Westinghouse Non-Propietary Class 3

WCAP-16438-NP
Revision 1

June 2006

FMEA of AP1000 Protection and Safety Monitoring System

WCAP-16438-NP
Revision 1

FMEA of AP1000 Protection and Safety Monitoring System

Bruce Cook
Technology Standards and Reliability

June 2006

Reviewer: Raymond R. Senechal*
Reactor Protection Systems II

Approved: Timothy C. Wilson*, Manager
PMS Project Manager

Approved: Larry E. Erin*, Manager
Reactor Protection Systems I

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

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

TABLE OF CONTENTS

LIST OF TABLES iv

LIST OF FIGURES v

LIST OF ACRONYMS AND TRADEMARKS vi

REFERENCES viii

1 INTRODUCTION 1-1
1.1 PURPOSE 1-1
1.2 SCOPE 1-1
1.3 CONCLUSIONS 1-2

2 ARCHITECTURE OVERVIEW 2-1
2.1 BPL PROCESS STATION 2-1
2.2 LCL PROCESS STATION 2-2
2.3 REACTOR TRIP INTERFACE 2-4
2.4 ILC PROCESS STATION 2-5
2.5 NIS SUBSYSTEM 2-6
2.6 ICP PROCESS STATION 2-7
2.7 ITP PROCESS STATION 2-8
2.8 MTP PROCESS STATION 2-8
2.9 QDPS/SAFETY DISPLAY SUBSYSTEM 2-9
2.10 QDPS PROCESS STATION 2-9
2.11 POWER DISTRIBUTION 2-10
2.12 DEFAULT ACTIONS 2-11

3 FMEA METHODOLOGY 3-1

4 FMEA TABLES 4-1
4.1 BPL PROCESS STATION 4-2
4.2 LCL PROCESS STATION 4-9
4.3 REACTOR TRIP INTERFACE 4-20
4.4 ILC PROCESS STATION 4-26
4.5 NIS SUBSYSTEM 4-35
4.6 ICP PROCESS STATION 4-50
4.7 ITP PROCESS STATION 4-54
4.8 MTP PROCESS STATION 4-59
4.9 QDPS/SAFETY DISPLAY SUBSYSTEM 4-61
4.10 QDPS PROCESS STATION 4-63
4.11 POWER DISTRIBUTION 4-67

LIST OF TABLES

Table 2-1 LCL Processor Assignments (Division B) 2-3

Table 4-1 Failure Criticality Classes 3-2

Table 4-2 Failure Detectability Classes 3-2

LIST OF FIGURES

Figure 2-1 PMS One Line Architecture 2-14
Figure 2-2 Typical PMS Division Configuration (Division B Shown) 2-15
Figure 2-3 Reactor Trip Interface Relay Matrix 2-16

LIST OF ACRONYMS AND TRADEMARKS

AC160	Advant Controller Series 160
ADC	Analog to Digital Converter
AF100	Advant Fieldbus 100
AOV	Air Operated Valve
ASIC	Application Specific Integrated Circuit
BCC	Bistable/Coincidence Logic Cabinet
BIOB	Backplane Input Output Bus
BPL	Bistable Processor and Logic
CIM	Component Interface Module
CPS	Counts Per Second
CRC	Cyclic Redundancy Check
CS	Communication Section (of the PM646A Module)
DAS	Diverse Actuation System
DDS	Data Display and Processing System
DO	Digital Output
DSP	Dedicated Safety Panel
ESF	Engineered Safety Features
FMEA	Failure Modes and Effects Analysis
FOM	Fiber Optic Modem
FPD	Flat Panel Display
HOV	Hydraulic Operated Valve
HSI	Human System Interface
HSL	High Speed Link
HV	High Voltage
ICP	Interface Communication Processor
ILC	Interposing Logic Cabinet
IR	Intermediate Range
ISO	Isolator
ITP	Interface and Test Processor
LCL	Local Coincidence Logic
LCO	Limiting Condition for Operation
MCC	Motor Control Center
MCR	Main Control Room
MOV	Motor Operated Valve
MTP	Maintenance and Test Processor
MSV	Mean Squared Voltage
NIMOD	Nuclear Instrumentation Module
NIS	Nuclear Instrumentation Subsystem

LIST OF ACRONYMS AND TRADEMARKS (cont.)

PC	Personal Computer
PLS	Plant Control System
PM	Processor Module
PMS	Protection and Safety Monitoring System
PR	Power Range
PS	Processor Section (of the PM Module)
QDPS	Qualified Data Processing System
RCP	Reactor Coolant Pump
RMS	Root Mean Square
RPS	Reactor Protection System
RNC	Remote Node Controller
RSR	Remote Shutdown Room
RSW	Remote Shutdown Workstation
RTCB	Reactor Trip Circuit Breaker
RTD	Resistance Temperature Detector
RTDN	Real Time Data Network
SHA	Software Hazards Analysis
SIR	Shunt trip Interface Relay
SMS	Special Monitoring System
SOV	Solenoid Operated Valve
SR	Source Range
STA	Shunt Trip Attachment
TU	Termination Unit
UIR	Undervoltage Interface Relay
UPS	Uninterruptible Power Supply
UVTA	Undervoltage Trip Attachment
WDT	Watchdog Timer
WR	Wide Range
XIR	Auxiliary Interposing Relay

REFERENCES

Following is a list of references used throughout this document.

1. ANSI/IEEE 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems"

2. APP-GW-GL-700, "AP1000 Design Control Document"

3. APP-GW-J4-001, Rev. B, "AP1000 I&C System Design Specification" (proprietary)

4. NABU-DS-00092-GEN, Rev. 1, "Safety Platform System Design Requirements" (Proprietary)

5. WNA-DS-00931-SSP, Rev. 0, "Production Specification of the Advant Controller 160" (Proprietary)

6. WCAP-15775, Rev. 2, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report"

7. WCAP-15776, Rev. 0, "Safety Criteria for the AP1000 Instrumentation and Control Systems"

8. WCAP 16097-P-A, Appendix 3, Rev. 0, "Common Qualified Platform – Digital Plant Protection System" (Proprietary)

9. WCAP-16096-NP-A, Rev. 1A, "Software Program Manual for Common Q Systems"

10. APP-OCS-J7-001, Rev. A, "Operations and Control Centers System System Specification Document" (Proprietary)

11. NABU-DS-00102-GEN, Rev. 2, "Component Interface Module (CIM) Hardware Requirements Specification" (Proprietary)

12. NABU-DS-00109-GEN, Rev. 1, "Application Specification for CIM Universal Logic" (Proprietary)

13. WNA-CN-00031-GEN, Rev. 2, "Reliability Calculation of the Component Interface Module" (Proprietary)

14. WCAP-7211, Rev. 5, "Proprietary Information and Intellectual Property Management Policies and Procedures"

REFERENCES (cont.)

