level logic calculations, such as actuation of the passive residual heat removal system. It receives inputs from the BPL subsystems, the MCR and RSR fixed-position switches.

2. The ESF component control function consists of the Integrated Logic Processors (ILPs), which perform the component fan-out for each ESF system-level actuation, and component interface modules (CIMs) that provide the capability for on/off control of individual safety-related plant components. The CIMs receive inputs from the ILPs and from the plant control system (PLS).

2.2.3.2.1 ESF Coincidence Logic Function

[

]^{a,c} The primary functions of the ESF logic processors are to process inputs, calculate system-level actuation, combine the automatic actuation with the manual actuation and manual bypass data, and transmit the data to the ILPs. To perform the ESF coincidence logic calculations, the ESF processors require data from the BPL subsystems, and also use manual inputs (such as setpoints and system-level blocks and resets) from the MCR and the remote shutdown workstation.

The ESF logic processors perform the following functions:

- Receive bistable data supplied by the four divisions of BPL subsystems and perform 2oo4 voting on this data.

- Implement system-level logic and transmit the output to the ILP processors for ESF component fan-out and actuation.

- Process manual system-level actuation commands received from the MCR and RSR.

Figure 2-3 illustrates the interconnection of BPL subsystems to ESF logic processors for the Common Q architecture.

2.2.3.2.2 Engineered Safety Features Component Control Function

The ESF component control function is implemented with redundant ILPs and CIMs that provide a distributed interface between the safety system and the plant operator for control of non-modulating safety-related plant components. Non-modulating control relates to the opening or closing of solenoid valves and solenoid pilot valves, and the opening or closing of motor-operated valves and dampers. The ESF component control function implements criteria established by the fluid systems designers for permissive and interlock logic applied to the component actuations. It also provides the plant operator with information on the equipment status, such as indication of component position (full closed, full open, valve moving), component control modes (manual, automatic, local, remote), or abnormal operating condition (power not available, failure detected).

[

]^{a,c}

Figure 2-3 illustrates the communication between the ESF coincidence logic and the ESF control logic for the Common Q architecture.

2.2.4 Integrated Communications Processor Subsystem

[ ]^{a,c} One ICP subsystem is located in each of the four independent divisions of the PMS. The divisions are physically separated and electrically isolated from each other. The following description illustrates the operation of one of the four identical divisions.

[

]^{a,c}

The data sent to the other PMS divisions and the data received from the other PMS divisions is used only by the QDPS for display in the MCR to meet Regulatory Guide 1.97 (Reference 22) Post-Accident Monitoring System requirements and for diagnostic purposes. This data is not used for any reactor trip or ESF actuation function.

[

]^{a,c}

2.2.5 Interface and Test Processor Subsystem

[

]^{a,c} The divisions are physically separated and electrically isolated from each other. The following description illustrates the operation of one of the four identical divisions.

[

]a,c

[

]a,c

2.2.6 Maintenance and Test Panel Subsystem

[

]a,c The following description illustrates the operation of one of the four identical divisions.

The MTP provides the human-interface to the safety system and is used for maintenance and test functions. The MTP provides the means for the technician to perform the following functions:
[

]a,c

Within each division of the safety system, one Flat Panel Display System, the MTP, provides access to calibration data, surveillance testing, establishment of conditions (surveillance test conditions, calibrations, functional bypass, etc.), and functional software modifications. The MTP is contained in the Maintenance and Test Cabinet (MTC) located in the I&C equipment room. A Function Enable keyswitch on the MTP must be set to the 'ENABLE' position prior to any operation that may take a safety function out of service or change the status of a safety function (e.g., surveillance test conditions, calibrations, functional bypass, etc.). When the Function Enable keyswitch is enabled, a visual alarm is generated on the Safety Display in the MCR. When the Function Enable keyswitch is disabled, all surveillance test conditions are removed and all external inputs to the Safety System functions are restored.

Each MTP consists of a touch screen video display and a PC Node Box, as depicted in Figure 2-2. The MTP is described in References 2 and 3 and was accepted by the NRC via the Safety Evaluation Reports in Reference 2.

[

]a,c

The MTP also has non-volatile memory used for storing setpoints, calibration constants, and maintenance information to support system "warm" starts.

2.2.6.1 Setpoint and Calibration Constant Changes

[

]^{a,c}

2.2.6.2 Program Changes

The AC160 is designed to load software in two ways. One way is to program the AC160 over the AF100 bus. Even though this network and the only programming source (the MTP) are totally contained within a division of the PMS, this mode of programming is prevented. This is accomplished by using the AC160 Function Chart Builder tool to configure the equipment to not accept AF100 bus programming.

The other way to load software into the AC160 is by a serial connection between the division's MTP and the AC160. Within a division, a separate cable is routed from the MTC to each cabinet containing an AC160 processor module (PM646A). This configuration allows for software loading to any processor module within a division from the MTP. The software loading cable is normally disconnected on each end.

[

]^{a,c}

To perform a software update, the cable (coming from the cabinet containing the target processor module) in the MTC is connected to the MTP. The opposite end of the software loading cable is connected to the target AC160 processor module (PM646A) and the software update is performed from the MTP. The cable is alternately connected to each processor module in the cabinet requiring a software update. Upon completion of all software updates in the cabinet, both sides of the software download cable are disconnected. This process is repeated for each cabinet containing a processor module requiring an update.

2.2.6.3 Interface to Plant Control System

[

]^{a,c}

2.2.7 Sequence of Events Subsystem

The PMS BPL and LCL subsystems provide sequence of events (SOE) points to the PLS for SOE recording. [

]^{a,c}

2.2.8 Watchdog Timer Implementation

[

]^{a,c}

a,c

Figure 2-4 Watchdog Timer Configuration

Table 2-1 Processor Module WDT Arrangement Watchdog Timer Summary a,c

3 EXTERNAL SYSTEM INTERFACES & COMMUNICATIONS

Communication within the safety system consists primarily of the four intra-divisional safety communication networks and safety datalink interfaces. A summary of the safety-to-non-safety system communications is provided in this report. A more detailed description of safety-to-non-safety system communications is provided in WCAP-16674-P, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components" (Reference 30).

3.1 INTRA-DIVISIONAL COMMUNICATIONS VIA AF100 BUS

Within each PMS division, the internal functions and the safety portions of both the In-core Instrumentation System and Operations and Control Centers are integrated using an intra-divisional AF100 bus. This network is part of the Westinghouse Common Q Platform (see References 2 and 3) and is referred to as the Common Q network. The AF100 is a high-performance, deterministic communication bus, intended for communication between AC160 Controllers and Flat Panel display systems within the same division. The AF100 bus is not used for reactor trip or ESF actuation. The transmission rate is 1.5 Mbit/second or faster. The network provides real-time data distribution of data within a division. Real-time data distribution is defined as the scheduled periodic broadcast of real-time data pertaining to the plant processes. On the AF100 bus, real-time data distribution is referred to as process data transfer. [

]^{a,c}

The AF100 process data transfer is a deterministic protocol which has priority over the nondeterministic message transfers. Message transfers are used for such off-line functions as interrogating the Programmable Logic Controller (PLC) internal error buffer, or loading an application program into the PLC. Such message transfers are non-deterministic such that their interruption by process data transfers has no significant impact on the system. [

]^{a,c}

An AF100 bus is totally contained within each division of the Safety System. The physical extent of each AF100 bus is limited to its corresponding I&C equipment room, the MCR, and the raceways between the two. On-site access is not provided in any other location. There is no offsite access to the PMS.

3.1.1 Real-Time Data Distribution

Real-time data distribution is accomplished using process data transfer communication on the AF100 bus. [

]^{a,c}

[

]a,c

The Advant Ovation® Interface (AOI) gateway in each PMS division transfers certain real-time data from a division's AF100 bus to the non-safety Real-Time Data Network to support control and information system functions performed in the non-safety system. This functionality is discussed in more detail in Section 3.3.

3.1.2 Access Control

The four PMS intra-divisional Common Q networks are only accessible in the divisional equipment rooms and in the MCR. Access is not available in any of the other Operation and Control Centers. The networks are not accessible from off-site locations.

3.2 INTRA-DIVISIONAL AND INTER-DIVISIONAL COMMUNICATIONS VIA HIGH SPEED LINKS

The PMS uses point-to-point serial links to communicate certain data within and across PMS divisions. These links are part of the Westinghouse Common Q Platform (see References 2 and 3) and are referred to as the Common Q HSLs. The HSL is a serial RS 422 link using High-Level Datalink Control (HDLC) protocol with a 3.1 Mbits/second transfer rate. Each Common Q processor module has one independent transmit link (output to two ports) and two independent receive links. The transmit and receive links are independent of each other. Each is a purely unidirectional point-to-point link without acknowledgement from the receiver. The data is optically isolated if it leaves the cabinet suite. The optical isolation is provided by the use of fiber-optic media converters and fiber-optic cable.

3.2.1 Planned Data Exchange

HSL data communications between two Common Q processor modules is referred to as planned data exchange.

