

Westinghouse Non-Proprietary Class 3

WCAP-17179-NP
APP-GW-GLR-144
Revision 2

July 2010

AP1000™ Component Interface Module Technical Report



WCAP-17179-NP
APP-GW-GLR-144
Revision 2

AP1000™ Component Interface Module Technical Report

Thomas W. Tweedle*
Senior Engineer, FPGA Platform Engineering & Systems

July 2010

Reviewer: Stephen G. Seaman*
Fellow Engineer, Safety System Engineering & Services

Kyra K. Durinsky*
Project Manager, Component Interface Module Redesign

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

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

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

© 2010 Westinghouse Electric Company LLC
All Rights Reserved

REVISION HISTORY

RECORD OF CHANGES

Revision	Author	Description
0	Thomas W. Tweedle	Initial Release
1	Thomas W. Tweedle	<p>This update incorporates the following changes:</p> <ul style="list-style-type: none"> Added additional CIM technical overview information to Section 2.1. This information includes a description of the CIM/SRNC feedback signals, and the differences between the SRNC and Ovation® RNC. This section has been updated as part of RAI-SRP7.0-ICE-06. Added additional information for the Z port connections, subsection 2.3.1.1.4. This section has been updated per RAI-SRP7.0-ICE-01. Added additional information on CIM addressing inputs and their functions, subsection 2.3.1.1.5. This section has been updated per RAI-SRP7.0-ICE-08. Updated description of the CIM priority logic, including the block overload description, subsection 2.3.1.2.4. This section has been updated per RAI-SRP7.0-ICE-04. Updated information on CIM modes of operation, subsection 2.3.1.2.8. This section has been updated per RAI-SRP7.0-ICE-05. Updated information on SRNC modes of operation, subsection 2.3.2.2.6. This section has been updated per RAI-SRP7.0-ICE-05. Updated the definitions page to define additional terms relating to the CIM/SRNC operational modes. These definitions have been updated per RAI-SRP7.0-ICE-05. Updated the Westinghouse/CS Innovations development process to describe the high quality software development process (Section 2.7) and Figure 2-10. This section and figure have been updated per RAI-SRP7.0-ICE-11. Updated Figure 2-3, "CIM Block Diagram," for clarity of isolation points. This figure has been updated per RAI-SRP7.0-ICE-07. Added References 22 and 23 to support updated text in applicable sections. Fixed minor typographical and grammatical errors. <p>This update is a Class 3 DCP implementation.</p>

RECORD OF CHANGES (cont.)

Revision	Author	Description
2	Thomas W. Tweedle	<p>This update incorporates the following changes:</p> <ul style="list-style-type: none">• The definition of “default state” is revised in the definitions section per RAI-SRP7.0-ICE-05.• Deleted the CIM development process description, Section 2.7, per RAI-SRP7.0-ICE-11.• Added additional information to Section 2.5.3 to describe the failure modes of the HSL/X bus links between PMS and the CIMs. This additional information is per RAI-SRP7.0-ICE-03.• Updated CIM block diagram, Figure 2-3, to more clearly define the isolation points. This update is per RAI-SRP7.0-ICE-07.• Deleted cyber security information. This information is deleted as a result of RAI-SRP-DAS-11 which states that all cyber security information shall be deleted from various technical reports, including the CIM technical report. <p>This update is a Class 3 DCP implementation.</p>

TABLE OF CONTENTS

LIST OF TABLES	viii
LIST OF FIGURES	ix
ACRONYMS AND TRADEMARKS	x
DEFINITIONS	xi
REFERENCES	xiii
1 INTRODUCTION	1-1
1.1 PURPOSE	1-1
1.2 SCOPE	1-1
2 TECHNICAL DESCRIPTION	2-1
2.1 CIM SYSTEM OVERVIEW	2-1
2.2 CIM SYSTEM DESCRIPTION	2-2
2.3 HARDWARE DESCRIPTION	2-4
2.3.1 Component Interface Module	2-4
2.3.2 Safety Remote Node Controller	2-12
2.3.3 Transition Panels	2-16
2.3.4 Base Plates	2-17
2.3.5 Branch Terminator	2-21
2.4 SYSTEM INTERFACES	2-21
2.4.1 Communications Interfaces	2-21
2.4.2 Class 1E/Non-1E Isolation	2-22
2.4.3 Discrete Interfaces	2-22
2.4.4 Actuators Controlled by CIM	2-22
2.5 SYSTEM DIAGNOSTICS AND FAULT INDICATIONS	2-23
2.5.1 Diagnostics	2-23
2.5.2 Fault Indications	2-26
2.5.3 X Bus Failures	2-28
2.6 SYSTEM OPERATION	2-29
2.6.1 Time Response	2-29
2.6.2 CIM and SRNC Operational Modes	2-29
2.7 EQUIPMENT QUALIFICATION	2-29
2.8 RELIABILITY	2-30
2.8.1 FMEA	2-30
2.8.2 MTBF	2-30
2.9 DIVERSITY	2-30
2.9.1 Design Diversity	2-30
2.9.2 Equipment Diversity	2-30
2.9.3 Functional Diversity	2-31
2.9.4 Human Diversity	2-31
2.9.5 Signal Diversity	2-31
2.9.6 Software Diversity	2-31
2.9.7 Diversity Summary	2-31

TABLE OF CONTENTS (cont.)

	2.10	HUMAN FACTORS AND MAINTENANCE CONSIDERATIONS	2-31
	2.11	OPERATING HISTORY	2-32
3		REGULATORY COMPLIANCE	3-1
	3.1	IEEE 603	3-1
	3.2	DI&C-ISG-04	3-1
	3.2.1	DI&C-ISG-04, Section 1, "Interdivisional Communications"	3-1
	3.2.2	DI&C-ISG-04, Section 2, "Command Prioritization"	3-3

LIST OF TABLES

Table 2-1	CIM LED Designations	2-6
Table 2-2	SRNC LED Designations	2-12

LIST OF FIGURES

Figure 2-1	CIM System	2-3
Figure 2-2	CIM Output Devices	2-5
Figure 2-3	CIM Block Diagram	2-11
Figure 2-4	SRNC Block Diagram	2-15
Figure 2-5	Double Width Transition Panel	2-16
Figure 2-6	Single Width Transition Panel	2-17
Figure 2-7	CIM Base Plate with CIMs Installed	2-18
Figure 2-8	SRNC Base Plate with SRNCs Installed	2-20
Figure 2-9	Overlap Testing	2-24

ACRONYMS AND TRADEMARKS

Acronyms used in the document are defined in WNA-PS-00016-GEN, "Standard Acronyms and Definitions" (Reference 16), or included below to ensure unambiguous understanding of their use within this document.