15. WCAP-16592-P, Rev. 0, "Software Hazard Analysis of AP1000 Protection and Safety Monitoring System," (Proprietary)

1 INTRODUCTION

1.1 PURPOSE

A Failure Modes and Effects Analysis (FMEA) is performed on the plant protection system to reveal potential single failure modes. ANSI/IEEE 352-1987 (Reference 1) identifies the purposes of an FMEA as follows:

a. To assist in selecting design alternatives with high reliability and high safety potential during early design phases

b. To ensure that all conceivable failure modes and their effects on the operational success of the system have been considered

c. To list potential failures and identify the magnitude of their effects

d. To develop early criteria for test planning and the design of test and checkout systems

e. To provide a basis for quantitative reliability and availability analyses

f. To provide historical documentation for future references to aid in the analysis of field failures and consideration of design changes

g. To provide input data for tradeoff studies

h. To provide a basis for establishing corrective action priorities

i. To assist in the objective evaluation of design requirements related to redundancy, failure detection systems, fail-safe characteristics, and automatic and manual override

An FMEA was performed (Reference 8) for the generic Common Qualified Platform Digital Plant Protection System, of which the AP1000 Protection and Safety Monitoring System (PMS) is an example. However, there are architectural differences between the system analyzed in that report and the one applied to AP1000. Therefore, this report contains a specific analysis for the AP1000 PMS.

This analysis addresses system failures from the viewpoint of hardware failure initiated events. A separate Software Hazard Analysis is provided for events that could lead to software malfunction (Reference 15).

1.2 SCOPE

The FMEA is applied to the electronic portions of the PMS excluding sensors, squib valve controllers and actuators. The reactor trip switchgear is included.

The details of the squib valve interface have been excluded from the scope of the analysis.

Particular attention is paid to failure modes that may affect the time response of the safety functions. This is done to determine the extent to which time response testing must be performed during the operation of the plant.

There is two-out-of-four (2/4) logic for each parameter that initiates protective action when two or more divisions agree that a parameter is no longer within the acceptable limit. The software in the four divisions is functionally identical.

Reference 9 covers the activities in the software design, implementation, verification and validation process.

The defense in depth approach is implemented by the Diverse Actuation System (DAS). The DAS consists of diverse sensors, signal conditioning, trip recognition logic, trip actuation circuitry and software from the PMS. The DAS is not included in the scope of this FMEA.

Proprietary information contained within this report is marked in accordance to the procedures of Reference 14.

1.3 CONCLUSIONS

The assignment of Engineered Safety Feature (ESF) equipment to specific Interposing Logic Cabinet (ILC) cabinets and the details of the interface to the plant equipment have a bearing on the impact of single failures in this part of the system, which are addressed in the detailed design. However, the following conclusions can be drawn about the PMS system architecture.

a. Due to the high degree of redundancy within the reactor trip interface, a single failure of the electronics does not prevent a division from responding to a valid actuation signal for reactor trip.

b. Single failures may prevent the actuation of an individual ESF component, or may lead to its spurious actuation; however, plant safety is retained through the redundant ESF components actuated from other divisions. The effects of the spurious actuations of the equipment on the plant operation are addressed as design basis accidents in the Design Control Document (Reference 2).

c. Single failures may prevent information display through one QDPS/Safety Display; however, all monitored process variables will remain available through redundant measurements on the displays of other divisions.

d. Failures affecting protective functions are detectable by either diagnostics or planned periodic surveillance tests.

e. Several failures have been identified (with a 'C' in the fault classification) that depend on the periodic surveillance test for their detection. The design of the test facilities and sequence, and the interval at which the testing is performed, takes these failures into account.

2 ARCHITECTURE OVERVIEW

The overall architecture of the PMS is shown, in simplified form, in Figure 2-1. This diagram shows the communication interfaces among the various cabinets and process stations that make up the system that consists of four divisions. Divisions B and C are identical in content and contain a full complement of the equipment. Divisions A and D each contain a subset of the equipment to provide a four channel redundancy where specified by the system requirements.

This analysis focuses on Division B as being representative of each division. Differences between the divisions will be so noted when the differences are significant. Figure 2-2 provides a detailed diagram of this division's equipment. The analysis considers each process station or sub-system as outlined below.

2.1 BPL PROCESS STATION

There are two Bistable Processor and Logic (BPL) process stations located in separate cabinets, PMS-JD-BCCB01 and PMS-JD-BCCB02. The BPLs receive input from process sensors, both analog and digital, and perform bistable functions, making the logical decision that the plant condition has exceeded pre-established limits. This includes, in the case of the over-temperature and over-power delta T channels, the computation of setpoint values based on multiple process sensor inputs. Operational bypass logic, such as that applied to the source range Nuclear Instrumentation Subsystem (NIS) channels, is performed in the NIS process station.

Each BPL contains a single PM processor module that has two parts, a functional processor and a communications processor. The communications processor transmits the partial trip signals (bistable results) to the Local Coincidence Logic (LCL) process stations in every division. A single message is transmitted, and is electrically 'split' to go to all destinations. The High Speed Link (HSL) connections to both LCLs in the same division are "copper" connections, while those going to other divisions are fiber optic, using transmit/receive modem pairs. All HSL connections are unidirectional. The functional processor part of the PM module scans the input modules, converts the process signals to engineering values (if not already done by the I/O modules), compares the values to setpoints (the bistable function) and passes the results to the communications processor for transmittal to the LCLs.

As part of the process value conversion function, the signals are validated. Signals that are outside of the valid range, or whose input module is determined to be failed by self-diagnostics, are set to 'BAD' quality. The bistable outputs associated with signals of 'BAD' quality are set to the tripped state and the bistable output signals are themselves given BAD quality. In addition to the bistable output value and the quality value, each bistable has two additional signals that can be manually set or removed via the Maintenance and Test Processor (MTP) console. These are the CHANNEL BYPASS signal and the FORCE PARTIAL TRIP signal. These are set independently for the two BPL process stations in the division. Resolution of the vector of bistable output values is performed by the processors of the LCL process station as described in Section 2.2.

A CI communications module in each BPL stores status information for transmission on the AF100 bus. Operator actions made through the division's QDPS/Safety Display are received from the AF100 bus via the CI communications module. This connection also provides for maintenance of the BPL software and setpoints from the MTP.

Sensor inputs are shared between the two BPL processors within a division. This sharing is done via a current loop connection or, in the case of Resistance Temperature Detector (RTD) inputs, a parallel connection. The sensor input values may be replaced by test injection signals, received via the AF100 bus, under control of a hardwired Test Enable keyswitch (digital) input and a test enable software signal also received via the AF100 bus. Injecting a signal in one BPL does not affect the use of that signal in the other BPL of the division.

Certain sensor signals are sent to the control system through analog isolation devices. These signals are used to regulate the primary process variables to keep them within the safety limits. The isolators prevent faults on the non-safety side from causing effects to the safety circuits that could prevent them from accomplishing their assigned safety functions. In the control system, signal validation techniques, such as median signal selection, are applied to reduce the multiple redundant measurements of each process parameter to a single value that best represent the process parameter.