The planned data exchange mode is when two processors are connected via the HSL for the exchange of predefined data packets. Processors on each end of the HSL are configured to send/receive a predefined set of data. [

]a,c

3.2.2 Bistable Processor Logic to Local Coincidence Logic Communication

The PMS uses Common Q HSLs to transfer the partial trips, partial actuations, and related status information calculated in the BPL controllers to the LCL controllers. These links are used both locally within a division and externally across divisions. The links going across divisions use fiber-optic media converters and fiber-optic cable to provide the electrical isolation required by IEEE 603 (Reference 7). The links are true point-to-point links and provide the communication isolation envisioned in IEEE 7-4.3.2 (Reference 23), Annex G.

3.2.3 Local Coincidence Logic to Integrated Logic Processor Communication

The PMS uses Common Q HSLs to transfer ESF system-level actuations and related status information calculated in the LCL controllers to ILPs that actually control the safety components. These links are only used locally with in a division.

3.2.4 Integrated Communication Processor to Integrated Communication Processor Communication

The PMS uses Common Q HSLs to transfer data to support the QDPS function and data to support cross-division diagnostics between divisions. These links are only used externally across divisions. The links going across divisions use fiber-optic media converters and fiber-optic cable to provide the electrical isolation required by IEEE 603 (Reference 7). The links are true point-to-point links and provide the communication isolation envisioned in IEEE 7-4.3.2 (Reference 23), Annex G.

3.2.5 Integrated Logic Processor to Safety Remote Node Controller

The PMS uses Common Q HSLs to transfer ESF component-level actuations and related status information between the ILP controllers and the safety components. These links are used locally within a division.

3.3 COMMUNICATION BETWEEN SAFETY AND NON-SAFETY EQUIPMENT

The PMS implements data flows between safety and non-safety equipment using divisionalized unidirectional gateways and individual analog and digital signals as shown in Figure 3-1. Five cases are identified in the figure and labeled Case A through Case E. The cases are discussed in more detail in the following sections.

3.3.1 Isolated Sensor Loop Signal to Non-Safety (Case A)

Analog inputs required for both control and protection functions (e.g., Pressurizer Pressure) are processed independently with separate input circuitry. The input signals are classified as safety-related and are, therefore, isolated in the PMS cabinets before being sent to the PLS as individual hardwired analog signals. An example of this type of interface is shown as Case A on Figure 3-1 and is identical to the type of interface in existing Westinghouse plants.

Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by Reference 7). They also provide functional isolation by preventing the non-safety system from adversely affecting the safety function.

a.c

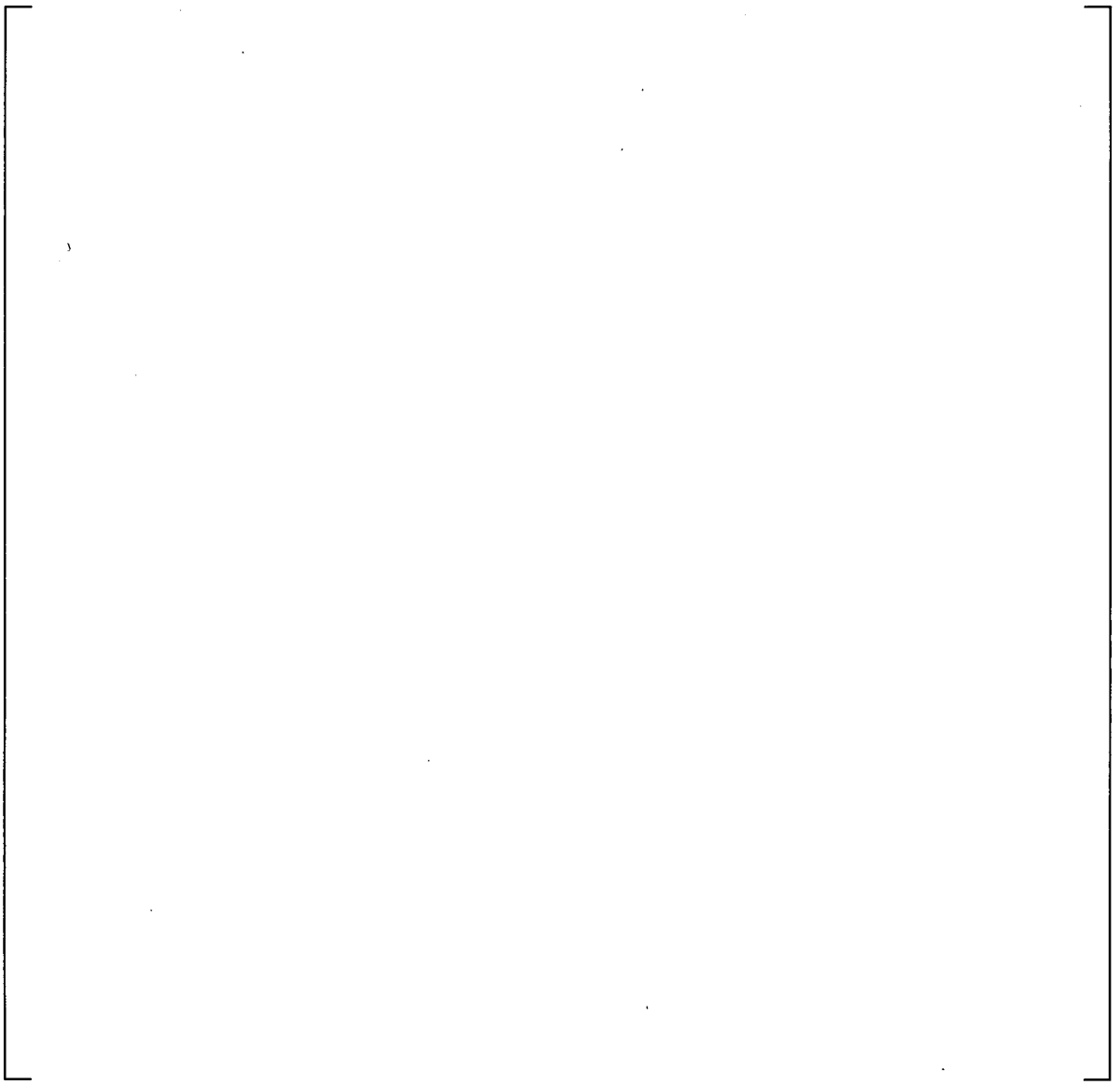

Figure 3-1 Data Flows Between Safety and Non-Safety Equipment

3.3.2 Isolated Analog and Digital Signals to Non-Safety (Case B)

The PMS also provides data to non-safety equipment pertaining to analog and discrete digital signals calculated within the PMS (e.g., Over-Temperature ΔT Margin to Trip). These signals are classified as safety-related and are, therefore, isolated in the PMS cabinets before being sent to the non-safety equipment as individual hardwired analog or discrete digital signals. Typically, the resulting signals are sent to the PLS. The PMS also directly actuates selected non-safety components (e.g., pressurizer heater block and feed water pump trip). These isolated hardwired analog or discrete digital signal interfaces are identical to those in existing Westinghouse plants. An example of this type of interface is shown as Case B on Figure 3-1.

In all cases, qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603 {Reference 7}). They also provide functional isolation by preventing the non-safety system from adversely affecting the safety function.

3.3.3 Isolated Unidirectional Datalink Signals to Non-Safety (Case C)

Various process-related signals (analog input signals, analog signals calculated within the PMS, digital signals calculated within the PMS and SOE signals) are sent to the DDS for information system (plant computer) purposes. Non-process signals are also provided to the DDS for information system purposes. The non-process outputs inform the DDS of cabinet entry status, cabinet temperature, DC power supply voltages, and subsystem diagnostic status, etc. There are also process-related signals that are sent from PMS to PLS that do not require the low transmission latency or the control system segmentation provided by the dedicated signal interfaces described for Cases A and B.

The AOI gateway in each PMS division connects the division's internal network to the non-safety Real-Time Data Network, which supports the remainder of the I&C system. Each gateway has two subsystems. One is the safety subsystem, which is part of the PMS division and interfaces to the Common Q network. The other is the non-safety subsystem, which is part of DDS and interfaces to the Emerson Ovation network. The two subsystems are connected by a fiber-optic link. This type of interface is shown as Case C on Figure 3-1.

The flow of information between the two gateway subsystems is strictly from the safety subsystem to the non-safety subsystem. The unidirectional nature of the gateway is assured by the use of a single unidirectional fiber to connect the two gateway subsystems. Within the safety system, the fiber is connected to an optical transmitter. Within the non-safety system, the fiber is connected to a fiber-optic receiver. This arrangement provides electrical isolation between the systems (as required by IEEE 603 {Reference 7}) and prevents all data flow (data, protocols, and handshaking) from the non-safety system to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2 {Reference 23}, Annex G). It also provides functional isolation by preventing the non-safety system from adversely affecting the safety function. This implementation is shown in Figure 3-2.

The safety software for the AOI gateway has two parts. The first part is the Ethernet driver that is part of the QNX® operating system. The QNX operating system was commercially dedicated and the dedication report was accepted by the NRC as part of the Common Q Safety Evaluation Report process.

