Safety I&C System Description and Design Process

Non Proprietary Version

December 2008

Ⓒ2008 Mitsubishi Heavy Industries, Ltd.
All Rights Reserved

Revision History

Revision	Date	Page (section)	Description
0	March 2007	All	Original issued
1	July 2007		The following items are revised based on NRC comments or erratum correction.
		xii	List of Acronyms "Design Certification Document" →"Design Control Document"
		5 (3.1)	Erratum correction (b) "Invokes IEEE Std. 603-1991" → "(h) Invokes IEEE Std. 603-1991"
		10 (3.3)	Conformance to RG 1.209 is added.
		17 (4.1)	Figure 4.1-1 is modified. ・ Erratum correction "operational procedure VDU" → "operating procedure VDU" ・ The figure is changed to colored Figures.
		21 (4.1)	(11)"Operation Procedures VDU Processor" →"Operating Procedure VDU Processor"
		22 (4.1)	Description of engineering tool is modified. ・ "portable personnel computer" →"personnel computer" ・ Description for administrative control of engineering tool connection is added.
		27 (4.1)	Description of the input route for DAS signal is added.
		31 (4.2.1)	Description of the sensor inputs signal to PSMS is added.
		34 (4.2.3)	Description of SLS I/O module is modified. ・ "power interface devices" → "Power interface (PIF) modules" ・ Description of PIF modules is added.
		44 (4.2.6)	Figure 4.2-2 is changed to colored Figures.

Revision	Date	Page (section)	Description
1 (continued)		49 (4.5)	Figure 4.4-1 is modified. ・ Erratum correction "Manual RT signal for …" ・ The figure is changed to colored Figures.
		50,51 (4.5)	Figure 4.4-2 and 4.4-3 are changed to colored Figures.
		54 (5.1.7)	Erratum correction in Figure 5.1-1 "conponent" → "component"
		60 (5.2.5)	Composition of Electrical Power is modified. ・ "non-safety AC" → "safety-rerated AC" ・ Description of non-safety AC transfer is deleted. ・ "Emergency Generators through qualified isolation devices" → "Alternate Power Source"
		61,62 (5.2.5)	Figure 5.2-1, 5.2-2 and 5.2-3 are modified. ・ Transformer is changed to Safety Class in Figure 5.2-1 and 5.2-2. ・ "Emergency Generator" is changed to "Alternate AC Power Source" in Figure 5.2-3. ・ "Safety Division" and "Example of UPS for Backup Power Source" is deleted in Figure 5.2-3.
		71 (6.4.1)	Description of Engineering Tools is modified.
		82 (7.0)	Description of document availability is added.
2	December 2008		The following items are revised based on RAI response (UAP-HF-08144), and erratum correction and clarification are implemented.
		xiv	List of Acronyms ・ Balance of Plant (BOP) is added ・ "Combined Licensing" →"Combined License"
		2, 3 (3.1)	Description of conformance to GDC 15 is added to follow the response (UAP-HF-08144) to RAI-01.

Revision	Date	Page (section)	Description
2 (continued)		6 (3.1)	Erratum correction "Commision's" → "Commission's"
		7 (3.3)	The title of RG 1.97 is corrected.
		10 (3.3)	Description of conformance to RG 1.204 is added to follow the response (UAP-HF-08144) to RAI-02.
		10 (3.3)	Description of conformance to RG 1.206 is added to follow the response (UAP-HF-08144) to RAI-03.
		11 (3.4)	Description of conformance to BTP 16 is deleted to follow the response (UAP-HF-08144) to RAI-03.
		16 (4.1)	Diverse Actuation System is added to (3) Non-safety I&C list for clarification.
		16 (4.1)	"Fully multiplexed including class 1E signals" is deleted from (4) Data communication list because this was doubly described.
		17 (4.1)	Figure 4.1-1 is replaced with the one in Revision 1 of US-APWR Design Control Document Chapter 7. In addition, the configuration of communication for Operating Procedure VDU is added to follow the response (UAP-HF-08144) to RAI-10, and the note for maintenance network is added for clarification.
		18 (4.1)	Figure 4.1-2 is replaced with the one in Revision 1 of US-APWR Design Control Document Chapter 7 to ensure figure resolution for NRC electronic submittal. (Contents are not changed.)
		19 (4.1)	Figure 4.1-3 is replaced with the one in Revision 1 of US-APWR Design Control Document Chapter 7.
		21 (4.1)	Description of communication for Operating Procedure VDU is added to follow the response (UAP-HF-08144) to RAI-10.
		26 (4.1)	C (8) "Turbine Control System" is replaced with "Balance of Plant Control System" in consistence with overall system architecture (Figure 4.1-1).
		33 (4.2.2)	Bypass and override function of ESF actuation is added in consistent with Revision 1 of US-APWR Design Control Document Chapter 7.

Revision	Date	Page (section)	Description
2 (continued)		42 (4.2.5)	Description of safety function performance is modified for clarification.
		67 (6.2.1)	Figure 6.2-1 is clarified to follow the response (UAP-HF-08144) to RAI-15.
		83, 84 (7.0)	Future Licensing submittal related to GDC 15, RG1.204, RG1.206 and ESF function (4.2.2) is added to Table 7-1.
		85 (8.0)	The title of MUAP-07007 Topical Report is corrected.
		116 (C.1)	Description of Malfunction and spurious actuations from Operational VDU is added to follow the response (UAP-HF-08144) to RAI-38.

© 2008
MITSUBISHI HEAVY INDUSTRIES, LTD.
All Rights Reserved

This document has been prepared by Mitsubishi Heavy Industries, Ltd. ("MHI") in connection with its request to the U.S. Nuclear Regulatory Commission ("NRC") for a pre-application review of the US-APWR nuclear power plant design. No right to disclose, use or copy any of the information in this document, other than by the NRC and its contractors in support of MHI's pre-application review of the US-APWR, is authorized without the express written permission of MHI.

This document contains technology information and intellectual property relating to the US-APWR and it is delivered to the NRC on the express condition that it not be disclosed, copied or reproduced in whole or in part, or used for the benefit of anyone other than MHI without the express written permission of MHI, except as set forth in the previous paragraph.

This document is protected by the laws of Japan, U.S. copyright law, international treaties and conventions, and the applicable laws of any country where it is being used.

Mitsubishi Heavy Industries, Ltd.
16-5, Konan 2-chome, Minato-ku
Tokyo 108-8215 Japan

Abstract

This topical report describes the Design of the MHI digital safety systems and the Design Process that will be used for the remaining work needed to apply these systems to specific nuclear power plants. MHI seeks NRC approval of this Design and Design Process for application to the safety systems of the US-APWR and for replacement of current safety systems in operating plants. The digital safety systems were developed by MHI for nuclear power plants in Japan. For applications in the US, this report demonstrates conformance of the Design and Design Process to all applicable US Codes and Standards. These include:

- Code of Federal Regulations
- Regulatory Guides
- Branch Technical Positions
- NUREG-Series Publications
- IEEE-Standards
- Other Industry Standards

MHI's fully computerized I&C system provides significant benefits to the safety of nuclear power, such as reduction of operations and maintenance work load, which reduces the potential for human error. Based on experience in Japan, MHI's digital I&C systems improve the reliability and availability for plant operation.

To fully understand MHI's safety systems, this topical report provides an overview of MHI's overall I&C system, which includes both safety and non-safety systems. Non-safety systems are briefly described with emphasis on their interface to the safety systems. MHI's overall I&C system is categorized into four echelons, these are Human System Interface System (HSIS), Protection and Safety Monitoring System (PSMS), Plant Control and Monitoring System (PCMS) and Diverse Actuation System (DAS).

The non-safety related PCMS provides automatic controls for normal operation. The safety related PSMS provides automatic reactor trip and engineered safety features actuation. These same safety and non-safety functions may be manually initiated and monitored by operators using the HSI System, which includes both safety and non-safety related sections. The HSI System is also used to manually initiate other safety and non-safety functions that do not require time critical actuation, including safety functions credited for safe shutdown of the reactor. After manual initiation from the HSI System, all safety functions are executed by the PSMS, and all non-safety functions are executed by the PCMS. The HSI System also provides all plant information to operators, including critical parameters required for post accident conditions.

The PCMS and PSMS utilize the MELTAC digital platform which is described in a separate topical report. Maximum utilization of a common digital platform throughout a nuclear plant reduces maintenance, training and changes due to obsolescence, thereby minimizing the potential for human error. The potential for common cause failure (CCF) in these systems is minimized due to the simplicity of their basic design, the maturity of the MELTAC platform and MHI's design process (based on operation in Japan), the elevated quality programs applied to both systems, and the significant functional diversity within the numerous computers that compose these systems. Regardless of this very low potential for common cause failure, the DAS is provided to accommodate beyond design basis common cause software failures that

could adversely affect the PSMS and PCMS concurrent with operational occurrences and design basis accidents. The DAS provides diverse automation for time critical functions and diverse HSI to allow the operator to monitor critical safety functions and manually actuate safety process systems.

The information provided in this report emphasizes the safety system designs for the US-APWR. MHI expects to apply these same designs to upgrades in operating plants, with minor changes to accommodate plant specific configurations. Those changes would be described in specific Plant Licensing Documentation. The basic system descriptions, conformance to codes and standards, the design process and analysis methods are generically applicable to all applications.