Acronym	Definition
ALS	Advanced Logic System
AOV	Air Operated Valve
CIM	Component Interface Module
CRC	Cyclic Redundancy Check
DAS	Diverse Actuation System
DC	Direct Current
DWTP	Double Width Transition Panel
EMC	Electromagnetic Compatibility
ESD	Electrostatic Discharge
FMEA	Failure Mode and Effects Analysis
FPGA	Field Programmable Gate Array
HSL	High Speed Link
I&C	Instrumentation and Control
I/O	Input/Output
ISG	Interim Staff Guidance
LED	Light Emitting Diode
MOV	Motor Operated Valve
MTBF	Mean Time Before Failure
NRC	Nuclear Regulatory Commission
PCB	Printed Circuit Board
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
RNC	Remote Node Controller
SOV	Solenoid Operated Valve
SRNC	Safety Remote Node Controller
SWTP	Single Width Transition Panel
TWI	Two Way Interface
Vdc	Volts Direct Current

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

AP1000[™] is a trademark of Westinghouse Electric Company LLC.

Ovation[®] is a registered trademark of Emerson Process Management.

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

DEFINITIONS

Term	Definition
AC160	Asea Brown Boveri (ABB) Advant [®] Controller Series 160. An ABB open control system family product line.
CIM System	A system of Component Interface Module (CIM) components that work together to provide component control with command prioritization from safety and non-safety systems. The CIM system components consist of the CIM, Safety Remote Node Controller (SRNC), Double Width Transition Panel (DWTP), Single Width Transition Panel (SWTP), and branch terminator.
Default State	<p>The state of the CIM output devices and the CIM data passed from the SRNC to the CIM, when the CIM and SRNC are not in operational mode.</p> <p>The default state of the CIM output devices is described in R004.50, "Component Interface Module Hardware Requirements Specification," WNA-DS-01271-GEN, Revision 7. [</p> <p style="text-align: right;">J^{a,c}</p> <p>The default state of the CIM data passed from the SRNC to the CIM is described in R004.2, "Safety System Remote Node Controller Requirements," WNA-DS-01272-GEN, Revision 5. [</p> <p style="text-align: right;">J^{a,c}</p>
Operational Mode	A mode of operation where the power supplied to the Field Programmable Gate Array (FPGA) is within the predetermined acceptable range. In this mode, the CIM and SRNC are fully functional and operational.
Ovation	A real-time monitoring and control system product of Emerson Process Management.

Term

Reset Mode

[

$$\mathcal{I}^{a,c}$$

The processor module that is used in the AC160 application.

A standard connector that is used in the CIM system.

REFERENCES

1. IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc.
2. Deleted.
3. "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-04, Task Working Group #4, Highly-Integrated Control Rooms – Communications Issues (HICRe)," U.S. Nuclear Regulatory Commission, September 2007.
4. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," Lawrence Livermore Nuclear Laboratory, December 1994.
5. Deleted.
6. 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," U.S. Nuclear Regulatory Commission, August 2007.
7. Regulatory Guide 1.106, Rev. 1, "Thermal Overload Protection for Electric Motors on Motor-Operated Valves," U.S. Nuclear Regulatory Commission, March 1977.
8. WNA-DS-01271-GEN (Proprietary), Rev. 7, "Component Interface Module Hardware Requirements Specification," Westinghouse Electric Company LLC.
9. WNA-DS-01272-GEN (Proprietary), Rev. 5, "Safety System Remote Node Controller Requirements Specification," Westinghouse Electric Company LLC.
10. Deleted.
11. Deleted.
12. Deleted.
13. WCAP-15775, Rev. 4, "AP1000 Instrumentation and Control Defense-In-Depth and Diversity Report," Westinghouse Electric Company LLC.
14. WCAP-15776, Rev. 0, "Safety Criteria for the AP1000 Instrumentation and Control Systems," Westinghouse Electric Company LLC.
15. WCAP-16438-P (Proprietary), Rev. 2, "FMEA of AP1000 Protection and Safety Monitoring System," Westinghouse Electric Company LLC.
16. WNA-PS-00016-GEN (Proprietary), Rev. 4, "Standard Acronyms and Definitions," Westinghouse Electric Company LLC.

REFERENCES (cont.)

17. Deleted.
18. 6105-10003 (Proprietary), "SRNC Hardware Specification," CS Innovations, LLC.
19. 6105-20003 (Proprietary), "CIM Hardware Specification," CS Innovations, LLC.
20. 6105-10004 (Proprietary), "SRNC FPGA Specification," CS Innovations, LLC.
21. 6105-20004 (Proprietary), "CIM FPGA Specification," CS Innovations, LLC.
22. WCAP-17184-P (Proprietary), Rev. 1, "AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report," Westinghouse Electric Company LLC.
23. APP-PMS-J4-102 (Proprietary), Rev. 0, "AP1000 Protection and Safety Monitoring System Software Requirements Specification," Westinghouse Electric Company LLC.

1 INTRODUCTION

1.1 PURPOSE

The purpose of this report is to describe the Component Interface Module (CIM) system components. The intent of this technical report is to obtain U.S. Nuclear Regulatory Commission (NRC) review and approval for use of the CIM system components in the AP1000™ nuclear safety-related instrumentation and control (I&C) application, and to identify the bounding conditions under which approval is granted.