The second part of the AOI gateway software was developed by Westinghouse. This software followed the process specified for "Important to Safety" software in WCAP-16096-NP-A, "Software Program Manual for Common Q Systems" (Reference 31) (the SPM), for safety software. The SPM was accepted by the NRC as part of the Safety Evaluation Report (SER) process for the Common Q Platform.

The AOI uses a physically unidirectional transmission fiber-optic datalink from the PMS to the non-safety system. The AOI gateway has no protection function in the PMS. The reliability of the PMS to perform its safety function is not dependent on the AOI gateway being functional.

For SOE signals such as partial trip signals, reactor trip signals, and engineered safety feature (ESF) actuation signals, each division provides the signals to the SOE system/interface via a unidirectional fiber-optic link. The flow of information is strictly from the safety subsystem to the non-safety SOE system/interface. The unidirectional nature of the link is assured by the use of a single unidirectional fiber. The safety end of the fiber is connected to an optical transmitter. The non-safety end of the fiber is connected to a fiber-optic receiver. This arrangement provides electrical isolation between the safety and non-safety portions of the system (as required by IEEE 603-1991 {Reference 7}) and prevents all data flow (data, protocols, and handshaking) from non-safety to safety (providing the communication isolation envisioned by IEEE 7-4.3.2-1993 {Reference 23}, Annex G). It also provides functional isolation by preventing the non-safety equipment from adversely affecting the safety function. This type of interface is a variation of Case C in Figure 3-1.

a,c

Figure 3-2 Example Implementation of Case C Data Flow

3.3.4 System-Level Safety Functions from RSR Fixed-Position Switches and Non-Safety Interlock of PMS Test Functions (Case D)

In the RSR, the non-safety manual controls of system-level safety functions (actuations, manual blocks and resets, manual reactor trip) originate from dedicated switches. The individual discrete digital signals are classified as non-safety-related and are, therefore, isolated in the PMS cabinets before being used. At the RSR, a fiber-optic transmitter encodes the switch contact state to send over the fiber-optic cable. In the PMS, the fiber-optic receiver decodes the data, recreates the switch contact state on its discrete output signal to the AC160 rack in the Safety System. Electrical isolation is provided via the fiber-optic connection. There is no metallic path to conduct an electrical fault in to the PMS. This type of interface is shown as Case D on Figure 3-1.

Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603 {Reference 7}).

Functional isolation provided by logic within the PMS prevents this data flow from inhibiting the safety function. First, the functionality associated with these controls is disabled until operation is transferred from the MCR to the RSR. Thus, these controls are disabled except in the extremely unlikely situation of having to evacuate the MCR. This transfer is accomplished by the divisionalized Class 1E transfer switches, which are connected directly to the LCL controllers in each division. Additionally, when the controls are enabled, their functionality is limited to that defined in the PMS functional design because the information transferred is only in the form of discrete digital signals (i.e., there is no computer software-based communication). Specifically, the manual system-level ESF actuations and the manual reactor trip inputs can only initiate safety functions, not inhibit them. The manual system-level blocks are subject to initiation permissives and to automatic removal. The manual system-level resets only remove the system-level actuation signals; they do not cause any components to change state. An additional signal is required to cause a component to change state.

To reduce the chance of the spurious actuation of a function that would require simultaneous operation of dual switches in the MCR, dual switches and signal paths are also provided for that function in the RSR. Two simultaneous failures would be required to cause a spurious actuation.

Certain PMS test functions are subject to interlocks from non-safety equipment. The purpose of these interlocks is to assure that the plant is properly aligned for the test. The individual hardwired discrete digital signals are classified as non-safety-related and are, therefore, isolated in the PMS cabinets before being used.

Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 7}) and prevent all but the required data flow from the non-safety equipment to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2-1993 {Reference 23}, Annex G).

Functional isolation provided by logic within the PMS prevents this data flow from inhibiting the safety function. The functionality associated with these signals only affects the ability to perform tests. The interlocks do not affect automatic or manual safety functions.

3.3.5 Non-Safety Control of Safety Components (Case E)

PLS provides component-level soft controls in the MCR/RSR for most safety components. Additionally, PLS provides automatic control of some safety components for non-safety functions. The non-safety to safety data flows are not implemented using communication links; rather, they are implemented using discrete digital signals. However, to reduce the number of signals (cables) that must be run from the non-safety system to the safety system, the non-safety system's remote I/O capability is used to deliver the signals to the safety system and to accept component status signals from the safety system. Specifically, a remote I/O node from the non-safety system is physically located within each division of the safety system. The remote I/O node is electrically isolated from the non-safety system by the fiber-optic remote I/O bus. The node is powered by the safety system and the portions of the node not performing a safety function are qualified as associated Class 1E equipment. This type of interface is shown as Case E on Figure 3-1.

The Associated Class 1E equipment, including the Remote Node Controller (RNC) shall meet the requirements of IEEE Standard 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuit" (Reference 24), Clauses 5.5.2 and Clause 5.5.3. Specifically, the equipment shall be part of the safety system qualification program that will demonstrate that when it is subject to environmental, electromagnetic, and seismic stressors, it does not degrade the Class 1E circuits below an acceptable level. The environmental, electromagnetic, and seismic stressors used for these tests are the same as those used to qualify the Class 1E equipment in the same cabinet.

The remote I/O node includes one or more Class 1E CIMs. Internally, these modules contain the equivalent of a discrete digital output module. The resulting discrete digital output signals, corresponding to the demands from the non-safety system, are made available to non-processor based priority logic also contained in the CIM. The priority logic within the CIM combines the non-safety demands with Class 1E automatic actuation signals and Class 1E manual actuation signals from the PMS subsystem. As applied to AP1000, if either system demands a move to the actuated state, the component is moved to the actuated state; otherwise if either system demands a move to the unactuated state, the component is moved to the unactuated state. The CIMs also contain the equivalent of a discrete digital input module. It is used to read component status and internal CIM status. This information is made available to the non-safety system. Thus, at the point of interface to the priority logic, there are two unidirectional data flows: (1) demands going from non-safety to safety and (2) status going from safety to non-safety. Each of these data flows is implemented as simple discrete digital signals not as a communication link.

As mentioned above, the remote I/O bus that is used to connect the non-safety system to the associated Class 1E remote node is fiber-optic. This arrangement provides electrical isolation between the safety system and the non-safety system as required by IEEE 603 (Reference 7). The remote I/O node controller and the communication function within the CIM implement the communications, and only the resulting discrete digital signals interface with the Class 1E priority logic in the CIM. The simple discrete signal interface within the CIM provides the communication isolation envisioned by IEEE 7-4.3.2 (Reference 23), Annex G. Although the remote I/O bus uses bidirectional communications, the simple discrete signal interface between the communication function and the Class 1E priority logic assures that the only data reaching the logic are the intended commands. The priority logic within the CIM provides functional isolation by implementing the priority logic and by only implementing the functionality

defined in the PMS functional design. This implementation is shown in Figure 3-3. More information on the CIM is presented in Section 5.

3.4 MANUAL CONTROL OF SAFETY SYSTEMS AND COMPONENTS

The AP1000 I&C system provides for the manual control of the system-level safety functions and component-level safety functions.

3.4.1 Manual System-Level Control

Several mechanisms are provided to initiate the system-level actuation of ESF functions. Once the functions are actuated, the associated plant components move to their actuated state. Upon removal of the system-level actuation, the plant components remain in their actuated state until they are restored to their unactuated state by component-level controls. Controls are also provided for other ESF system-level commands such as blocks and resets.

- PMS Manual ESF System-Level Actuations from the MCR – The normal mechanism to actuate the ESF system is to use dedicated switches located in the MCR. Switches are located on the PDSP and the Secondary Dedicated Safety Panel (SDSP). The MCR system-level actuation switches are cabled directly from the switches in the MCR to the LCL located in the bistable coincidence cabinets in each instrument room. These switches are processed by the LCL in each PMS division. The resulting commands then fan-out to the ILPs and the CIMs implementing the actuated function.

- PMS Manual ESF System-Level Blocks and Resets from the MCR – The normal mechanism to control ESF blocks and resets is to use soft controls located on the divisionalized safety displays in the MCR. The safety displays are located on the PDSP. These commands are transmitted over the intra-division Common Q Network and are processed by the LCL in the PMS division.

- DDS Manual ESF System-Level Actuations from the RSR – In the event of an evacuation of the MCR, the mechanism to actuate the ESF system is to use the non-Class 1E dedicated switches located in the RSR. The signals pass through qualified isolators in the PMS. The isolators provide electrical and communication isolation. These switches are processed by the LCL in each PMS division. Logic in the LCL provides functional isolation. First, the controls are disabled unless operation is transferred to the RSR. Second, the functionality is limited to that defined in the PMS functional design. From the LCL, the commands fan-out to the ILPs and the CIMs implementing the actuated function.