2.2 LCL PROCESS STATION

There are two LCL process stations located in separate cabinets, the same as those that contain the BPL process stations. Each LCL receives eight HSL connections containing the partial trip and partial actuation signals, one from each of the two BPLs in each of the four divisions. The process stations combine the partial trips via majority voting logic to actuate the reactor trip breakers in the division and combine the partial actuations to send system level ESF actuations to the component actuation logic performed in the ILC process stations.

Each LCL contains four PM processor modules, each of which has two parts, a functional processor and a communications processor. The communications processor is capable of receiving two HSL connections (hence the need for four processors to handle the eight connections) and to transmit one HSL connection. The receive connections are distributed among the four processors such that the two connections from a given division are handled by different processors. Table 2-1 shows the LCL processor assignments. Note that in each LCL, two processors perform the reactor trip logic, one processor performs the ESF actuation logic, and one processor is only used for HSL communication.

The data received via HSL connections is shared between the four processors through the global memory segment of the CI. Each functional processor uses the two connections it receives directly and the other six by way of the global memory. Each logical signal is resolved, on a point by point basis, according to the signal value, its quality, the CHANNEL BYPASS and FORCE PARTIAL TRIP states and the quality status of the HSL receiver channel over which the point is received. If a signal has BAD quality or if its receive channel has BAD quality then the signal from the other BPL is used. In the condition that signals of GOOD quality are available from both BPLs of a division, a logical OR of the FORCE PARTIAL TRIP OR SIGNAL VALUE AND NOT BYPASS is used. If both signals have BAD quality, then a default value, based on the preferred failure mode, which is TRUE for reactor trip actuations and FALSE for ESF actuations, is used. The resulting signals from the four divisions are passed on to the two out of four (2/4) or two out of three (2/3) voting logic.

Table 2-1 LCL Processor Assignments (Division B)			
LCL Station	**Processor**	**BPL TO LCL HSLs**	**Function of Processor**
LCL-1	PM1	DIV A BPL-1, DIV D BPL-2	Reactor trip DO
LCL-1	PM3	DIV B BPL-2, DIV C BPL-1	Reactor trip DO
LCL-1	PM2	DIV C BPL-2, DIV B BPL-1	ESF functions with HSL to ILC
LCL-1	PM4	DIV D BPL-1, DIV A BPL-2	HSL input only
LCL-2	PM2	DIV C BPL-2, DIV B BPL-1	Reactor trip DO
LCL-2	PM4	DIV D BPL-1, DIV A BPL-2	Reactor trip DO
LCL-2	PM1	DIV A BPL-1, DIV D BPL-2	ESF functions with HSL to ILC
LCL-2	PM3	DIV B BPL-2, DIV C BPL-1	HSL input only

Each of the reactor trip LCL processor modules generates two Reactor Trip signals, one for the undervoltage trip relay matrix and one for the shunt trip relay matrix. These signals are sent to the relay matrices via hard-wired outputs. Each processor module accesses a dedicated Digital Output (DO) relay output module (DO) to reduce the extent of lost functionality in the event of a single failure. The DO signals are combined with the contacts of the Watchdog Timer (WDT) to cause fail safe action upon failure of the processor. The trip relay matrices are discussed in further detail in Section 2.3.

A functional requirement of the PMS is that a Reactor Trip actuation shall be performed when the Safety Injection or Automatic Depressurization functions are initiated by either automatic or manual means. This feature is done by the LCL processor that performs ESF functions sending a digital (software) signal to the two LCL processors performing reactor trip functions by way of the global memory feature of the CI module. The reactor trip functional processors then combine this signal with those from the BPL channel voting logic to generate the outputs sent to the trip interface matrix.

The logic signals received by the HSLs can be substituted by test injection signals, received via the AF100 bus, under control of the status of the Test Enable keyswitch (digital) input and a test enable software signal both of which are received via the AF100 bus. Only the enable signals from the LCL's own division are applied. Also, the digital output signals sent to the DO modules for reactor trip may be substituted for testing under the same controls.

Each LCL process station has an extension chassis that houses digital input modules. These digital inputs receive hardwired system level manual actuation signals from the Main Control Room (MCR) and from the Remote Shutdown Room (RSR). These digital input modules also receive the MCR/Remote Shutdown Room (RSR) transfer switch signals that allow control to be transferred to the remote shutdown room in the event of main control room evacuation. The manual reactor trip does not use the digital input modules; rather it is connected directly to the trip interface matrix, as is discussed in Section 2.3. Multiple digital input channels are used for each actuation function so that a single failure will neither prevent actuation of the division function at the system level nor cause spurious actuation of that function. As described in Reference 4, the system level manual actuation controls are either 1 out of 2 (1/2) (either

one of two controls are required for operation) or 2 out of 2 (2/2) (both of two controls on separate consoles are required). The later case is used for "onerous" actuations[1] that would have significant consequences if used inappropriately. To support this functional fault tolerance, all redundant controls of the same actuation are input to different DI modules in the LCL.

2.3 REACTOR TRIP INTERFACE

The interface between the LCL process stations and the reactor trip switchgear is shown in Figure 2-3. One division is shown, but all four are identical. The interface consists of two relay matrices, one for the undervoltage trip actuation (relays UIR1 through UIR4) and one for the shunt trip attachment actuations (SIR1 through SIR4). The circuits are divided between the two cabinets housing the BPL and LCL process stations and are designed such that either of the cabinets may be de-energized for maintenance without defeating the functionality of the trip interface or causing the trip breakers of the division to be opened.

Power (48VDC) for the interface relay coils is provided by both cabinets and is auctioneered so that single failure of one supply will not trip the breakers of the division. This power is also used to supply the holding voltage to the Undervoltage Trip Attachments (UVTA) of the breakers. Power for the shunt trip attachments is supplied from the trip breakers (the same power as the closing circuit is used) and is switched by the relay matrix.

The undervoltage relay matrix operates on the 'de-energize to trip' principle. Dropping out one relay in each cabinet will de-energize the 48VDC sent to the UVTA coils of the two trip breakers in the division. The undervoltage coils are wired in parallel. The Undervoltage Interface Relay (UIR) coils are driven by DO output relay contacts wired in series through the WDT contact of the processor module that drives the particular relay output. The UVTA circuit is wired through the manual trip switches located on the MCR desk. Operating either manual trip switch will disrupt the UVTA current in all four divisions.

The shunt trip relay matrix operates on the 'energize to trip' principle. Picking up one relay in each cabinet will energize the Shunt Trip Attachment (STA) in both trip breakers. Auxiliary contacts (52a) in each breaker open the STA circuit when the breaker is open to relieve the interface relays from having to switch off these inductive loads, thus extending the life of the Shunt Trip Interface Relay (SIR) contacts. The SIR coils are also driven by DO contact outputs, but working in the opposite logic sense from those of the UIR relays. The processor module WDT is wired in parallel with the DO output contacts so that the SIR relays will be energized upon time-out of the WDT.