The CIM system components are logic based modules that do not use microprocessors or software for operation, but instead utilize architecture based on programmable technology. The logic is implemented using field programmable gate array (FPGA) technology. The CIM system components have been developed as nuclear safety-related (Class 1E) products by CS Innovations, a 10 CFR Part 50, Appendix B supplier (Reference 6) and wholly owned subsidiary of Westinghouse Electric Company.

1.2 SCOPE

The scope of this report is limited to the CIM system components. These components include the hardware and their associated external interfaces []^{a,c} described in Section 2.2. This technical report considers the CIM system applied in the AP1000 plant.

2 TECHNICAL DESCRIPTION

2.1 CIM SYSTEM OVERVIEW

The CIM system is designed to interface a field component to the Protection and Safety Monitoring System (PMS) and the Plant Control System (PLS). The CIM priority logic function arbitrates between PMS and PLS demands. The CIM component control logic generates a component demand based on the priority logic outputs and field component feedback signals.

Communication with the PMS is accomplished with the Safety Remote Node Controller (SRNC) assembly. []^{a,c} The SRNC module accepts a high speed link (HSL) connection. []^{a,c} The SRNC communicates with each CIM through a safety bus known as the X bus. The X bus is an independent, bidirectional link between the CIM and the SRNC. The PMS communication link is known as the X port. The SRNC assembly and X bus structure is depicted in Figure 2-1.

The PMS can send an open, close, or stop demand. In addition to the PMS demands received over port X, the PMS can also send three configuration commands to the CIM. These commands are port Y enable, maintenance mode, and output test enable. []^{a,c}

The CIM feedback and status signals are transmitted to the SRNC via the X bus. The CIM and SRNC status and feedback signals are transmitted to Common Q via the HSL. []^{a,c}

The CIMs communicate with the PLS through an Ovation[®] Remote Node Controller (RNC). The Ovation RNC bus is known as the Y bus. The CIM can receive PLS demands from the RNC and transmit status feedback information to the RNC.

The Ovation RNC and the SRNC are physically different modules, designed and built by different companies. The Ovation equipment is a standard Emerson Process Management product. The SRNC (and CIM) have been developed by CS Innovations for the AP1000 application. The SRNC modules do not fit into or connect with the Ovation RNC modules or base plate assembly. The Ovation RNC connection is a fiber optic connection, while the SRNC connection is a DB-25 copper connection. The physical differences between the Ovation RNC and SRNC preclude maintenance errors.

A manual control located on each CIM provides local maintenance and test features for each field component. []^{a,c} A status bit is sent to the PMS and PLS processors when local mode is enabled.

The CIM has two Z port inputs that can be used for connection with a high priority system. These inputs are not used in the AP1000 application (subsection 2.3.1.1.4).

2.2 CIM SYSTEM DESCRIPTION

The CIM system comprises one to thirty-two CIMs assembled on one to sixteen CIM base plates, two SRNCs assembled on one SRNC base plate, one double width transition panel (DWTP), up to two single width transition panels (SWTP), and one to four branch terminating devices. The CIM system can have one to four branches of CIMs; each branch can have one to eight CIMs. Each CIM controls one component, and each CIM base plate can accommodate one or two CIMs. The SRNC base plate provides for two SRNC modules that comprise the redundant safety system communication.

The DWTP connects two branches of CIMs to the SRNC base plate, redundant 24 volts direct current (Vdc) power supplies and the non-safety Ovation RNC. The DWTP also provides two connectors for interconnection with the SWTP. The SWTP connects one branch of CIMs to the DWTP.

The CIM base plate back plane printed circuit board (PCB) distributes the X and Y buses to each CIM and extends the X and Y buses to the next base plate. The CIM back plane PCB also distributes redundant power supply feeds to each CIM and extends the power supply feeds to the next base plate. The base plate connects the CIM to the field component through the use of terminal blocks, facilitating rapid maintenance and repair activities without disturbing field wiring.