- Diverse Actuation System (DAS) Manual ESF System-Level Actuations from the MCR – In the event of a postulated common mode failure of the PMS, certain ESF functions can be actuated though diverse means. Dedicated switches for these functions are located on the DAS Panel in the MCR. These switches allow the ESF functions to be actuated through a path independent of the PMS and the DAS automatic actuation logic; for example, through a separate pilot solenoid on air-operate valves, through separate igniters on squib valves, and through separate inputs to the motor control center for motor-operated valves. All switches on the DAS panel are disabled until the DAS panel is enabled by a separate switch in the MCR.

a,c

Figure 3-3 Implementation of Case E Data Flow

3.4.2 Manual Component-Level Control

Normal manual component-level control of safety components is provided by the PMS or PLS. PMS component control is provided for components that meet any of the following criteria:

- Component actuation could cause a breach in the reactor coolant boundary
- Component actuation could cause an overpressurization of a low pressure system
- Component actuation cannot be reversed from the control room (e.g., squib valves)
- Operator action is required to manipulate controls to maintain safe conditions after the protective actions are completed

Components meeting these criteria are listed in Section 7.2 of WCAP-16674-P (Reference 30).

For safety components that have normal manual component-level control from PLS:

- PLS Manual ESF Component-Level Control from the MCR – The normal mechanism to control these ESF components at the component level is to use soft controls from the non-safety workstations located in the MCR. The soft control commands are transferred over the non-safety Real-Time Data Network to a non-safety controller. The controller then sends the command to the appropriate CIMs in the PMS via the remote I/O bus. The fiber-optic remote segment of the remote I/O bus provides electrical isolation. The communication function within the remote node controller (RNC) and the CIM provide communication isolation. The CIM priority logic function provides functional isolation.
- PLS Manual ESF Component-Level Control from the RSR – In the event of an evacuation of the MCR, the mechanism to control these ESF components at the component-level is to use soft controls from the non-safety workstations located in the RSR. They are implemented in the same manner as described for those in the MCR.
- PLS Manual ESF Component-Level Control from the Equipment Rooms – Safety components that have normal manual component-level control from PLS can also be controlled at the component level using dedicated maintenance and test switches located on CIMs that are part of PMS and are located in the equipment rooms. These switches have priority over other PLS and PMS demands.

For safety components that have normal manual component-level control from the PMS:

- PMS Manual ESF Component-Level Control from the MCR – The normal mechanism to control these ESF components at the component level is to use soft controls located on the divisionalized safety displays in the MCR. The soft controls use a multi-step sequence to reduce the chance of spurious actuation. The safety displays are located on the Primary Dedicated Safety Panel. These commands are transmitted over the intra-division Common Q network and are processed by the ILPs in that PMS division.

- PMS Manual ESF Component-Level Control from the Equipment Rooms – In the event of an evacuation of the MCR, the mechanism to control these ESF components at the component-level is to use dedicated maintenance and test switches located on CIMs in the equipment rooms.

- DAS Manual ESF Component-Level Control from the Southern End of the Auxiliary Building – In the event of large-scale damage to the northern most portion of the auxiliary building (where most of the I&C is located), the DAS provides the ability to manually actuate groups of squib valves from a location in the southern end of the auxiliary building.

3.4.3 Justification for Use of Common Electronics for Manual and Automatic ESF Actuations

The AP1000 meets the requirements of Reference 7. The single failure requirement is met through the use of divisional redundancy.

In addition to the single failure criterion, Paragraph 6.2.1 in Reference 7 requires manual means to actuate, at the division level, the automatically-initiated protective actions. The manual means "shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment..." The requirement for "minimum of equipment" does not specify whether or not the equipment can be common to the automatic initiation.

Regulatory Guide 1.62, "Manual Initiation of Protective Actions" (Reference 27), states that "the amount of equipment common to both manual and automatic initiation should be kept to a minimum."

For the AP1000, manual ESF system actuation is accomplished through dedicated manual actuation switches in the control room. These switches are processed by high quality, Class 1E software. Manual actuation logic includes permissives, resets, and sequencing logic that are a function of the plant conditions as shown in Figure 7.2-1 of Reference 1. The implementation of the manual actuation depends on a relatively small number of digital components. If no digital circuitry was included in the manual actuation circuitry, there would be a significant amount of additional circuitry, relays, timers, and wiring, thus, more than a "minimum of equipment" would be utilized.

ESF component actuation is accomplished from the following sources:

- Automatic system-level actuation by the safety system
- Manual system-level actuation from the MCR
- Manual component-level actuation from MCR
- Manual system-level actuation from the RSR
- Manual component-level actuation from the RSR
- Automatic system-level actuation from the DAS
- Manual system-level actuation from the DAS

These sources need to be combined with a method for prioritization and the DAS actuation is required to be diverse. If signals from all of these sources were combined at the final actuation device, and if no digital circuitry was included, there would be a significant amount of additional circuitry needed for each component, further exceeding the "minimum of equipment" requirement.

The AP1000 design minimizes the use of common equipment by using common digital circuits in Level 2 LCL and Level 3 ILP and CIM to arbitrate the prioritization (permissives, blocks, resets, etc.) and actuation of ESF components from the sources identified above.

Implementation of this functionality at the component-level (below Level 3) would require hundreds of individual component control switches, latching relays, fan-out relays, prioritization relays, timers, discrete circuits, and wiring. Implementation of this functionality at Level 3 would also require fan-out relays, prioritization relays, timers, discrete circuits, and wiring. The use of relays instead of digital circuits would be very complicated and difficult to maintain. Periodic testing of relays is costly, difficult, and contributes to the potential for human error.

Many of the manual controls must interact with signals generated within the PMS. Some of the manual actuations are interlocked with signals generated automatically within the Level 1 BPL logic (e.g., Manual Stage 4 Automatic Depressurization System (ADS) actuation that is interlocked with either the third stage ADS actuation signal or low Reactor Coolant System (RCS) wide rage pressure signals (see Figure 7.2-1, Sheet 15 of 20 of Reference 1).

Implementation of this functionality at Level 2 provides a much simpler design. Digital circuits have higher reliability than relays. For the AP1000 design, the functions performed in the LCL and ILP are redundant within each division. The internal redundancy is provided in the design to facilitate the following:

- Continuous monitoring of processor performance
- Use of signal quality assignments
- Online testability with half of a division in test while the other half remains operational
- Self-revealing diagnostics
- Reduces the potential for limiting condition(s) for operation because the minimum number of operable channels can be maintained under many failure scenarios

In AP1000, the ESF system-level actuation enters the process at the same point as in a conventional Westinghouse plant (i.e., where the prioritization logic is performed).

Reference 27 states that "action-sequencing functions and interlocks... associated with the final actuation devices and actuated equipment may be common if individual manual initiation at the component or channel level is provided in the control room." Reference 27 does not specify that the manual initiation at the component-level is required to be safety grade.

In AP1000, component-level actuation in the control room is accomplished via soft control for each component as discussed in subsection 3.4.2. Safety component control is provided for components that meet any of the following criteria:

- Component actuation could cause a breach in the reactor coolant boundary

- Component actuation could cause an over pressurization of a low pressure system
- Component actuation cannot be reversed from the control room (e.g., squib valves)
- Operator action is required to manipulate controls to maintain safe conditions after the protective actions are completed

Component control of the other safety components is accomplished through non-safety controls.

The following provides additional information regarding AP1000 design compliance with revisions to software common cause failure requirements in IEEE Standard 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 25).

> The 1998 revision of IEEE Standard 603 (Reference 25) contains Paragraph 5.16, which addresses software common-mode failures. This paragraph allows the use of manual actuation and non-safety-related systems, components, or both, as a means to accomplish the function that would otherwise be defeated by a software common cause failure. Reference 25 points to Reference 23 to determine if diversity is necessary.
>
> NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems" (Reference 26), provides guidance for diversity that applies to AP1000 at the plant level. The AP1000 DAS provides a combination of automatic and manual controls to address software common cause failures in accordance with Reference 26.
>
> The AP1000 DAS provides manual initiation of reactor trip and selected functions. The manual actuation function of the DAS is implemented by hard-wiring the controls located in the MCR directly to the final loads in a way that completely bypasses the PMS path and the DAS automatic logic. These DAS manual actuation circuits are a non-safety equivalent to the hard-wired manual reactor trip circuitry and meet the requirements in Paragraph 5.16 of Reference 25, and Reference 26 as described in the previous two paragraphs.

Based on these points, AP1000 complies with Reference 7 and is a good, reliable, and sound design based on the technology available today.

4 SAFETY DISPLAY AND QUALIFIED DATA PROCESSING SYSTEM

Safety-related display instrumentation provides the operator with information to determine the effect of automatic and manual actions taken following reactor trip due to a Condition II, III, or IV event as defined in the accident analysis. This instrumentation also provides for operator display of the information necessary to meet Regulatory Guide 1.97 (Reference 22).

