ENCLOSURE 4

APP-GW-GLR-065-NP

Revision 1

"AP1000 I&C Data Communication and Manual Control of Safety Systems and Components"

(Non-Proprietary)

Westinghouse Non-Proprietary Class 3

WCAP-16674-NP
APP-GW-GLR-065
Revision 1

May 2009

AP1000 I&C Data Communication and Manual Control of Safety Systems and Components

F-3.4.1-1 Rev 1

DOCUMENT COVER SHEET

TDC: _____ Permanent File: _____

DOCUMENT NO.	REVISION	PAGE	ASSIGNED TO	OPEN ITEMS (Y/N)
APP-GW-GLR-065	1	1 of 50	W-Strong	N

DOCUMENT STATUS: ☐ PRE ☐ CFC ☐ CAE ☒ DES

Westinghouse Acceptance of AP1000 Design Partner Document by:

_____
(Name and Date)

ALTERNATE DOCUMENT NUMBER: WCAP-16674-NP WORK BREAKDOWN #: GW

ORIGINATING ORGANIZATION: Westinghouse Electric Company LLC

TITLE: **AP1000 I&C Data Communication and Manual Control of Safety Systems and Components**

ATTACHMENTS:	DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION:
CALCULATION/ANALYSIS REFERENCE:	APP-GW-GEE-156, R1 APP-GW-GEE-184, R1 APP-GW-GEE-190, R0 APP-GW-GEE-327, R0 APP-GW-GEE-388, R0 APP-GW-GEE-387, R1

ELECTRONIC FILENAME	ELECTRONIC FILE FORMAT	ELECTRONIC FILE DESCRIPTION
APP-GW-GLR-065	PDF	EDMS

LEGAL REVIEW See Form 36	SIGNATURE / DATE **(If processing electronic approval select option)**
PATENT REVIEW See Form 36	SIGNATURE / DATE

ORIGINATOR(S) Albert W. Crew	SIGNATURE / DATE **(If processing electronic approval select option)** **Electronically Approved*** **	
REVIEWER(S) John G. Ewald	SIGNATURE / DATE **Electronically Approved*** **	
	SIGNATURE / DATE	
	SIGNATURE / DATE	
VERIFIER(S) Thomas P. Hayes	SIGNATURE / DATE **Electronically Approved*** **	Verification Method: Independent Review

__Plant Applicability__: ☒ All AP1000 plants except: No exceptions
☐ Only the following plants:

APPLICABILITY REVIEWER** J. A. Speer	SIGNATURE / DATE **Electronically Approved*** **
RESPONSIBLE MANAGER* John S. Strong/Erin M. Smith for	SIGNATURE / DATE **Electronically Approved*** **

* Approval of the responsible manager signifies that the document and all required reviews are complete, the appropriate proprietary class has been assigned, electronic file has been provided to the EDMS, and the document is released for use.

*** ***Electronically approved records are authenticated in the electronic document management system. When a document is approved, this footnote is replaced by a footnote with a date stamp.***

WCAP-16674-NP
APP-GW-GLR-065
Revision 1

AP1000 I&C Data Communication and Manual Control of Safety Systems and Components

Albert W. Crew*, Consulting Engineer
I&C Development
Repair, Replacement and Automation Systems

May 2009

Reviewers: John G. Ewald*, I&C Engineer
Nuclear Power Plants

Thomas P. Hayes*, AP1000 Consultant
Repair, Replacement and Automation Systems

Approved: John S. Strong*, RRAS AP1000 NuStart/DOE Program Manager
Erin M. Smith* for John S. Strong
Repair, Replacement and Automation Systems

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

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

REVISION HISTORY

RECORD OF CHANGES

Revision	Author	Description
A	Albert W. Crew	Preliminary
0	Albert W. Crew	Initial Release
1	Albert W. Crew	Cover Page -- Updated revision number and date. Title Page -- Updated revision number and date. Table of Contents – Update to match itemized changes. Acronyms and Trademarks -- Added a list of Acronyms and Trademarks. References -- Editorial Changes: Moved References from Section 9 to front matter. Replaced the reference to TR-42 with a reference to the proposed amendment to the AP1000™ certified design. Corrected the title of WCAP-16675-P and changed the reference to the latest version. Added References 9. Added IEEE-384-1992 per NRC RAI SRP7.1-19. Added the Common Q SPM per NRC RAI-SRP7.9-05. Added WCAP-16791 for clarity. Figure 2.1 -- DCP APP-GW-GEE-387: NIS function no longer has a dedicated connection to the AF100 network. Editorial Changes: Removed AF100 bus detail. Removed cabinet allocation detail from PMS section. Used function list instead of cabinet names. Added "From PMS" input to NSSS cabinet. Figure 3-1 -- Editorial Change: Added new figure/clarification regarding network topology per NRC RAI-SRP7.9-10. Figure 5-1 -- DCP APP-GW-GEE-387: NIS no longer has a dedicated AF100 connection; DCP APP-GW-GEE-388: Figure revised to show SOE datalink. Editorial Changes: Figure is no longer proprietary since it was released in an ISA paper. Removed AF100 bus detail. Removed cabinet allocation detail. Removed "Located in" tags. Used function names instead of cabinet names. Relocated "Case B" to match text in TR-89. Added an example of Case D applied to signals from non-safety equipment. Figure 5-2 -- Editorial Changes: Changed caption to indicate that the configuration shown is only an example. Labeling changed to clearly show the safety and non-safety portions of the gateway per NRC RAI-SRP7.9-05. Figure 5-3 -- Editorial Changes: Changed the obsolete term "WEStation" to "Non-Safety Portion of the Gateway." DCP APP-GW-GEE-327: Figure further revised to more closely reflect the new CIM design. Figure 6-1 -- Editorial Change: Expanded the scope of the figure to include the DAS connection. The figure now more closely matches the text. This change was previously requested by NuStart.

RECORD OF CHANGES (Cont'd)

Revision	Author	Description
1 (Cont'd)		Figure 6-2-- DCP APP-GW-GEE-327: Picture updated to show the new CIM resulting from the DCP. Figure 6-3 -- DCP APP-GW-GEE-327: Revised figure to reflect the new CIM design. The non-safety communication function is not shared between CIM modules and the priority logic uses "System-based Priority." Section 1 -- Editorial Change: Added clarification that situations where downstream components (valves, breakers, etc.) receive independent demands from both safety and non-safety I&C systems are beyond the scope of this document. Section 2 -- Editorial Changes: Removed detail regarding the safety system cabinet names and the allocation of functions to cabinets. Added clarification regarding the use of the AF100 bus with PMS per NRC RAI-SRP7.9-03. Section 3.1 -- Editorial Changes: Clarified Ovation® network capacity. Added clarification regarding network topology per NRC RAI-SRP7.9-10. Corrected "broadcast" to "multicast." Section 3.1.1 -- Editorial Change: Remove bracketing since this information has been disclosed in NRC RAI-SRP7.9-10. Section 3.1.2 -- Editorial Change: Added clarification regarding network protocols per NRC RAI-SRP7.9-10. Removed discussion of "root guard," as it is extraneous. Section 3.1.3 -- Editorial Changes: Clarified security features of network uplinks. Clarified access control and included a reference to WCAP-16791. Generalized the cyber security related information. For the AP1000 domestic market, the details are in Reference 12. Section 3.1.3.1 -- Editorial Changes: Clarified the definition of "remote." Clarified "On-Site" access description. Section 3.1.3.2 -- Editorial Change: Clarified remote access features. Clarified "Off-Site" access description and included a reference to WCAP-16791. Generalized the cyber security related information. For the AP1000 domestic market, the details are in Reference 12. Section 3.1.4 -- Editorial Change: Added new section/clarification regarding network capacity per NRC RAI-SRP7.9-10. Section 3.1.5 -- Editorial Change: Added new section/clarification regarding Data Storm Control per NRC RAI-SRP7.9-10. Section 3.1.6 -- Editorial Change: Added new section/clarification regarding network performance analysis per NRC RAI-SRP7.9-10. Section 3.2 -- Editorial Change: Added introduction to Section 3.2 Section 3.2.1 -- Editorial Changes: Corrected datalink application server point capacity. Removed "MHI" acronym.

RECORD OF CHANGES (Cont'd)

Revision	Author	Description
1 (Cont'd)		Section 3.2.2 -- Editorial Changes: Clarified that both local and remote I/O cabinets can be used to terminate field cables. In response to NRC RAI-TR88-009 as documented in WCAP-16767, Rev. 0, changed "RS-485" to "Ethernet." This is not a design change; it is correcting the TR to match the design. Section 3.2.3.2 -- Editorial Change: Updated Ovation FOUNDATION™ Fieldbus capabilities. Clarified that the applicability to AP1000 is being evaluated. Section 3.2.3.3 -- Editorial Change: Updated Ovation Profibus-DP® capabilities. Section 3.2.3.4 -- Editorial Change: Updated Ovation DeviceNet™ capabilities. Section 5 -- Editorial Change: Replaced the reference to TR-42 with a reference to the proposed amendment to the AP1000 certified design. Section 5.1.2 -- DCP APP-GW-GEE-388: Revised this section to include unidirectional SOE datalinks. Editorial Changes: Provided further clarification of the SOE interface beyond that shown in the DCP. Added clarification per NRC RAI SRP7.9-05 and NRC RAI-SRP7.9-06. Section 5.2.1 -- Editorial Changes: Provided clarification regarding the functional isolation between the Remote Shutdown Room inputs and the PMS. Added clarification to ITAAC compliance statements indicating that isolation is provided. Added clarification that Case D also applies to test interlock signals from non-safety equipment. Section 5.2.2 -- Editorial Changes: Added clarification that: • This section applies to normal MCR/RSR manual component-level soft controls, • Safety system status is returned to the non-safety system, and • The ITAAC compliance statements were revised to include the return of safety system status information. Added clarification per NRC RAI SRP7.1-19. Added clarification regarding the simple discrete interface within the CIM, per NRC phone conference of 5/1/2009. Section 6 -- Editorial Changes: Added a clarification that the CIM output device and the field circuit are completely tested during the periodic surveillance test. The change was previously requested by NuStart. In response to NRC RAI-TR88-014, as documented in WCAP-16767, Rev. 0, clarified the operator notification of off-normal positioning of the CIM local manual switch. Added clarification that the operation of the continuous on-line diagnostics does not adversely affect the CIMs ability to respond to safety or non-safety demands. DCP APP-GW-GEE-327: Text revised to reflect the new CIM design resulting from the DCP. Although the CIM provides "System-based Priority," as applied in