MHI's I&C systems take advantage of capabilities within digital technology that were not available for analog systems. Some of these design aspects may not be readily familiar to all NRC reviewers and there may be minimum NRC or industry guidance for their review. Therefore this document puts special emphasis on the explanation of these aspects of the design and their conformance to codes and standards. The following are key examples of these areas:

a. Multi-channel operator stations
b. HSI to accommodate reduced operator staffing
c. Operation under degraded conditions
d. Integrated RPS/ESFAS with functional diversity
e. Common cause failure modes for Defense-in-Depth and Diversity (D3) analysis
f. Credit for leak detection in D3 analysis
g. Common output modules for PSMS/PCMS and DAS
h. Control system failure modes for safety analysis
i. Credit for self-diagnostics for technical specification surveillances
j. Unrestricted bypass of one safety instrument channel
k. Minimum inventory of HSI
l. Computer based procedures

MHI specifically seeks NRC approval of the design aspects identified above. However, MHI understands that complete approval of items a, b, c, e, f, k and l will require additional consideration of Human Factors Engineering and CCF coping analysis which are described in the HSI and D3 topical reports, respectively. For these items MHI seeks approval of only the I&C aspects described in this topical report.

This report distinguishes descriptions applicable to the US-APWR and descriptions for operating plants, where there is a clear need for this distinction. Where there are no distinctions, the description is generically applicable to the US-APWR and a broad range of operating plants, although not necessarily all operating plants. When this topical report is referenced for a plant specific Licensing Amendment Request, the Plant Licensing Documentation will identify any areas of this topical report that are not applicable.

Table of Contents

List of Tables
List of Figures
List of Acronyms

1.0 PURPOSE 1
2.0 SCOPE 1
3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE 2
3.1 Code of Federal Regulations 2
3.2 Staff Requirements Memoranda 6
3.3 NRC Regulatory Guides 6
3.4 NRC Branch Technical Positions 10
3.5 NUREG-Series Publications (NRC Reports) 12
3.6 IEEE Standards 12
3.7 Other Industry Standards 14
4.0 SYSTEM DESCRIPTION 16
4.1 Overall I&C System Architecture 16
4.2 Detailed Description of Safety-Related Systems 31
4.2.1 Reactor Protection System (RPS) 31
4.2.2 ESF Actuation System (ESFAS) 32
4.2.3 Safety Logic System 33
4.2.4 Safety Grade HSI System 35
4.2.5 Plant Control and Monitoring System 37
4.2.6 Diverse Actuation System 42
4.3 PSMS Self-diagnostics Features 46
4.4 PSMS Manual Testing and Calibration Features 46
4.4.1 Manual Testing 46
4.4.2 Manual Calibration 48
4.4.3 Response Time 49
4.5 PSMS On-line Maintenance 49
5.0 DESIGN BASIS 53
5.1 Key Technical Issue 53
5.1.1 Multi-Channel Operator Station 53
5.1.2 HSI to Accommodate Reduced Operator Staffing 53
5.1.3 Operation under Degraded Conditions 54
5.1.4 Integrated RPS & ESFAS with Functional Diversity 54
5.1.5 Common Cause Failure Modes for Defense-in-Depth and Diversity analysis 54
5.1.6 Credit for Leak Detection in Defense-in-Depth and Diversity Analysis 55
5.1.7 Output Module for PSMS/PCMS and DAS 55
5.1.8 Control System Failure Mode 56
5.1.9 Credit for Self-Diagnostics for Technical Specification Surveillance 56
5.1.10 Unrestricted Bypass of One Safety Instrument Channel 57
5.1.11 Minimum Inventory of HSI 57
5.1.12 Computer Based Procedures 58
5.2 General Design Features 60
5.2.1 Seismic 60
5.2.2 Environmental Qualification 60
5.2.3 Fire Protection 60

5.2.4 EMI/RFI Compatibility 61
5.2.5 Electrical Power 61
6.0 DESIGN PROCESS 64
6.1 Design Process Overview 64
6.2 Software Life Cycle Process Control 67
6.2.1 Organization 67
6.2.2 Roles and Responsibilities 67
6.3 Requirements, Implementation and Design Outputs for Software Life Cycle Process 68
6.3.1 Software Life Cycle Process Requirements 68
6.3.2 Software Life Cycle Process Implementation 70
6.3.3 Software Life Cycle Process Design Outputs 71
6.4 Life Cycle Process 71
6.4.1 Access Control 72
6.4.2 Design Change Management 72
6.4.3 Cyber Security Management 72
6.4.4 Life Cycle Management 73
6.5 Analysis Method 74
6.5.1 FMEA Method 74
6.5.2 Reliability Analysis Method 75
6.5.3 Response Time Analysis Method 76
6.5.4 Accuracy Analysis Method 77
6.5.5 Heat Load Analysis Method 79
6.5.6 Seismic Analysis Method 79
6.5.7 EMI Analysis Method 80
6.5.8 Fire Protection Analysis 81
7.0 FUTURE LICENSING SUBMITTALS 83
8.0 REFERENCES 85

Appendix A Conformance to IEEE 603-1991 86
A.1. Scope 86
A.2. Definitions 86
A.3. References 86
A.4. Safety System Designation 86
A.4.1 Design Basis Events 86
A.4.2 Safety Functions and Corresponding Protective Actions 86
A.4.3 Permissive Conditions for Each Operating Bypass Capability 86
A.4.4 Variables Required to be Monitored for Protective Action 87
A.4.5 The Minimum Criteria for Each Action Controlled by Manual Means 91
A.4.6 Spatially Dependent Variables 92
A.4.7 Range of Conditions for Safety System Performance 92
A.4.8 Functional Degradation of Safety Functions 92
A.4.9 Reliability 93
A.4.10 The Critical Points in Time or the Plant Conditions 93
A.4.11 Equipment Protective Provisions 93
A.4.12 Other Special Design Basis 94
A.5. Safety System Criteria 94
A.5.1 Single Failure Criterion 94
A.5.2 Completion of Protective Action 95
A.5.3 Quality 95
A.5.4 Equipment Qualification 95

A.5.5 System Integrity....95
A.5.6 Independence....95
A.5.6.1 Between Redundant Portions of a Safety System....95
A.5.6.2 Between Safety Systems and Effects of a Design Basis Event....96
A.5.6.3 Between Safety Systems and Other Systems....96
A.5.6.3.1 Interconnected Equipment....96
A.5.6.3.2 Equipment in Proximity....96
A.5.6.3.3 The Effects of a Single Random Failure....96
A.5.6.4 Detailed Independence Criteria....97
A.5.7 Capability for Test and Calibration....97
A.5.8 Information Displays....98
A.5.8.1 Displays for Manually Controlled Actions....98
A.5.8.2 System Status Indication....98
A.5.8.3 Indication of Bypasses....98
A.5.8.4 Location of Displays....99
A.5.9 Control of Access....99
A.5.10 Repair....99
A.5.11 Identification....99
A.5.12 Auxiliary Features....100
A.5.13 Multi-Unit Stations....100
A.5.14 Human Factors....100
A.5.15 Reliability....100
A.5.16 Common Cause Failure (IEEE 603-1998)....101
A.6. Sense and Command Features - Functional and Design Requirements....102
A.6.1 Automatic Control....102
A.6.2 Manual Control....102
A.6.3 Interaction between the Sense and Command features and other Systems....104
A.6.4 Derivation of System Inputs....104
A.6.5 Capability for Testing and Calibration....104
A.6.6 Operating Bypasses....105
A.6.7 Maintenance Bypass....105
A.6.8 Setpoint....107
A.6.8.1 Setpoint Uncertainties....107
A.6.8.2 Multiple Setpoints....107
A.7. Executive Features - Functional and Design Requirements....108
A.7.1 Automatic Control....108
A.7.2 Manual Control....108
A.7.3 Completion of Protective Action....108
A.7.4 Operating Bypass....109
A.7.5 Maintenance Bypass....109
A.8. Power Source Requirements....109

Appendix B Conformance to IEEE 7-4.3.2 -2003....110
B.1. Scope....110
B.2. References....110
B.3. Definitions and abbreviations....110
B.4. Safety System Design Basis....110
B.5. Safety System Criteria....110
B.5.1 Single Failure Criterion....110
B.5.2 Completion of Protective Action....110
B.5.3 Quality....110

B.5.3.1 Software Development 110
B.5.3.1.1 Software quality metrics 110
B.5.3.2 Software tools 110
B.5.3.3 Verification and Validation 111
B.5.3.4 Independent V&V (IV&V) requirements 111
B.5.3.5 Software configuration management 111
B.5.3.6 Software project risk management 111
B.5.4 Equipment Qualification 111
B.5.4.1 Computer system testing 111
B.5.4.2 Qualification of existing commercial computers 111
B.5.5 System Integrity 111
B.5.5.1 Design for computer integrity 111
B.5.5.2 Design for test and calibration 111
B.5.5.3 Fault detection and self-diagnostics 112
B.5.6 Independence 112
B.5.7 Capability for Test and Calibration 114
B.5.8 Information Displays 114
B.5.9 Control of Access 114
B.5.10 Repair 114
B.5.11 Identification 114
B.5.12 Auxiliary Features 114
B.5.13 Multi-Unit Stations 114
B.5.14 Human Factors 114
B.5.15 Reliability 114
B.6. Sense and Command Features - Functional and Design Requirements 114
B.7. Executive Features - Functional and Design Requirements 114
B.8. Power Source Requirements 114

Appendix C Prevention of Multiple Spurious Commands and Probability Assessment 115
C.1. Prevention of Multiple Spurious Commands 115
C.2. Probability Assessment 117

List of Tables

Table 6.5-1	Typical FMEA Table	...75
Table 7-1	Future Licensing Submittals	...83
Table A.4.4-1	Reactor Trip Variables, Ranges	...88
Table A.4.4-2	Engineered Safety Features Actuation, Variables, Ranges	...90
Table A.5.16-1	Diverse Parameters in Two Separate Controller Groups	...101