4.1 SAFETY DISPLAY FUNCTION

[

]^{a,c} Upon loss of all alternating current (AC) power (station blackout), all four divisions of safety displays are available for the first 24 hours. After 24 hours, only Divisions B and C (excluding Class IE position indication signals for valves and electrical breakers) safety displays are available to conserve power drain from the 72-hour batteries.
[

]^{a,c}

The primary functions of the safety displays are as follows:
[

]^{a,c}

Each safety display consists of a flat panel display unit and a PC Node Box. [

]^{a,c} The operator can navigate among the various display pages of the safety displays. Provisions are provided for temporary connection of a keyboard to the front of the display unit.

a,c

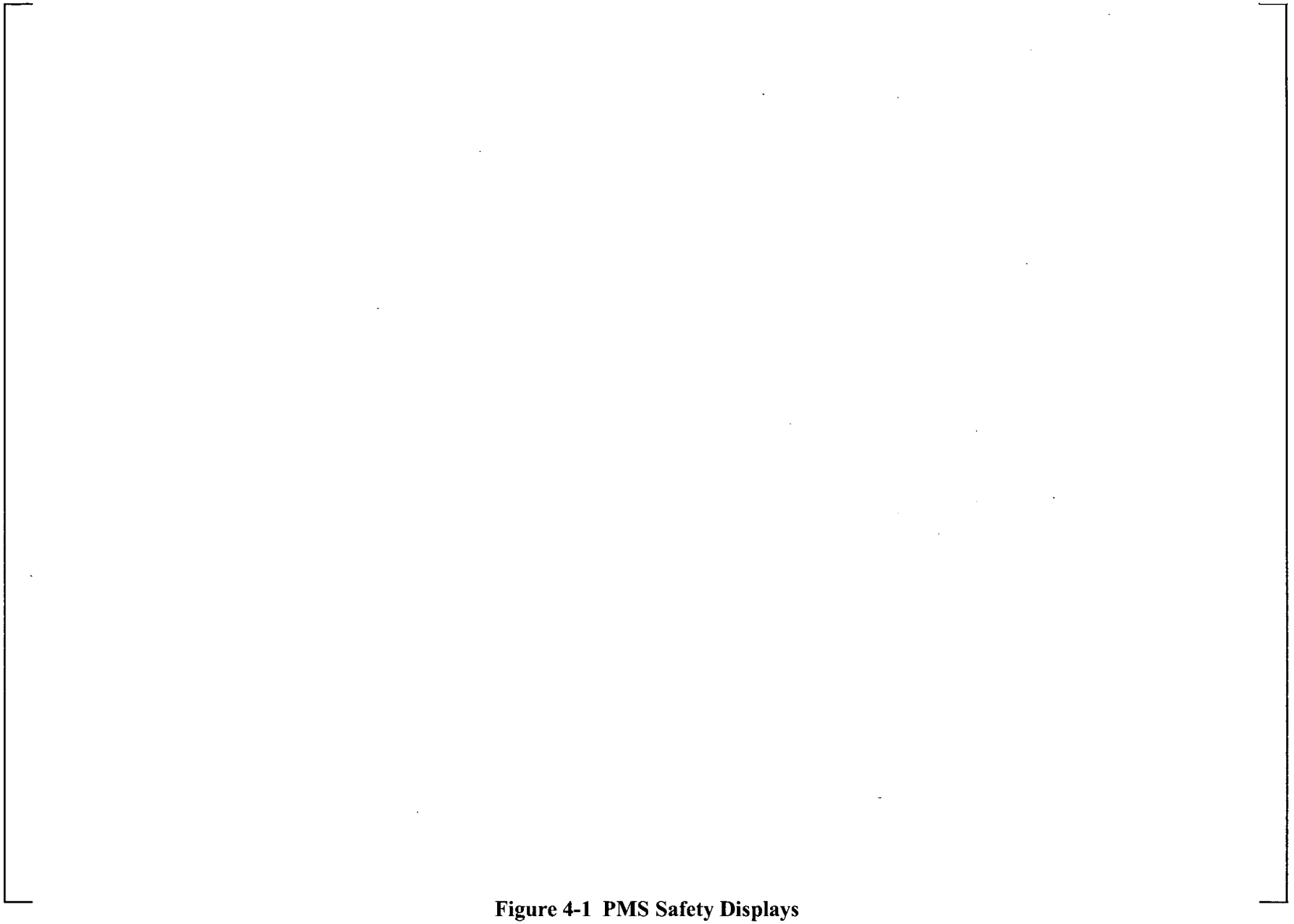

Figure 4-1 PMS Safety Displays

[

]^{a,c} Manual control of all other safety components is accomplished from the non-safety operator workstations, via the non-safety Real-Time Data Network, RNC, and CIM.

For NI calibration, the safety display provides the operator the ability to enter, store, and change the gain and offset for the NI PR upper flux signal and lower flux signal. No calibration of the SR or IR is required.

4.2 QUALIFIED DATA PROCESSING SUBSYSTEM

The QDPS of the PMS provides safety-related display of selected parameters in the control room.

Two QDPS subsystems are provided in the PMS architecture. One QDPS subsystem is located in Division B and the other QDPS subsystem is located in Division C. The divisions are physically separated and electrically isolated from each other. The description provided below illustrates the operation of one of the two identical QDPS subsystems.

The QDPS subsystems are a redundant configuration consisting of dedicated sensor inputs, shared sensor inputs, a QDPS subrack, and qualified display units in the MCR, as shown in Figure 4-1.

The QDPS subsystems perform the following functions:

- Provide safety-related data processing and display.
- Provide the operator with sufficient operational data to safely shut the plant down in the event of a failure of the other display systems.
- Provide qualified and nonqualified data to the Real-Time Data Network for use by other systems in the plant, via the intra-divisional AF100 bus and the MTP, as previously described.
- Process data for MCR display, and to meet Regulatory Guide 1.97 (Reference 22) requirements.
- Provide data to the MCR, the RSR, the plant computer, other non-safety-related devices, and nonqualified emergency response facilities.

PMS Divisions B and C each contain one QDPS subsystem, designated "QDPS" as shown in Figure 4-1. Each QDPS subsystem contains a communication module for the interface between the QDPS subsystem and the intra-divisional AF100 bus.

The QDPS subsystem contains one processor module. The processor module performs data reduction and calculations of group values, subcooled margin, and inadequate core cooling conditions.

Each QDPS subsystem also contains analog input modules. The analog input modules provide the interface between the dedicated and shared sensors and the processor module.

Plant data is input to the QDPS subsystem in several ways:

- Dedicated sensors directly connected to the QDPS subsystem
- Shared sensors that have protective functions as well as QDPS functions
- Plant data from other PMS divisions

Dedicated sensors are connected directly to the analog input modules in the QDPS subsystem. These sensors do not perform any reactor trip or ESF actuation function and are used only for various QDPS functions.

[

]^{a,c}

The QDPS variables to be displayed are identified in APP-PMS-J1-001, "AP1000 Protection and Monitoring System Functional Requirements" (Reference 9).

Power is provided to the QDPS subsystems from the Class 1E DC and uninterruptible power supply (UPS) system for 72 hours after a loss of all AC power (station blackout). After 72 hours, the ancillary diesel generators provide power for the QDPS subsystem.

5 PLATFORM DESCRIPTION

5.1 HARDWARE

This section provides a description of the major components of the Common Q hardware platform used for the AP1000 PMS. The Common Q Platform was developed by Westinghouse for use in multiple safety-related systems such as the Reactor Protection System, Post-Accident Monitoring System, Core Protection Calculator System, Engineered Safety Features Actuation System, Diesel Load Sequencer, and Plant Protection Systems.

The Common Q Platform is Class 1E. Therefore, all of its building blocks are Class 1E. The Common Q Platform consists of the following major building blocks that can be used to design a specific safety system:

- AC160 with PM646 processor module
- S600 input and output modules
- Flat Panel Display System for human-machine interface consisting of the MTP and safety display
- Power supply
- CIM
- Termination units
- SRNC
- Cabinets

The Common Q Topical Reports (References 2 and 3) have been reviewed by the NRC. The NRC Safety Evaluation Reports (SERs) approving the use of Common Q for safety-related applications are contained in Reference 2. In addition, in November 2002, the Swedish regulatory body, SKi, provided Unit 1 at Oskarshamn nuclear power plant (NPP) approval to load fuel with Westinghouse Common Q product used in the Reactor Protection System. The Common Q product was extensively reviewed, led by the Oskarshamn NPP. The review also included a third-party evaluation performed by Colenco Power Engineering, Ltd. Furthermore, on behalf of Oskarshamn NPP, Westinghouse utilized TÜV product service for an independent evaluation of the Common Q software. The Common Q hardware was independently assessed by two independent certified organizations: Wyle Laboratories in the United States and DELTA Development Technology AB in Sweden.

5.1.1 Advant Controller 160 (AC160)

The AC160 controller is used for executing the protection algorithms in safety-related system applications.

The Westinghouse AC160 (see Figure 5-1) is a high-performance modular controller with multiprocessing capability for logic control. It can be used standalone, or as an integrated controller in a distributed control system, communicating with other Advant power equipment. The processor module used in the Common Q applications is the PM646.

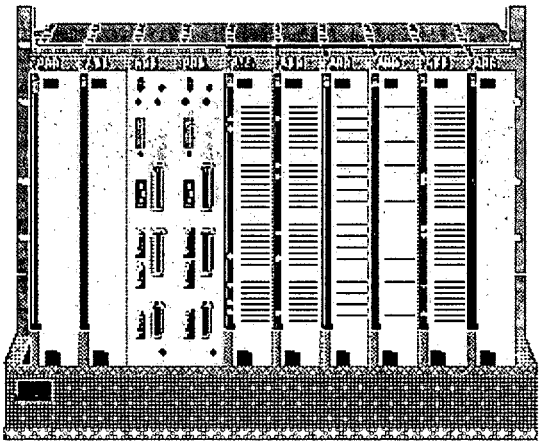

Figure 5-1 AC160 Station

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

To provide scalability in performance and reliability, up to six processor modules can be used concurrently in one controller. The processor modules within an AC160 controller share data with each other using the global memory resident on the AF100 bus Communication Interface Module (Model CI631).