RECORD OF CHANGES (Cont'd)

Revision	Author	Description
1 (Cont'd)		AP1000, "State-based Priority" is still achieved. Section 6.1 -- DCP APP-GW-GEE-327: Revised text to reflect the new CIM design. Section 6.1.1 -- DCP APP-GW-GEE-327: Revised text to reflect the new CIM design. Section 6.1.2 -- DCP APP-GW-GEE-327: Section deleted. This function is now described in the next section resulting from the DCP. Section 6.1.2 (was Section 6.1.3) -- DCP APP-GW-GEE-327: Text revised to reflect the new CIM design resulting from the DCP. Section 6.1.2.1 (was Section 6.1.3.1) -- DCP APP-GW-GEE-327: Text revised to reflect the new CIM design resulting from the DCP. Section 6.1.2.2 (was Section 6.1.3.2) -- DCP APP-GW-GEE-327: Text revised to reflect the new CIM design resulting from the DCP. Section 6.1.3.1 (was 6.1.4) -- DCP APP-GW-GEE-327: Revised text to reflect the new CIM design. Editorial Change: Corrected section number. Clarified (as in Section 6) operator notification of off-normal positioning of the CIM local manual switch. Section 6.1.3.2 (was 6.1.4.1) -- DCP APP-GW-GEE-327: Revised text to reflect the new CIM design. Editorial Change: Corrected section number. Section 7.1 -- DCP APP-GW-GEE-190: Since this DCP moved the safeguards panel from the reactor operator's console back to the Primary Dedicated Safety Panel, removed the mention of the RO console. Section 7.2 -- Editorial Changes: Replaced the definition of "onerous component" with the criteria for components requiring manual component level control from PMS and a list of such components. Added clarification that the DAS controls in the auxiliary building operate groups of valves. Added clarification per NRC RAI-SRP7.9-ICE-08, but generalized the cyber security related information. For the AP1000 domestic market, the details are in Reference 12. Note: The DCP tracking database indicated that DCP APP-GW-GEE-184 and DCP APP-GW-GEE-156 could potentially impact this document. Those DCPs were reviewed and no actual impacts were found.

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

LIST OF TABLES

None.

LIST OF FIGURES

ACRONYMS AND TRADEMARKS

Acronyms	Definition
AC160	Advant Controller 160
AF100	Advant FieldBus 100
AOI	Advant to Ovation Interface
CDP	Cyclic Data Packet
CIM	Component Interface Module
CMF	Common Mode Failure
COL	Combined Operating License
Common Q	Common Qualified
DAS	Diverse Actuation System
DC	Direct Current
DCP	Design Change Proposal
DDS	Data Display and Processing System
EOF	Emergency Operations Facility
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Actuation System
FPGA	Field Programmable Gate Array
HART®	Highway Addressable Remote Transducer
HSI	Human-System Interface
I&C	Instrumentation and Control
IIS	In-core Instrumentation System
ILP	Integrated Logic Processor
I/O	Input/Output
ISA	Instrumentation, Systems and Automation Society
ITAAC	Inspections, Tests, Analyses and Acceptance Criteria
LCL	Local Coincidence Logic
LCS	Local Control Station
MCR	Main Control Room
NAP	Nuclear Application Program
NIS	Nuclear Instrumentation System
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OCS	Operation and Control Centers
OLEDB	Object Linking and Embedding Database
OSC	Operations Support Center
OSI	OSIsoft, Inc.
PCB	Printed Circuit Board
PI	A product of OSIsoft, Inc.
PLC	Programmable Logic Controllers
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
QDPS	Qualified Data Processing System
RCS	Reactor Coolant System

ACRONYMS AND TRADEMARKS (Cont'd)

Acronyms	Definition
RLC	R-line Link Controller
RNC	Remote Node Controller
RNS	Residual Normal Heat Removal System
RSR	Remote Shutdown Room
RTP	RTP Corporation
RTS	Reactor Trip System
SER	Safety Evaluation Report
SOE	Sequence of Events
SMS	Special Monitoring System
TC	Thermocouple
TCP/IP	Transmission Control Protocol/Internet Protocol
TOS	Main Turbine Control and Diagnostics System
TSC	Technical Support Center
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network

REFERENCES

1. WCAP-16097-P-A, Rev. 0 (Proprietary), "Common Qualified Platform Topical Report," Westinghouse Electric Company LLC. (This document is also referred to as CENPD-396-P-A, Revision 02.)

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

3. NRC Document 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, Revision 1 (TAC No. MB0780)," June 22, 2001.

4. NRC Document 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.

5. APP-GW-GL-700, Rev. 15, "AP1000 Design Control Document," Westinghouse Electric Company LLC.

6. APP-GW-GL-700, Rev. 17, "AP1000 Design Control Document," Westinghouse Electric Company LLC.

7. WCAP-16675-P, Rev. 1 (Proprietary), "AP1000 Protection and Safety Monitoring System Architecture Technical Report," Westinghouse Electric Company LLC.

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

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

10. WCAP-16096-NP-A, Rev. 1A, "Software Program Manual for Common Q Systems," Westinghouse Electric Company LLC.

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

12. WCAP-16791-P, Rev. 1, "AP1000 Cyber Security Implementation," Westinghouse Electric Company LLC.

1 INTRODUCTION

This document provides technical information regarding:

1. Data communication between the functional systems that comprise the AP1000™ Instrumentation and Control (I&C) system and between the AP1000 I&C system and external systems. (Situations in which downstream components {valves, breakers, etc.} receive independent demands from both safety and non-safety I&C systems are beyond the scope of this document.)

2. The Component Interface Module (CIM) that is used to interface the I&C system to safety system components.

3. The manual control of the safety system at the system level and the component level.

Submittal of this information allows for early Nuclear Regulatory Commission (NRC) review of the communication design and compliance with applicable regulatory guidance and criteria prior to completion of the detailed design. This document will be used to address Protection and Safety Monitoring System (PMS) Design Inspections, Tests, Analyses and Acceptance Criteria (ITAAC) and Combined Operating License (COL) item closure.

2 AP1000 I&C ARCHITECTURE

A high-level overview of the AP1000 I&C architecture is shown in Figure 2-1. The architecture is divided into the following functional systems:

- Safety System
  - Protection and Safety Monitoring System (PMS) – the safety grade protection and safety monitoring system detects off-nominal conditions and actuates appropriate safety functions necessary to achieve and maintain safe shutdown. The PMS is implemented using the Westinghouse Common Qualified (Common Q) Platform described in WCAP-16097-P-A, "Common Qualified Platform Topical Report" (Reference 1), and accepted by the United States Nuclear Regulatory Commission in References 2, 3, and 4.
- Non-Safety Systems[1]
  - Plant Control System (PLS) – the plant control system provides the functions required for normal operation from cold shutdown through full power.
  - Data Display and Processing System (DDS) – the data display and processing system provides data that result in alarms and displays for both normal and emergency plant operations to the equipment used for processing. It includes the displays, the real-time data network, the alarm system, the Nuclear Application Programs (NAPs), the logging function, and the archiving function.
  - Main Turbine Control and Diagnostic System (TOS) – the turbine protection and controls.
  - Special Monitoring System (SMS) – the special monitoring system consists of standalone diagnostic systems that preprocess data from specialized sensors. An example includes the Digital Metal Impact Monitoring System.
- Other Systems
  - Diverse Actuation System (DAS) – the diverse actuation system is a non-safety system that provides an alternate means of initiating reactor trip, actuating selected engineered safety features, and monitoring plant information. This system addresses the unlikely coincidence of a postulated plant transient and a postulated common mode failure (CMF) in the PMS. The DAS is a non-safety system, but has special design process requirements due to its mission.
  - In-core Instrumentation System (IIS) – the primary function of the in-core instrumentation system is to provide data for a three-dimensional flux map of the reactor core. This is a non-safety function. The secondary function is to provide the PMS with thermocouple

[1] The PLS functions and the DDS functions are both implemented on a common integrated platform. In practice, the differentiation between the two functional systems is somewhat artificial.

(TC) signals for the post-accident inadequate core-cooling monitor. This is a safety function. The tertiary function is to provide the DAS with a separate set of thermocouple signals. This is a non-safety function. The safety and non-safety functions share only the mechanical instrumentation assemblies that are placed within the reactor. Separate signal processing electronics are used.

- Operation and Control Centers (OCS) System – the operation and control centers system includes the main control room (MCR), the technical support center (TSC), the operations support center (OSC), the remote shutdown room (RSR), the emergency operations facility (EOF), and the Local Control Stations (LCSs). From an I&C point of view, the OCS represents the integration of AP1000 human-system interface (HSI) resources from the PMS, PLS, TOS, DDS, and DAS. It, therefore, has portions that are safety grade and portions that are non-safety grade.