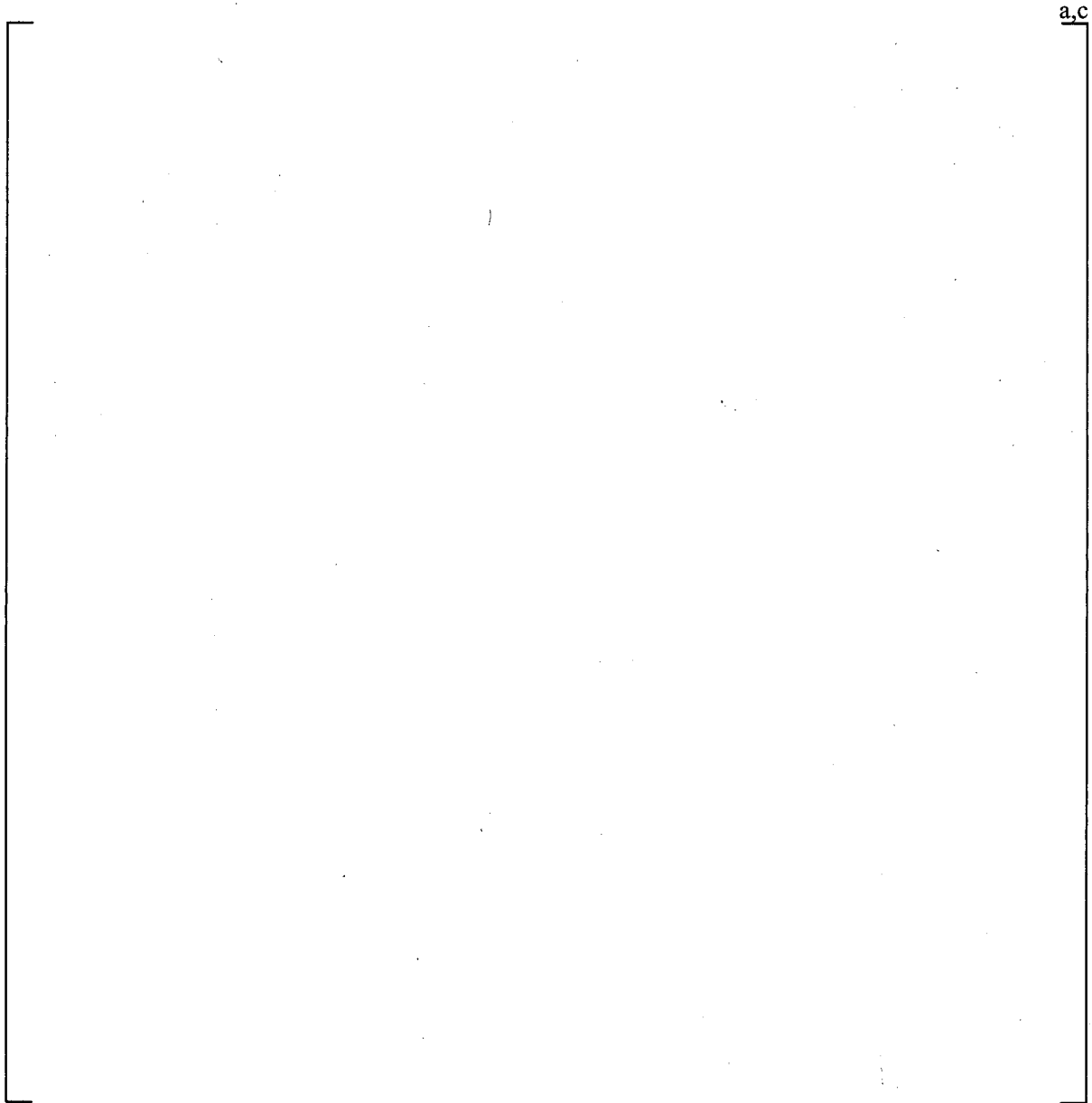


Figure 2-1 CIM System

2.3 HARDWARE DESCRIPTION

The five standard components of the CIM system are described below.

2.3.1 Component Interface Module

[]^{a,c}

2.3.1.1 Module Level Functional Description

2.3.1.1.1 Power Supply

The CIM supports a redundant 24 Vdc power supply feed. The redundant power supply feed is []^{a,c} utilized within the CIM. Transient voltage suppression is provided for over voltage protection. [

] ^{a,c}

2.3.1.1.2 Field Input Circuits

The CIM supports []^{a,c} digital inputs that can receive field component feedback information. [

] ^{a,c} The status of each field input is available to the PMS and the PLS.

[]^{a,c}

2.3.1.1.3 Local Control Input Circuits

The CIM includes a local control interface located on the front panel of the CIM. [

] ^{a,c} The status of the local control []^{a,c} is available to the PMS and the PLS for indication of CIM status.

2.3.1.1.4 Z Port Input Circuits

The CIM supports two digital inputs that can receive commands from a high priority system. [

] ^{a,c}

The Z port inputs are not used in the AP1000 application. [

] ^{a,c}

[]^{a,c} The design of the Z port terminal connections are dissimilar to the connections used for the X and Y ports. The Z port terminal block connections are designed to mitigate a short circuit condition across the terminal connectors. Normal maintenance activities do not utilize the Z port input connections, thus precluding a maintenance error.

2.3.1.1.5 Address Input Circuits

[

] ^{a,c}

2.3.1.1.6 Output Circuits

The CIM has two outputs to interface with the field device. [

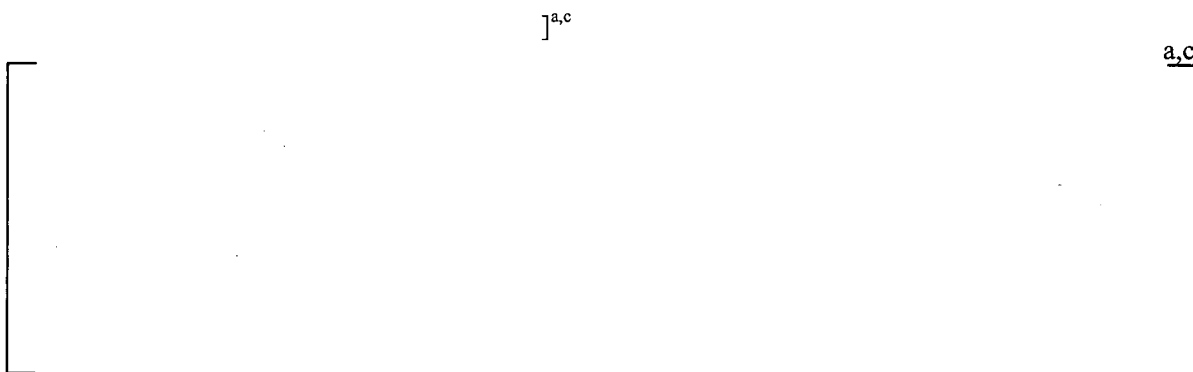


Figure 2-2 CIM Output Devices

2.3.1.1.7 LED Indicators

The CIM has twenty-one light emitting diodes (LEDs) located on the front panel for indication of the module status. [

] ^{a,c}

Table 2-1 CIM LED Designations

a,c[illegible]

2.3.1.2 FPGA Level Functional Description

[

] ^{a,c}

2.3.1.2.1 X Bus Communication Functions

The X bus communication function provides the communications interface between the CIM and SRNC.

[

] ^{a,c} The X bus protocol is described in subsection 2.4.1.2.

[

] ^{a,c}

2.3.1.2.2 Y Bus Communication Functions

The Y bus communication function provides the communications interface between the CIM and Ovation RNC. The Y bus protocol is described in subsection 2.4.1.3.

[

] ^{a,c}

[

|

] ^{a,c}

2.3.1.2.3 Communication Buffers

[

] ^{a,c}

2.3.1.2.4 Priority Logic

[

] ^{a,c}

The priority logic function takes inputs from the X port, Y port, Z port and local control port. [

] ^{a,c}

The priority logic module has [] ^{a,c} output signals that interface to the component control logic. [

] ^{a,c}

2.3.1.2.5 Component Control Logic

The component control logic interfaces the field component with the []^{a,c} priority logic. The component control logic utilizes []^{a,c} feedbacks from the field component. []

[]^{a,c} The PLS and the PMS monitor the available feedback from the component and can generate discrepancy detection signals if the component motion does not start or if the component does not reach the commanded state in a predetermined amount of time.

