Westinghouse Non-Proprietary Class 3

WCAP-16675-NP
APP-GW-GLR-071
Revision 0

February 2007

AP1000 Protection and Safety Monitoring System Architecture Technical Report

Westinghouse

WCAP-16675-NP
APP-GW-GLR-071
Revision 0

AP1000 Protection and Safety Monitoring System Architecture Technical Report

Carl A. Vitalbo, Fellow Engineer
Safety and Monitoring Systems, RRAS

February 2007

Reviewer: Thomas P. Hayes*, I&C Lead
New Plant Engineering

Approved: Andrew P. Drake*, RRAS AP1000 NuStart Program Manager
Repair, Replacement and Automation Services

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

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

© 2007 Westinghouse Electric Company LLC
All Rights Reserved

FOREWORD

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 Platform (Common Q). This document describes the Common Q implementation of the AP1000 PMS. The Common Q Platform is described in "Common Qualified Platform" Reference 2 and "Common Qualified Platform Integrated Solution" (Reference 3). The Common Q Platform was accepted by the Nuclear Regulatory Commission (NRC) in ML003740165 (Reference 4), ML011690170 (Reference 5), and ML0305507760 (Reference 6).

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).

This architecture report does not address recent cyber security concerns. I&C design features to address cyber security concerns will be the subject of a separate report.

TABLE OF CONTENTS

LIST OF TABLES vii

LIST OF FIGURES ix

LIST OF ACRONYMS AND ABBREVIATIONS xi

DEFINITIONS xiii

REFERENCES xv

1 AP1000 PMS FUNCTIONAL REQUIREMENTS 1-1
- 1.1 REACTOR TRIP FUNCTIONS 1-1
- 1.2 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM FUNCTIONS 1-2
- 1.3 QUALIFIED DATA PROCESSING SYSTEM 1-4
- 1.4 COMPONENT CONTROL FUNCTIONS 1-4

2 AP1000 PROTECTION AND SAFETY MONITORING SYSTEM DESCRIPTION 2-1
- 2.1 PMS ARCHITECTURE 4 DIVISION OVERVIEW 2-1
- 2.2 PMS ARCHITECTURE 1 DIVISION DETAIL 2-3
  - 2.2.1 Nuclear Instrumentation Subsystem 2-4
  - 2.2.2 Bistable Processor Logic Subsystem 2-8
  - 2.2.3 Local Coincidence Logic Subsystem 2-11
  - 2.2.4 Integrated Communications Processor Subsystem 2-16
  - 2.2.5 Integrated Test Processor Subsystem 2-16
  - 2.2.6 Maintenance and Test Panel Subsystem 2-18

3 EXTERNAL SYSTEM INTERFACES & COMMUNICATIONS 3-1
- 3.1 INTRA-DIVISIONAL COMMUNICATIONS VIA AF100 BUS 3-1
  - 3.1.1 Real-Time Data Distribution 3-1
  - 3.1.2 General Communications 3-1
  - 3.1.3 Access Control 3-2
- 3.2 INTRA-DIVISIONAL AND INTER-DIVISIONAL COMMUNICATIONS VIA HIGH SPEED LINKS 3-2
  - 3.2.1 Planned Data Exchange 3-2
  - 3.2.2 Bistable Processor Logic to Local Coincidence Logic Communication 3-2
  - 3.2.3 Local Coincidence Logic to Integrated Logic Processor Communication 3-3
  - 3.2.4 Integrated Communication Processor to Integrated Communication Processor Communication 3-3
- 3.3 COMMUNICATION BETWEEN SAFETY AND NON-SAFETY EQUIPMENT 3-3
  - 3.3.1 Isolated Sensor Loop Signal to Non-Safety (Case A) 3-3
  - 3.3.2 Isolated Analog and Digital Signals to Non-Safety (Case B) 3-5
  - 3.3.3 Isolated Gateway Signals to Non-Safety (Case C) 3-5
  - 3.3.4 System-Level Safety Functions from RSR Fixed Position Switches (Case D) 3-7
  - 3.3.5 Non-Safety Manual Component-Level Control of Safety Components (Case E) 3-7

TABLE OF CONTENTS (cont.)

3.4 MANUAL CONTROL OF SAFETY SYSTEMS AND COMPONENTS 3-8
3.4.1 Manual System-Level Control 3-8
3.4.2 Manual Component-Level Control 3-10

4 SAFETY DISPLAY AND QUALIFIED DATA PROCESSING SYSTEM 4-1
4.1 SAFETY DISPLAY FUNCTION 4-1
4.2 QUALIFIED DATA PROCESSING SUBSYSTEM 4-3

5 PLATFORM DESCRIPTION 5-1
5.1 HARDWARE 5-1
5.1.1 Advant® Controller AC160 5-1
5.1.2 S600 Input and Output Modules 5-5
5.1.3 Flat Panel Display System 5-7
5.1.4 Common Q Power Supply 5-9
5.1.5 Component Interface Module 5-11
5.1.6 I/O Termination Units 5-12
5.2 SOFTWARE DESCRIPTION 5-13
5.2.1 AMPL Programming Language 5-14
5.2.2 ACC Function Chart Builder 5-14
5.2.3 Configuration Management 5-15
5.2.4 Flat Panel Display Software and Tools 5-16

6 MAINTENACE, TESTING AND CALIBRATION 6-1
6.1 SELF-DIAGNOSTIC TESTS 6-1
6.1.1 Processor and I/O Modules 6-1
6.1.2 Communication Modules 6-2
6.2 ON-LINE VERIFICATION TESTS 6-3
6.2.1 Sensor Input Check 6-3
6.2.2 Trip Bistable Test 6-4
6.2.3 Local Coincidence Logic Test 6-4
6.2.4 Initiation Logic Test 6-4
6.2.5 Programmable Logic Controller Execution Test 6-4
6.3 CALIBRATION 6-4
6.4 BYPASS AND PARTIAL TRIP CONDITIONS 6-5
6.4.1 Bypass Condition 6-6
6.4.2 Partial Trip Condition 6-6

7 SUMMARY AND CONCLUSION 7-1

LIST OF TABLES

None.