The major non-safety systems (DDS, PLS, TOS, SMS) and the non-safety portions of both the IIS and OCS are integrated using a plant-wide real-time data distribution network. That network is implemented using the Emerson Ovation® network.

Within each PMS division, the internal functions and the safety portions of both IIS and OCS are integrated using an intra-division ABB AF100 network. This network is part of the Westinghouse Common Q platform, is described in the Common Q topical report (Reference 1) and is referred to as the Common Q Network. Specifically, the AF100 bus is used to allow the various AC160 controllers and Flat Panel Display Systems within a division to exchange information for maintenance, test, diagnostic, communication (to the non-safety system), display, and manual control. The majority of the dataflow is from the AC160 controllers to the Flat Panel Display Systems (for display and for communication to the non-safety system). Therefore, the AF100 bus is used to integrate information exchange among the AC160 controllers performing the Engineered Safety Feature Actuation System (ESFAS) and reactor trip functions and the Flat Panel Display Systems. The AF100 is not in the sensor-to-reactor trip path or sensor-to-ESFAS-actuation path. The ESFAS and reactor trip functions do not require information from each other to perform their safety functions.

In order to support the DDS and OCS functions, there is a need to transfer a large amount of data from the safety portions of the I&C system to the non-safety portions of the I&C system. To achieve this data transfer, there are four unidirectional gateways, one for each of the PMS divisions. The Advant® to Ovation Interface (AOI) communication gateways allow the PMS divisions to provide data to the non-safety systems. The AOI gateway comprises a non-safety portion connected to the Ovation network and a safety system portion connect to the Common Q network in each division. The design of this gateway meets Class 1E to non-Class 1E separation requirements.

The DAS is separate, independent, and diverse from the PMS. It is also separate from the PLS. Its only connections to the PLS are contact outputs used to facilitate reporting of DAS actuations and faults to the operator via the DDS.

In conclusion, the AP1000 I&C system consists of: one safety system (PMS) which has four independent divisions, four non-safety systems (PLS, DDS, TOS, and SMS), and two systems that perform both safety and non-safety functions (IIS and OCS). Within each safety division, the PMS internal functions (Nuclear Instrumentation System {NIS}, Qualified Data Processing System {QDPS}, Reactor Trip

System RTS, Engineered Safety Feature Actuation System {ESFAS}, and the Component Logic System) and the safety portions of IIS and OCS are integrated using the Common Q Network. The non-safety systems (PLS, DDS, TOS, and SMS), the non-safety portions of IIS and OCS, and the safety system data (via the AOI gateways) are integrated using the Emerson Ovation network. The DAS is separate, independent, and diverse from the PMS and separate from the PLS.

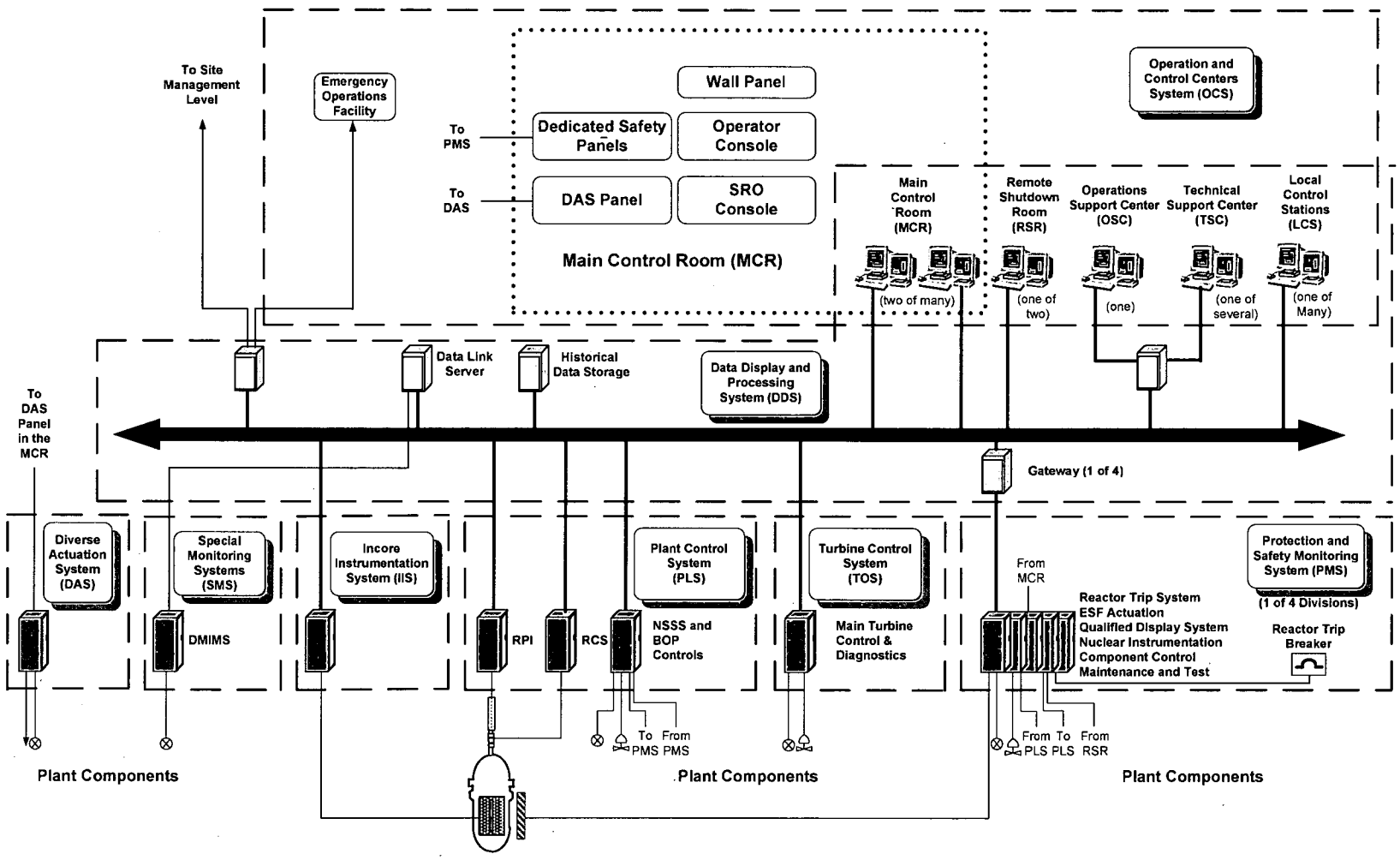

Figure 2-1 High-Level Overview of the AP1000 I&C Architecture

3 NON-SAFETY COMMUNICATION

Non-safety communication consists primarily of the non-safety communication network and the non-safety datalink interfaces.

3.1 NON-SAFETY COMMUNICATION NETWORK

The non-safety communication network is implemented using the Ovation network. It is a robust, fault-tolerant, high-speed, commercially available communications network designed for mission critical process control applications.

The network is comprised of a number of high-speed Ethernet switches[2] configured in a redundant, two-tiered, hierarchical, tree topology as shown in Figure 3-1.

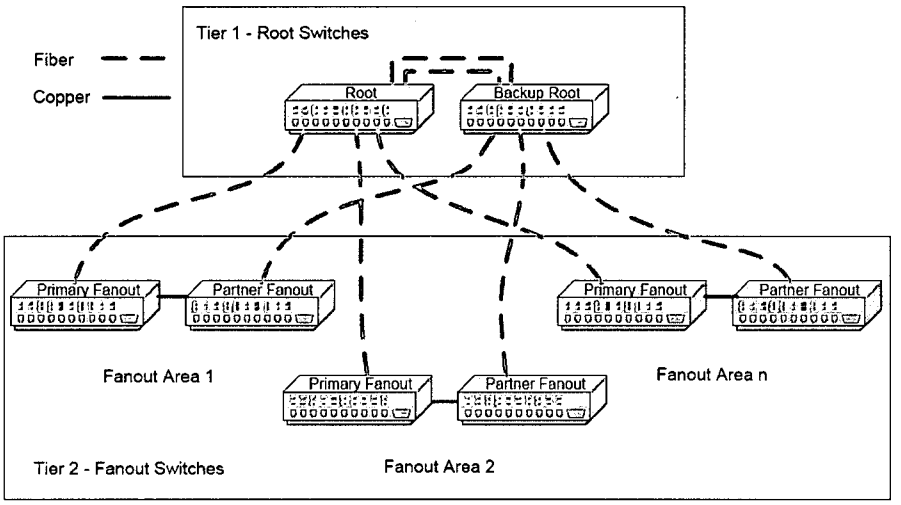

Figure 3-1 Ovation Network Topology

The network uses unaltered Ethernet protocols, high-speed Ethernet switches, and full-duplex cabling (fiber or copper unshielded twisted pair {UTP}). [

]^{a,c}

[2] The material presented here uses the term "switch" to refer to the communications devices that comprise the backbone of the network. Switches provide the minimum capability required to implement the network. Devices with more capabilities, such as routers, may also be used for this function.

The network provides real-time data distribution and general purpose communication. Real-time data distribution is defined as the scheduled periodic multicast 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.

3.1.1 Real-Time Data Distribution

Real-time data distribution within the non-safety system supports the integration within functional systems and among functional systems, including the integration between the safety system and non-safety systems.

The network supports the automatic periodic transmission of data at two rates: one sample per second and ten samples per second. The total periodic data capacity is 200,000 point values per second.