List of Figures

Figure 4.1-1	The Overall Architecture of the I&C System	...17
Figure 4.1-2	Typical HSI System Architecture in Main Control Room	...18
Figure 4.1-3	Layout of Main Control Room	...19
Figure 4.1-4	Configurations of the Reactor Protection System	...28
Figure 4.1-5	Configurations of the ESFAS,SLS, and Safety Grade HSI	...29
Figure 4.1-6	Configurations of the Reactor Trip Breakers	...30
Figure 4.2-1	Configuration of RSC/MCR Transfer System	...44
Figure 4.2-2	Electrical Independence Features between PCMS and PSMS	...45
Figure 4.4-1	Overlap Testability for Reactor Trip	...50
Figure 4.4-2	Overlap Testability for ESF Actuation	...51
Figure 4.4-3	Overlap Testability for Safety VDU	...52
Figure 5.1-1	Signal Interface of Output Module	...55
Figure 5.1-2	Configuration Example of Reactor Control System	...59
Figure 5.2-1	Safety UPS for PSMS	...62
Figure 5.2-2	Electrical Power Source for PSMS	...62
Figure 5.2-3	Non-safety UPS for PCMS	...63
Figure 5.2-4	Electrical Power Source for PCMS	...63
Figure 6.1-1	Safety System Development Process	...66
Figure 6.2-1	Organizational Structure to Control the Software Life Cycle Process	...67
Figure 6.5-1	Typical FTA for Failure of ESF Actuation	...76
Figure 6.5-2	Breakdown Response Time for Reactor Trip	...77
Figure 6.5-3	Typical Calculation Model for Channel Uncertainty of the Instrumentation Loop	...78
Figure 6.5-4	Configuration of Fire Protection for Diverse Actuation System	...82
Figure A.6.2-1	Manual Control	...103
Figure B.5.6-1	Software Isolation (Non-Safety VDU / Safety System)	...113
Figure C.2-1	Probability Assessment Flow	...117

List of Acronyms

ALR	Automatic Load Regulator
ATWS	Anticipated Transient Without Scram
AVR	Auto Voltage Regulator
BISI	Bypassed or Inoperable Status Indication
BOP	Balance of Plant
CCB	Configuration Control Board
CCF	Common Cause Failure
CDF	Core Damage Frequency
COL	Combined License
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CRDM	Control Rod Drive Mechanism
DAS	Diverse Actuation System
DMC	Date Management Console
DBA	Design Basis Accident
DC	Design Certification
DCD	Design Control Document
DHP	Diverse HSI Panel
DI	Digital Input
DO	Digital Output
ECC	Error Check and Correct memory
ECCS	Emergency Core Cooling System
EHG	Electro-Hydraulic Governor
ELM	Engineering Line Manager
EMI	Electro-Magnetic Interference
EOF	Emergency Operations Facility
EPM	Engineering Project Manager
EPS	Emergency Power Supply system
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Actuation System
FMEA	Failure Modes and Effects Analyses
FTA	Fault Tree Analysis
HDSR	Historical Data Storage and Retrieval
HSI	Human System Interface
HSIS	Human System Interface System
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
ICTS	In-Core Temperature System
ID	Identification
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
IV&V	Independent Verification and Validation
LBLOCA	Large Break Loss Of Coolant Accident

LCO	Limiting Condition for Operation
LDP	Large Display Panel
LERF	Large Early Release Frequency
LOCA	Loss Of Coolant Accident
LOOP	Loss Of Offsite Power
M/G	Motor Generator
MCR	Main Control Room
MELCO	Mitsubishi Electric Corporation
MHI	Mitsubishi Heavy Industries
MSLB	Main Steam Line Break
MTBF	Mean Time Between Failure
NIS	Nuclear Instrumentation System
OBE	Operational Basis Earthquake
PAM	Post Accident Monitor
PCMS	Plant Control and Monitoring System
PIF	Power Interface
PRA	Probabilistic Risk Assessment
PRC	Process Recording Computer
PSMS	Protection and Safety Monitoring System
QA	Quality Assurance
RCS	Reactor Coolant System
RFI	Radio Frequency Interface
RG	Regulatory Guide
RHR	Residual Heat Removal
RMS	Radiation Monitoring System
RO	Reactor Operator
RPS	Reactor Protection System
RSC	Remote Shutdown Console
RSR	Remote Shutdown Room
RT	Reactor Trip
RTA	Reactor Trip Actuation
RTB	Reactor Trip Breaker
RTD	Resistance Temperature Detector
SDCV	Spatially Dedicated Continuously Visible
SER	Safety Evaluation Report
SLS	Safety Logic System
SBO	Station Black Out
SPDS	Safety Parameter Display System
SRSS	Statistical Square Root Sum
SSA	Signal Selection Algorithm
SSE	Safe Shutdown Earthquake
SWC	Surge Withstand Capability
Tcold	reactor coolant inlet Temperature
Thot	reactor coolant outlet Temperature
TMI	Three Mile Island

TR	Topical Report
TSC	Technical Support Center
UMC	Unit Management Computer
UPS	Uninterruptible Power Supply
UV	Under Voltage
V&V	Verification and Validation
VDU	Visual Display Unit

1.0 PURPOSE

The purpose of this Topical Report is to describe the Mitsubishi Heavy Industries (MHI) Safety System and the Design Process used by MHI for that system. MHI seeks approval from the US Nuclear Regulatory Commission for the use of the MHI Safety System for new nuclear plants and for operating nuclear plants.

The Design Process described in this report is applicable to all MHI Safety Systems for either new plants or operating plants. The system descriptions are directly applicable to the MHI US-APWR. For operating plants the basic design features that ensure regulatory compliance are maintained, as described in this report. However, due to plant differences, specific changes in implementation detail will be described in Plant Licensing Documentation (e.g. License Amendment Request or Final Safety Analysis Report).

2.0 SCOPE

In this report the complete set of safety and non-safety systems is referred to as the Overall I&C System. The safety system described in this report is referred to as the Protection and Safety Monitoring System (PSMS). Description of the protective functions such as automatic initiating parameters, measured variables and assumptions in the safety analysis should be considered typical. Specific descriptions of protective functions are described in Plant Licensing Documentation.

The PSMS includes the Reactor Protection System, Engineering Safety Feature Actuation System, the Safety Logic system and the Safety Grade Human Systems Interface (HSI) System. MHI seeks approval for the PSMS including its interface to non-safety systems such as the Plant Control and Monitoring System (PCMS) and the Diverse Actuation System (DAS). These non-safety systems are described in this report only to the extent necessary to understand the PSMS interface. These non-safety system descriptions should be considered typical. Specific non-safety system descriptions are described in Plant Licensing Documentation.

The PSMS is built on the MELTAC Platform which is described in a separate Digital Platform Topical Report. In addition, the MELTAC Platform is applied to the Plant Control and Monitoring System. The MELTAC equipment applied for non-safety applications is the same design as the equipment for safety applications. However, there are differences in Quality Assurance methods for design and manufacturing.

3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE

This section identifies compliance to applicable codes and standards and conformance with applicable NRC guidance, as appropriate. Unless specifically noted, the latest version issued on the date of this document is applicable. The following terminology is used in this section:

Plant Licensing Documentation – This refers to plant level documentation that is specific to a group of plants or a single plant, such as the Design Certification Document, Combined Operating Licensing Application, Final Safety Analysis Report, or License Amendment Request.

Equipment - This refers to the components that are the subject of this Topical Report. “Equipment” includes the MHI safety related digital I&C systems and the MELCO safety related digital I&C platform. “Equipment” does not include the MHI non-safety digital I&C or HSI systems nor the MELCO non-safety digital I&C or HSI platforms. It is noted that the MHI non-safety digital I&C systems utilize the MELCO non-safety digital I&C platform which is the same as the MELCO safety related digital I&C platform. However, some QA aspects of design and manufacturing are not equivalent between safety and non-safety systems/platforms.

3.1 Code of Federal Regulations

(1) 10 CFR 50 Appendix A: General Design Criteria for Nuclear Power Plants

GDC 1 : Quality Standards and Records
The Quality Assurance program meets the requirements of 10CFR50 Appendix B.

GDC 2 : Design Bases for Protection against Natural Phenomena
This Equipment is seismically qualified. The Equipment is located within building structures that provide protection against other natural phenomena. Specific buildings and Equipment locations are described in Plant Licensing Documentation.

GDC 4 : Environmental and Dynamic Effects Design Bases
This Equipment is located in a mild environment that is not adversely effected by plant accidents.

GDC 5 : Sharing of Structures, Systems, and Components
In general, there is no sharing of this Equipment among nuclear power units. Any sharing is discussed in specific Plant Licensing Documentation.

GDC 12 : Suppression of Reactor Power Oscillations
Specific reactor trip functions implemented within this Equipment are described in Plant Licensing Documentation.

GDC 13 : Instrumentation and Control
Specific instrumentation and control functions implemented within this Equipment are described in Plant Licensing Documentation.

GDC 15 : Reactor Coolant System Design
Steady state and transient analyses are performed to assure that RCS design conditions are not exceeded during normal operation. Protection and control

setpoints implemented within this Equipment are based on these analyses. Specific analysis and setpoints are described in Plant Licensing Documentation.

GDC 17 : Electric Power Systems
The electric power sources for this Equipment and the plant components controlled by this Equipment are discussed in Plant Licensing Documentation. This document describes the interface requirements for these power sources.

GDC 19 : Control Room
This Equipment provides the safety related Human System Interfaces (HSI) for the control room. The MHI non-safety digital I&C systems and the MELCO non-safety digital I&C platform provide non-safety HSI for the control room. The Human Factors design aspects of the HSI and the control room design are described in the HSI System Topical Report.

GDC 20 : Protection System Functions
Specific protection system functions implemented within this Equipment are described in Plant Licensing Documentation.