Each processor module supports two high-speed communication links (i.e., HSLs). The HSLs are used to communicate data to other channels of the safety system. These datalinks are electrically isolated using fiber-optic cable.

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 bus, global memory, I/O, and the HSL.

The processor module has a built-in, independent WDT module that provides annunciation and a channel trip if a protective function is rendered inoperable due to processor failures.

Fiber-optic media converters are used for electrical isolation of data communication connections to/from other safety channels and non-safety systems.

The configuration possibilities of AC160 cover a wide range of functions, such as logic and sequence control, data and text handling, arithmetic, reporting, and regulatory control. Several AC160 stations may be connected via the AF100 bus. The AF100 bus is a high-performance serial communications system featuring fast, real-time exchange of process data between the application programs in different AC160 stations.

Using redundant processor modules and redundant main power supplies, increased reliability and availability of the AC160 can be achieved.

AC160 is fully modular. The subracks are normally installed in cabinets. All process connections are made to screw terminals on connection units or by crimp contacts.

With the excellent performance it offers, the following wide range of functions are supported, including logical control, analog signal processing, and feedback control:

Logical operations and time delays:

- Sequential control
- Feedback control
- Arithmetical operations
- Pulse counting
- Communication via Advant Fieldbus 100

The central processing unit (CPU) module PM646 (see Figure 5-2) is a powerful multiprocessing CPU module for the AC160 system for the control and supervision of processes and equipment in power plant environments. The processor module PM646 is based on 32-bit Motorola MC68360 processors. The processor modules are placed in positions 3 through 8 of the basic station, and it is possible to have more than one processor module in one station (multiprocessing). These processor modules can be combined in pairs in CPU-redundancy mode, or they can be independent from each other with up to six processor modules placed in one station or in a combination of several stations. The PM646 module contains two 32-bit microprocessor boards: a processor section and a communications section.

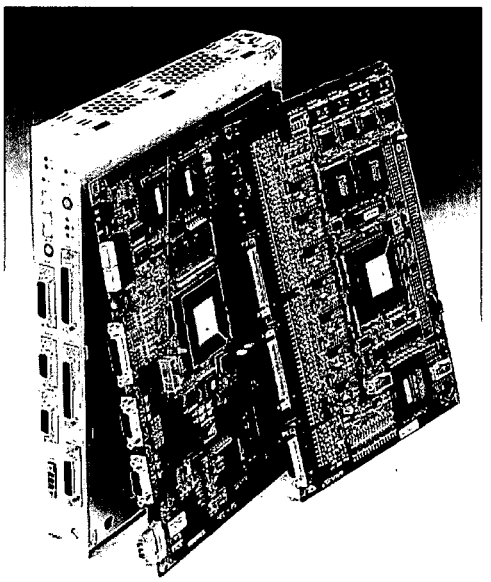

Figure 5-2 PM646 Processor Module

Processor section:

- Contains application code
- Non-volatile flash programmable read only memory (PROM) for application program
- Sends data to CI631 communication interface module for use on the AF100 bus
- Contains RS232 programming port
- Performs most of the self-diagnostics (WDT and memory checking)
- Stores data to be transmitted via HSL in dual-port memory for use by the communications section
- Retrieves HSL receive data from dual-port memory stored by communications section
- User configurable cycle time (2 milliseconds to 20 seconds)

Communications Section:

- Handles the two HSL communication ports (RS422 Interface, 3.1 Mbits/second communication protocol meets IEEE 7-4.3.2 {Reference 23} communications requirements)

- Stores information received by HSLs in dual-port memory for use by processor section

- Retrieves information in dual-port memory for transmission out of HSL

Fast data communication between processor modules in different stations or between two processor modules is provided with the HSL connectors located on the front panel of the PM646. This HSL connection is used to transmit data between two controllers without using the AF100 bus. It is a fast point-to-point connection between the controllers. The receive and transmit channels use a subset of the HDLC protocol.

5.1.2 S600 Input and Output Modules

The AC160 uses the S600 I/O system. The S600 family of input and output modules contains all the traditional cards such as analog inputs (including differential inputs, thermocouples, and RTDs), analog outputs, digital inputs, digital outputs, rotational/speed sensing inputs, and pulse counting.

S600 I/O modules (see Figure 5-3) typically contain 16 or 32 input or output channels, depending on the module. The I/O modules are placed in the AC160 controller subrack. I/O modules can also be inserted into the controller extension subrack. The extension subracks communicate with the main AC160 controller subrack via a hardwired bus extension. Process signals are connected to the front of the I/O modules via prefabricated cables from the field terminal blocks or termination units.

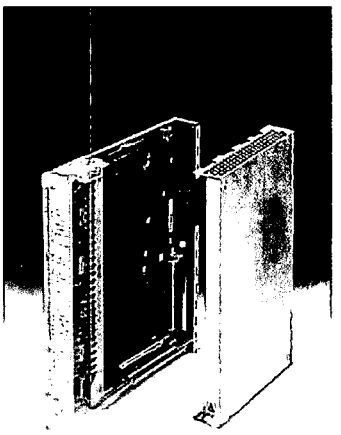

Figure 5-3 S600 I/O Module

The system software in the AC160 automatically supervises and checks that all I/O modules are operating correctly at system startup and by the application interfacing with the module during normal operation. The status of the module is indicated by two light emitting diodes (LEDs): RUN (green during normal operation) and ALARM (red when a fault is detected). More detailed diagnostic information is available by means of the MTP.

S600 I/O modules can be replaced during system operation (hot swap). The modules are housed in a sheet-steel enclosure that protects the circuit boards. The enclosure has openings at the top and bottom for air convection. The prefabricated cable carrying the process signals from the field terminal blocks is connected to the front edge of the I/O module, and is removable to facilitate module replacement.

The S600 I/O modules can be connected in a redundant configuration to improve the reliability of critical control loops.

The S600 I/O module types utilized in the safety system equipment are discussed in the following sections:

5.1.2.1 Analog Input Modules

The analog input modules convert analog input signals from transmitters to digital values required by the controller module.

- AI688 – 16 differential input channels, 0/4-20 mA, 0-1 V, 0-10 V.
- AI687 – 16 thermocouple input channels, Types J, K, E with cold reference junction compensation.
- AI687 – 8 RTD input channels, Pt100, Pt200 (and 8 thermo-couple, 0-100 mV).

- AI687 – 16 different input channels, 0-100mV.

- 0/4-20 mA inputs are accommodated by current-to-voltage conversion in the I/O termination units.

5.1.2.2 Analog Output Modules

The analog output module converts the digital signals from the controller module to the analog signals needed for control, indication, etc.

- AO650 – 8 channels, 0/4-20 mA, +20 mA, 0/1-5 V, 0-10 V, +10 V into load impedance of less than or equal to 600 Ohms (current output), and greater than or equal to 1.2 kOhm (voltage output), 12-bit resolution.

5.1.2.3 Digital Input Modules

The digital input modules convert the binary signals from the field to the internal signal levels required by the controller module.

- DI620 – 32 channels, 24 VDC, opto-isolated in groups of 8.
- DI621 – 32 channels, 48 VDC, opto-isolated in groups of 8.

5.1.2.4 Digital Output Modules

The digital output modules convert the digital signals from the controller module to the binary or contact output signals needed for control, indication, etc.

- DO620 – 32 channels, 48 VDC, 600 mA, transistor source output, opto-isolated in groups of 8.
- DO625 – 16 channels, 24 VDC, 2.4 A, solid state switch output, isolated in groups of 2.
- DO630 – 16 channels, 230 VDC/AC, 2.4 A, relay contact output, coil-to-contact isolation.

5.1.2.5 Pulse Counting, Rotational Speed Input Processing

The pulse counter module registers and processes fast pulse signals at repetition rates up to 100 kHz.

- DP620 – 5 channels, 5 V, 24 V, +13 mA, less than 100 kHz, Up/Down Counting, Frequency/Difference Measurement, Position, Rotation/Speed.

5.1.2.6 Total S600 I/O Capacity Per Control Station

- I/O channels (soft limit) up to 1500.
- I/O modules (soft limit) up to 75.

Qualified signal isolators are utilized to provide signal isolation for analog and digital signals where required to satisfy the requirements for independence and isolation.

5.1.3 Flat Panel Display System

The Flat Panel Display System (FPDS) is the human-machine interface for the Common Q safety system. It consists of a touch screen video display and a PC Node Box. The FPDS is qualified and licensed for Class 1E applications. When mounted in a system cabinet, the FPDS is usually referred to as the MTP. When mounted in the MCR, it is referred to as the safety display.