3.1.2 General Communications

The Ovation network supports network standard communications protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol/Internet Protocol (UDP/IP) for general purpose communications. Within the Ovation system, general purpose communications based upon standard protocols are used for aperiodic data, including file-type data transferred from the historian and plant database to be presented at the HSI, plant informational data messages, alarm messages, and sequence of events (SOE) messages to the plant historian for long-term historical storage. This communication occurs on the same physical media as the real-time periodic data, but is implemented in such a way as to preserve the design philosophy of guaranteeing the real-time periodic data transmission without loss, degradation, or delay, even during plant upsets.

The Ovation network can also simultaneously support non-Ovation general purpose communications on the same physical network. [

]^{a,c}

3.1.3 Access Control

While the Ovation open interfaces provide enhanced connectivity, the control network is protected from the outside world via the use of security devices and software. The network can be configured to provide secure communications with the remainder of the plant business and engineering systems. If required, additional security devices may be implemented between the Ovation network and higher levels in the network hierarchy that permit bidirectional communication. See Reference 12 for information relating to the AP1000 domestic market.

3.1.3.1 On-Site

On-site access to Ovation information is through a local login at a workstation physically attached to the Ovation Network. The Ovation system provides a tool set to permit the configuration of an integral

security scheme, where the combination of the user's login privileges, the physical workstation, and the local/remote access method determines the functionality that can be performed in that session. In this context, "remote" is still within the Ovation network, e.g., remote access to a particular workstation in the Ovation network from another workstation in the Ovation network. [

]^{a,c}

3.1.3.2 Off-Site

Off-site access to Ovation information is provided via secure servers that provide methods for delivering Ovation information to external, non-Ovation resources, ensuring that this communication cannot interfere with Ovation operation. Off-site access to view-only Ovation data can be employed using security appliances to enforce unidirectional communication to less secure networks (see Reference 12).

The data access servers provide standard methods for accessing information from the Ovation network for use by engineering and business applications. These server interfaces are designed to support both human interaction (e.g., Intranet-view-only of control system data) and programmatic interfaces (e.g., Object Linking and Embedding Database {OLEDB} provider access to historical information for use in programs). Additionally, Ovation provides standard reporting tools that can be used to generate periodic reports that can be generated and stored in standard applications format (such as Microsoft® Excel®).

Off-site access from the EOF and the Utility/Business Operations network will be implemented using the various methods outlined above, the details of which will be determined during system design.

3.1.4 System Capacity

With respect to periodic data, the network is designed to support up to 200,000 point values per second using a nominal percentage of the overall network bandwidth. The values per second number is obtained by combining the number of points originated at the one second frequency at a 1:1 ratio, with those points originated at a tenth of a second frequency at a 10:1 ratio. For example, if a system contains 50,000 one second points and 500 tenth of a second points, the total point values per second is 55,000 = ((50,000 * 1) + (500 * 10)). The network load associated with periodic data origination is constant; it does not change during plant upset conditions. The Ovation vendor has thoroughly tested the network at the 200,000 point values per second limit. The total point count continues to be defined as the AP1000 design progresses. A design goal is to limit the number of point values per second to the extent possible. The exact number of point values per second, and therefore the base load on the network, will be evaluated as the design is finalized.

With respect to aperiodic data, the network load is variable, but managed. As described previously, aperiodic network data includes: alarm message data, historical archival and retrieval data, and print requests. Alarm message data will be minimized to the extent possible by limiting the number of points subject to alarm checking and by carefully selecting alarm limits to minimize nuisance alarms. A similar engineering analysis will be performed to determine the number of points subject to historical data

collection. A comprehensive evaluation of data collection deadbands will be performed to ensure optimal collection sampling rates, which will limit the number of data samples transferred over the network to the historian. An additional component of aperiodic network traffic is that generated by station staff. Operations and engineering personnel located within the main control area can request historical data for display on historical reviews. This data is retrieved from the historian and transferred over the network for display at the Operator Station. Personnel can also request data from the system to be directed to printers in order to produce hardcopies. This aperiodic network load does NOT include requests for plant data from users external to the main control area, e.g., technical support center, enterprise network users, etc. Request for data by these "external users" is managed outside the plant I&C network and therefore has no impact on non-safety network load.

3.1.5 Data Storm Control

Storm control is configured on the Ovation network to ensure that highway availability requirements are satisfied given the unlikely possibility that a software or hardware malfunction, or a malicious network attack, would introduce a packet storm on the control system highway.

Storm control is implemented with configuration settings provided by the switch operating system. In general, each port subject to storm control is configured with traffic ingress block and restoration settings. These values are typically a percentage of the total available bandwidth that can be used by the broadcast or multicast traffic. When traffic entering a port exceeds the pre-defined block value, packet forwarding on the port is blocked. Packet forwarding resumes when the traffic falls below the predefined "restore forwarding" setting. [

]^{a,c}

Storm control is put in place to protect the network from data storms produced as a result of atypical conditions including: hardware malfunctions; deliberate cyber attacks; and errors introduced by humans. The thresholds are set on a per port basis such that native Ovation traffic – periodic process point data; aperiodic alarm message traffic, etc. – will not activate the storm control function. [

]^{a,c} As the system design is finalized, the overall point count, and the point distribution across the drops, will be defined to a level to permit a more detailed analysis of overall network load, as well as the network load attributed to a specific drop. This information, in conjunction with vendor data, will be used to confirm that the data storm threshold settings are appropriate.

In addition to the system storm control configuration installed on the network switches, the Ovation controller has been hardened against excessive network traffic through the implementation of a software

modification that prioritizes critical control functionality over network communications. This capability, used in conjunction with control logic design that requires no inputs from the network, permits the controller to continue to control critical plant operations during a network storm or a complete loss of network event.

3.1.6 Analysis

As described above, the load on the AP1000 non-safety network consists of periodic and aperiodic data. Periodic data consists of a maximum of 200,000 point values per second resulting in a constant base load on the network. An AP1000 design goal is to utilize much less than the maximum available point values per second. This will provide additional spare capacity and will result in a lower base load on the network. As the design is finalized, a firm number of point values per second will be determined. This will be used to calculate the base network load, and therefore, the network bandwidth available for aperiodic data communications. Analytical justification of network capacities will be reviewed for correctness. In general, the network load due to aperiodic data traffic is expected to be very small in relation to the overall bandwidth of the system. The aperiodic data levels can be managed through careful system configuration. Network impacts associated with station staff in the main control area is somewhat limited by the number of operators and Operator Stations and the number of engineers and Engineering Stations.

Based on the current evaluation of expected network traffic, the single network design will meet or exceed all system capacity and network loading requirements. Westinghouse will continue to evaluate the expected network loading impacts associated with both periodic and aperiodic data communication and refine the network design as required to ensure reliable network operation.

3.2 NON-SAFETY DATALINK INTERFACES

Non-safety datalinks are employed to transmit data between various systems. The interfaces to these systems must be carefully designed to preserve the integrity of the AP1000 control system network. To that end, mitigative strategies will be employed to ensure that defense in depth is maintained throughout the network. Cyber security assessments of each datalink pathway and associated assets/systems will be used as a basis for determining the specific mitigative measures that may need to be deployed.

3.2.1 Standalone Systems

The Ovation system supports standard and custom datalinks, both at the controller and workstation level. Controller-level interfaces include standard interfaces to Allen-Bradley programmable logic controllers (PLCs), and GE Mark V/VI, Toshiba, and Mitsubishi Heavy Industries turbine control systems, as well as a standard Modbus® interface and OSI PI historian interface. At the controller level, the datalink interface can be accomplished via a standard input/output (I/O) module (the R-line Link Controller {RLC}), or via Fast Ethernet communications interfaces at the controller processor level. RLC interfaces are used for low-speed or low-capacity interfaces such as component monitoring. Ethernet interfaces at the controller level are used for higher-speed information or larger amounts of data, such as interfacing to a PLC-based local control system. For both the RLC links and the Ethernet controller links, the interface can be supplied redundantly, and is designed in such a way that the controller can utilize the information in standard Ovation control schemes just as native I/O points.

Workstation datalinks include both standard and custom link implementations. Custom links are generally provided to interface to non-standard protocols, as is typically encountered in the retrofit market. Standard links are available for interfacing, for example, to foreign I/O such as RTP I/O, Modbus over Ethernet, and for standard serial communications such as RS-232. The AOI is an example of a Westinghouse standard workstation datalink. Any workstation that functions as a datalink application server can provide the interfaced information to the Ovation network with up to 10,000 process points per drop, supporting all scan and alarming features.

3.2.2 Remote I/O

The Ovation system supports the use of remote I/O so that I/O modules can be clustered close to field devices, minimizing field cabling costs and also accommodating harsher environments. Remote I/O is in contrast to local I/O, which is housed in the same cabinet as the controller or next to it in an extended cabinet. For local I/O, all I/O modules reside in up to four cabinets, which are placed side by side. All field wiring leads to local or remote cabinets. [

]^{a,c}

3.2.3 Non-Safety Smart I/O Fieldbuses

The Ovation system supports Highway Addressable Remote Transducer (HART™) I/O, FOUNDATION™ Fieldbus, Profibus-DP®, and DeviceNet™ smart I/O interfaces. The Ovation fieldbus solution is modular, and a single controller can simultaneously interface to fieldbus devices, HART I/O modules, conventional I/O modules, and third-party I/O.

3.2.3.1 HART I/O

The Ovation controller supports native HART I/O modules. HART is technology that provides a digital information signal superimposed on a 4-20 mA traditional sensor loop. The digitized signal provides up to four HART multivariables which provide additional information from HART-enabled devices, eliminating additional cabling required to provide the same information using traditional sensors and control output devices.