[]

[]^{a,c}

2.3.1.2.6 LED Control Module

The LED control module is used to interface the CIM FPGA with twenty-one LED indicators (subsection 2.3.1.1.7). The LED control module receives status and control information from the field inputs, outputs, internal logic states and test functions to determine the status of each indicator.

2.3.1.2.7 FPGA Test Functions

The CIM FPGA contains []^{a,c} test features for the safety system actuation path. These test features are described in subsection 2.5.1.1.1.

2.3.1.2.8 Operational Modes of the CIM

The CIM has design features to provide deterministic operation of the CIM. [When power is applied, direct current to direct current (DC/DC) power converters provide the required FPGA voltages from the 24 Vdc supply. Voltage supervisors connected to the power supply outputs hold the FPGA in reset mode for a predetermined amount of time after the voltage output has stabilized.

The FPGA will be placed into reset mode any time the FPGA power supplies operate outside the allowable range. The FPGA power supplies will operate outside their allowable range when:

[]^{a,c}

| • [

|

] ^{a,c}

a.c

Figure 2-3 CIM Block Diagram

2.3.2 Safety Remote Node Controller

[]^{a,c}

2.3.2.1 Module Level Functional Description

2.3.2.1.1 Power Supply

The SRNC supports a redundant 24 Vdc power supply feed. The redundant power supply feed is []^{a,c} utilized within the SRNC. Transient voltage suppression is provided for over voltage protection. []

] ^{a,c}

2.3.2.1.2 LED Indicators

The SRNC has seven light emitting diodes (LEDs) located on the front panel for indication of the module status. []

] ^{a,c}

Table 2-2 SRNC LED Designations

a,c

2.3.2.2 FPGA Level Functional Description

[]^{a,c}

2.3.2.2.1 HSL Communication Functions

The HSL communication functions interface the SRNC to the PM646A. []^{a,c}

[

] ^{a,c}

2.3.2.2.2 X Bus Communication Functions

[

] ^{a,c}

2.3.2.2.3 Communication Buffers

[

] ^{a,c}

2.3.2.2.4 LED Control Module

The LED control module is used to interface the SRNC FPGA with seven LED indicators (subsection 2.3.2.1.2). The LED control module receives status and diagnostic information to determine the status of each indicator.

2.3.2.2.5 FPGA Test Functions

The SRNC FPGA contains []^{a,c} test features for the safety system actuation path. These test features are described in subsection 2.5.1.1.1.

2.3.2.2.6 Operational Modes of the SRNC

The SRNC has design features to provide deterministic operation of the SRNC. []^{a,c}

a,c

Figure 2-4 SRNC Block Diagram

2.3.3 Transition Panels

2.3.3.1 Double Width Transition Panel

The DWTP connects []^{a,c} CIM base plates to the SRNC base plate, Ovation RNC assembly, and redundant 24 Vdc power feeds. []



Figure 2-5 Double Width Transition Panel

2.3.3.2 Single Width Transition Panel

The SWTP connects one CIM base plate branch to the DWTP. []

] ^{a,c}

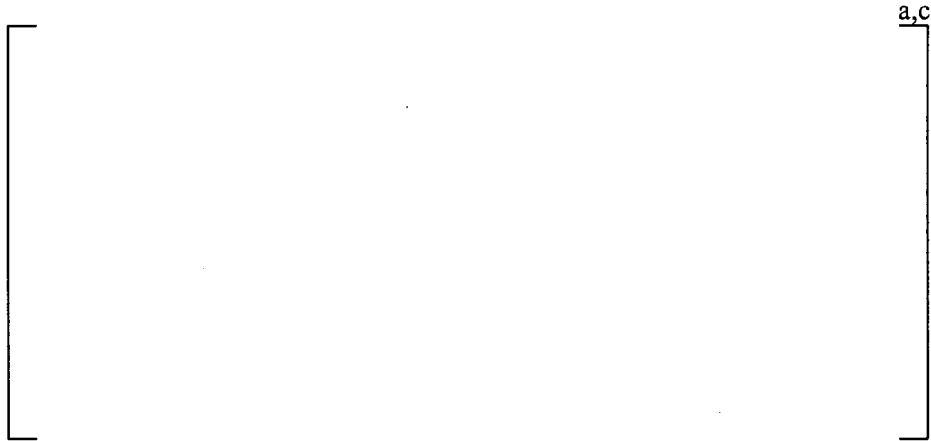


Figure 2-6 Single Width Transition Panel

2.3.4 Base Plates

The CIM and SRNC base plates provide a physical mounting location for the CIM and SRNC modules.