LIST OF FIGURES

Figure 2-1 AP1000 PMS Architecture 4 Division Overview 2-2

Figure 2-2 PMS Architecture 1 Division Detail 2-5

Figure 2-3 Division Redundancy 2-9

Figure 3-1 Data Flows Between Safety and Non-Safety Equipment 3-4

Figure 3-2 Implementation of Case C Data Flow 3-6

Figure 3-3 Implementation of Case E Data Flow 3-9

Figure 4-1 PMS Safety/QDPS Displays 4-2

Figure 5-1 AC160 Station 5-2

Figure 5-2 PM646 Processor Module 5-4

Figure 5-3 S600 I/O Module 5-5

Figure 5-4 Flat Panel Display System 5-8

Figure 5-5 PC Node Box 5-8

Figure 5-6 Common Q Power Supply Assembly 5-10

Figure 5-7 Typical Common Q Power Supply Plug-in Modules 5-11

Figure 5-8 Component Interface Module 5-12

LIST OF ACRONYMS AND ABBREVIATIONS

1oo2	One-out-of-two
1oo3	One-out-of-three
2oo2	Two-out-of-two
2oo3	Two-out-of-three
2oo4	Two-out-of-four
ADC	Analog-to-Digital Converter
AF100	Advant® Fieldbus 100
AMPL	Advant® Master Programming Language
BPL	Bistable Processor Logic
CD	Compact Disk
CIM	Component Interface Module
CPU	Central Processing Unit
DAC	Digital-to-Analog Converter
DCD	Design Control Document
D/D	Digital-to-Digital Isolator
E/O	Voltage-to-Optical Isolator
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FMEA	Failure Modes and Effects Analysis
FOR	Fiber-Optic Receiver
FOT	Fiber-Optic Transmitter
FPD	Flat Panel Display
HDLC	High-Level Datalink Control
HSL	High Speed Link
I/E	Current-to-Voltage Isolator
I/I	Current-to-Current Isolator
I/O	Input/Output
ICP	Integrated Communications Processor
ILP	Integrated Logic Processor
IR	Intermediate Range
ITP	Integrated Test Processor
LCL	Local Coincidence Logic
MCR	Main Control Room
MG	Motor Generator
MTP	Maintenance and Test Panel
NI	Nuclear Instrumentation
NIMOD	Nuclear Instrumentation Module
NIS	Nuclear Instrumentation Subsystem
NRC	Nuclear Regulatory Commission
PDSP	Primary Dedicated Safety Panel
PLC	Programmable Logic Controller
PLS	AP1000 Plant Control System
PM	Processor Module
PMS	Protection and Safety Monitoring System

LIST OF ACRONYMS AND ABBREVIATIONS (cont.)

PR	Power Range
PROM	Programmable Read Only Memory
QDPS	Qualified Data Processing System
RG	Regulatory Guide
RNC	Remote Node Controller
ROC	Reactor Operators Console
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
SR	Source Range
SRAM	Static Random Access Memory
ST	Shunt Trip
UV	Undervoltage
V&V	Verification and Validation
WDT	Watchdog Timer

Advant, AdvaCommand, AdvaInform, AdvaBuild, AdvaSoft and AdvaControl are registered trademarks of ABB Process Automation Corporation.

Ethernet is a registered trademark of Xerox Corp.

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

Ovation is a mark of Emerson Process Management. Other marks are the property of their respective owners.

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

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:

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 (Reference 7, Section 2).

Onerous Actuation:

System or component actuation that causes a breach of the reactor coolant system pressure boundary or a need to shut down the plant to cold shutdown conditions to effect repairs.

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).

DEFINITIONS (cont.)

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:

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

REFERENCES

1. APP-GW-GL-700, Rev. 15 (Non-Proprietary), Chapter 7, "AP1000 Design Control Document," Westinghouse Electric Company LLC.

2. CENPD-396-P, Rev. 1 (Proprietary), "Common Qualified Platform," May 2000, and WCAP-16097-NP-A (Non-Proprietary), May 2003.

3. CENPD-396-P, Appendix 4, Rev. 2 (Proprietary), "Common Qualified Platform Integrated Solution," April 2001, and WCAP-16097-NP-A, Appendix 4 (Non-Proprietary), May 2003.

4. ML003740165, "Acceptance for Referencing of Topical Report CENPD-396-P, Rev. 01, 'Common Qualified Platform' and Appendices 1, 2, 3 and 4, Rev. 1 (TAC No. MA1677)," August 11, 2000.

5. ML011690170, "Safety Evaluation for the Closeout of Several of the Common Qualified Platform Category 1 Open Items Related to Reports CENPD-396-P, Revision 1 and CE CES 195, Rev. 01 (TAC No. MB0780)," June 22, 2001.

6. ML0305507760, "Acceptance of the Changes to Topical Report CENPD-396-P, Rev. 01, 'Common Qualified Platform,' and Closeout of Category 2 Open Items (TAC No. MB2553)," February 24, 2003.