GDC 21 : Protection System Reliability and Testability
This Equipment includes automated testing with a high degree of coverage, and additional overlapping manual test features for the areas that are not covered by automated tests. Most manual tests may be conducted with the plant on line, and with the Equipment bypassed or out of service. Equipment that cannot be tested with the plant on line can be tested with the plant shutdown. Depending on the system design for a specific plant, the Equipment is configured with N or N+1 redundancy, where N is the number of divisions needed for single failure compliance. For systems with N+1 redundancy this GDC is met with one division bypassed or out of service. The redundancy configuration for each plant system is described in other digital system licensing documentation.

GDC 22 : Protection System Independence
Redundant divisions are physically and electrically isolated to ensure that failures that originate in one division cannot propagate to other divisions. All Equipment is qualified to ensure that the Equipment is unaffected by adverse conditions that may concurrently effect multiple divisions. Interlocks between redundant divisions and administrative controls ensure maintenance is performed on one division at a time.

GDC 23 : “Protection System Failure Modes”
All detected failures are alarmed. The Reactor Trip functions are designed to fail to an actuated trip state on loss of all power, on failures that are not automatically detected, or on failures that are automatically detected and would prevent proper execution of the trip function. The Engineered Safety Features functions are designed to fail to an unactuated state. The unactuated state avoids spurious plant transients, therefore it is considered the safe state.

GDC 24 : Separation of Protection and Control Systems
Redundant divisions of the protection systems are physically and electrically isolated from the non-safety control systems. Where safety sensors are shared between control and protection systems, signal selection logic in the control system prevents erroneous control actions due to single sensor failures. Eliminating these

erroneous control actions prevents challenges to the protection system while it is degraded due to the same sensor failure. Where non-safety signals control safety systems or components, logic in the safety systems ensures prioritization of safety functions.

GDC 25 : Protection System Requirements for Reactivity Control Malfunctions
Specific functions implemented within this Equipment to protect against Reactivity Control Malfunctions are described in Plant Licensing Documentation. Specific features designed into the MHI non-safety control systems to limit the extent of Reactivity Control Malfunctions are described in Plant Licensing Documentation.

GDC 29 : Protection against Anticipated Operational Occurrences
The Equipment achieves an extremely high probability of accomplishing its safety functions through components with conservative design margins, redundancy to accommodate random failures, a quality program that minimizes the potential for design or manufacturing errors.

(2) 10CFR50.34 (f)(2) Post-TMI Requirements

- (iii) Control room
  The Human Factors design aspects of the HSI and the control room are described in the HSI System Topical Report.

- (iv) Safety Parameter Display
  The non-safety HSI systems provide safety parameter displays in the control room. Some data presented on safety parameter displays originates in this Equipment.

- (v) Bypassed and inoperable status indication
  This indication is provided by this Equipment and by the non-safety HSI system. All bypassed or inoperable signals for safety systems originate in this Equipment.

- (xi) Relief and safety valve position Indication
- (xii) Auxiliary feedwater system initiation and flow indication
- (xiii) Pressurizer heater control
- (xiv) Containment isolation systems
- (xvii)Accident monitoring instrumentation
- (xviii)Inadequate core cooling monitoring
- (xix) Instruments for monitoring plant conditions following core damage
- (xx) Pressurizer level indication and controls for pressurizer relief and block valves
  Specific functions implemented within this Equipment to meet the Post-TMI requirements, items xi thru xx above, are described in Plant Licensing Documentation.

(3) 10 CFR 50.36 Technical specifications

- (1) Safety limits, limiting safety system settings, and limiting control settings.
  This Equipment is used to maintain safety limits. The MHI non-safety control systems are used to maintain control limits.

- (2) Limiting conditions for operation.
  This Equipment is configured with N or N+1 redundancy, as discussed above for

compliance to GDC 21. For systems with N+1 redundancy there are no limiting conditions for operation (LCO) related to bypassed or out of service conditions for a single instrument channel.

- (3) Surveillance requirements
  This Equipment includes extensive automatic testing, as discussed above for compliance to GDC 21. Provisions are included for periodic surveillances to confirm the operability of the automatic test features and to manually test features of the system that are not tested automatically. Most manual tests may be conducted with the plant on line. Functions that cannot be tested with the plant on line are tested during plant shutdown. The test interval for all manual tests is based on reliability and risk based analysis.

(4) 10 CFR 50.49 Environmental Qualification of Electric Equipment Important To Safety For Nuclear Power Plants
This Equipment is located in a mild environment. A mild environment is an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences. Therefore this criteria is not applicable. This criteria is applicable to some instrumentation that interfaces to this Equipment. The qualification of this instrumentation is described in Plant Licensing Documentation.

(5) 10 CFR 50.55a

- (a)(1) Quality Standards for Systems Important to Safety
  This Equipment was originally developed under a Japanese nuclear quality program that is equivalent to 10CFR50 Appendix B. Other licensing documents describe this equivalence. An approved 10CFR 50 Appendix B quality program is now in effect for all Equipment.

- (h) Invokes IEEE Std. 603-1991
  See conformance to IEEE 603-1991

(6) 10 CFR 50.62 ATWS Rule
The Diverse Actuation System (DAS), which is used to actuate plant systems for ATWS mitigation, is described briefly in this Topical Report, and in more depth in the Topical Report for Defense in Depth and Diversity. The DAS is diverse from this Equipment, with the exception of the final module that interfaces to plant components. This common module is described in this Topical Report. The diversity between this Equipment and the DAS is described in the Topical Report for Defense in Depth and Diversity.

(7) 10 CFR 52.47

- (a)(1)(iv) Resolution of Unresolved and Generic Safety Issues
- (a)(1)(vi) ITAAC in Design Certification Applications
- (a)(1)(vii) Interface Requirements
  Conformance to the requirements in items iv thru vii, above, are described in Plant Licensing Documentation.

- (a)(2) Level of Detail
  The content of this Topical Report, together with the additional information described in other digital system Topical Reports and Plant Licensing Documentation, is sufficient to allow the NRC staff to reach a final conclusion on all safety questions associated with the design. The information includes performance requirements and design information

sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant.

- (b)(2)(i) Innovative Means of Accomplishing Safety Functions
  In the near term, the Equipment is expected to be applied to conventional I&C safety and non-safety functions typical of current operating plants and new evolutionary plants. In the longer term, the Equipment is expected to be applied to more innovative safety functions as may be typical of new passive plants. All specific plant safety functions are described in Plant Licensing Documentation.

(8) 10 CFR 52.79(c) ITAAC in Combined Operating License Applications
The inspections, tests, analyses and acceptance criteria that demonstrate that this Equipment has been constructed and will operate in conformity with the Commission's final safety conclusion, will be described in the Plant Licensing Documentation.

3.2 Staff Requirements Memoranda

(1) SRM to SECY 93-087

- II.Q Defense against Common Cause Failures in Digital I&C Systems
  Compliance is described in the Topical Report on Defense-in-Depth and Diversity.

- II.T Control Room Annunciator (Alarm) Reliability
  Alarm signals are generated from this Equipment and from MHI non-safety I&C systems. Alarm annunciators are provided by the MHI non-safety HSI system, which is internally redundant. The overall integrated design conforms to separation and independence criteria between safety divisions and between safety and non-safety divisions.

3.3 NRC Regulatory Guides

(1) RG 1.22 Periodic Testing of Protection System Actuation Functions
See GDC 21 compliance. Protection actuation functions are completely testable through a combination overlapping automatic and manual tests. Manual tests can only be conducted when a division is bypassed. Divisions are interlocked to prevent concurrent bypassing of redundant functions in more than one redundant division.

(2) RG 1.29 Revision 3 Seismic Design Classification
The Equipment is designated Seismic Category I. Specific portions of the Equipment whose continued function is not required are designated Seismic Category II. Seismic Category II Equipment is designed so that the Safe Shutdown Earthquake (SSE) will not cause a failure which will reduce the functioning of the safety function to an unacceptable level.

(3) RG 1.47 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
See compliance to 10CFR50.34 (f)(2)(v). Alarms are provided for all bypassed or inoperable safety functions; these alarms are provided on selectable displays. Spatially dedicated continuously visible alarm displays are provided for any bypassed or inoperable condition that prevents actuation of the safety function at the division level. The ability to

manually actuate bypassed or inoperable alarms at the division level is provided for conditions that are not automatically detected.

(4) RG 1.53 Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems
-endorses IEEE Std 379-2000
See compliance to GDC 21 and 24. Safety functions are designed with N or N+1 divisions. Each safety division is independent from the other safety divisions and from non-safety divisions. Independence ensures that credible single failures cannot propagate between divisions within the system and therefore can not prevent proper protective action at the system level. Single failures considered in the divisions are described in the Failure Modes and Effects Analyses (FMEA) for each system. The FMEA for the Equipment is provided in this topical report. The FMEA for specific plant applications is discussed in Plant Licensing Documentation.

(5) RG 1.62 Manual Initiation of Protective Actions
All RPS and ESFAS safety functions can be manually initiated at the system level by conventional switches located in the main control room. Additional system level manual initiation switches may also be located at the Remote Shutdown panel, depending on the specific plant design; these are described in Plant Licensing Documentation. Manual initiation requires a minimum of Equipment and the Equipment common to manual and automatic initiation paths is kept to a minimum, by bypassing automated measurement channel bistable functions. No credible single failure in the manual, automatic or common portions will prevent initiation of a protective action by manual or automatic means.

(6) RG 1.75 Physical Independence of Electric Systems
-endorses IEEE 384-1992
Redundant safety divisions are physically and electrically independent of each other and physically and electrically independent of any non-safety divisions. Physical independence is maintained either by the required distance or by barriers which prevent propagation of fire or electrical faults. Electrical independence is maintained by fiber optic cable communication interfaces or conventional isolators, such as opto-couplers, relays or transformers. Conventional isolators include fault interrupting devices such as fuses or circuit breakers. Conventional isolators prevent propagation of transverse and common cause faults from the maximum credible energy source. Fiber optic cable communication interfaces, and specifications and qualification of conventional isolators are discussed in this Topical Report.