[]^{a,c}

2.3.4.1 CIM Base Plate

[

] ^{a,c}

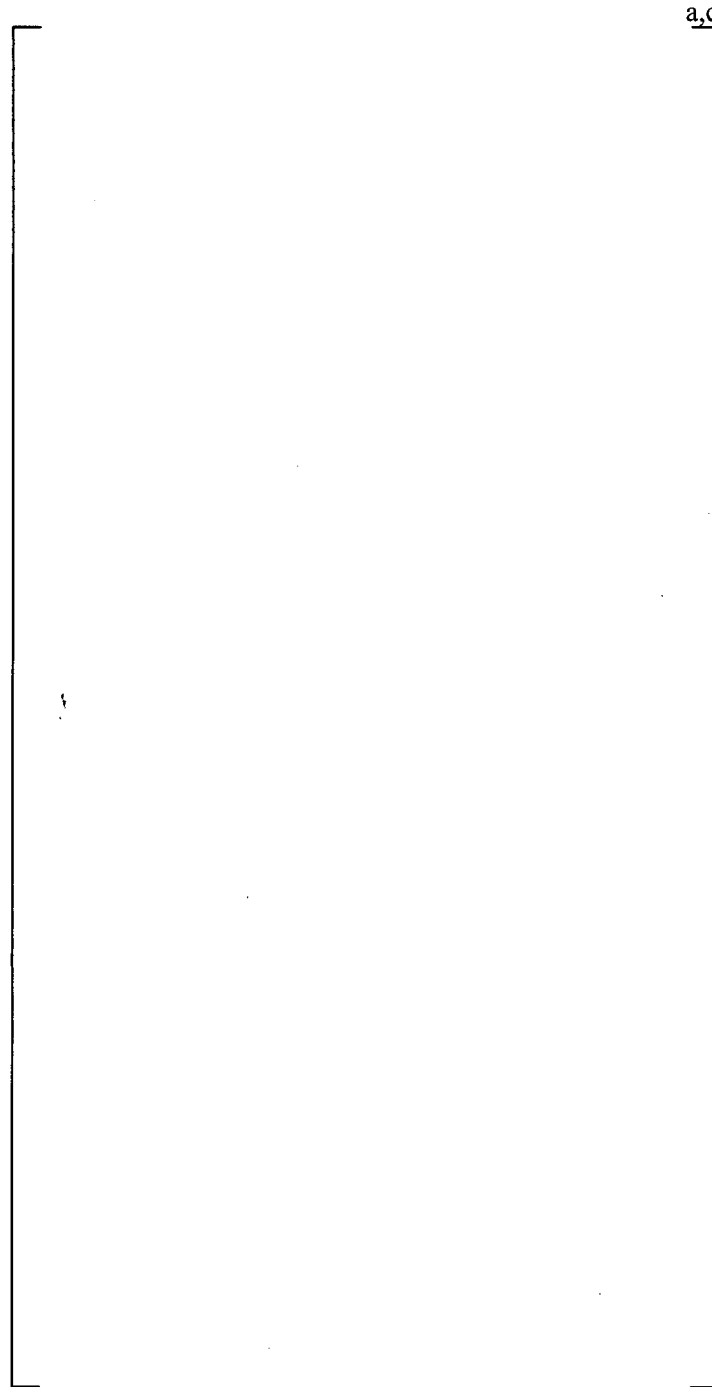


Figure 2-7 CIM Base Plate with CIMs Installed

Note: This figure is for illustrative purposes only and may not represent the final configuration or connection as installed into the PMS.

2.3.4.2 SRNC Base Plate

[

] ^{a,c}

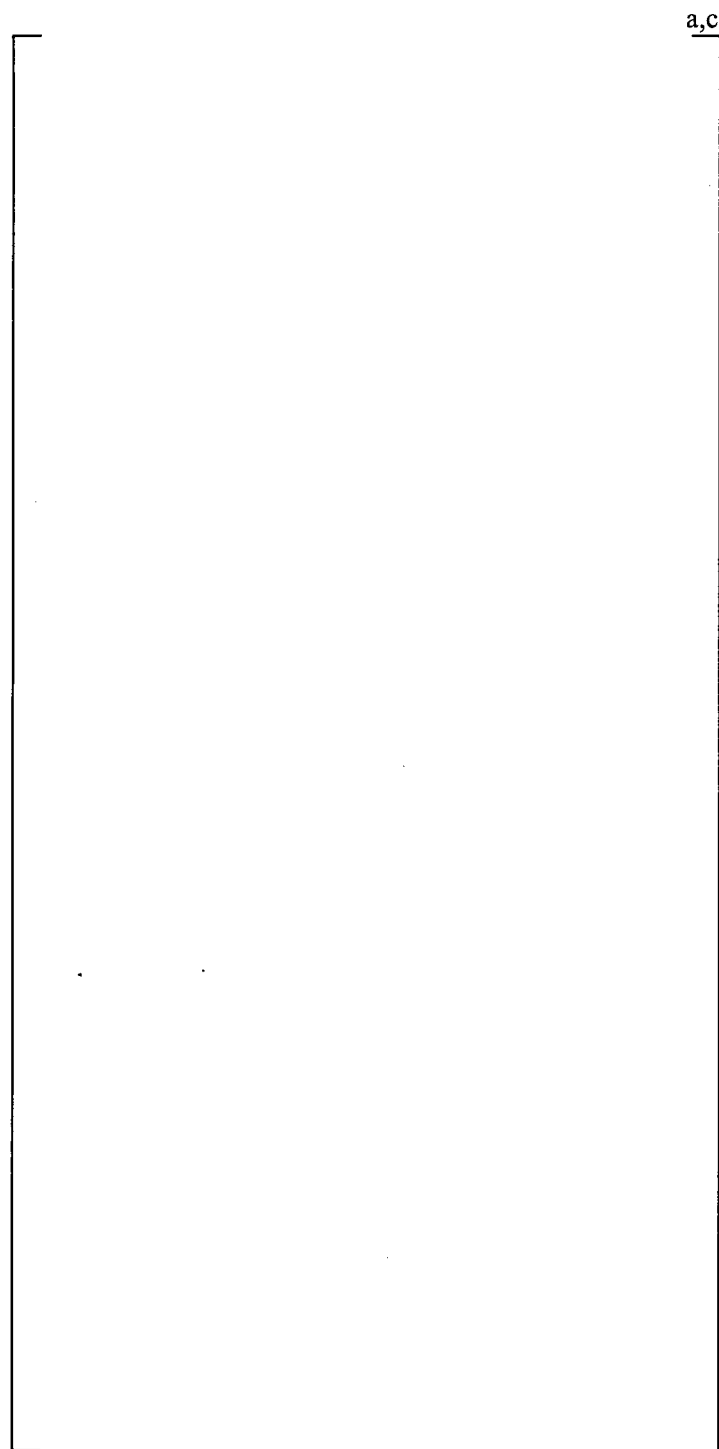


Figure 2-8 SRNC Base Plate with SRNCs Installed

Note: This figure is for illustrative purposes only and may not represent the final configuration or connection as installed into the PMS.