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), "Safety Criteria for the AP1000 Instrument and Control Systems," April 2002.

9. APP-PMS-J1-003, Rev. B (Proprietary), "PMS Functional Requirements for Nuclear Startup Protection," Westinghouse Electric Company LLC.

10. APP-PMS-J1-004, Rev. B (Proprietary), "PMS Functional Requirements for Nuclear Overpower Protection," Westinghouse Electric Company LLC.

11. APP-PMS-J1-005, Rev. B (Proprietary), "PMS Functional Requirements for Core Heat Removal Protection," Westinghouse Electric Company LLC.

12. APP-PMS-J1-006, Rev. B (Proprietary), "PMS Functional Requirements for Primary Overpressure Protection," Westinghouse Electric Company LLC.

13. APP-PMS-J1-007, Rev. B (Proprietary), "PMS Functional Requirements for Loss of Heat Sink Protections," Westinghouse Electric Company LLC.

14. APP-PMS-J1-008, Rev. B (Proprietary), "PMS Functional Requirements for Main Steam Line and Feedwater Isolation," Westinghouse Electric Company LLC.

REFERENCES (cont.)

15. APP-PMS-J1-009, Rev. B (Proprietary), "PMS Functional Requirements for Safeguards Actuation Protections," Westinghouse Electric Company LLC.

16. APP-PMS-J1-002, Rev. B (Proprietary), "PMS Functional Requirements for Reactor Trip," Westinghouse Electric Company LLC.

17. APP-PMS-J1-010, Rev. B (Proprietary), "PMS Functional Requirements for Containment Protection and Other Protection," Westinghouse Electric Company LLC.

18. APP-PMS-J1-012, Rev. B (Proprietary), "PMS Functional Requirements for the Automatic Depressurization System," Westinghouse Electric Company LLC.

19. APP-PMS-J1-011, Rev. B (Proprietary), "PMS Functional Requirements for Turbine-Related Protection," Westinghouse Electric Company LLC.

20. APP-PMS-J4-001, Rev. E (Proprietary), "Post-Accident Monitoring System Functional Specification," Westinghouse Electric Company LLC.

21. WCAP-16438-P (Proprietary), "FMEA of AP1000 Protection and Safety Monitoring System," June 2006.

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 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc, 2003.

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 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-J1-003, "PMS Functional Requirements for Nuclear Startup Protection" (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 APP-PMS-J1-004, "PMS Functional Requirements for Nuclear Overpower Protection" Reference 10

5. Power Range High Positive Flux Rate Reactor Trip as described in Reference 10

6. Over-temperature ΔT Reactor Trip as described in APP-PMS-J1-005, "PMS Functional Requirements for Core Heat Removal Protection" (Reference 11)

7. Overpower ΔT Trip as described in Reference 11

8. Reactor Trip on Low Pressurizer Pressure as described in Reference 11

9. Reactor Trip on Low Reactor Coolant Flow as described in Reference 11

10. Reactor Trip on Reactor Coolant Pump Underspeed as described in Reference 11

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

12. Pressurizer High Pressure Reactor Trip as described in APP-PMS-J1-006, "PMS Functional Requirements for Primary Overpressure Protection" (Reference 12)

13. Pressurizer High Water Level Reactor Trip as described in Reference 12

14. Reactor Trip on Low Water Level in any Steam Generator as described in APP-PMS-J1-007, "PMS Functional Requirements for Loss of Heat Sink Protections" (Reference 13)

15. High-2 Steam Generator Water Level in Any Steam Generator as described in APP-PMS-J1-008, "PMS Functional Requirements for Main Steam Line and Feedwater Isolation" (Reference 14)

16. Automatic Depressurization Systems Actuation Reactor Trip as described in APP-PMS-J1-009, "PMS Functional Requirements for Safeguards Actuation Protections" (Reference 15)

17. Core Makeup Tank Actuation Reactor Trip as described in Reference 15

18. Reactor Trip on Safeguards Actuation as described in Reference 15

19. Manual Reactor Trip as described in APP-PMS-J1-002, "PMS Functional Requirements for Reactor Trip" (Reference 16)

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 15

2. Containment Isolation as described in APP-PMS-J1-010, "PMS Functional Requirements for Containment Protection and Other Protection" (Reference 17)

3. In-Containment Refueling Water Storage Tank Injection as described in Reference 15

4. Core Makeup Tank Injection as described in References 13 and 15

5. Automatic Depressurization System Actuation (Stages 1-3 and Stage 4) as described in APP-PMS-J1-012, "PMS Functional Requirements for the Automatic Depressurization System" (Reference 18)

6. Reactor Coolant Pump Trip as described in Reference 15

7. Main Feedwater Isolation as described in Reference 14

8. Passive Residual Heat Removal Actuation as described in References 12, 13, and 15

9. Turbine Trip as described in APP-PMS-J1-011, "PMS Functional Requirements for Turbine-Related Protection" (Reference 19)

10. Containment Recirculation as described in Reference 15

11. Steamline Isolation as described in Reference 14

12. Steam Generator Blowdown System Isolation as described in Reference 13

13. Passive Containment Cooling Actuation as described in Reference 17

14. Startup Feedwater Isolation as described in Reference 14

15. Boron Dilution Block as described in Reference 9

16. CVS Isolation as described in References 12 and 15

17. Steam Dump Control as described in Reference 14

18. Main Control Room Isolation as described in Reference 17

19. Auxiliary Spray and Purification Line Isolation as described in Reference 1, Section 7.3.1.2.18

20. Containment Air Filtration Isolation as described in Reference 17

21. Refueling Cavity Isolation as described in Reference 1, Section 7.3.1.2.21

22. CVS Letdown Isolation as described in Reference 1, Section 7.3.1.2.22

23. Pressurizer Heater Block as described in Reference 1, Section 7.3.1.2.23

24. Steam Generator Relief Isolation as described in Reference 14

25. Normal Residual Heat Removal Containment Isolation as described in References 15 and 17

26. Demineralized Water Transfer and Storage System Isolation as described in Reference 1, Sheet 7.2-29

27. Reactor Vessel Head Vent valve control (no reference available)

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, and the data display and processing system.