(7) RG 1.89 Qualification for Class 1E Equipment for Nuclear Power Plants
-endorses IEEE323-1974
The environmental qualification of this Equipment is by an appropriate combination of type testing and analysis. This Equipment is located in a mild environment that is not adversely effected by plant accidents. Therefore qualification for temperature, humidity and radiation is by analysis of component specifications, room ambient conditions and heat rise calculations for the installed configuration. Seismic qualification and EMI qualification are by type testing. This Equipment has no known aging mechanisms; random failures will be detected through periodic surveillance and testing.

(8) RG 1.97 Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants
-endorses IEEE Std. 497-2002
This Equipment is used to process and display signals from accident monitoring

instrumentation of all variable types. It meets all the applicable requirements. Signals from some accident monitoring instrumentation are also transmitted from this Equipment to the non-safety HSI system for displays and alarms. Independence is maintained between all divisions. Specific accident monitoring instrumentation is described in Plant Licensing Documentation.

(9) RG 1.100 Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants
This Equipment is designated Seismic Category 1. It is designed and qualified to withstand the cumulative effects of a minimum of five (5) Operational Basis Earthquakes (OBEs) and one (1) Safe Shutdown Earthquake (SSE) without loss of safety function or physical integrity. The input spectrum is selected to envelope all anticipated applications. Conformance to this envelope for specific applications is discussed in Plant Licensing Documentation.

(10) RG 1.105 Setpoints for Safety-Related Instrumentation
-endorses ISA-S67.04-1994 and ANS-10.4-1987
The uncertainties associated with the Equipment are described in the Digital Platform Topical Report. This includes uncertainties for signal conditioning modules, signal splitters, instrument loop power suppliers and analog to digital converters. The uncertainties associated with specific process instrumentation and the resulting safety related setpoints are described in Plant Licensing Documentation. The methodology used to combine all uncertainties to establish safety related setpoints is described in this Topical Report.

(11) RG 1.118 Periodic Testing of Electric Power and Protection Systems
-endorses IEEE 338-1987
See compliance to GDC 21, 10CFR50.36 and RG 1.22. All safety functions are tested either automatically or manually. Manual tests do not require any system reconfiguration, such as jumpers or fuse removal.

(12) RG 1.151 Instrument Sensing Lines
-endorses ISA-S67.02
Compliance is described in Plant Licensing Documentation.

(13) RG 1.152 Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants
-endorses IEEE 7-4.3.2-2003
The methods used for specifying, designing, verifying, validating and maintaining software for this Equipment complies with these requirements. The life cycle process for the digital platform software is described in the Digital Platform Topical Report. The life cycle process for the system application software is described in this Topical Report. The methods used for controlling cyber threats throughout the life cycle are described in these documents.

(14) RG 1.153 1996 Criteria for Safety Systems
-endorses IEEE Std 603-1991
Compliance with the General Design Criterion identified in this Regulatory Guide is discussed above. Compliance with IEEE 603-1991 is discussed below.

(15) RG 1.168 Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

-endorses IEEE Std 1012-1998 and IEEE Std 1028-1997
This Equipment uses processes for verification, validation, reviews and audits that comply with this Regulatory Guide. The design processes for the digital platform are described in the Digital Platform Topical Report. The design processes for the digital safety systems are described in this Topical Report.

(16) RG 1.169 Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 828-1990 and IEEE Std 1042-1987
This Equipment is designed and maintained using a Configuration Management process that complies with this Regulatory Guide. The Configuration Management process for the digital platform is described in the Digital Platform Topical Report. The Configuration Management process for the digital safety systems is described in this Topical Report.

(17) RG 1.170 Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 829-1983
The test documentation for this Equipment complies with this Regulatory Guide. The test documentation for the digital platform is described in the Digital Platform Topical Report. The test documentation for the digital safety systems is described in this Topical Report.

(18) RG 1.171 Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 1008-1987
Unit testing for this Equipment complies with this Regulatory Guide. This unit testing for the digital platform is described in the Digital Platform Topical Report. Unit testing for the digital safety systems is described in this Topical Report.

(19) RG 1.172 Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 830-1993
The Software Requirements Specifications for this Equipment complies with this Regulatory Guide. The Software Requirements Specifications for the digital platform are described in the Digital Platform Topical Report. The Software Requirements Specifications for the digital safety systems are described in this Topical Report.

(20) RG 1.173 Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 1074-1995
The Software Life Cycle Process for this Equipment complies with this Regulatory Guide. The Software Life Cycle Processes for the digital platform is described in the Digital Platform Topical Report. The Software Life Cycle Processes for the digital safety systems is described in this Topical Report.

(21) RG 1.180 Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems
-endorses MIL-STD-461E, IEC 61000 Parts 3, 4, and 6, IEEE Std C62.41-1991, IEEE Std C62.45-1992, IEEE Std 1050-1996
This Equipment complies with the EMI/RFI requirements of this standard. Qualification testing for the digital platform is described in the Digital Platform Topical Report.

Requirements and features of the digital safety systems that ensure compliance to the platform qualification envelope are described in this Topical Report.

(22) RG 1.209 Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants
-endorses IEEE323-2003
This Equipment, which consists of safety-related computer-based I&C systems, is located in a mild environment. There is no change in the environment due to plant accidents. This equipment is tested and analyzed to satisfy the mild environmental qualification requirements.

(23) RG 1.204 Guidelines for Lightning Protection of Nuclear Power Plants
Conformance to RG 1.204, regarding the design of the plant's lightening protection system (LPS), is described in Plant Licensing Documentation.

(24) RG 1.206 Combined License Applications for Nuclear Power Plants
For new plant applications the level of detail needed for the NRC staff to make a final safety determination is described in Plant Licensing Documentation. This document is intended to supplement the information provided in COL (Combined License) applications. This document may be referenced directly or indirectly (via reference to a certified design which references this document).

3.4 NRC Branch Technical Positions

(1) BTP HICB-1 Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System
(2) BTP HICB-2 Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines
(3) BTP HICB-3 Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service
(4) BTP HICB-4 Guidance on Design Criteria for Auxiliary Feedwater Systems
(5) BTP HICB-5 Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors
(6) BTP HICB-6 Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode
Compliance with BTP HICB 1 thru 6, above, is described in Plant Licensing Documentation.

(7) BTP HICB-8 Guidance for Application of Regulatory Guide 1.22
All functions of the protection system are testable at power.

(8) BTP HICB-9 Guidance on Requirements for Reactor Protection System Anticipatory Trips
In general there are no non-safety anticipatory trips used in the protection system. Any exception to this will be described in Plant Licensing Documentation. If any non-safety trips are used in the protection system the following requirements are met:

- All non-safety equipment is isolated from the safety system to prevent electrical fault propagation and adverse communication interaction.
- Safety functions have priority over all non-safety functions.

- Analysis demonstrates that credible non-safety signal failures do not result in plant conditions that are outside the boundary of the safety analysis.

(9) BTP HICB-10 Guidance on Application of Regulatory Guide 1.97
The Equipment complies with this BTP for processing all instrumentation signals. However, RG 1.97 Revision 4 has superseded Revisions 2 and 3, for which this BTP was written. Therefore, where there are conflicts, the Equipment meets the requirements of RG 1.97 Revision 4.

(10) BTP HICB-11 Guidance on Application and Qualifications of Isolation Devices
-endorses IEEE Std 472, ANSI Std C62.36, ANSI Std C62.41, ANSI Std C62.45
See compliance to RG 1.75. Isolation devices are qualified in compliance to these standards.

(11) BTP HICB-12 Guidance on Establishing and Maintaining Instrument Setpoints
See compliance to RG 1.105.

(12) BTP HICB-13 Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors
The methods used for periodically verifying the accuracy and response time of RTDs complies with this standard. The method is described in Plant Licensing Documentation.

(13) BTP HICB 14 Guidance on SW Reviews for Digital Computer Based I&C Systems
-endorses IEEE Std 730
See compliance to RG 1.168 thru 1.173.

(14) BTP HICB-16 Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
This guidance was withdrawn. See compliance to RG 1.206.

(15) BTP HICB-17 Guidance on Self-Test and Surveillance Test Provisions
See compliance to GDC 21, 10CFR50.36, RG 1.22 and RG 1.118. Surveillance testing taken together with automatic self-testing provides a mechanism for detecting all failures.

(16) BTP HICB 18 Guidance on Use of Programmable Logic Controllers in Digital Computer Based I&C Systems
This Equipment is not a commercial-grade computer system; it was designed originally for nuclear safety applications in Japan. Since its development it has been deployed in numerous non-safety nuclear applications in Japan and will be deployed in nuclear safety applications in Japan in the near future. All of this operating experience in Japan is directly applicable to expected nuclear safety applications in the US.

(17) BTP HICB 19 Guidance on Evaluation of Defense in Depth and Diversity in Digital Computer Based I&C Systems
The MHI safety related digital I&C systems utilize the MELCO safety related digital I&C platform. The MHI non-safety digital I&C systems utilize the MELCO non-safety digital I&C platform. The two MELCO platforms are essentially the same, however some QA aspects of design and manufacturing are not equivalent between safety and non-safety platforms. The Defense-in-Depth and Diversity Topical Report describes the diversity within the safety and non-safety I&C systems. The report also describes the methodology for coping with a common cause failure of all of these systems and provides and example of this

methodology for one Design Basis Accident (DBA). Coping for all DBAs is described in Plant Licensing Documentation.

(18) BTP HICB 21 Guidance on Digital Computer Real Time Performance
The real-time performance for this Equipment complies with this BTP. The method for determining response time performance for the digital safety systems (including the digital platform) is described in this Topical Report. The response time performance for digital platform components is described in the Digital Platform Topical Report. Requirements for system response time for conformance with the plant design basis and the response time of actual plant systems is described in Plant Licensing Documentation.