2.3.5 Branch Terminator

The branch terminator is installed on the last CIM base in each branch. [

] ^{a,c}

2.4 SYSTEM INTERFACES

2.4.1 Communications Interfaces

2.4.1.1 High Speed Link

The PM646A processor and SRNC module communicate with the HSL protocol. [

] ^{a,c}

2.4.1.2 X Bus

The communication protocol that CIMs and the SRNC use to communicate is the X bus protocol. [

] ^{a,c}

2.4.1.3 Y Bus

The communication protocol that is used with the PLS is the Ovation I/O bus. [

] ^{a,c}

2.4.2 Class 1E/Non-1E Isolation

[

] ^{a,c}

2.4.3 Discrete Interfaces

The CIM has four sets of discrete interfaces that are used for control and connection with plant components. The field input circuits (subsection 2.3.1.1.2) connect with status feedback indicators that receive component status information. The local control input circuits (subsection 2.3.1.1.3) provide a local interface for the CIM. [^{a,c}

The Z port input circuits (subsection 2.3.1.1.4) connect with a high priority system. The CIM outputs (subsection 2.3.1.1.5) interface the CIM open and close commands to the field device.

2.4.4 Actuators Controlled by CIM

The CIM interfaces with components of the following types:

- Motor Control Centers
- AOVs
- SOVs
- Circuit Breakers
- Squib Valves

[

] ^{a,c}

2.5 SYSTEM DIAGNOSTICS AND FAULT INDICATIONS

2.5.1 Diagnostics

2.5.1.1 Continuous Diagnostics

2.5.1.1.1 Safety Path Testing

[

] ^{a,c}

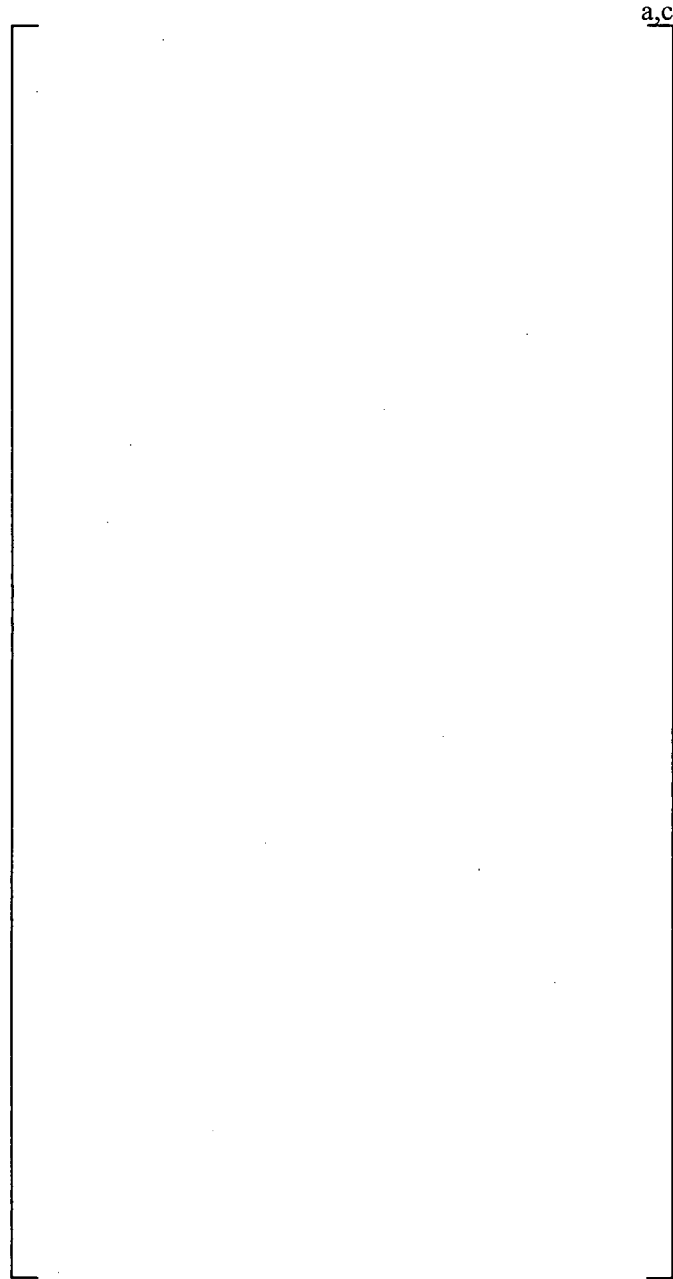


Figure 2-9 Overlap Testing

[

] ^{a,c}

[

] ^{a,c}

2.5.1.1.2 Additional Continuous Diagnostics

The following sections detail additional diagnostics for the CIM and SRNC modules that support safety path testing.

SRNC – Power Supply Monitors

The SRNC monitors the 24 Vdc power supply feed [^{a,c} to ensure the supplied voltage is within the operating range of the SRNC. If the voltage is not within range, the SRNC will visually indicate this condition on the front panel status LEDs, as well as transmit this condition to the PMS and the PLS.

[

] ^{a,c}

CIM – Ground Fault Detection

The field feedback inputs are provided with ground fault detection capabilities. A ground fault occurs if there is current flow between the field input channel and earth ground. This condition is transmitted to the PMS and the PLS.

CIM – Power Supply Monitors

The CIM monitors the 24 Vdc power supply feed to ensure the supplied voltage is within the operating range of the CIM. [

] ^{a,c}

[

] ^{a,c}

2.5.1.2 Periodic Diagnostics

[

] ^{a,c}

2.5.2 Fault Indications

2.5.2.1 Local Indications

Specific fault indications are indicated locally on CIM and SRNC front panel LED display. The fault indications are listed as follows. For an explanation of the front panel indicators, see subsection 2.3.1.1.7 for the CIM and subsection 2.3.2.1.2 for the SRNC.

CIM:

- [] ^{a,c}
- 24V-A LED indicator not lit: The 24V-A power supply feed does not have a voltage applied that is in the operating range of the CIM.
- 24V-B LED indicator not lit: The 24V-B power supply feed does not have a voltage applied that is in the operating range of the CIM.
- Flashing Z-Port LED indicator: Ground fault or 48 Vdc wetting power supply failure.
- Flashing Field Input LED indicator: Ground fault or 48 Vdc wetting power supply failure.
- X bus indicator not lit: The CIM is not communicating on the X bus.
- Y bus indicator not lit: The CIM is not communicating on the Y Bus.