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 DC uninterruptible Power Supply system. The plant control system and the data display and processing system 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 data display and processing system also provides an alternate display of the variables, which are displayed by the PMS. Electrical separation of the data display and processing system 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:

- 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
- Process data for main control room (MCR) display, and to meet Regulatory Guide 1.97 (Reference 22) requirements
- Provide 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 Plant Control System (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/QDPS 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 4 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/QDPS 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 Q hardware Platform, which comprises the PMS configuration for the AP1000. The Common Qualified Platform described in References 2 and 3 was accepted by the NRC in References 4, 5, and 6.

a,c

Figure 2-1 AP1000 PMS Architecture 4 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 2oo3 (two-out-of-three) logic from a 2oo4 (two-out-of-four) 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 bistable processor logic (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 shutdown.

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.

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

[

]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.

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 and is capable of measuring overpower excursions up to 200 percent of full power. 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, with over-range capability extending to 200 percent. 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 Intermediate Range 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 NI cabinet. The Common Q hardware is described in References 2 and 3.

The Common Q 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 setpoints and 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

[ ]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

[

]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 processor module performs all pressure, temperature, level, and flow algorithms and compares 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

[

]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 failsafe trip output signal to the reactor trip switchgear.

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

[

]a,c

[

]a,c

2.2.3.1 Reactor Trip Coincidence Logic

[

]a,c

[

]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

[

]a,c

2.2.3.1.1 Reactor Trip Switchgear Interface and Initiation Logic

[

]a,c

[

]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 can be accomplished from the MCR by redundant momentary switches. The switches directly interrupt the power from the voting logic, actuating the UV and ST attachments. 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

[

]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 description provided below 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

[

]a,c

2.2.5 Integrated Test Processor Subsystem

[

]a,c The divisions are physically separated and electrically isolated

from each other. The description provided below illustrates the operation of one of the four identical divisions.

[

]a,c

[

]a,c

[

]a,c

[

]a,c

[

]a,c

2.2.6 Maintenance and Test Panel Subsystem

[

]a,c The description provided below 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

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 in References 4, 5, and 6.

[

]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 Changes

[

]a,c

2.2.6.2 Program Changes

[

]a,c

2.2.6.3 Interface to Plant Control System

[

]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.

3.1 INTRA-DIVISIONAL COMMUNICATIONS VIA AF100 BUS

Within each PMS division, the internal functions and the safety portions of both 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 Safety/QDPS 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 and general purpose communication. Real-time data distribution is defined as the scheduled periodic broadcast of real-time data pertaining to the plant processes. General purpose communication is defined as the aperiodic exchange of data for other purposes, such as system operation, diagnostics, maintenance, etc. On the AF100 bus, real-time data distribution is referred to as process data transfer and general purpose communication is referred to as message transfer. [

]a,c

3.1.1 Real-Time Data Distribution

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

]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 General Communications

General communication is accomplished using message transfer services. Message transfer is not performed cyclically like process data transfer, but only when one (or more) of the attached communication interfaces have something to send. Message transfer does not influence process data transfer in any way. Process data transfer remains deterministic. [

]a,c

Within the PMS, general communication is primarily used for diagnostic purposes. Security is maintained since the ability to remotely program the AC160 controllers and Safety/QDPS display systems over the AF100 bus has been disabled in the PMS.

3.1.3 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).

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.

3.3 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. 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) and prevent 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). 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 the PLS pertaining to analog and 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 PLS as individual hardwired analog or digital signals. This type of interface is shown as Case B 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 IEEE 603 [Reference 7]) and prevent 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). They also provide functional isolation by preventing the non-safety system from adversely affecting the safety function.

3.3.3 Isolated Gateway Signals to Non-Safety (Case C)

Various process-related signals (analog inputs signals, analog signals calculated within the PMS, and digital signals calculated within the PMS) are sent to the Data Display and Processing System (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 Advant®/Ovation® Interface (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.

a,c

Figure 3-2 Implementation of Case C Data Flow

3.3.4 System-Level Safety Functions from RSR Fixed Position Switches (Case D)

The non-safety manual controls of system-level safety functions (actuations, manual blocks and resets, manual reactor trip) originate from dedicated switches in the RSR. The individual hardwired digital signals are classified as non-safety-related and are, therefore, isolated in the PMS cabinets before being used. 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]) and prevent all but the required data flow from the non-safety system to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2 (Reference 23) Annex G).

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 the vast majority of the time. 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. Specifically, the manual system-level ESF actuations and the manual reactor trip inputs can only initiate safety functions, not inhibit them; the blocks are subject to initiation permissives and to automatic removal; and resets are only effective if the initiating conditions have been eliminated.

3.3.5 Non-Safety Manual Component-Level Control of Safety Components (Case E)

The manual component soft controls originate in the PLS. 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. 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 circuits. This type of interface is shown as Case E on Figure 3-1.