An Auxiliary Interposing Relay (XIR) is wired with a normally closed (shelf state) contact that spans across the shunt trip relay matrix. The coil of this relay is connected in parallel with the UVTA and thus is energized under normal operation. This relay serves two purposes. First, it transfers the action of the manual trip switches to the shunt trip attachments so that upon manual trip actuation, both the UVTA and the STA of each breaker is activated. Second, it provides for independent testing of the STA function

[1] Onerous actuation is defined as that which causes a breach of the RCS pressure boundary or a need to shut down the plant to cold conditions to effect repairs.

through a normally closed test pushbutton in its coil circuit. This button is located on the switch panel within one of the cabinets. A separate test pushbutton will switch off the UVTA outputs, but not the XIR. Thus the diverse breaker actuations can be independently tested.

Current sensing resistors are provided in each leg of the undervoltage relay matrix and across each leg of the shunt trip relay matrix. The voltages across these resistors are monitored by the Interface and Test Processor (ITP) process station as part of its routine system diagnostics. With these voltage samples it is possible to observe the action of each LCL trip processor module and contact output independently under the condition that the other processors are in their normal states.

The eight reactor trip breakers (two in each division) are arranged, as shown in Figure 7.1-7 of the AP1000 Design Control Document (Reference 2), to interrupt three phase power to the rod control cabinets. Opening the breakers from any two of the four divisions de-energizes the control rod drives thus allowing the rods to drop into the reactor core by gravity.

2.4 ILC PROCESS STATION

The ILC process stations, located in the Interposing Logic Cabinets (ILC) implement the actuation of safety system equipment in response to the ESF system level commands generated in the LCL process stations. The system level signals are broken down to the individual actuation signals to actuate each component associated with a system-level engineered safety feature. For example, a single safeguards actuation signal must trip the reactor and the reactor coolant pumps, align core makeup tank valves and initiate containment isolation. The interposing logic accomplishes this function (with the exception of reactor trip). The power interface transforms the low level signals to voltages and currents needed to operate the actuation devices. The actuation devices, in turn, control motive power to the final engineered safety feature component.

The ILC cabinet contains redundant process stations, each receiving HSL connections from the two LCL process stations that generate the system-level automatic commands. The two ILC process stations output the component actuation commands through separate DO channels which are combined on a Component Interface Module (CIM) for Air Operated Valve (AOV), Hydraulic Operated Valve (HOV), Motor Operated Valve (MOV), switchgear, and squib operated valves. The details of the CIM design are contained in References 17 and 18. The two ILC process stations use the hardwired port X inputs to the CIM. Configuration of the CIM determines whether the actuation logic is a logical OR of the two process stations, or a logical AND, depending on the need to prevent spurious actuations on single failures. Failure modes of the CIM are discussed in detail in Reference 13. The interface to the squib operated valves will also use CIMs. Two CIMs in separate cabinets are used, one to charge the igniter circuit and the other to fire the squib. This separation is done to prevent spurious actuations, even in the event of hot shorts due to fire.

System level manual actuations are hardwired (to the LCL process station) from switches in the main control room and in the remote shutdown room. These actuations are there combined with the automatic actuations and are "fanned out" to the various components that are designated to act as a system. Thus the path to the ILC for both automatic and manual system level actuations uses the HSL connections from the LCL process stations.

Component level manual control is accomplished in two ways, depending on the consequences of spurious actuation. Components with onerous consequences are controlled via the QDPS/Safety Display. Other components are controlled via the PLS.

Component level manual commands for components with onerous consequences originate in the QDPS/Safety Displays as soft controls. They are sent from the divisional QDPS/Safety Display to the ILC process stations via the AF100 bus. The ILC combines the manual component commands with automatic demands from the LCLs and passes the result to the CIM modules via hardwired digital interface. The component level logic performed by the CIM provides command latching and command termination at end of travel.

Component level manual commands for safety components that do not have onerous consequences originate in the non-safety PLS system as soft control actions on the graphic displays. They are then sent via PLS remote I/O branches to the CIM modules located in the ILC cabinets. The CIM modules give priority to safety actuations of the plant equipment, but in the absence of safety actuations allow the normal manual operation of the equipment to be done. The component level logic performed by the CIM downstream of the priority logic provides command latching and command termination at end of travel. For motor operated valves, the motion is stopped on thermal overload conditions if the command origin was the non-safety system, however, if the actuation came from the safety system, this condition causes an alarm to be actuated and motion continues.

2.5 NIS SUBSYSTEM

The NIS Subsystem processes the signals from the excore neutron flux measurement detectors to permit monitoring of reactor power based on the level of neutron flux around the core. Full range of reactor power is provided by the NIS Subsystem using three overlapping ranges. The three ranges are: Source Range (SR), Intermediate Range (IR) and Power Range (PR). The Source Range (SR) covers the lowest levels of reactor power, including refueling operations, where neutron flux is low enough to allow neutron events to be counted. The output of the Source Range is a logarithmic signal that covers the lowest measurable six decades of power. The PR provides a linear indication of reactor power in the range that the reactor is designed to operate. The PR measures power levels up to 120 percent of full power, and down to less than 1 percent of full power. The IR provides a reactor power indication that covers almost the entire range of reactor power. This range covers ten decades of reactor power, and thus fully overlaps the PR and most of the SR. It may alternatively be designated as Wide Range (WR) as is the case in Figure 2-2. For all ranges, the detectors are fixed in place in detector wells, without the need to move them in to or out of measuring position based on reactor mode.

The NIS Subsystem consists of one cabinet per division each containing three Nuclear Instrumentation Modules (NIMOD), one for each range (source, intermediate/wide and power). These modules are the special electronics needed to convert neutron flux instrumentation signals into the standard input levels of digital protection systems. They include the high voltage power supplies necessary for neutron detectors. The NIS cabinet also contains two Common Q process stations. Each NIS process station is connected to both of the BPL process stations discussed in Section 2.1. The NIS process stations perform the special signal processing required for neutron flux instrumentation channels.

The SR system has four fixed SR detectors (1 per division) that are used for normal subcritical operation and for monitoring during refueling. The SR detector is connected to a pre-amplifier which boosts the detector's small electrical pulses and transmits them to a front-end SR NIMODs. Within the SR NIMOD, the amplitudes of the pulses are compared to the discriminator setting. The result is used to ensure that only pulses from neutrons are counted. The standard SR NIMOD has provisions to allow injection of a test signal for channel testing and provide an audible indication of the count rate to the control room via fiber optic cable. A signal is provided from the LCL process stations to the SR NIMOD to turn off the detector's high voltage supply to protect the detectors when the source range limit has been exceeded. The NIS process stations receive the NIMOD's output signals as a train of pulses whose frequency is determined in order to perform the high flux and doubling rate protection functions. These signals are converted to representative count rate values that are sent to the BPL process stations via HSLs where they are used for protection functions during shutdown and plant startup modes of operation.