3.5 NUREG-Series Publications (NRC Reports)

(1) NUREG-0737, Supplement 1 Clarification of TMI Action Plan Requirements
This Equipment is used for compliance with the following TMI Action Plan Requirements:
- Plant Safety Parameter Display – This Equipment provides safety related data to the MHI non-safety HSI system which provides this display for the control room and for emergency support facilities.
- Indication and Control for Safety Components (e.g. relief valves, pressurizer heaters, containment isolation valves), Inadequate Core Cooling Monitoring and Instrumentation for Accident Monitoring - This Equipment provides safety related controls and monitors safety related instruments to generate safety related displays. Alarms and non-safety displays are generated by the MHI non-safety HSI system.

(2) NUREG-0800 Chapter 7 of the USNRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Rev 4
This Equipment fulfills all safety related requirements of this NUREG for monitoring safety related plant instrumentation and controlling safety related plant components. Descriptions of specific plant systems are described in Plant Licensing Documentation.

(3) NUREG/CR-6303 Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems
The design of this Equipment is described in this Topical Report. The assessment of diversity within this Equipment and between this Equipment and other I&C systems is described in the Diversity and Defense-in-Depth Topical Report. The Diversity and Defense-in-Depth Topical Report also describes the method of coping with common cause failure vulnerabilities.

(4) NUREG/CR-6421 A Proposed Acceptance Process for Commercial-Off-the-Shelf (COTS) Software in Reactor Applications
This NUREG is not applicable to this Equipment since there is no COTS software. All software has been designed for nuclear applications.

3.6 IEEE Standards

(1) IEEE 7-4.3.2 2003 Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations
This Equipment conforms to all requirements of this standard, as augmented by RG 1.152, including key requirements for:
- Software quality and life cycle processes

- Independent Verification and Validation
- Communications independence

A detailed discussion of compliance to all aspects of IEEE7-4.3.2 is provided in Appendix B.

(2) IEEE 323 2003 Qualifying Class 1E Equipment for Nuclear Power Generating Systems
This Equipment is qualified in compliance with this standard, as augmented by RG 1.89.

(3) IEEE 338 1987 Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
This Equipment conforms to this standard, as augmented by RG 1.22.

(4) IEEE 344 1987 Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
This Equipment conforms to this standard as augmented by RG 1.100.

(5) IEEE 379 2000 Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems
This Equipment conforms to this standard as augmented by RG 1.53.

(6) IEEE 383 1974 Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations
The cable and electrical connections used within this Equipment and between this Equipment conform to this standard, including requirements for flame retarding qualification requirements. Cables for interfaces to/from this equipment to other I&C systems and components are discussed in Plant Licensing Documentation.

(7) IEEE 384 1992 Criteria for Independence of Class 1E Equipment and Circuits
This Equipment conforms to this standard as augmented by RG 1.75. All safety functions are implemented within multiple divisions with physical separation and electrical independence between redundant safety divisions and between safety and non-safety divisions. Electrical independence is accomplished primarily through the use of fiber optic technology. Independence of electrical circuits is accomplished with isolators and physical separation or barriers, such as conduits.

(8) IEEE 420 1982 Design and Qualification of Class 1E Control Board, Panels and Racks.
Standard enclosures for this Equipment conform to this standard. These enclosures are described in this Topical Report. Other enclosures, including any deviations from this standard, are described in Plant Licensing Documentation.

(9) IEEE 472 IEEE Guide for Surge Withstand Capability (SWC) Tests
As stated in BTP HICB-11, this standard is currently intended for electrical protective relaying applications; it is not intended for digital systems. Therefore this Equipment complies with the surge withstand requirements of ANSI C62.41 and ANSI C62.45.

(10) IEEE 494 1974 Method for identification of Documents Related to 1E Equipment.
The documentation for this Equipment conforms to this standard by having the term “Nuclear Safety Related” applied on the face of each document and drawing that is provided to the licensee. Generic documents and drawings used only for internal use by MHI do not contain this designation.

(11) IEEE 497 2002 Accident Monitoring Instrumentation for Nuclear Power Generating Stations
See compliance for RG 1.97.

(12) IEEE 603 1991 Safety Systems for Nuclear Power Generating Stations
1998 version is currently not endorsed by NRC
This Equipment conforms to this standard, as augmented by RG 1.153, including key requirements for:

- Single failures
- Completion of Protective Action
- Quality
- Qualification
- Independence
- Testability
- Monitoring and Information
- Bypasses

A detailed discussion of compliance to all aspects of IEEE603 is provided in Appendix A.

(13) IEEE 730 1989 Software Quality Assurance Plans

(14) IEEE 828 1990 IEEE Standard for Software Configuration Management Plans

(15) IEEE 829 1983 Software Test Documentation

(16) IEEE 830 1993 IEEE Recommended Practice for Software Requirements Specifications

(17) IEEE 1008 1987 IEEE Standard for Software Unit Testing

(18) IEEE 1012 1998 IEEE Standard for Software Verification and Validation Plans (2004 not yet endorsed by NRC)

(19) IEEE 1016 1987 IEEE Recommended Practice for Software Design Descriptions

(20) IEEE 1028 1997 IEEE Standard for Software Reviews and Audits

(21) IEEE 1042 1987 IEEE Guide To Software Configuration Management

(22) IEEE 1074 1995 IEEE Std for Developing Software Life Cycle Processes
1997 version not yet endorsed by NRC
The software design process and documentation for this Equipment conforms to the requirements of IEEE 730 thru 1074, above.

3.7 Other Industry Standards

(1) ANS-10.4 1987 Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry
The computer programs used to develop setpoints for this Equipment conform to this standard, as endorsed by RG 1.105.

(2) ANSI C62.41 IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits
This Equipment complies with the sections of this standard endorsed by RG 1.180.

(3) ANSI C62.45 IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits
This Equipment complies with the sections of this standard endorsed by RG 1.180.

(4) IEC 61000 Electromagnetic compatibility (EMC)
This Equipment complies with the following sections of this standard:
- IEC 61000-4-2: Testing and measurement techniques - Electrostatic discharge immunity tests. Basic EMC publication
- IEC 61000-4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test. Basic EMC publication
- IEC 61000-4-5: Testing and measurement techniques - Surge immunity test
- IEC 61000-4-12: Testing and measurement techniques - Oscillatory waves immunity test.

(5) ISA-S67.04 1994 Setpoints for Nuclear Safety Related Instrumentation Used in Nuclear Power Plants
See compliance to RG 1.105. The methodology used to develop setpoints for this Equipment conforms to this standard, as endorsed by RG 1.105.

(6) MIL-STD-461E Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment
This Equipment complies with this standard as referenced in RG 1.180. This standard replaces MIL-STD-461D and MIL-STD-462D.

4.0 SYSTEM DESCRIPTION

Nuclear power plant instrumentation senses various plant parameters and transmits appropriate signals to the control systems during normal operation, and to the reactor trip and engineered-safety feature systems during abnormal and accident conditions.

The instrumentation and control (I&C) systems presented in this Topical Report provide protection against unsafe reactor operation during steady-state and transient power operation. The primary purpose of the I&C systems is to provide automatic initiating signals, automatic and manual control signals, and monitoring displays to mitigate the consequences of faulted conditions.

Descriptions are given in Section 4.1 for the Overall I&C System architecture, Section 4.2 for the more detail system description of safety-related systems, Section 4.3 for the self-diagnostics features, Section 4.4 and 4.5 for the testability features.

4.1 Overall I&C System Architecture

The MHI Overall I&C System is fully digital. It has been developed and applied in a step-by-step approach in Japanese PWR plants.
General specifications of the Overall I&C System are summarized below:

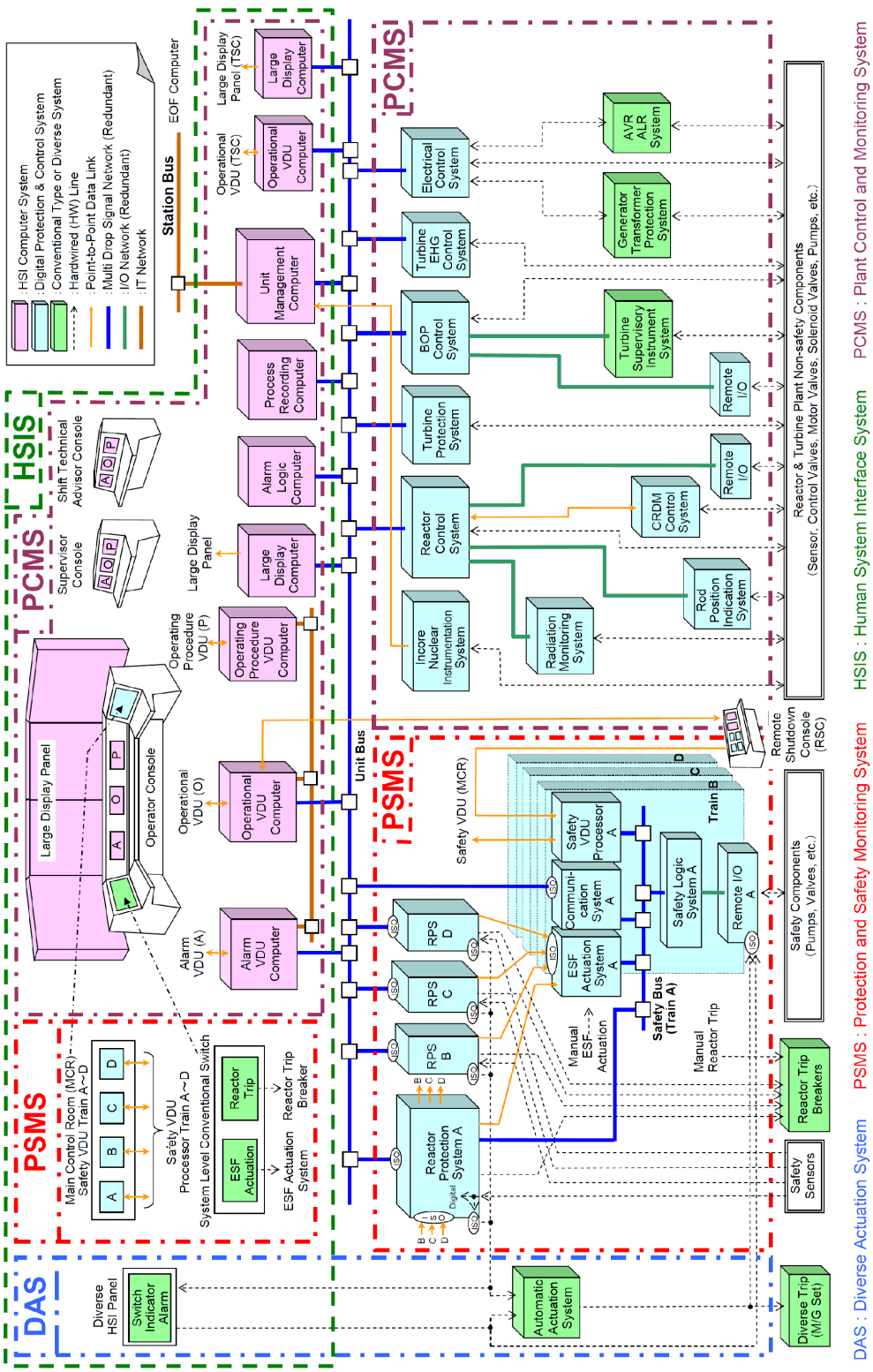
(1) Main control board
- Fully computerized
- Consists of safety Visual Display Units (VDU) and non-safety VDU
- Minimal conventional switch, only for regulatory compliance (e.g. RG 1.62)

(2) Safety I&C
- Fully digital
- Consists of Mitsubishi Electric Corporation (MELCO) MELTAC Platform
- Four train redundant Reactor Protection System
- Four train redundant ESF Actuation System
- Four train redundant Safety Logic System for component control
- Four train redundant Safety Grade HSI System

(3) Non-safety I&C
- Fully digital
- Consists of MELTAC Platform
- Duplex redundant digital architecture for each control and process monitoring sub-system
- Diverse Actuation System

(4) Data communication
- Fully multiplexed including class 1E signals
- Consists of multi-drop data bus and serial data link
- Uses fiber optics communication networks for noise immunity and isolation between redundant safety divisions and between safety and non-safety systems

The architecture of the Overall I&C System is shown in Figure 4.1-1.



Note: Each train of the PSMS and the PCMS has maintenance network per division.

Figure 4.1-1 The Overall Architecture of the I&C System

The Overall I&C System consists of the following four echelons as illustrated in Figure 4.1-1;

a. Human System Interface (HSI) System
b. Protection and Safety Monitoring System (PSMS)
c. Plant Control and Monitoring System (PCMS)
d. Diverse Actuation System (DAS)

The following sections summarize the function of each I&C echelon in Figure 4.1-1.

a. Human System Interface (HSI) System

This section provides an overview of the complete HSI System, which includes the HSI portions of the Protection and Safety Monitoring System, the Plant Control and Monitoring System and the Diverse Actuation System. The hardware and software aspects of the HSI portion of the Protection and Safety Monitoring System are described in detail in this Topical Report. The Human Factors Engineering aspects and the detail functional design of the complete HSI System are also described in the HSI System Topical Report.

Figure 4.1-2 and 4.1-3 show the typical HSI system architecture in Main Control Room (MCR) and the layout of the MCR respectively. The actual MCR layout design for a specific plant is described in Plant Licensing Documentation. The following sections describe the major components of the HSI echelon:

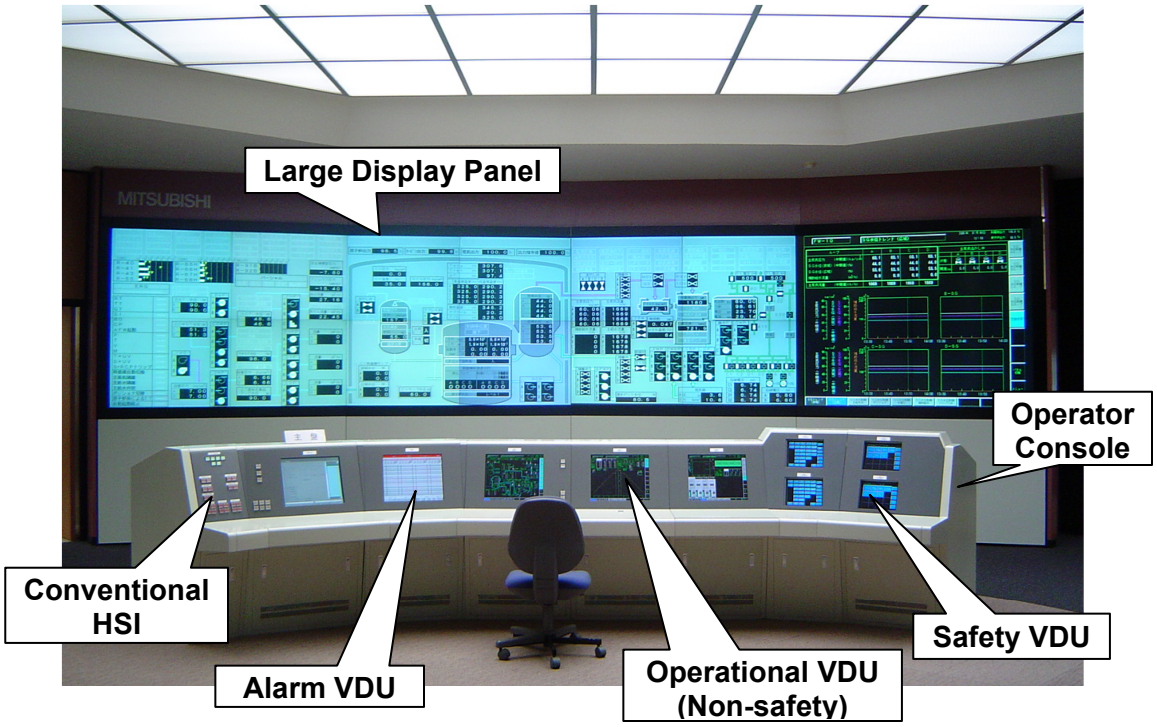


Figure 4.1-2 Typical HSI System Architecture in Main Control Room

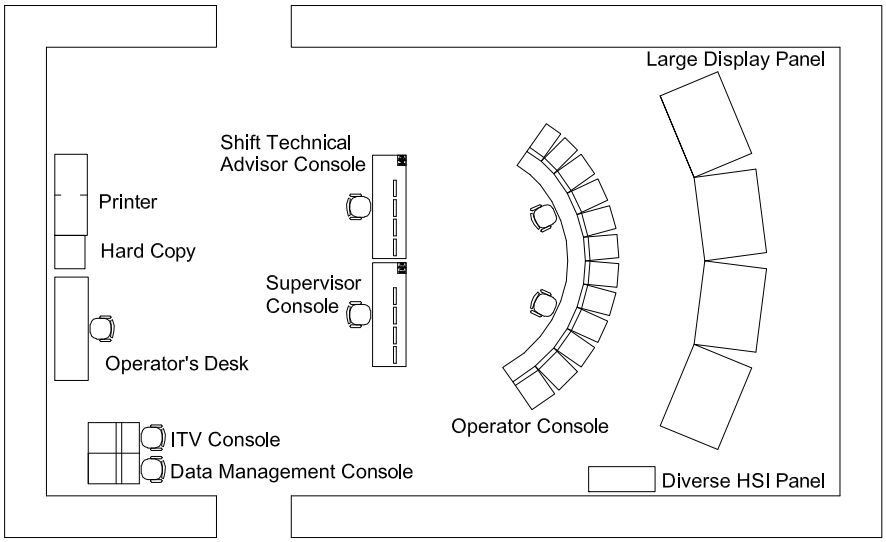


Figure 4.1-3 Layout of Main Control Room

(1) Operator Console

Plant information and controls (i.e. for all safety and non-safety divisions) are displayed and accessed on the non-safety Operational VDU screens of the Operator Console. All operations from the Operator Console are available using touch screens or other pointing devices on the non-safety Operational VDUs. Safety VDUs on the Operator Console provide access to safety information and controls using touch screens. There is one or more Safety VDU for each safety train.

Conventional switches for system level actuation are also installed on the Operator Console. The typical hardwired functions are below.

- Reactor trip
- Emergency core cooling system (ECCS) actuation
- Turbine trip
- Containment vessel spray actuation
- Containment vessel isolation
- Main steam line isolation
- Main control room ventilation isolation

In conformance with RG 1.62, the switches for the safety functions identified have hardwired signal paths that bypass as much computer based processing as is practical. This is discussed in more detail in subsequent sections.

For the US-APWR the Operator Console allows one Reactor Operator (RO) to control the plant under all normal and abnormal plant conditions, except conditions where the HSI System itself is degraded. The Operator Console will also accommodate continuous operation by two ROs. Operation by one or two ROs is at the discretion of the utility. Operation with one or two ROs and operation under degraded HSI conditions is discussed in the HSI System Topical Report. The number of operators accommodated at the Operator Console design for other plants and operation under degraded HSI conditions for other plants is described in Plant Licensing Documentation.