The remote I/O node includes one or more Class 1E CIMs. Internally, these modules contain the equivalent of a digital output module. The resulting 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. If conflicting demands are present, the safe state of the component takes priority. The CIMs also contain the equivalent of a 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 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 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 safe state based priority 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, the Secondary Dedicated Safety Panel (SDSP), and the Reactor Operator's Console. 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/QDPS displays in the MCR. The Safety/QDPS 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.

a,c

Figure 3-3 Implementation of Case E Data Flow

- 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 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.

3.4.2 Manual Component-Level Control

ESF components are divided into two categories: those whose actuation have onerous consequences and those whose actuation do not have onerous consequences. Onerous consequences are defined as those that cause a breach of the Reactor Coolant System (RCS) pressure boundary or cause a need to shut down the plant to cold conditions to effect repairs. Manual component-level control is implemented differently for the two categories.

For components whose actuations do not have onerous consequences:

- 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 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.

For components whose actuations have onerous consequences:

- 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/QDPS displays in the MCR. The soft controls use a multi-step sequence to reduce the chance of spurious actuation. The Safety/QDPS 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 the squib valves from a location in the southern end of the auxiliary building.

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

[Four Safety/QDPS displays are provided in the PMS architecture, as shown in Figure 4-1. One Safety/QDPS display is associated with each of the four independent divisions of the PMS.][a,c] Upon loss of all AC power (station blackout), all four divisions of Safety/QDPS displays are available for the first 24 hours. After 24 hours, only Divisions B and Division C Safety/QDPS displays are available to conserve power drain from the 72 hour batteries.

The primary functions of the Safety/QDPS displays are as follows:

[

]^{a,c}

Each Safety/QDPS 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/QDPS displays. Provisions are provided for temporary connection of a keyboard to the front of the display unit.

a,c

Figure 4-1 PMS Safety/QDPS Displays

[

]a,c

Components with onerous consequences are defined as those components that create a breach of the RCS boundary or a need to shut down the plant to cold conditions to effect repairs. Manual control of all other safety components is accomplished from the non-safety operator workstations, via the non-safety Real Time Data Network, remote node controller (RNC) and CIM.

For NI calibration, the Safety/QDPS display provides the operator the ability to enter, store, and change the gain and offset for the NI Power Range upper flux signal and lower flux signal. No calibration of the Source Range or Intermediate Range 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 described earlier.
- 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

[

]a,c

The QDPS variables to be displayed are identified in APP-PMS-J4-001, "Post-Accident Monitoring System Functional Specification" Reference 20.

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:

- Advant® Controller 160 (AC160) with PM646 Processor Module
- S600 Input and Output Modules
- Flat Panel Display System for human-machine interface consisting of the MTP, Safety/QDPS display and Operators Module
- Power supply
- Component Interface Module (CIM)
- Termination Units
- Cabinets

The Common Q Topical Reports (References 2 and 3) have been reviewed by the NRC. The NRC Safety Evaluation Reports (SER) approving the use of Common Q for safety-related applications are contained in References 4, 5, and 6. In addition, the Swedish regulatory body, SKi, provided Unit 1 at Oskarshamn Nuclear Power Plant (NPP) in November 2002 approval to load fuel with Westinghouse Common Q product used in the Reactor Protection System. The Common Q product was extensively reviewed, lead 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 USA and DELTA Development Technology AB in Sweden.

5.1.1 Advant® Controller AC160

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

Westinghouse's Advant® Controller 160 (AC160), 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.

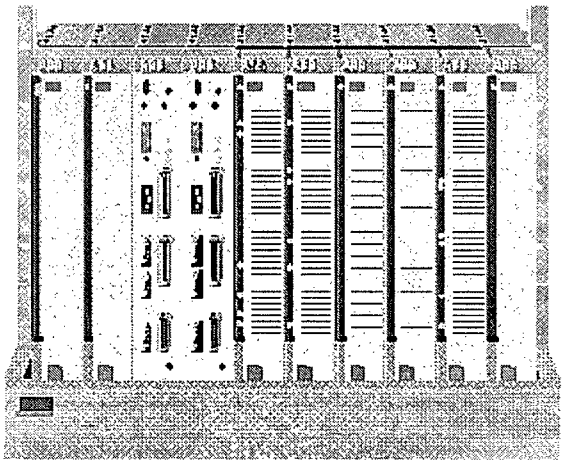

Figure 5-1 AC160 Station

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
- Time stamping

The computer processing unit (CPU) module PM646 (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.

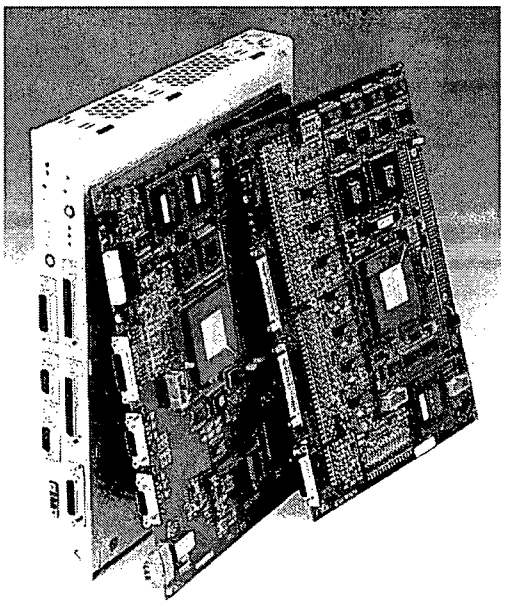

Figure 5-2 PM646 Processor Module

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 Advant® Controller 160 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, pulse counting, position measurement and strain gauge applications.