5.1.3.1 Touch Screen Display

The video display is a qualified thin-film transistor (TFT) color display with capacitive touch screen capability. Three sizes are available: 12-inch, 15-inch, and 19-inch diagonal measurement. The 12-inch display is typically used for an operator's module. The 15-inch display is typically used for the MTP display. Because of its larger viewing area, the 19-inch display is typically used for safety displays in the MCR.

5.1.3.2 PC Node Box

The PC Node Box is the interface between the AF100 bus and the flat panel video display.

The PC Node Box contains the following components:

- Industrial Computer

  The dual boot computer contains an Intel® embedded systems group processor with non-volatile flash memory. The qualified QNX® operating system software provides the graphical user interface and is used for on-line mode and during surveillance testing. A Windows®-based application (MTP only) is used for off-line mode to load AC160 software or to perform AC160 diagnostics.

- AF100 Communication Interface Module
- Digital Input/Output Interface
- Removable Storage Device
- Input/Output Ports, Keyboard, and Mouse

5.1.4 Common Q Power Supply

The Common Q power supply is a modular power supply system. Various modules are available to accommodate different output voltages. AC input power to the Common Q power supply system is 100 to 140 VAC, 200 to 260 VAC at a line frequency of 45 to 65 Hz, or 90 to 350 VDC.

Power supply modules are single output supplies that can range from 120 watts to 480 watts output ratings. Voltages from 5 to 48 VDC can be supported.

The power supply can support single or dual power feeds. Redundant power supply configurations are supported by diode auctioneering. Faults in one redundant supply do not affect the other redundant supply from operating normally. Redundant modules can be replaced while the power supply remains energized

without disturbing the powered system. The redundant power supply is monitored by the system, and failures are detected and alarmed. The power supply has over-voltage and over-temperature protection, soft start, and a high power factor. The power supply can be mounted in the top or bottom of a cabinet.

5.1.5 Component Interface Module

[

]^{a,c}

5.1.6 I/O Termination Units

I/O termination units provide an interface between the S600 I/O modules and the field circuits. There is a separate type of termination unit to interface to each of the I/O module types. Each type of termination

unit provides termination points for the field wiring, including individual terminals for cable shields. Each type of unit also provides signal disconnects and test points to support system testing and maintenance. In addition, the following features are provided:

- AI Termination Unit – Provides loop power (30 V), isolated per module. Provides separate connection for signal sharing. There are three configurations: voltage inputs (0-10 V and thermocouples), current inputs (4-20 mA, with current-to-voltage dropping resistors), and RTD inputs.
- AO650 Termination Unit – Provides termination, disconnects and test points only.
- DI621 Termination Unit – Provides contact wetting voltage (48 V) and ground fault detection, isolated per four groups of eight inputs each. Provides separate connection for signal sharing.
- DO620 Termination Unit – Output power (externally supplied) is fused and distributed to four groups of eight outputs each.
- Termination Unit with Relay Disconnect – Provides local or remote control to disconnect the field inputs and allow manual injection of test signals. Also provides local and remote indication of test status.
- Termination Unit with Y-Feedthrough – Provides two output points for each input point.
- High Speed Link Termination Unit – Provides copper-to-copper or copper-to-fiber interfaces to fan-out the HSL signal from the PM646 processor module.
- Reactor Trip Matrix Termination Unit – Provides the ability to manually test the RTCB via the UV and ST coils. Monitors the PM646 WDT contact output to provide preferred failure mode operation. Provides interface between the manual reactor trip switches and the RTCB.
- 2oo3 Vote and Pulse Termination Unit – Provides hardwired 2oo3 relay voting and discrete circuit pulse timeout to mitigate postulated common mode software failures. Also provides trickle current test to verify load circuit continuity.

5.1.7 Safety Remote Node Controller

The SRNC provides an interface between the AC160 controller and the CIM. The main functions of the SRNC are:

- Receive data from the AC160 controller via a high-speed serial datalink
- Error checking on high-speed serial data
- Transmit data to the CIM via a serial bus
- Receive data from the CIM via a serial bus
- Transmit data to the AC160 controller via a high-speed serial datalink

5.2 SOFTWARE DESCRIPTION

This section provides a description of the Common Q AC160 software platform used for the safety-related systems.

The AC160 software consists of a real-time operating system, task scheduler, diagnostic functions, communication interfaces, and user application programs, all of which reside on flash PROM in the PM646 processor module. 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. The base software includes the executable code for the standard set of logic blocks (PC elements). In addition, custom PC elements can be created as an extension to the base software.

Application programming is accomplished by configuring and interconnecting items from a library of predefined function blocks, called PC elements, and Database (DB) elements. The PC elements and DB elements are combined into programs that form a complete control function.

Application programming is done on an Intel processor based personal computer using the AMPL Control Configuration (ACC) software development environment. The target code is generated and saved to a write only compact disc. The MTP includes a DVD-ROM drive to support loading of the target code.

5.2.1 AMPL Programming Language

Process control applications are configured in AMPL, a function block language with graphic representation that is especially developed for process control applications. The language is characterized by each function being seen as a building block with inputs and outputs.

A program written in AMPL is referred to as an AMPL program and the building blocks are called PC elements. The range of ready-to-use PC elements is wide and powerful. Control loops can be combined with motor control, startup, and shutdown sequences and fast interlocking logic (with cycle time down to 2 milliseconds), all in the same control program and using the same high-level function block oriented language, AMPL. Custom PC elements can also be written in a high-level language (C) and added to the library.

In addition to functional PC elements, AMPL contains a number of structural elements for division of an AMPL program into suitable modules, which can be managed and executed individually. The modules can be given different cycle times and priorities so that both fast and slow control operations can be managed by the same AMPL program.

The inputs and outputs of an element are connected to the inputs and outputs of other elements or to process I/O points. Picking these elements and making these connections constitute the configuration work.

The resulting AMPL program can then be documented graphically.

5.2.2 ACC Function Chart Builder

The Function Chart Builder of ACC enables development of AMPL application programs graphically, using a tree editor, a function chart editor, or a combination of both. The combination is particularly powerful in that the tree-structured view provides a hierarchical overview for efficient navigation, while the function chart view provides the functional details and a perfect basis for programming and program editing. Configuration in AMPL is essentially a matter of inserting program elements, or type circuits, onto diagram sheets and connecting these elements to other elements and to objects in the database. Program element manuals are available as part of the built-in help. Other important productivity features include repetition of the latest command, repetition of the latest setting, and the inclusion of an apply button in dialog boxes wherever appropriate.

Features of the Function Chart Builder include AC160 using the corresponding libraries

The following functions are provided by the ACC Function Chart Builder:

- Tree editor for control program structures
- Editing of function charts
- PC (AMPL) source code editing and syntax checking in node mode (Syntax errors can be listed together with the code in a second window to facilitate corrections.)
- Automatic consistency to the engineering database
- Symbolic addressing of signals
- Use of calculated symbols (parameters)
- Generation and back-translation of application programs and database source code (can be used for transfer purposes between different process stations and engineering systems. The graphic representation after back-translation from the target station is the same as if the program was entered directly into the Function Chart Builder, ensuring engineering consistency.)
- Graphical documentation of application programs in function chart representation and in tree representation
- Database and cross-reference documentation in list representation
- Testing and fault tracing
- Dynamic display of variables; display and modification of parameters with function chart representation (off-line mode)

- Forcing of inputs and outputs (in the development stage only)
- Reading/setting of date and time

5.2.3 Configuration Management

Application software modifications are accomplished via the ACC engineering tool via one of two modes: off-line or on-line.

5.2.3.1 Off-line Mode

In the off-line mode, the application function charts are modified to obtain the desired functionality with the ACC engineering tool disconnected from the Advant Controller station. Extensive self-checks within the engineering tool preclude illegal programming operations. When the modified function chart is completed, new source code is generated in an American National Standard Code for Information Interchange (ASCII) text format for archiving. New target code (machine code) for the entire application program is also compiled by ACC.

At this point, the ACC tool is connected to the Advant Controller to be modified. The connection can be made directly to the controller's CPU module or remotely via the Advant field communications network. Via ACC, the controller's application program is blocked (alarm received) and the new target code is downloaded and saved into the CPU module's flash PROM (non-volatile memory). Numerous self-checks are conducted to ensure the download is completed successfully.

The new application program is unblocked and testing is conducted to validate the functionality of the modified program. The extent of validation testing is determined by the verification and validation (V&V) plan approved for the software modification.

5.2.3.2 On-line Mode

In on-line mode, the ACC engineering tool is connected to the Advant Controller during modification of program function charts. This permits the controller to remain operational throughout the modification process. While disabled on installed system controllers, this feature is very useful for debugging software modifications on a test platform prior to deployment in the plant.

In the on-line mode, operational target code is only re-compiled and downloaded for the portion of the program that is modified. In addition to the self-checks described for the off-line mode, numerous confirmatory messages are provided to prevent inadvertent actions.

Following modification, validation testing would be conducted as determined by the respective V&V plan.