SRNC:

- 24V-A LED indicator not lit: The 24V-A power supply feed does not have a voltage applied that is in the operating range of the CIM.
- 24V-B LED indicator not lit: The 24V-B power supply feed does not have a voltage applied that is in the operating range of the CIM.

- X bus indicators: LED indicators are provided for the X bus branches. The indicator is not lit when the SRNC is not communicating on the specific X bus branch.
- HSL indicator not lit: The SRNC is not communicating across the HSL.

2.5.2.2 Remote Indications

Specific fault indications are sent to the PMS and the PLS via each respective communication link. The following list details the fault indications that are sent:

CIM:

[

]a,c

SRNC:

[

] ^{a,c}

2.5.3 X Bus Failures

[

] ^{a,c}

- [

] ^{a,c}

2.6 SYSTEM OPERATION

2.6.1 Time Response

Time response of the CIM system is defined by the requirements listed in References 8 and 9.

2.6.2 CIM and SRNC Operational Modes

Operational mode of the CIM and SRNC modules will begin once the transition from reset mode has occurred (subsections 2.3.1.2.8 and 2.3.2.2.6). The operational mode of the CIM and SRNC is not affected during different modes (test, normal operation, etc.) the plant may operate in. The CIM priority and component control logic does not change for any plant operational mode.

2.7 EQUIPMENT QUALIFICATION

The CIM system components will undergo two sets of equipment qualification tests. The first set will be completed under the CS Innovations process. [

] ^{a,c} The second set of tests will be conducted under the Westinghouse process. [

] ^{a,c}

2.8 RELIABILITY

2.8.1 FMEA

The Failure Mode and Effects Analysis (FMEA) is a qualitative evaluation which identifies failure modes that contribute to a system's unreliability. The FMEA identifies significant single failures and their effects or consequences on the system's ability to perform its functions. [

] ^{a,c}

2.8.2 MTBF

[

] ^{a,c}

2.9 DIVERSITY

[

] ^{a,c} The following evaluation will focus on the diversity requirements for the CIM and SRNC and support the two aforementioned diversity evaluations.

The CIM and SRNC provide the control of the safety-related components through the PMS. This actuation path must be diverse from the path that is provided in the Diverse Actuation System (DAS). [

] ^{a,c}

2.9.1 Design Diversity

Design diversity is the use of different methods to solve similar problems. [

] ^{a,c}

2.9.2 Equipment Diversity

Equipment diversity is the use of different hardware to perform similar safety functions. [

] ^{a,c}

[

] ^{a,c}

2.9.3 Functional Diversity

Two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects. [

] ^{a,c}

2.9.4 Human Diversity

The purpose of human diversity is to reduce the chance of common errors in similar designs. [

] ^{a,c}

2.9.5 Signal Diversity

Signal diversity is the use of different sensed parameters to initiate protective action. [

] ^{a,c}

2.9.6 Software Diversity

Software diversity is the use of different programming or algorithms to perform the same or similar functions. [

] ^{a,c}

2.9.7 Diversity Summary

All of the elements must be evaluated to determine if adequate diversity is provided. [

] ^{a,c}

2.10 HUMAN FACTORS AND MAINTENANCE CONSIDERATIONS

The following human factors considerations have been incorporated into the designs of the CIM and SRNC modules. These human factors considerations support maintenance and test features for PMS.

- [

] ^{a,c}

- Module Replacement

The CIM and SRNC base plates have been designed with rigid metal guides to ensure proper module alignment and mating with the backplane. The modules have two thumb screw fasteners to secure the module into the base plate assembly.

- Module Indicators

The CIM and SRNC indicators are straightforward in their design to minimize the chance of misinterpretation. Failures and off-normal conditions are clearly indicated by the behavior of the module indicators.

- Pre-configured Modules

CIM and SRNC FPGA cores are configured prior to shipment and cannot be altered by the customer. This approach improves configuration control of CIM system components and prevents maintenance errors.

- Electrostatic Discharge (ESD)

The CIM and SRNC are qualified for ESD resistance.

- Local Controls

The CIM local controls are designed for their ease of use and indication. [

] ^{a,c}

- Test Points

The CIM base plate is designed with test points and field disconnect terminal blocks to aid in maintenance and troubleshooting activities. The field disconnects and test points can be used to test the signal path without disconnecting any field wiring from the base plate.

2.11 OPERATING HISTORY

The CIM function has been previously utilized in operating nuclear power plants. The CIM system components are newly designed assemblies and thus have no operating history. The first planned use of the redesigned CIM system assemblies is for the AP1000 plant application.

3 REGULATORY COMPLIANCE

3.1 IEEE 603

IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 1), establishes the minimum functional design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems. The criteria established in IEEE 603 provide a means for promoting safe practices for design and evaluation of safety system performance and reliability. [

] ^{a,c}

3.2 DI&C-ISG-04

The NRC Task Working Group #4, "Highly Integrated Control Rooms – Communications Issues" (Reference 3), has provided interim NRC staff guidance on the review of communications issues. The interim NRC staff guidance contains three sections: Interdivisional Communications, Command Prioritization, and Multidivisional Control and Display Stations. The third section provides guidance for control displays, which is not applicable to components of the CIM system.

3.2.1 DI&C-ISG-04, Section 1, "Interdivisional Communications"

Section 1 of DI&C-ISG-04 (Reference 3) provides guidance on communications, including transmission of data and information, among components in different electrical safety divisions and communications between a safety division and equipment that is not safety-related. This interim staff guidance (ISG) does not apply to communications within a single division. The ISG provides twenty staff positions in this section. The following statements are the responses to each of the twenty staff positions provided in the ISG.

[

] ^{a,c}

| [

|

] ^{a,c}

[

] ^{a,c}

3.2.2 DI&C-ISG-04, Section 2, “Command Prioritization”

Section 2 of DI&C-ISG-04 (Reference 3) provides guidance applicable to a prioritization device, which receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device. The ISG provides ten staff positions in this section. The following statements are the responses to each of the ten staff positions provided in the ISG.

[

] ^{a,c}