The PR system has eight PR detectors (2 per division). The two detectors in each division are arranged vertically, upper and lower flux signals, to allow information on reactor power distribution to be calculated as well as the total reactor power. Preamplifiers are not used in the PR. The PR detectors are connected directly to the PR NIMOD. Detector current is converted to a voltage by the NIMOD and this signal is transmitted to the NIS process stations. The NIS process stations process these signals and perform the required calculations including scaling the neutron flux signals to represent reactor power, and send the results to the BPL process stations via HSLs.

The IR system has four detectors (1 per division). As in the SR channel, a preamplifier is used to boost the low level detector signal to a more easily transmitted signal. The IR preamplifier is located in the same area as the SR preamplifier. Two forms of the detector output are used. At low power levels, individual neutron events are counted as in the SR. At higher powers, the pulses overlap enough that a white noise signal is formed. This signal is filtered to produce a Mean Square Voltage (MSV) or Cambelling signal. The MSV signal is proportional to reactor power. To process these two modes, the preamplifier outputs three signals (CPS, MSV1 and MSV2, the latter being a gain of 10 higher than the other MSV signal) to the IR NIMOD. The CPS signal consists of pulses that are "shaped" by the NIMOD and then passed on to the NIS process stations where they are counted. A scaling divider is provided in the pulse stream path. The other two signals are root-mean-square (RMS) measurements of the white noise amplitude. The second signal is different from the first by a gain of 10. The processor selects between these two signals, based on range, and then squares the result to arrive at a signal proportional to reactor power. The NIS process station uses the inputs from the NIMOD to calculate power levels and rate of change signals, which are sent to the BPL via HSLs.

Digital outputs from the NIS process stations are used to control the NIS amplifiers. These functions include turning off the SR high voltage power supply when the function is blocked to prevent burnout of the detectors by high flux, and enabling calibration. The digital outputs from the two NIS process stations are logically ANDed so that both must act to turn on the SR power supply or to select the divide by 16 on IR pulse channel.

2.6 ICP PROCESS STATION

Each division of the PMS has an Interface Communication Processor (ICP) located in the same cabinet as the Maintenance and Test Panel (MTP) and the Interface and Test Processor (ITP). The ICP gathers

signals that will be used in the non-safety control systems and sends them through digital-to-analog converters and qualified isolators to the control cabinets. Signals are segmented into five groups with each group having its own analog output module so that if a failure occurs, only one group is affected. These segmentation groups correspond to the major control functions (e.g., reactor power control, steam generator level control, etc.) which are also segmented within the non-safety control system. A given signal may be present in multiple groups. Sensor signals that are 4-20 mA current loops are sent to the non-safety control system directly, through isolation devices, and do not pass through the ICP. ICP signals are those that are compensated or otherwise are calculated within the PMS.

In addition to the primary function of the ICP described above, each ICP is cross connected to its counterparts in the other divisions to allow signals to be shared for the purpose of display on the QDPS/Safety Displays (see Section 2.9). This permits all redundant measurements to be displayed side by side on each division's display where they can be compared by the operator.

Two processor modules are present in the ICP to receive the three HSLs from other divisions; however, no functional redundancy is performed between the two processors. The ICP process station contains a CI communications module to communicate with the other process stations in the division via the divisional AF100 network.

2.7 ITP PROCESS STATION

The ITP process station monitors the status of the division's cabinets and performs diagnostics that require information beyond that available in the individual processors and summarize the diagnostic performed by the individual processors to activate a system trouble alarm when some problem is detected. The ITP process stations in the four divisions are interconnected via fiber optically isolated HSL connections so that comparisons of sensor values can be made.

Two processor modules are present in the ITP to receive the three HSL connections from other divisions; however, no functional redundancy is performed between the two processors. The ITP process station contains a CI communications module to communicate with the other process stations in the division via the divisional AF100 network.

Key-lock switches, located in the cabinet housing the ITP station, are scanned by digital input modules in the ITP process station. These switches enable test and maintenance functions to be performed, and are provided as a further level of access control (beyond the cabinet door locks) to support administrative control of these functions.

2.8 MTP PROCESS STATION

The MTP process station is located in the same cabinet as the ITP and ICP process stations. It provides local display of the division status, and provides the means to conduct surveillance testing of the division (typically done during plant shutdown) as well as software maintenance of the various processors within the division. It is through the MTP that the software is loaded into the division processors under control of a software load enable key lock switch.

The MTP consists of a PC node box and a flat panel display with associated keyboard. Both are qualified for application to the monitoring and maintenance functions of the PMS. The PC node box also contains an Ethernet interface module through which it connects to a gateway on the Real Time Data Network (RTDN). Through this gateway, the MTP provides information on system status and process measurements for display and historical recording to the DDS. The network media between the MTP PC node box and the gateway workstation is a unidirectional fiber optic cable to provide the required electrical isolation.

2.9 QDPS/SAFETY DISPLAY SUBSYSTEM

Each of the four PMS divisions contains a QDPS/Safety Display located on the DSP in the MCR. Each QDPS/Safety Display consists of a PC node box and a flat panel display unit with a navigation device. The PC node box is on the AF100 network of the division it is in. All divisional process stations provide status information for display via the AF100 network.

Manual actuations of permissives, blocks, resets and system level resets originate at the QDPS/Safety Display as soft controls. They are sent from the QDPS/Safety Display PC node box via the AF100 network to the BPL and LCL process stations in the division. In the receiving process station, the actuation commands are applied to the functional logic controlling the equipment as appropriate for the given manual command.

In addition to providing status and actuation of the PMS divisions, the QDPS/Safety Display panel provides the QDPS display information. Each QDPS/Safety Display indicates process variables required for monitoring and controlling the post event plant state. The process variables are defined by Regulatory Guide 1.97.

The operator makes display selections using the navigational device.

2.10 QDPS PROCESS STATION

The QDPS process stations reads process measurements that are required for post-accident monitoring but are otherwise not needed by the PMS for safety actuations. In addition, most signals that are needed for both QDPS and safety actuations and that are required to be available up to 72 hours following the event, are input to the QDPS process station. These latter signals are sent via shared current loop to the BCC cabinet as well. This arrangement allows non-essential cabinets to be powered from the 24 hour batteries in the event of a total blackout.

There are two QDPS process stations, one in each of divisions B and C. Processed measurements are sent to all four QDPS/Safety Displays by way of the ICP process station, inter-divisional HSL connections and the divisional AF100 networks (see Section 2.6). The division B and C QDPS process stations are also cross-connected via the HSL connections (division B sends data to division C and vice versa). The purpose of this cross-connection is to allow process variable signals to be validated by comparison of redundant measurements. Also, when relying on equipment powered from the 72 hour battery bus, the cross connection enables division B and C QDPS signals to be viewed on either QDPS/Safety Display in the event of failure of one of the QDPS/Safety Displays.

2.11 POWER DISTRIBUTION

The Class 1E 125 VDC and Uninterrupted Power Supply (UPS) system provide reliable power for the PMS cabinets required for the plant instrumentation, control, monitoring and other vital functions needed for shutdown of the plant. In case of a total loss of off-site and on-site AC power sources, the DC batteries provide electrical power for operation of the required DC and AC instrument loads.