The Ovation HART input module has eight inputs, with each input having an individual HART modem (supporting up to four HART multivariables), and individual channel-to-channel isolation. The Ovation HART output module has four channels, also with individual HART modems per channel, and individual channel-to-channel isolation.

The HART I/O modules can support both traditional 4-20 mA devices and HART devices on the same card.

3.2.3.2 FOUNDATION Fieldbus

FOUNDATION Fieldbus H1 is typically used for analog-type devices such as sensors and modulating control valves. There is a large assortment of "smart" devices available with the interface.

The Ovation FOUNDATION Fieldbus solution is modular and scalable. The interface between the FOUNDATION Fieldbus instrumentation and the Ovation controller is via native Ovation FOUNDATION Fieldbus interfaces modules. There are up to 8 FOUNDATION Fieldbus interface modules per controller, with each interface modules supporting two Fieldbus segments, and up to 16 devices per segment. Typically, up to 12 devices are utilized per segment, with fewer devices if the segment is used for closed loop control. Evaluation of the applicability of Ovation FOUNDATION Fieldbus for AP1000 is part of the ongoing I&C system design.

3.2.3.3 Profibus-DP

Profibus-DP is typically used for digital ON/OFF type devices. In addition to being supported by the appropriate devices, it is suitable for long distances while remaining less sensitive to power, grounding, polarity, and resistance concerns.

The interface between the Profibus devices and the Ovation controller is via native Ovation Profibus interface modules operating as a DP-V2 Profibus master. Each Ovation Profibus I/O module supports communication with two segments and up to 126 field devices [

]^{a,c}

3.2.3.4 DeviceNet

DeviceNet is a field-proven interface for discrete actuators and sensors. The Ovation DeviceNet interface uses a standard Ethernet switch, attached to the Ovation controller via the controller standard Modbus/TCP third-party I/O capability. [

]^{a,c}

3.2.3.5 Asset Management

Another important component of the intelligent field interface solution is the Asset Management Solutions (AMS™) Suite of software. AMS software and the associated SNAP-ON™ applications are a suite of software solutions for streamlining all maintenance activities relative to instrumentation and

valves in a process plant. This package can be integrated into the Ovation workstation and Ovation controller to give the user direct access to all intelligent devices connected to the Ovation I/O. With AMS integrated into Ovation, digitized HART or FOUNDATION Fieldbus parameters such as valve position can be mapped to Ovation process points which can be used anywhere required in the Ovation Distributed Control System. AMS provides direct visibility from the Ovation workstation to each "smart" device in the plant that is connected to Ovation.

4 SAFETY COMMUNICATION

Communication within the safety system consists primarily of the four intra-divisional safety communication networks and safety datalink interfaces.

4.1 SAFETY COMMUNICATION NETWORKS

Within each PMS division, the internal functions and the safety portions of both IIS and OCS are integrated using an intra-divisional ABB Advant Fieldbus 100 (AF100) network. This network is part of the Westinghouse Common Q Platform (see Reference 1) and is referred to as the Common Q Network.

The AF100 is a high-performance, deterministic communication network, intended for communication between Advant Controller 160 (AC160) controllers and Flat Panel Display Systems within the same division. The transmission rate is 1.5 Mbit/second or faster.

Like the non-safety network, the AF100 provides real-time data distribution and general purpose communication. 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}

4.1.1 Real-Time Data Distribution

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

]^{a,c}

4.1.2 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 Flat Panel Display Systems over the AF100 has been disabled in the PMS.

4.1.3 Access Control

4.1.3.1 On-Site

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.

4.1.3.2 Off-Site Access

The four PMS intra-divisional Common Q networks are not accessible from off-site locations.

4.2 SAFETY DATALINK INTERFACES

4.2.1 Standalone Systems

The PMS interfaces to standalone systems such as the Radiation Monitoring System. These interfaces use simple analog and/or digital signals, as is common practice in current operating plants; these interfaces do not use network or datalink connections.

4.2.2 Remote I/O

The PMS does not use a remote I/O system.

4.2.3 Safety Smart I/O Fieldbuses

The PMS does not use smart I/O devices and their associated fieldbus communication buses (e.g., FOUNDATION Fieldbus and Profibus). It does use the ABB AF100 bus. However, the AF100 is not used as a smart I/O bus; rather, it is used to implement the Common Q network discussed previously.

4.2.4 Common Q High-Speed Links

The PMS uses high-speed links to serially communicate certain data within and across PMS divisions. These links are part of the Westinghouse Common Q Platform (see Reference 1). The functionality of these links within the PMS is described in WCAP-16675-P, "AP1000 Protection and Monitoring System Architecture Topical Report" (Reference 7).

5 COMMUNICATION BETWEEN SAFETY AND NON-SAFETY EQUIPMENT

The AP1000 certified design (see APP-GW-GL-700, "AP1000 Design Control Document" {Reference 5}), and the proposed amendment (Reference 6) include the following types of data flow between the safety and non-safety systems:

1. Data Flow from PMS to PLS for Control Purposes – this type of data flow is necessary since the PLS uses PMS sensor signal values and PMS calculated values as inputs to control functions. (See, for example, Tier 2 Section 7.1.2.1 in Reference 6.)

2. Data Flow from PMS to DDS for Information System Purposes – this type of data flow is necessary since the DDS is responsible for the traditional plant computer functions that include the display, processing, alarming, logging, and archiving of PMS process and system data. (See, for example, Tier 2 Section 7.1.1 in Reference 6.)

3. Data Flow from DDS to PMS for Safety System Actuation Purposes – this type of data flow is necessary to implement system-level actuation of the safety system from the remote shutdown room (RSR) which is entirely non-safety. (See, for example, the Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) 2.5.4-2(2) in Reference 6.)

4. Data Flow from PLS to PMS for Component Control Purposes – this type of data flow is necessary to implement soft control of safety system components from the PLS. (See, for example, Tier 2 Section 7.1.2.8 in Reference 6.)

The certified design establishes the following ITAACs (in Table 2.5.2 of Reference 6) regarding the implementation of these data flows:

7.a) The PMS provides process signals to the PLS through isolation devices.

7.b) The PMS provides process signals to the DDS through isolation devices.

7.c) Data communication between safety and non-safety systems does not inhibit the performance of the safety function.

7.d) The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls.

In the certified design, these data flows are primarily implemented using divisionalized bidirectional gateways. The proposed amendment (see Reference 6) changes the design to implement the various types of data flow in different manners. These changes allow:

- Reduced dependence on the gateways
- Unidirectional gateways

- Segmentation and network independence of the Nuclear Steam Supply System (NSSS) control functions within the PLS
- Clear delineation of the points of electrical, communication, and functional isolation

In the modified design, the required data flows are implemented using divisionalized unidirectional gateways and individual analog and digital signals as shown in Figure 5-1. Five cases are identified in the figure and labeled A through E. The cases are discussed in more detail in the following sections.

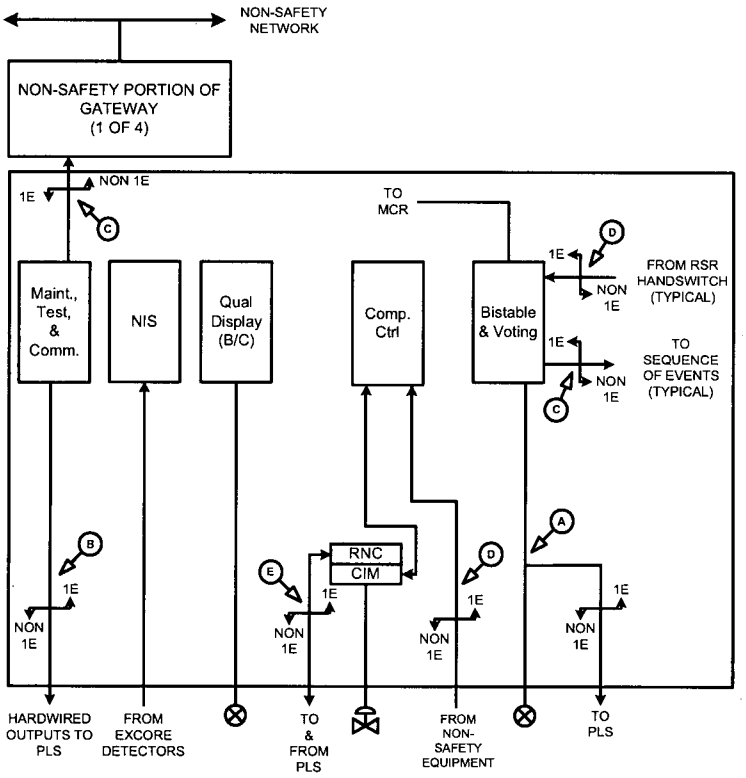

Figure 5-1 Data Flows Between Safety and Non-Safety Equipment

5.1 SAFETY TO NON-SAFETY DATA FLOW

5.1.1 Case A and Case B – Hardwired Signal Interfaces

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 5-1 and is identical to the type of interface in existing plants.

The PMS also provides data to the PLS pertaining to analog and digital signals calculated within the PMS (e.g., Over Temperature Delta Temperature 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 5-1 and is identical to the type of interface in existing Westinghouse plants.

In both cases, qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 8}) 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 7-4.3.2-1993 {Reference 9}, Annex G). They also provide functional isolation by preventing the non-safety system from adversely affecting the safety function.

Comparing these implementations against the ITAACs:

7.a) The PMS provides process signals to the PLS through isolation devices. – This ITAAC is met.

7.b) The PMS provides process signals to the DDS through isolation devices. – This ITAAC is not applicable to these data flows since the data flows are PMS to PLS data flows. However, the PLS does make this information available to the DDS.