S600 I/O modules (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.

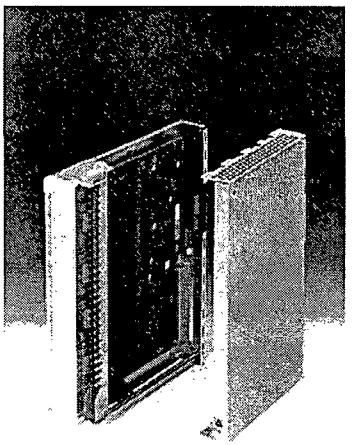

Figure 5-3 S600 I/O Module

The system software in the Advant® Controller 160 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 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.

- AI685: 16 differential input channels, 0/4-20 mA, +20 mA, 0-100 mV, 0-1 V, 0-10 V, + 10 V, 16 bit resolution
- 14 thermocouple input channels, Types J, K, E with cold reference junction compensation, 16 bit resolution
- 8 RTD input channels, Pt100, Pt200, 16 bit resolution
- 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) (Figure 5-4) 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/QDPS 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 18 inch diagonal measurement. The 12 inch display is typically used for an Operators Module. The 15 inch display is typically used for the MTP display. Because of its larger viewing area, the 18 inch display is used for Safety Displays in the MCR.

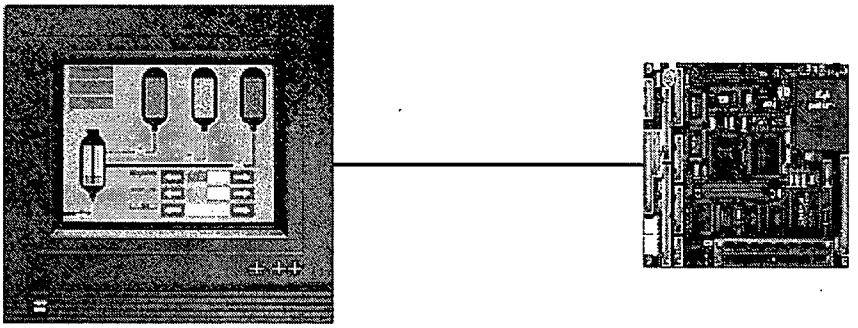

Figure 5-4 Flat Panel Display System

5.1.3.2 PC Node Box

The PC Node Box (Figure 5-5) is the interface between the AF100 bus and the flat panel video display.

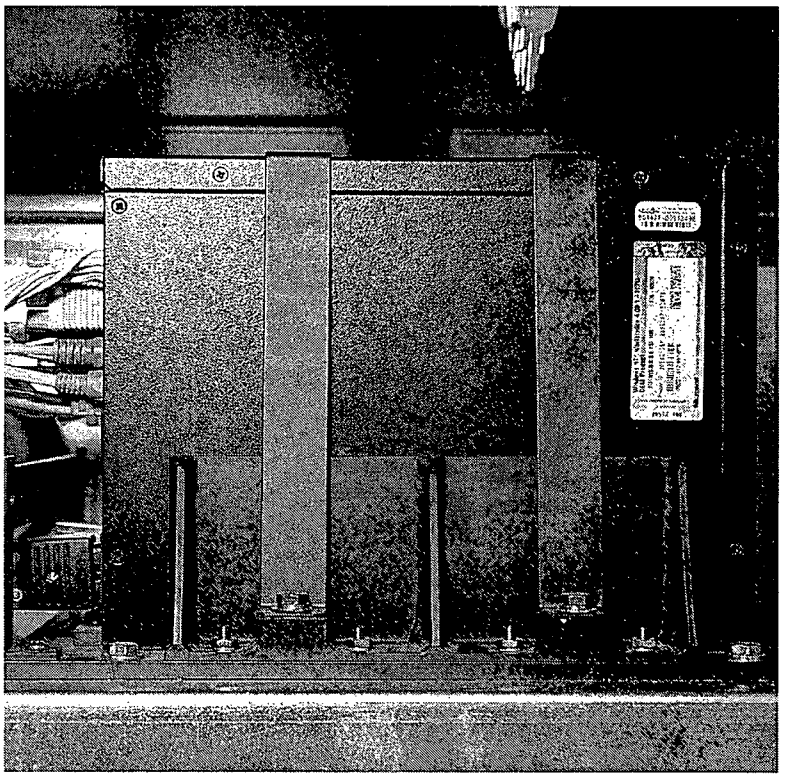

Figure 5-5 PC Node Box

The PC Node Box contains the following components:

- Single Board Computer

  The dual boot single board 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.

- CI527 Communication Interface Module

  The CI527 Communication Interface Module is used to access the AC160 AF100 bus.

- Ethernet Communication Board

  The Ethernet communication board supplies the interface to external non-safety systems such as the plant computer or distributed control systems. A fiber-optic media converter is used to provide Class 1E isolation between the safety system and the non-safety system.

- Digital Input/Output Board

  The digital input/output board is used for key-switch inputs and annunciator outputs, if required.

- Compact Disk Drive

  The CD drive is used to load new display software, load/store setpoints and tuning constants, and to store other status information at operator request.