The Class 1E 125 VDC and Uninterruptible Power Supply (UPS) systems are designed with four independent, Class 1E 125 VDC divisions (A, B, C, and D). Each division has one 24-hour battery bank. In addition, divisions B and C each have one 72-hour battery bank. Each battery bank has its own battery charger. Each of the four divisions is electrically isolated and physically separated to prevent a single event from causing the loss of more than one division.

The normal source of power for the Class 1E DC system is the non-Class 1E AC power system. Battery chargers serve as isolation devices for the connection between the Class 1E system and the non-Class 1E system. If the normal source of AC power is not available, the Class 1E batteries have sufficient capacity for the critical plant loads required for plant safe shutdown for a period of up to 72 hours.

The Class 1E DC and UPS system includes a single spare battery bank with spare battery charger. The spare battery bank and battery charger can replace any one of the 24-hour or 72-hour battery banks and associated battery chargers while maintaining electrical isolation and physical separation. In the case of a failure, maintenance or unavailability of the normal battery bank and the battery charger, the spare can be connected to the affected bus using permanently installed cable connections. The configuration of the spare battery connections permits connection of only one battery bank and battery charger at a time. Apart from normal maintenance and testing, the spare battery charger remains continuously energized to keep the spare battery fully charged and ready for replacing any battery on demand. The time required to connect the spare battery to a Class 1E division is much less than the time allowed for the Limiting Condition for Operation (LCO) associated with the loss of one Class 1E division.

Regulating transformers provide backup sources of power for the UPS system. If an inverter is inoperable or the Class 1E 125 VDC input to the inverter is unavailable, the load is transferred automatically to the backup AC source by a static transfer switch featuring a make-before-break contact arrangement. The diesel generator backed non-Class 1E power supply provides the backup power through the Class 1E regulating transformer.

A manual maintenance bypass switch with overlapping contacts provided at the inverter facilitates connection of the backup power source when the inverter is removed from service for maintenance. The automatic or manual transfer from one power source to another does not affect the ability of the PMS to perform its safety functions.

Each PMS cabinet has one power feed, distributed from the UPS output through a main circuit breaker. The power feed is input to a power supply containing redundant power supply modules. The power supply modules produce the 24 VDC and 48 VDC required by the various PMS modules. Auctioneering of the redundant voltages is performed internally. Other voltages (e.g., 5 VDC, +/- 12 VDC, etc.) are produced locally as needed. Each cabinet power converter is sized to provide the full cabinet load with

ample margin. The converters contain hold-up capacitors that allow a temporary interruption of the input power (40 ms), without degradation of the converter output.

2.12 DEFAULT ACTIONS

As part of the application level diagnostics that are designed into the PMS, a number of default actions are defined that have the intention of ensuring that failures lead to predefined safe states.

a. A sensor may fail such that its signal goes off-scale high or low. The signal quality for that sensor is set to BAD. Bistables for reactor trip functions are put into the tripped state, those for ESF functions are put into the non-tripped state. Majority voting of the function prevents spurious actuation (for 2/3 and 2/4 functions) and preserves capability to actuate if needed. Thus this is a safe state.

b. A sensor may fail in a way that it remains on-scale. The trip of this channel would either be early or late depending on the direction of the failure with relation to the high or low action of a bistable. Majority voting of the function prevents spurious actuation (for 2/3 and 2/4 functions) and preserves capability to actuate if needed. Thus this is a safe state. The failure is detected by the cross channel sensor checks performed by the ITP processor. An alarm to the operator is actuated when a sensor deviation is detected but no other action is taken.

c. Analog to digital converters in the BPL process stations may fail in a way that affects only a single channel, in which case the failure effects are similar to a sensor failure and either a) or b) will apply, or in a way that affect multiple channels although of different functions. In the latter case, self diagnostics performed by the converter signal the failure to the BPL processor which then sets the quality to BAD for all affected channels with the system response being as in a). A key difference between analog to digital converter failure and sensor failure is that in the case of converter failure, the signal is affected in only one of the redundant BPL processors. The other remains fully capable of performing the safety functions. Failures of a NIS process station, or the HSL connection connecting to its associated BPL process station, are treated the same as total failures of analog input modules.

d. If the BPL processor or any of its support modules fail, the processing will stop and no messages will be sent out via the HSL connections to the LCL process stations in all divisions. This is handled as in e).

e. If a HSL connection between the BPL and LCL process stations fails, either as a complete loss of communication or rejection of corrupted data as detected by Cyclic Redundancy Check (CRC), the LCL processor will set the signals carried in that connection to BAD quality. For majority voting functions, inputs with BAD quality are rejected such that the good signal from the affected division becomes the one that is effective (if both are good, they are logically ORed). If both signals from a given division for a particular actuation function are BAD, then that vote to the majority is set to TRUE for reactor trip functions and to FALSE for ESF actuation functions. Majority voting of the function prevents spurious actuation (for 2/3 and 2/4 functions) and preserves capability to actuate if needed. Thus this is a safe state.

f. If a LCL processor performing the reactor trip actuation function or any of its support modules fails, the processing will stop. The watchdog timer on its output will cause the relays in the trip voting matrix associated with that processor for both under-voltage and shunt trip to actuate. Coincidence logic of the trip interface matrix prevents the trip breakers of the division from being opened as a result of the failure, even if both reactor trip LCL processors are affected by the failure. Because of the action of the watchdog timer on the relays, the LCL processors in the other Bistable/Coincidence Logic Cabinet (BCC) of the affected division are able to open the trip breakers if needed. Furthermore, the reactor trip function can be accomplished by the other three RPS divisions even if the affected division's breakers are not opened. Thus this is a safe state.

g. If a LCL processor performing the ESF actuation function or any of its support modules fails, the processing will stop. Its output HSL connection to the ILC cabinets will stop communications. Within each ILC, the signals received via the affected connection are set to BAD quality and the component level actuation logic uses the signals with good quality received via the connection from the other BCC cabinet in the division. There is no loss of function, thus this is a safe state.

h. Failure of a HSL connection between the LCL process station and an ILC cabinet will have the same result as in g) however only one ILC cabinet will experience the described effect.

i. Failure of an ILC processor, or any of its supporting modules, will cause its processing to stop. Components that are handled by that processor will remain in their "as is" state. Redundancy of the ESF functions in other fluid system trains is sufficient to ensure that any needed safety function can be completed. Also, even with failure of the ILC processor those components without onerous consequences that have soft controls through the PLS can be manipulated via those manual controls. All components can be manipulated through the CIM local controls; however this requires access to the ILC cabinet. Therefore, this is a safe state.