7.c) Data communication between safety and non-safety systems does not inhibit the performance of the safety function. – This ITAAC is met.

7.d) The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls. – This ITAAC is not applicable to these data flows since the data flows are not used to implement non-Class 1E manual soft controls.

5.1.2 Case C – Unidirectional Network Datalink

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

The AOI gateway for each PMS division connects the division's internal network to the non-safety real-time data network, which supports the remainder of the instrumentation and control 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 5-1.

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 603-1991 {Reference 8}) 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 7-4.3.2-1993 {Reference 9}, 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 5-2.

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

The second part of the AOI gateway software was developed by Westinghouse. This software followed the process specified for "Important to Safety" software in WCAP-16096-NP-A, "Software Program Manual for Common Q Systems" (Reference 10) (the SPM), for safety software. The SPM was accepted by the NRC as part of the SER process for the Common Q Platform.

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

For SOE signals such as partial trip signals, reactor trip signals, and engineered safety feature (ESF) actuation signals, each division provides the signals to the SOE system/interface via a unidirectional fiber-optic link. The flow of information is strictly from the safety subsystem to the non-safety SOE system/interface. The unidirectional nature of the link is assured by the use of a single unidirectional fiber. The safety end of the fiber is connected to an optical transmitter. The non-safety end of the fiber is connected to a fiber-optic receiver. This arrangement provides electrical isolation between the safety and non-safety portions of the system (as required by IEEE 603-1991 {Reference 8}) and prevents all data flow (data, protocols, and handshaking) from non-safety to safety (providing the communication isolation envisioned by IEEE 7-4.3.2-1993 {Reference 9}, Annex G). It also provides functional isolation by preventing the non-safety equipment from adversely affecting the safety function. This type of interface is a variation of Case C in Figure 5-1.

Comparing this implementation against the ITAACs:

7.a) The PMS provides process signals to the PLS through isolation devices. – This ITAAC is met.

7.b) The PMS provides process signals to the DDS through isolation devices. – This ITAAC is met.

7.c) Data communication between safety and non-safety systems does not inhibit the performance of the safety function. – This ITAAC is met.

7.d) The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls. – This ITAAC is not applicable to this data flow since the data flow is not used to implement non-Class 1E manual soft controls.

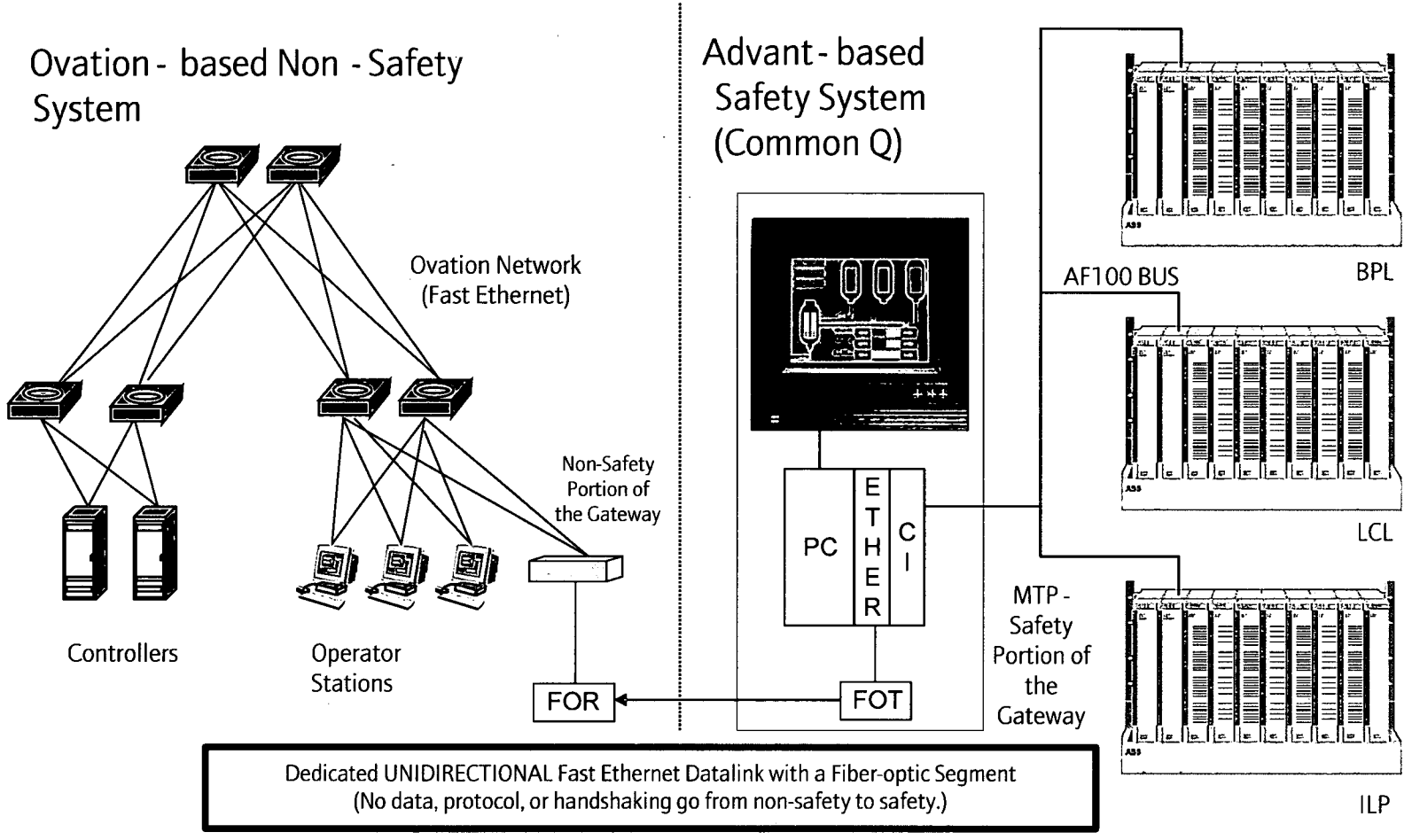

Figure 5-2 Example Implementation of Case C Data Flow

5.2 NON-SAFETY TO SAFETY DATA FLOW

The non-safety to safety data flows are not implemented using communication links; rather, they are implemented using discrete digital signals. These signals are used to implement non-safety manual control of system-level safety functions (actuations, manual blocks and resets, manual reactor trip), non-safety interlock of certain PMS test functions, and non-safety manual component-level control of safety components.

5.2.1 Case D – Non-Safety Manual Control of System-Level Safety Functions and Non-Safety Interlock of PMS Test Functions

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 5-1.

Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 8}) and prevent all but the required data flow from the non-safety system to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2-1993 {Reference 9}, 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, except in the extremely unlikely situation of having to evacuate the MCR. This transfer is accomplished by the divisionalized Class 1E transfer switches which are connected directly to the Local Coincidence Logic (LCL) controllers in each division. Additionally, when the controls are enabled, their functionality is limited to that defined in the PMS functional design because the information transferred is only in the form of discrete digital signals (i.e., there is no computer software-based communication). Specifically, the manual system-level ESF actuations and the manual reactor trip inputs can only initiate safety functions, not inhibit them. The manual system-level blocks are subject to initiation permissives and to automatic removal. The manual system-level resets only remove the system-level actuation signals; they do not cause any components to change state. An additional signal is required to cause a component to change state.

To reduce the chance of the spurious actuation of a function, switch contacts and communication paths are arranged in complementary pairs. Two simultaneous failures in opposite directions would be required to cause a spurious actuation.

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

Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 8}) and prevent all but the required data flow from the non-safety

equipment to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2-1993 {Reference 9}, Annex G).

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

Comparing this implementation against the ITAACs:

7.a) The PMS provides process signals to the PLS through isolation devices. – This ITAAC is not applicable since the data flow is specified as a DDS to PMS data flow. (Note, however, that electrical, communication, and functional isolation is provided.)

7.b) The PMS provides process signals to the DDS through isolation devices. – This ITAAC is not applicable since the data flow is specified as a DDS to PMS data flow. (Note, however, that electrical, communication, and functional isolation is provided.)

7.c) Data communication between safety and non-safety systems does not inhibit the performance of the safety function. – This ITAAC is met.

7.d) The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls. – This ITAAC is not applicable to this data flow since the data flow is not used to implement non-Class 1E manual soft controls.

5.2.2 Case E – Non-Safety Manual Component-Level Control of Safety Components

The normal MCR/RSR manual component soft controls originate in the PLS. To reduce the number of signals (cables) that must be run from the non-safety system to the safety system, the non-safety system's remote I/O capability is used to deliver the signals to the safety system and to accept component status signals from the safety system. Specifically, a remote I/O node from the non-safety system is physically located within each division of the safety system. The remote I/O node is electrically isolated from the non-safety system by the fiber-optic remote I/O bus. The node is powered by the safety system and the portions of the node not performing a safety function are qualified as Associated Class 1E equipment. This type of interface is shown as Case E on Figure 5-1.

The Associated Class 1E equipment, including the Remote Node Controller (RNC), shall meet the requirements of IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuit" (Reference 11), Clause 5.5.2 and Clause 5.5.3. Specifically, it shall be part of the safety system qualification program that will demonstrate that when it is subject to environmental, electromagnetic, and seismic stressors, it does not degrade the Class 1E circuits below an acceptable level. The environmental, electromagnetic, and seismic stressors used for these tests are the same as those used to qualify the Class 1E equipment in the same cabinet.

The remote I/O node includes one or more Class 1E CIM. 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 603-1991 (Reference 8). The remote I/O node controller (RNC) 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 from the communication function within the CIM to the Class 1E priority logic within the CIM provides the communication isolation envisioned by IEEE 7-4.3.2-1993 (Reference 9), 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 5-3. More information on the CIM is presented in Section 6.