- Connectors for serial and parallel ports, keyboard and mouse

5.1.4 Common Q Power Supply

The Common Q power supply is a 19 inch rack assembly with plug-in modules. Various modules are available to accommodate different output voltages. AC input power to the Common Q power supply system is 100 to 140 VAC or 200 to 260 VAC at a line frequency of 47 to 63 Hz.

All active power supply components are housed in plug-in modules to facilitate maintenance. All plug-in modules are plugged into a backplane mounted in a standard 19 inch rack-mount card cage 5.25 inches high. A removable fan drawer (1.75 x 19 inches) is mounted below the card cage for cooling. Overall, the chassis front panel is 7 inches high and 19 inches wide. The overall chassis depth is 15.25 inches. Additional space is required at the chassis rear for power input and output cabling and optional hold-down brackets.

The power supply consists of a minimum of one AC Line Filter Module and a Front-End Module to convert line AC power to approximately 300 VDC. One or more DC/DC Converter Modules convert the

300 VDC to a final DC output voltage in the range of 2 to 48 VDC. DC/DC Converter Modules can be connected in series for higher output voltages up to 98 VDC or in parallel for higher current output or redundancy. In redundant configurations, a second Filter and Front-End Module pair is provided to supply 300 VDC to the redundant DC/DC Converters. Redundant converters, operating at medium and high power output (150 to 400 W total output power), are normally configured to load share at 50 percent ± 5 percent. Redundant micro-power converters (less than 100 W) may be configured to operate in parallel with output isolation diodes, but they are not designed for 50 percent load sharing. Faults in one half of the redundant supply do not affect the other half 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. Maximum inrush current is less than 13 Amps-peak at 120 VAC and less than 20 Amps-peak at 240 VAC. Hold-up time for momentary loss of AC power is 24 milliseconds (minimum). The Common Q power supply can be mounted in the top or bottom of a cabinet.

Figure 5-6 is a typical Common Q power supply assembly. Figure 5-7 depicts the power supply plug-in modules.