j. Failure of a digital output module in the ILC process station could be such that it affects a single channel or multiple (all) channels. In the case of a single channel failure, it could prevent actuation of one ESF component (if the two ILC processors are logically ANDed) in which case the plant safety is assured through the redundant divisions of ESF equipment. Failure of a single channel could cause the spurious actuation of one ESF component (if the two ILC processors are logically ORed). This is the same as a CIM failure discussed in k). Failure of all channels could prevent changing any outputs, in which case by definition the controlled equipment fails "as is." Again plant safety is assured by the redundant divisions of ESF equipment. If the failure of all channels is in the I/O bus communication with the processor, then the digital output module will detect the failure and turn off all outputs, with the same effect as before. Therefore failures of this module lead to predefined safe states.

k. The majority of failures of a CIM will cause the equipment it controls to remain in previous state (fail "as is"). A small percentage of CIM failures could result in the equipment being spuriously actuated into the opposite state. The result (valve motion, etc.) could lead to an impact on the plant process, which would subsequently require further safety system action to mitigate. In such a case, the failure will only affect a single component, thus all remaining safety functions are available, even if they are affected by one of the single failures discussed in a) through i). Thus this is a safe state. Note that for squib valve interfaces, two CIM modules are involved such that

no single failure, including hot shorts that may result from a fire, will result in spurious actuation of the valve.

a.c

Figure 2-1 PMS One Line Architecture

a,c

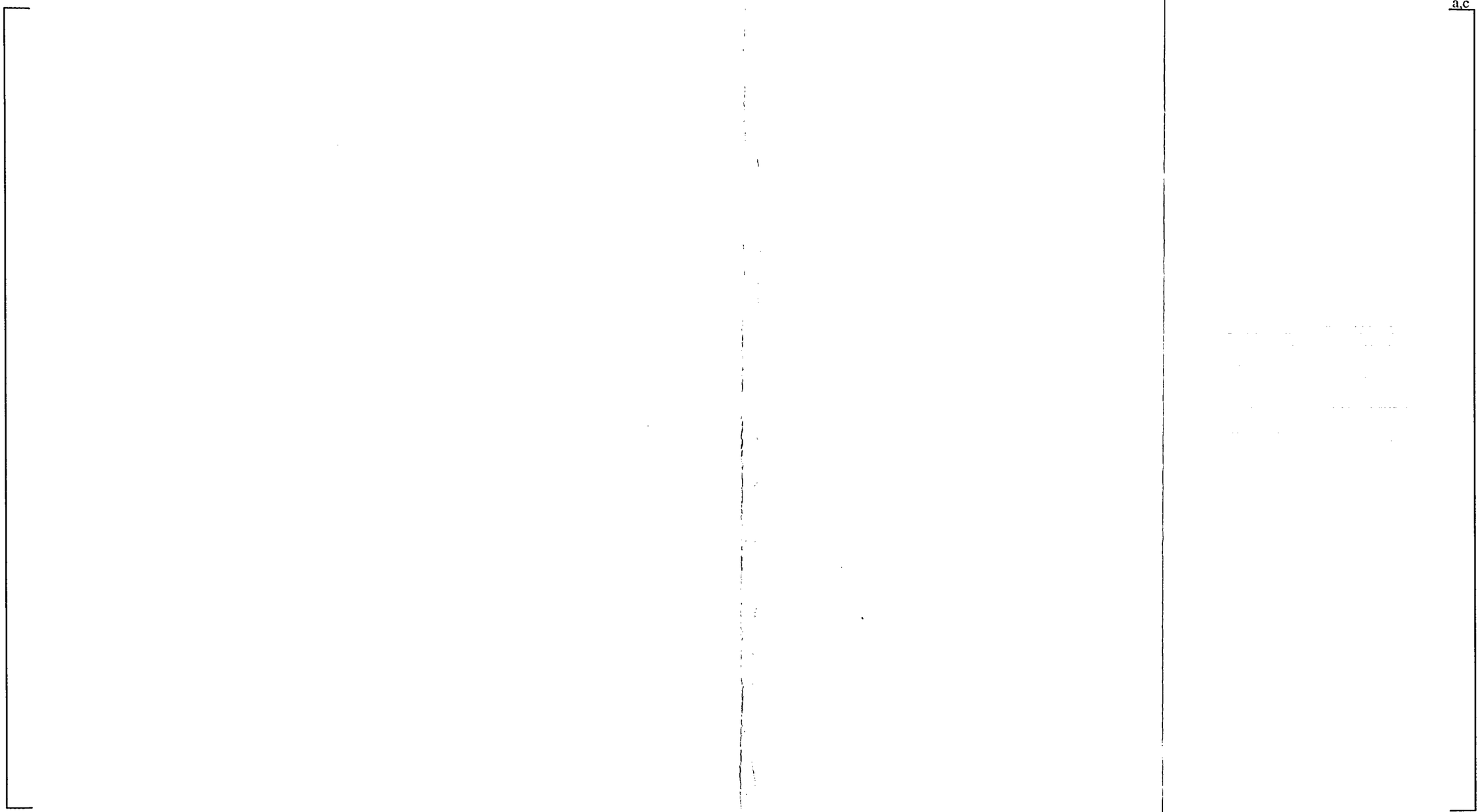

Figure 2-2 Typical PMS Division Configuration (Division B Shown)