Comparing this implementation against the ITAACs:

7.a) The PMS provides process signals to the PLS through isolation devices. – This ITAAC is met for the status information provided to PLS.

7.b) The PMS provides process signals to the DDS through isolation devices. – This ITAAC is met for the status information provided to DDS.

7.c) Data communication between safety and non-safety systems does not inhibit the performance of the safety function. – This ITAAC is met.

7.d) The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls. – This ITAAC is met.

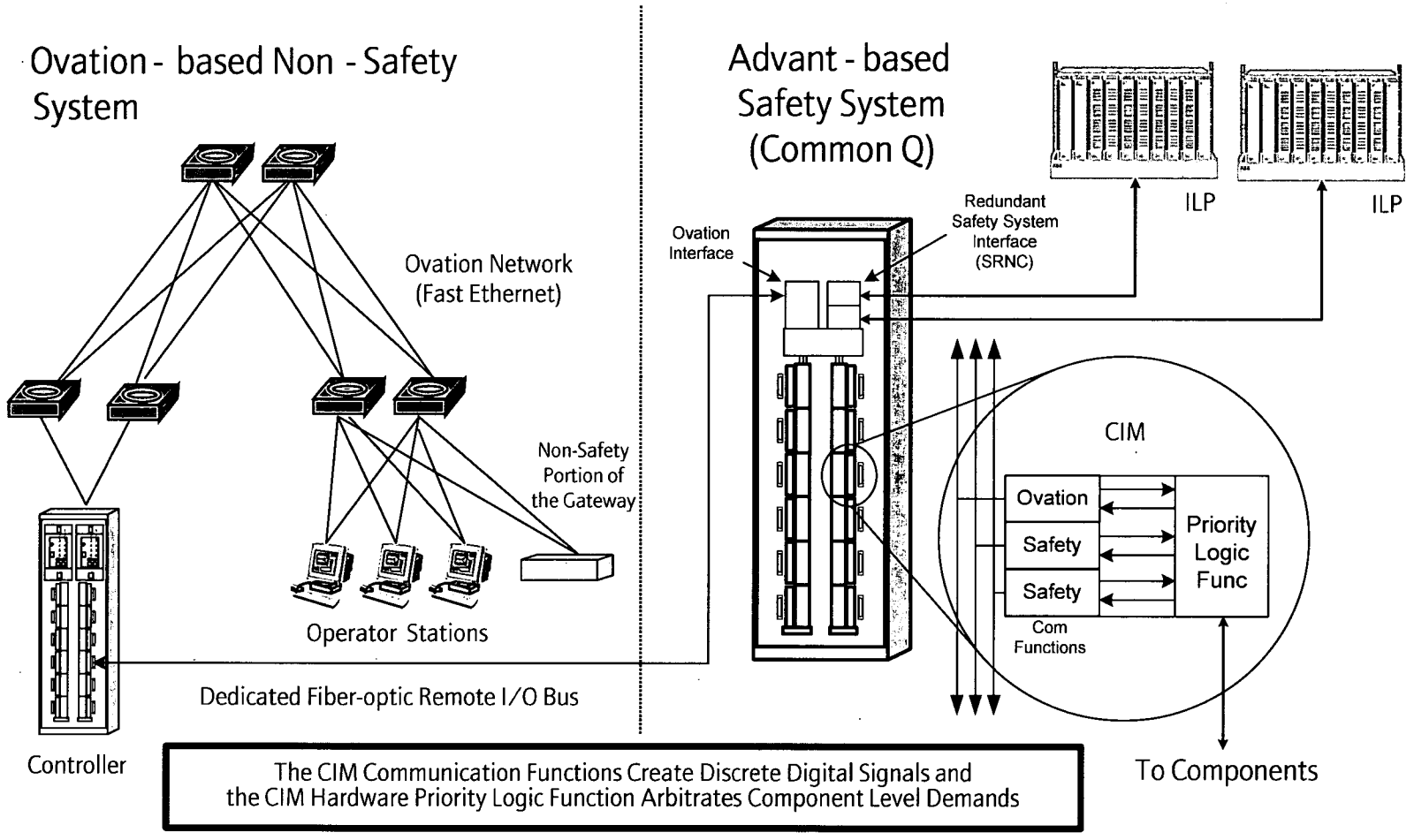

Figure 5-3 Implementation of Case E Data Flow

6 COMPONENT INTERFACE MODULE

The Component Logic System provides actuation, sequencing, monitoring, protection and manual control of various plant components. It also resolves the internal redundancy of the LCL and prioritizes demands from the non-safety system and the safety system.

[

]a,c

Specifically, the CIM is used to combine signals from the PLS soft controls and from the redundant ILPs in the PMS. [ ]a,c Demand signals from the Diverse Actuation System (DAS automatic functions and the DAS manual switches) bypass the CIM and interface to redundant component actuators or redundant inputs to the motor control centers.

a,c

Figure 6-1 CIM Functional Overview

[

]a,c

The CIM module typically arbitrates the component command signals received on two different ports: Port X and Port Y. Port X connects to [ ]a,c the PMS and Port Y connects to the PLS via the Ovation remote I/O bus. The algorithm used by the CIM to resolve conflicting demands from the two system ports is System-based Priority; the state demanded by Port X is always higher priority.

State-based Priority (specifically Safe-state Priority) is implemented on AP1000 by using the following two configurations:

- Components with Manual Component-Level Control from Port Y – Only one demand is enabled on Port X. It corresponds to the safe state of the component. If it is active, it has the highest priority since it is from Port X. If it is not active, Port Y can demand either state.

- Components with Manual Component-Level Control from Port X – All demands from Port Y are disabled. Therefore a conflict can not occur. The Port Y is used for monitoring only.

For AP1000, the automatic and manual system-level actuations are safety functions and are implemented in PMS. Manual component-level actuations are non-safety functions and are typically implemented in PLS. Once a PMS system-level actuation occurs, the associated plant components move to their actuated state. Upon reset of the PMS system-level actuation, the plant components remain in their actuated state until they are restored to their unactuated state by component-level commands that may originate in the PLS. To support this functionality, the CIM retains the current demanded state of the component.