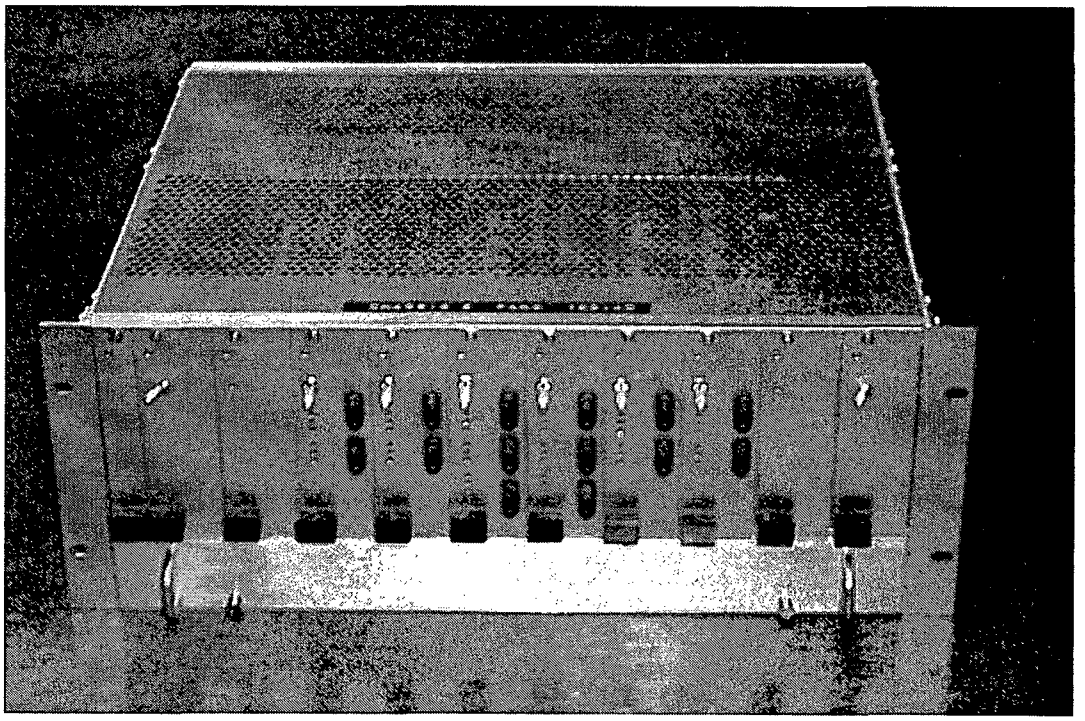

Figure 5-6 Common Q Power Supply Assembly

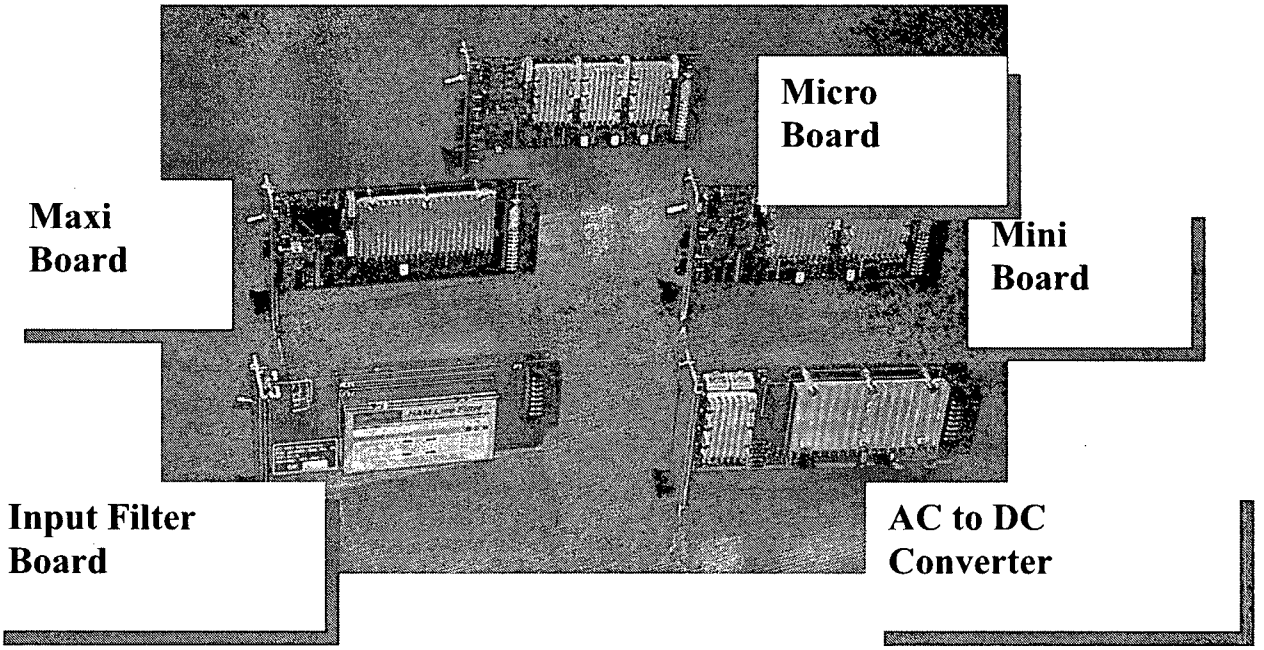

Figure 5-7 Typical Common Q Power Supply Plug-in Modules

5.1.5 Component Interface Module

[

]a,c

[

]a,c

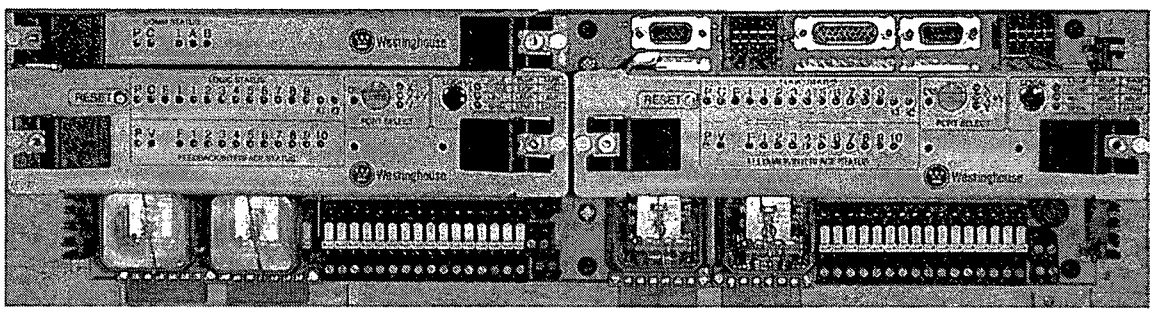

Figure 5-8 Component Interface Module

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:

- AI685 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.

5.2 SOFTWARE DESCRIPTION

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

The Advant® Controller 160 software consists of a real-time operating system, task scheduler, diagnostic functions, communication interfaces, and user application programs, all of which reside on flash PROM in the PM646 processor module. 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 Process Control (PC) elements, and Database elements, called DB elements. The PC elements and DB elements are combined into programs that form a complete control function.

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 CD-ROM. The MTP includes a CD-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, start-up, and shut-down 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 (Advant® Master Programming Language) application programs graphically, using either 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 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 this 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 de-bugging 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 multi-processing system that is designed such that displays are dynamically updated from data acquired from the AF100 network 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 network for the display application and other processes, sending configured data over the Advant®/Ovation® Interface (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 MAINTENACE, 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 operation. 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 elements 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 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 overlapping tests:

- Sensor Input Check
- Trip Bistable Test
- Local Coincidence Logic Test
- Initiation Logic Test
- PLC (Programmable Logic Controller) Execution 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 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 relay(s) 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 generation of heartbeat signals from the BPL, LCL, and ILP subsystem processors as an indication of their continued operation (execution of programs). If the heartbeat is not received within a specified length of time, the MTP and ITP will annunciate its loss.

6.3 CALIBRATION

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

Each NI subsystem power range 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/QDPS displays in the MCR. Using the Safety/QDPS 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/QDPS display is associated with a PMS division, the NI calibration operation must be repeated four times, once for each PMS division.

Safety algorithms containing temperature input signals also contain provisions for gain and offset calibration coefficients. The capability for this calibration is provided to the I&C technician via the MTP display in the PMS cabinet. Using the MTP display, the I&C technician navigates to the temperature input calibration display and enters the calculated gain and offset coefficients for each temperature input measurement in that division. Since each MTP display is associated with a PMS division, the temperature input calibration operation must be repeated four times, one for each PMS division. Periodic calibration is performed as required by the plant technical specifications.

For all other analog inputs, if the analog input cannot be calibrated, the associated input module is replaced.

Calibration verification is performed for the following equipment:

- Power supply voltages
- Pulse inputs
- Analog outputs

If the associated component fails the calibration, the component must be replaced.

6.4 BYPASS AND PARTIAL TRIP CONDITIONS

[

]a,c

[

]a,c

6.4.1 Bypass Condition

[

]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 not 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