a,c

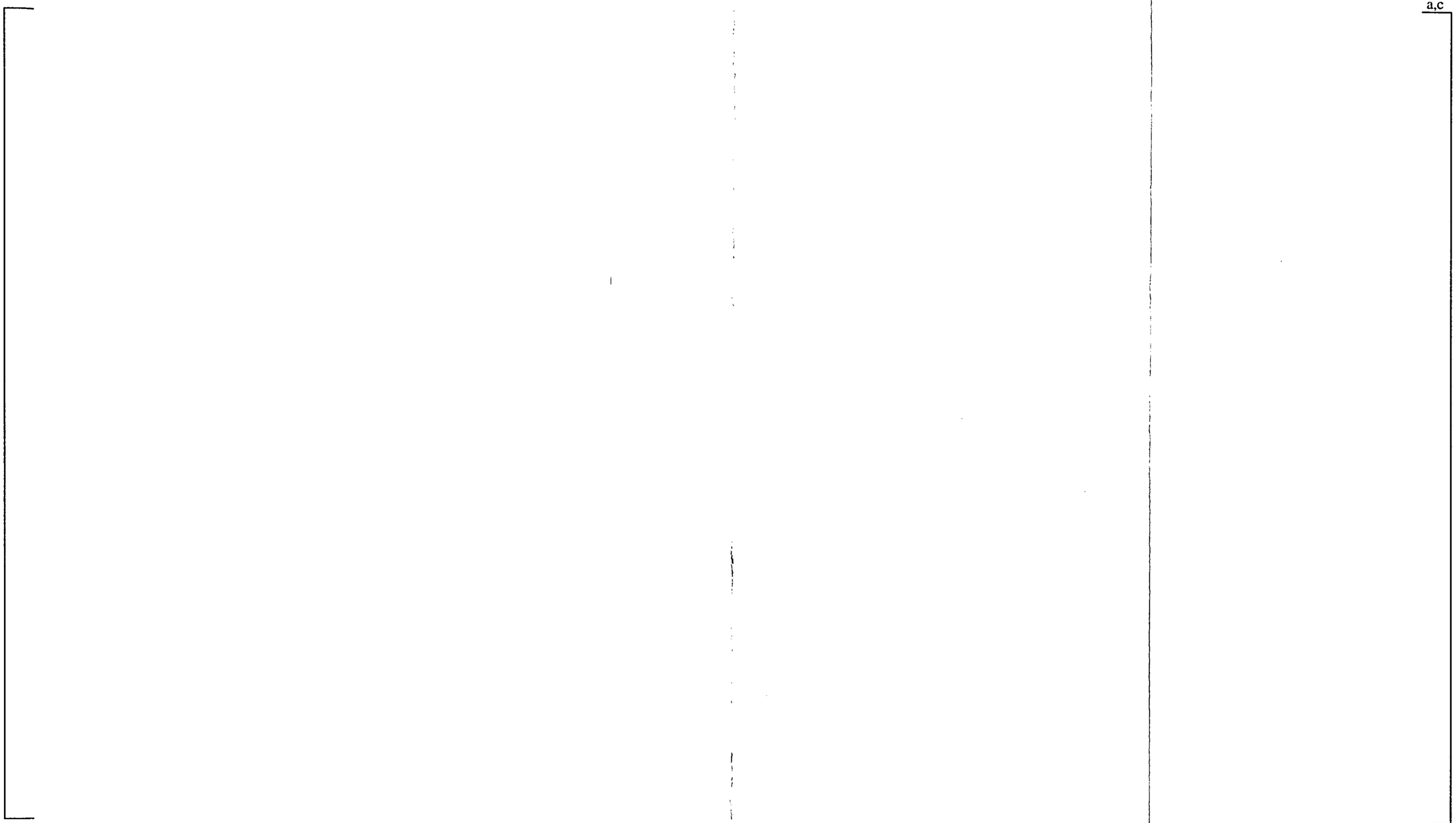

Figure 2-3 Reactor Trip Interface Relay Matrix

(This page intentional left blank)

3 FMEA METHODOLOGY

Each segment of the PMS described in Section 2 is analyzed in a separate FMEA table. The indenture level (i.e., level of abstraction) of the analysis is to the replaceable module. In certain cases, individual components (diodes, resisters, etc.) are discussed to the extent that they have a direct contribution to the accomplishment of the function of the segment. Identification of the component is consistent with the labeling of Figures 2-2 and 2-3.

Failure modes of the components are presented to the extent of their effect on the function of the component being analyzed. Thus, for instance, a computer module will be analyzed for failures such as inability to execute the store program, incorrect access of data, etc. rather than short or open circuits of its constituent elements. A finer level of detail is done for components directly involved in safety function actuation than is done for those performing monitoring and diagnostic functions.

The FMEA table prepared for each segment of the PMS contains the following columns:

Component	Identification of the module being analyzed using terminology consistent with Figures 2-2 and 2-3.
Failure Mode	Definition of the failure of the component in the terms of the specific function that is not performed and, where appropriate, a discrimination of the possible variations (e.g., fail high or fail low).
Symptoms and Local Effects Including Dependent Failures	The consequent effect(s) of the failure on the component or on its adjunct components. For instance, failure to execute a computer program will cause the computer to stop resetting the watchdog timer causing it to time out.
Effect on Protective Function	The effect of the failure on the ability to complete the protective function, including identification of any degradation in performance or degree of redundancy. Mitigating design features that prevent or limit this effect are discussed.
Method of Detection	Identification of the means by which the failure will come to the attention of the plant operation/maintenance staff.
Fault Classification	A code that ranks the criticality and detectability of the failure per the definitions given below.

Each row of the FMEA table is assigned a classification to facilitate identification of significant failures with regard to their criticality to the ability of the system to accomplish its required safety functions and to the effectiveness of diagnostics and/or surveillance tests to reveal the failures. The first part of this classification will be a Roman numeral indicating criticality as defined in Table 4-1.

Table 4-1 Failure Criticality Classes

Class	Meaning
I	Loss of capability to perform the safety function or spurious actuation of the safety function is a direct result of this failure.
II	The safety function can still be accomplished but at a degraded performance (accuracy, time response, etc.)
III	Redundancy is reduced to the point that a further single failure will prevent actuation of the safety function or cause spurious actuation.
IV	The failure requires restorative maintenance but does not otherwise prevent the functioning of the system.

The second part of the classification identifies the detectability of the failure according to the definitions provided in Table 4-2.

Table 4-2 Failure Detectability Classes

Class	Meaning
A	The failure is self revealing through the consequent action of plant equipment (valve motion, breaker tripping, etc.)
B	The failure is detected by diagnostic features of the system that actuate an alarm as a consequence.
C	The failure will be revealed by planned surveillance testing performed at the specified test interval.
D	The failure is not revealed unless uncovered by an additional failure(s) or by intentional investigation beyond the scope of normal surveillance testing.

4 FMEA TABLES

The following conditions are included in the basis of the FMEA analysis:

- The system is in full operation with all divisions in service as the initial condition prior to the postulated failure. Where planned operating modes would alter the character of the effect of the failure on the plant, these are identified and discussed.

- The system is running on normal power. Specifically, the full system is available as opposed to the subset available on the 72-hour batteries.

- For the purpose of the analysis, HSL connections are considered to be part of the transmitter, including the fiber optic modems (both transmit and receive) and the media (copper or fiber optic) making the physical connection.

- Failure of the AC160 backplane is not included in the analysis since it is a passive device with only a few pull up resistors. If failures (shorts or open circuits) were to occur, the effects would be the same as those of active module failures that are included in the analysis.

- The minimum inventory manual controls connected directly to the LCL process stations use dual, two-pole energize-to-actuate ungrounded dc circuits to allow switch and cabling failures to be tolerated (i.e. not result in spurious actuations). The single failure criterion for actuation (i.e. that a failure shall not prevent actuation) is provided through alternate switches.

The tables on the following pages contain the FMEA details for each of the major segments of the PMS that are described in Section 2.

4.1 BPL PROCESS STATION

a,c

a,c

a,c

a,c

a,c

a,c

a,c

4.2 LCL PROCESS STATION

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

4.3 REACTOR TRIP INTERFACE

a,c

a,c

a,c

a,c

a,c

a,c

4.4 ILC PROCESS STATION

NOTE: The analysis is performed at an abstract level discussing each segment as if it were a single cabinet. No specific equipment actuation effects are identified.

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

4.5 NIS SUBSYSTEM

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

4.6 ICP PROCESS STATION

a,c

a,c

a,c

a,c

4.7 ITP PROCESS STATION

a,c

a,c

a,c

a,c

a,c

4.8 MTP PROCESS STATION

a,c

a,c

4.9 QDPS/SAFETY DISPLAY SUBSYSTEM

a,c

a,c

4.10 QDPS PROCESS STATION

a,c

a,c

a,c

a,c

4.11 POWER DISTRIBUTION

a,c

a,c

a,c