The CIM supports continuous on-line diagnostics. [

]^{a,c}

6.1 IMPLEMENTATION

[

]^{a,c}

a,c

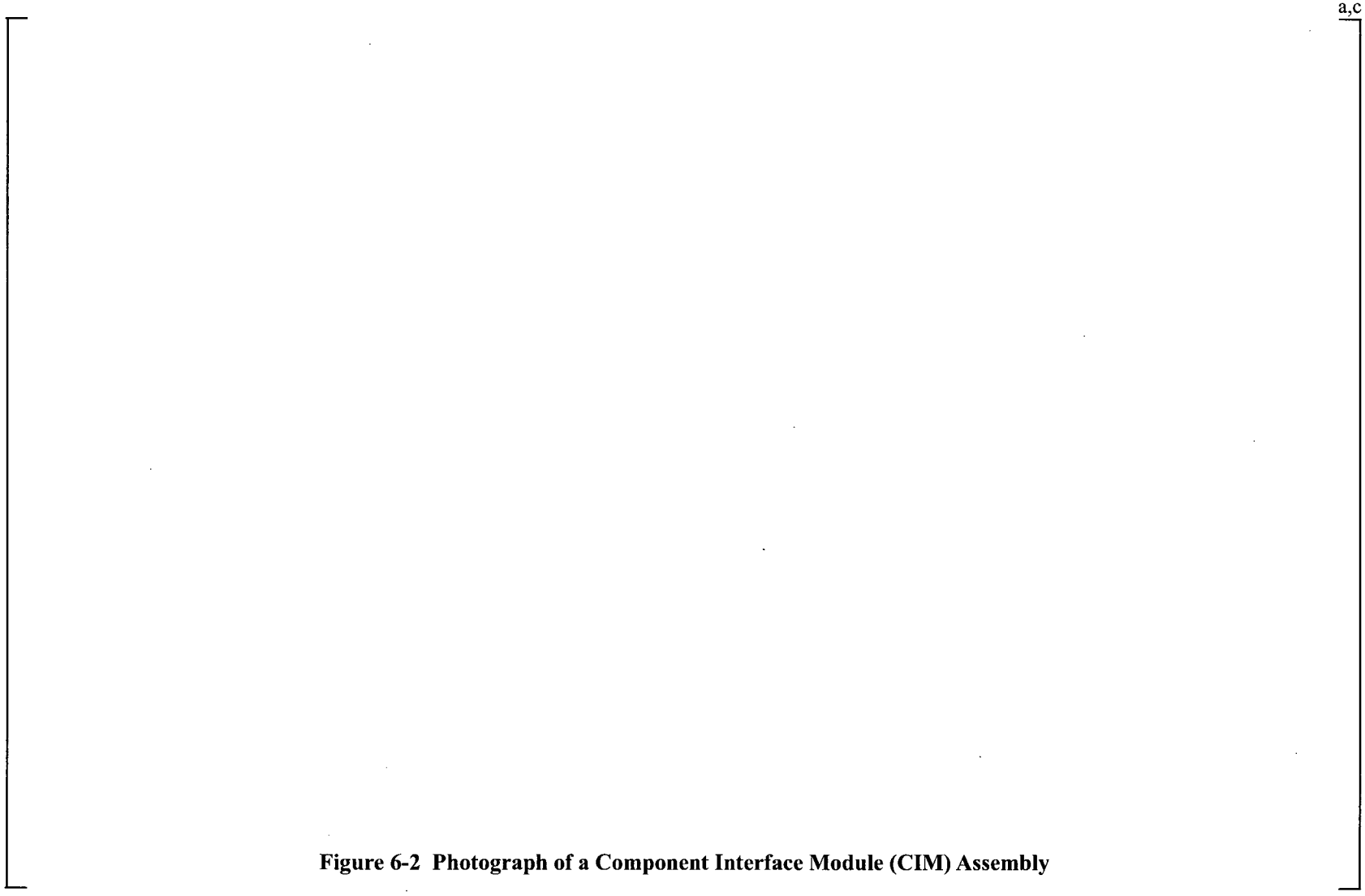

Figure 6-2 Photograph of a Component Interface Module (CIM) Assembly

a,c

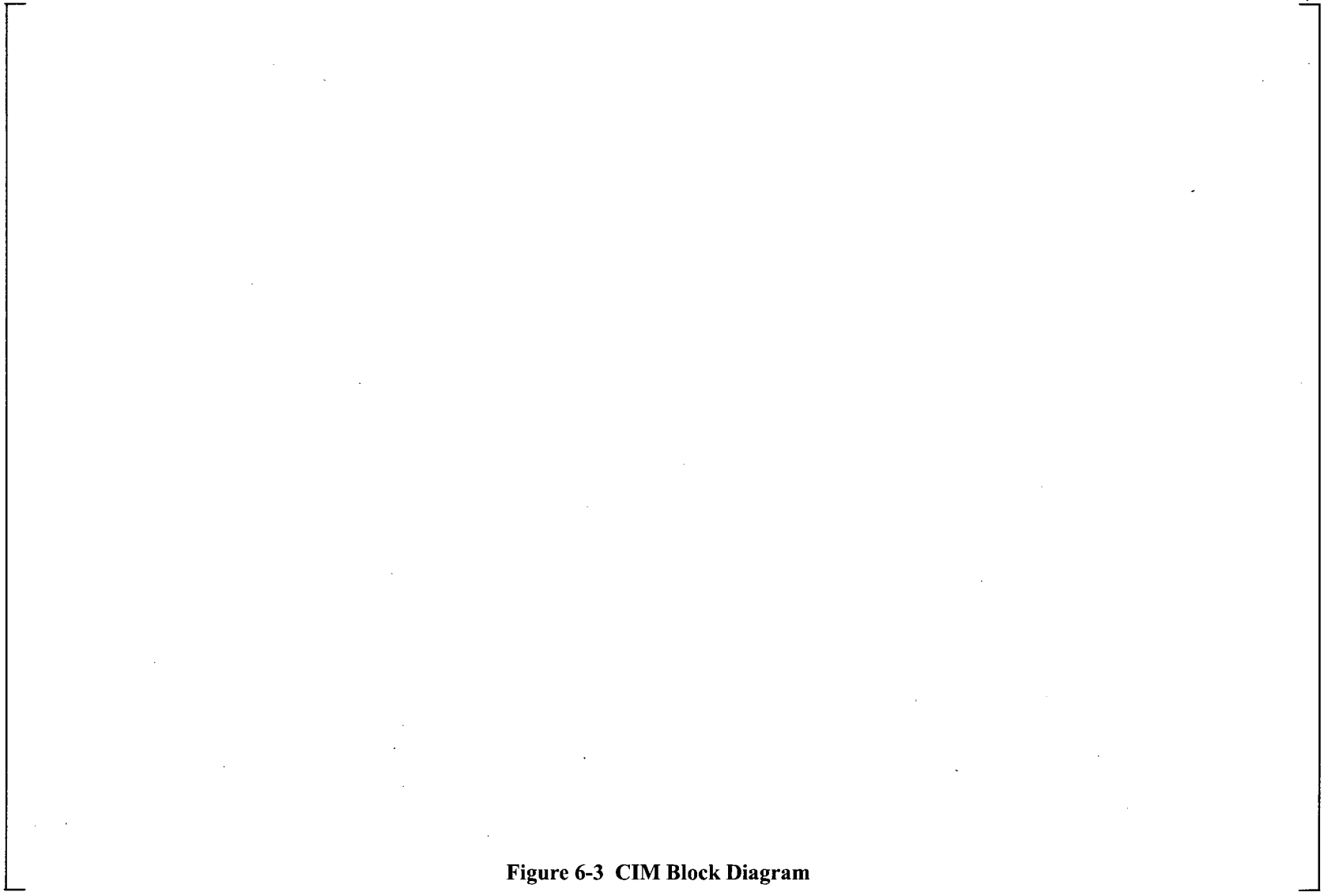

Figure 6-3 CIM Block Diagram

6.1.1 [ ]a,c

[

]a,c

6.1.2 Component Interface Module

[

]a,c

6.1.2.1 [ ]a,c

[

]a,c

6.1.2.2 [ ]a,c

[

]a,c

6.1.2.3 [ ]^{a,c}

[

]^{a,c}

6.2 IMMUNITY FROM POSTULATED SOFTWARE COMMON MODE FAILURE

[

]^{a,c}

The DAS provides a separate path to actuate the ESF components.

6.3 VALIDATION

[

]^{a,c}

6.4 EQUIPMENT QUALIFICATION

The criteria specified in Reference 1 are used for the equipment qualification.

7 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.

7.1 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 manually actuate the ESF system is to use dedicated switches located in the MCR. Switches are located on the Primary Dedicated Safety Panel and the Secondary Dedicated Safety Panel. These switches are processed by the LCL in each PMS division. The resulting commands then fan out to the ILPs and the CIMs implementing the actuated function.

- PMS Manual ESF System-level Blocks and Resets from the MCR – The normal mechanism to control ESF blocks and resets is to use soft controls located on the divisionalized safety displays in the MCR. The safety displays are located on the Primary Dedicated Safety Panel. 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.

- 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 separate from the PMS. For example, through a separate pilot solenoid on air-operated 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.

7.2 MANUAL COMPONENT-LEVEL CONTROL

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

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

Components meeting these criteria include:

All Squib Valves

- PXS-V118A
- PXS-V118B
- PXS-V120A
- PXS-V120B
- PXS-V123A
- PXS-V123B
- PXS-V125A
- PXS-V125B
- RCS-V004A
- RCS-V004B
- RCS-V004C
- RCS-V004D

All ADS Valves (with the exception of those that are normally in their actuated state)

- RCS-V001A
- RCS-V001B
- RCS-V002A
- RCS-V002B
- RCS-V003A
- RCS-V003B
- RCS-V004A this valve is also listed in the Squib Valve list
- RCS-V004B this valve is also listed in the Squib Valve list
- RCS-V004C this valve is also listed in the Squib Valve list
- RCS-V004D this valve is also listed in the Squib Valve list
- RCS-V011A
- RCS-V011B
- RCS-V012A

- RCS-V012B
- RCS-V013A
- RCS-V013B

Head Vent Valves

- RCS-V150A
- RCS-V150B
- RCS-V150C
- RCS-V150D

Residual Normal Heat Removal System (RNS) Valves

- RNS-V001A
- RNS-V001B
- RNS-V002A
- RNS-V002B
- RNS-V023

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

- PLS Manual ESF Component-Level Control from the MCR – The normal mechanism to control these ESF components at the component level is to use soft controls from the Ovation workstations located in the MCR. The soft control commands are transferred over the Ovation network to an Ovation controller. The controller then sends the command to the appropriate CIM modules in the PMS via the Ovation 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 module 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 Ovation workstations located in the RSR. They are implemented in the same manner as described for those in the MCR.

The non-safety displays provide the mechanism to access the soft controls by selecting a target area (or poke field) on a display. The means to access and display the soft controls enables the operator to view the associated graphics displays while undertaking control actions. The soft controls provide control of both safety and non-safety systems and components, and provide component actuation and regulation functions. They are accessible via the video display unit-based workstations on the operator's and supervisor's consoles in the MCR, although the control functionality is normally 'locked-out' at the supervisor's console.

The Ovation platform includes additional security features that provide multiple levels of security. Ovation user accounts will be setup to provide progressive levels of authorization based on user roles (e.g., operator, supervisor, engineer, maintenance, etc.) and the location of the workstation (i.e., main

control area, radwaste control area, local plant workstations). The levels of access can be assigned as view only, initiate control actions, acknowledge alarms, changing setpoints, etc. Each role provides a unique level of access determined during the detailed system design and implemented by the security administrator using a graded approach. Group access policies that limit workstation functionality based on the location of the workstation will be assigned to computer accounts. In addition, the Ovation control system resides within the most secure network. Network security measures ensure that while information can be communicated from a secure network workstation to a less secure network workstation, network communication is not possible in the opposite direction. Thereby, a person who has access to a lower security workstation on the local area network cannot access or operate a soft control on any higher security system.

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

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

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

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

8 CONCLUSIONS

This submittal provides technical information regarding:

1. Data communication between the functional systems that make up the AP1000 I&C system and between the AP1000 I&C system and external systems.

2. The CIM that is used to interface the I&C system to safety system components.

3. The manual control of the safety system at the system level and the component level.

Information is included on the data flows between the safety systems and the non-safety systems. The implementations are shown to meet the requirements of IEEE-603-1991 (Reference 8) and IEEE 7-4.3.2-1993 (Reference 9).

Information is included on the CIM that is used to implement non-safety control of safety components. The module is shown to meet the requirements of IEEE-603-1991 and IEEE 7-4.3.2-1993. It is shown to be free of postulated software common mode failure.

Information is included on the mechanisms the AP1000 I&C system provides for the manual control of the system-level safety functions and component-level functions. The mechanisms are shown to meet the requirements of IEEE-603-1991 and IEEE 7-4.3.2-1993.