5.2.4 Flat Panel Display Software and Tools

The Common Q FPDS software is a QNX-based multiprocessing system that is designed such that displays are dynamically updated from data acquired from the AF100 bus interface. The types of displays that can be developed for the FPDS include trends, lists, alphanumeric process displays, and maintenance

displays. The QNX Photon® microGUI® product is the runtime engine for the display application on the FPDS. In addition to the display application, other processes in the FPDS support receiving and transmitting data on the AF100 bus for the display application and other processes, sending configured data over the AOI, and monitoring the software integrity of the FPDS. The display application is created on a software developer's platform using the QNX Photon Application Builder.

6 MAINTENANCE, TESTING AND CALIBRATION

Maintenance and testing of the PMS consists of two types of tests: self-diagnostic tests and on-line verification tests. The self-diagnostic tests are built into the AC160 equipment and consist of numerous automatic checks to validate that the equipment and software are performing their functions correctly. On-line verification tests are manually initiated to verify that the safety system is capable of performing its intended safety function.

6.1 SELF-DIAGNOSTIC TESTS

6.1.1 Processor and I/O Modules

A variety of self-test diagnostic and supervision functions are performed by the PMS processors and I/O modules to continuously monitor their operations. Each of the modules has its own diagnostic functions. The processor module monitors the system as a whole by collecting all the diagnostic information and checking the consistency of the hardware configuration with the application software currently installed.

During power-up, the functions of the processor and the contents of the application and system flash PROM are checked as well as the internal Static Random Access Memory (SRAM) of the processor.

The processor system software includes diagnostic routines, which check the processor and the system during initialization and ensure system integrity during the execution of the application program.

The processor 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 automatically switched to the RUN mode. 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 the RUN mode and the error is indicated on the associated DB element.

Each module is equipped with the two LED indicators: FAULT and RUN. During normal operation, the green LED RUN is lit on all modules. The red LED FAULT illuminates only if a problem occurs on the module.

While the application program is running, the diagnostic routines continue checking operation without delaying or influencing the execution. Each processor (e.g., BPL, LCL, ILP) is monitored by the use of background diagnostics for the processor and I/O module faults. Failures on I/O modules are first detected by the individual module, which then passes failure status information to the processor (error buffer) where it is stored and acted upon. The supervision functions of the equipment are subdivided into the following groups:

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

The status of the modules and the I/O signals is indicated by the associated DB element. Missing modules are also signaled by the function supervising the configuration on the associated DB element. The status signals on the DB elements can be processed by the application program in the same way as other signals.

The I/O modules supervise whether or not the process termination edge connector is correctly inserted. If the edge connector is withdrawn, operation of the I/O module is immediately inhibited (i.e., it is no longer in the RUN state), and the error is indicated on the associated DB element module and the DB element's channel in the processor. If the process connector is not inserted, the module cannot be switched to RUN mode.

The software also monitors whether the processor has sufficient capacity to perform its functions within the times specified. If it does not, the processor inhibits the application program.

[

]^{a,c}

6.1.2 Communication Modules

The purpose of the AF100 bus communication modules is to provide communication between subsystems (e.g., BPL, LCL, ILP, MTP, ITP). The AF100 bus supports two different types of communications: process data and message transfer. Process data are dynamic data used to monitor and control the process, while message transfer is used for program loading (disabled for AP1000) and system diagnostics.

The communications modules are individually supervised by their own internal diagnostics and additional run-time diagnostics. In addition, the processor module performs continuous background diagnostics of the communications modules and automatically detects errors during operation. The processor module contains the error messages in the error buffer for system troubleshooting.

Each communications module is equipped with LEDs located on the front of the module to display the status of the module and operational state of the network. The LEDs provide initialization and operational information as follows:

- FAULT LED (Red) indicates a module failure (i.e., hardware or cable problem).
- RUN LED (Green) indicates normal operation and in RUN-mode.

- TRAFFIC LED (Green) is set when the communications module finds another device on the network.

- MASTER LED (Yellow) is set when the communications module is the bus master on the AF100 bus. Because every communications module is capable of being a bus master on the network, this LED can be seen to migrate between communications modules on the network.

- CONFIG OK LED (Yellow) indicates that the communications module has the same configuration as the current master communications module, therefore allowing it to participate in the sharing of the master responsibilities.

6.2 ON-LINE VERIFICATION TESTS

Via the MTP in conjunction with the ITP, the I&C technician can perform manually initiated on-line verification tests to exercise the safety system logic and hardware to verify proper system operation. Within each PMS division, the ITP interfaces with the NI subsystem, BPL subsystem, LCL subsystem, ILP subsystem, MTP, and the RTCB initiation relays to monitor and test the operational state of the PMS. The ITP together with the MTP provides overall on-line verification testing.

The on-line verification tests consist of the following tests:

- Sensor Input Check
- Trip Bistable Test
- Local Coincidence Logic Test
- Initiation Logic Test

Each of these tests is described in the following sections.

6.2.1 Sensor Input Check

[

]^{a,c}

6.2.2 Trip Bistable Test

The BPL subsystem processor module, bistable logic algorithms, digital output modules, communications modules, and interfacing wiring/networks can be tested by the ITP using manually initiated tests.

Via the MTP, ITP, and AF100 intra-division bus, the I&C technician can apply a digital test signal to the input of the BPL processor to force the bistable to trip. This trip is sent to the reactor trip LCL for processing in the 2oo4 logic matrix. The ITP verifies that the trip signal is present at all reactor trip LCLs in all divisions, indicating a successful transmission of the trip to all of the reactor trip LCLs.

6.2.3 Local Coincidence Logic Test

The reactor trip LCL processor module, coincidence logic algorithms, digital output modules, communications modules, and interfacing wiring/networks can be tested by the ITP using manually initiated tests.

Each LCL subsystem contains four reactor trip logic processors and two ESF logic processors. All of the processors perform the 2oo4 coincidence logic for reactor trip or Engineered Safety Features Actuation System (ESFAS), respectively. Each processor controls a separate digital output where the digital outputs from each processor are wired in a selective 2oo4 contact matrix initiation logic for the RTCB UV and ST coil outputs. This allows the ITP to test one processor at a time and cause a single digital output to actuate without causing a UV or ST trip. The ITP detects if one of the legs is open and thus knows if the test was successful. This test verifies that the logic and digital outputs are functioning correctly to perform their safety function.

6.2.4 Initiation Logic Test

As part of the manually initiated LCL reactor trip testing, the I&C technician, via the ITP, can manually force the four LCL reactor trip logic processors to set their digital output module outputs to their trip state. The digital output contacts are selected to force either the ST or UV initiation matrix to trip. This causes the reactor trip breaker to open. The ITP processor monitors the state of the RTCBs and transmits it to the other divisions' LCLs. The LCLs in the other divisions have an interlock to prevent the ITP in the other divisions from attempting to perform this test when one division is in test and the RTCB is open. The RTCB must then be manually closed prior to performing the same test in another division.

6.2.5 Programmable Logic Controller Execution Test

During normal operation, the MTP and ITP monitor failure and diagnostic information from the BPL, LCL, and ILP subsystem processors as an indication of their continued operation (execution of programs). Upon detection of a failure, the ITP will generate an alarm.

6.3 CALIBRATION

Calibration of the Common Q-based PMS system is limited to the NI signals and temperature input signals.

Each NI subsystem PR channel receives inputs from upper and lower ex-core detectors. For each detector input, the NI algorithm contains provisions for gain and offset calibration coefficients so that the upper and lower flux measurements can be adjusted for full-power operation. Since this calibration is normally performed once each shift, the capability for this calibration is provided to the operator via the safety displays in the MCR. Using the safety display, the operator navigates to the NI calibration display and enters the calculated gain and offset coefficients for the upper and lower detectors in that division. Since each safety display is associated with a PMS division, the NI calibration operation must be repeated four times, once for each PMS division.

For all other analog inputs, as well as pulse inputs and analog outputs, periodic calibration is not necessary. Calibration verification is performed for analog inputs, pulse inputs, and analog outputs. If an analog input module does not meet accuracy requirements, the module is replaced.

Calibration verification is also performed for the power supply voltages. If the associated power supply fails the calibration verification, it can be adjusted to restore the required output.

6.4 BYPASS AND PARTIAL TRIP CONDITIONS

[

]^{a,c}

6.4.1 Bypass Condition

[

]^{a,c}

[

]a,c

Automatic indication of bypass status is provided in the MCR in accordance with Regulatory Guide 1.47.
[

]a,c

6.4.2 Partial Trip Condition

Partial trips may be established for each of the individual bistable outputs in a similar manner to the bypasses. No limit is applied for the number of partial trip conditions in the safety system. Partial trip conditions in two or more divisions of the safety system will cause the associated reactor trip breakers to trip. The Function Enable keyswitch is required to be enabled prior to setting partial trips.

If any un-bypassed partial trip condition (including normal processing partial trips) exists, the LCL process station initiates a message on the division's AF100 bus indicating that a partial trip condition has been established. This causes a corresponding partial trip indication in the MCR.

7 SUMMARY AND CONCLUSION

[

]^{a,c}

[

]a,c

Based upon the AP1000 PMS architecture described herein and the information provided in WCAP-15776, "Safety Criteria for the AP1000 Instrument and Control Systems" (Reference 8), the AP1000 PMS architecture meets the requirements set forth in IEEE 603 (Reference 7).