(2) Large Display Panel

The Large Display Panel includes sufficient Spatially Dedicated Continuously Visible (SDCV) indications and alarms, so that the total status of the plant can be easily accessed without requesting VDU screens on the Operator Console. Important information for normal operation and important information for emergency or accident conditions are displayed on the Large Display Panel. Easy and reliable comprehension for all operating crew members is achieved from the information on this panel by continuously displaying high level plant conditions.

The Large Display Panel also includes a variable display which is selectable by the operation crew members. The operation crew members can share this information to enhance crew interaction and coordination.

(3) Supervisor Console

The Supervisor Console is designed for use by the main control room supervisor (i.e. Senior Reactor Operator). The Supervisor Console has the same non-safety VDU screens with the same operational capability as on the Operator Console. However, normally the Supervisor Console has monitoring capability only. All operation displays are selectable from the VDUs with touch screens or other pointing devices.

(4) Shift Technical Advisor Console

The Shift Technical Advisor Console is for the safety engineer. It is located in the Main Control Room (MCR). The Shift Technical Advisor Console has the same non-safety VDU screens with the same operational capability as the Operator Console. However, normally the Shift Technical Advisor Console has monitoring capability only. All operation displays are selectable from VDUs with touch screens or other pointing devices.

(5) Diverse HSI Panel

The Diverse HSI Panel consists of some conventional back-up switches and indicators. The Diverse HSI Panel is used in the case of a common cause failure of the safety and non-safety digital I&C systems.

(6) Process Recording Computer (PRC)

The Process Recording Computer provides historical data storage and retrieval (HDSR) functions. The system records process trends and all binary transitions such as alarms, equipment state changes etc. Historical data from the Process Recording Computer is accessible in the MCR on the Data Management Console (DMC).

(7) Alarm Logic Processor

The Alarm Logic Processor receives alarm signals from the safety and non-safety I&C equipment. This processor classifies these alarms according to their priority and their acknowledgement status, and transmits alarm status information to the Alarm VDU Processor and Large Display Panel Processor.

(8) Unit Management Computer (UMC)

The Unit Management Computer performs plant performance calculations, including core monitoring and fuel management applications. It also compiles data to create daily operations reports. Calculation results and reports are accessible in the MCR on the Data Management Console (DMC).

(9) Operational VDU Processor

The Operational VDU Processor manages information and graphic displays for the non-safety Operational VDUs located on the Operator Console, Shift Technical Advisor Console Supervisor Console and Remote Shutdown Console. It also receives operator commands such as screen navigation and soft control from the Operational VDUs.

(10) Alarm VDU Processor

The Alarm VDU Processor manages the displays for the Alarm VDUs located on the Operator Console, Shift Technical Advisor Console, and Supervisor Console. It also receives operator commands such as screen navigation and alarm acknowledgement from the Alarm VDUs.

(11) Operating Procedure VDU Processor

The Operating Procedure VDU Processor manages the displays for the Operating Procedure VDU located on the Operator Console, Shift Technical Advisor Console and Supervisor Console. It also receives operator commands such as procedure navigation, from the Operating Procedure VDU and Alarm VDU. The Operating procedure VDU communicates with the Operational VDU processors and the Alarm VDU processors.

(12) Large Display Processor

The Large Display Panel Processor manages the displays on the Large Display Panel.

(13) Safety VDU Processors

The Safety VDU Processors manage the displays on the Safety VDUs located on the Operator Console and the Remote Shutdown Console. They also receive operator commands such as screen navigation and soft control from the Safety VDUs. There is one Safety VDU Processor for each safety train, each located in separate fire area.

(14) Remote Shutdown Console (RSC)

The Remote Shutdown Console is used for achieving and maintaining safe shutdown conditions in the event that the MCR is not available due to any conditions, including fire which results in catastrophic damage to I&C equipment located in the MCR. For the US-APWR safe shutdown is defined as Cold Shutdown. The safe shutdown condition for other plants is defined in Plant Licensing Documentation.

The Remote Shutdown Console has the same non-safety VDU screens with the same operation, alarm and procedure capability as on the Operator Console. The Remote Shutdown Console also provides Safety VDUs for each safety train with the same operational capability as on the Operator Console.

(15) Technical Support Center (TSC) Computer

The TSC Computer provides plant data displays to assist in the analysis and diagnosis of abnormal plant conditions. The information available at the TSC is a subset of the same information available in the MCR.

(16) Emergency Operations Facility (EOF) Computer

The EOF Computer provides plant data displays to assist in the diagnosis of abnormal plant conditions and to evaluate the potential or actual release of radioactive materials to the environment. The information available at the EOF is a subset of the same information available in the MCR. The EOF computer also sends plant parameters to the NRC.

(17) Data Management Console (DMC)

The DMC is a common terminal unit of the UMC and PRC. The DMC display shows calculation results and reports which were provided by the UMC and historical information stored from the PRC.

(18) Engineering Tool

The Engineering Tool is a personnel computer. It is used for diagnosing module failures in the PSMS. It is also used for software maintenance and some periodic testing. Connections between the Engineering tool and the PSMS are electrically and functionally isolated. In addition, when a PSMS Controller is turned to the enable status to allow software changes from the Engineering Tool appropriate administrative controls are adopted as follows:

- Alarms are generated in the MCR for the Controller that is enabled for software changes.
- The Controller that is enabled for software changes is declared inoperable by plant Technical Specifications.

The use of the Engineering Tool is described in various sections, below.

b. Protection and Safety Monitoring System (PSMS)

The PSMS is discussed in detail in subsequent sections. This section provides a brief overview.

The PSMS encompasses all safety related I&C systems in the plant with the exception of some special instrumentation systems (e.g. neutron monitoring) and special purpose

controllers (e.g. Emergency Generator engine controls). The PSMS interfaces with these other safety related systems and components.

The following sections describe the major systems and components within the PSMS echelon:

(1) Reactor Protection System (RPS)

The Reactor Protection System has a configuration of four redundant trains, with each train located in a separate I&C equipment room. Each train receives process signals, including NIS (nuclear instrumentation system) and safety RMS (plant radiation monitoring system), from safety-related field sensors. These sensors are used for monitoring of critical safety functions, including post accident monitoring, for monitoring and control of plant safety systems and for reactor trip and ESF actuation. The logic functions within the RPS are limited to bi-stable calculations and voting for reactor trip and engineered safety features actuation.

Each train performs two-out-of-four voting logic for like sensor coincidence to actuate trip signals to the four trains of the Reactor Trip Breakers and actuate ESF signals to the four trains of the ESF Actuation System. Each train also includes a hardwired manual switch on the Operator Console to directly actuate the Reactor Trip Breakers. This switch bypasses the RPS digital controller.

This is a microprocessor based digital system that achieves high reliability through segmentation of primary and back-up trip/actuation functions, redundant 4 trains, failed equipment bypass functions, and microprocessor self-diagnostics, including data communications.

The system also includes features to allow manual periodic testing of functions that are not automatically tested by the self-diagnostics, such as actuation of reactor trip breakers. Manual periodic tests can be conducted with the plant on-line and without jeopardy of spurious trips due to single failures during testing.

Figure 4.1-4 shows the configuration of the Reactor Protection System. Figure 4.1-5 shows the configuration of the ESFAS, SLS, and Safety Grade HSI System, which are described below.

(2) ESF Actuation System (ESFAS)

The ESF Actuation System has up to four redundant trains, with each train located in a separate I&C equipment room. The number of trains corresponds with the number of ESF system trains in the plant.

Each ESFAS train receives the output of the ESF actuation signals from the all four trains of the Reactor Protection System. Each train receives manual train level actuation signals from corresponding train level switches on the Operator Console. There are two conventional switches for each train hardwired from the Operator Console to the ESFAS. Each ESF Actuation System train performs two-out-of-four voting logic for like system level coincidence to automatically actuate train level ESF actuation signals for its respective train of the Safety Logic System. Each ESF Actuation System train performs two-out-of-two voting logic for signals from the manual actuation switches on the Operator Console. The

ESF Actuation Systems also provides automatic load sequencing for the Safety Emergency Generators to accommodate the Loss of Offsite Power (LOOP) accident. Safety plant components are manually loaded on the non-safety Alternative Generator from the Safety Logic System for Station Blackout conditions.

This is a microprocessor based system that achieves high reliability through redundancy within each train and microprocessor self-diagnostics, including data communications. The system also includes features to allow manual periodic testing of functions that are not automatically tested by the self-diagnostics, such as manual system level actuation inputs. Manual periodic tests can be conducted with the plant on-line and without jeopardy of spurious system level actuation due to single failures during testing.

(3) Safety Logic System (SLS)

The Safety Logic System has one train for each plant process train. For the US-APWR there are four trains for some plant systems and two trains for others. The number of trains for other plants is described in Plant Licensing Documentation.

Each train of the Safety Logic System receives ESF system level actuation demand signals and LOOP load sequencing signals from its respective train of the ESF Actuation System. The Safety Logic System also receives manual component level control signals from the Operator Console and Remote Shutdown Console (Safety VDUs and Operational VDUs), and manual component level control signals from the hardwired back-up switches on the Diverse HSI Panel. The SLS also receives process signals from the RPS for interlocks and controls of plant process systems. This system performs the component-level control logic for safety actuators (e.g. motor-operated valves, solenoid operated valves, switchgear etc.)

The SLS controllers for each train are located in separate I&C equipment rooms. The system has conventional I/O portions and I/O portions with priority logic to accommodate signals from the Diverse Actuation System (which is discussed below). To minimize field cabling, the I/O for each train in the US-APWR is remotely distributed throughout the plant in close proximity to safety actuators. The location of the I/O for other plants is described in Plant Licensing Documentation.

This is a microprocessor based system that achieves high reliability through redundancy within each train and microprocessor self-diagnostics, including data communications. The system also includes features to allow periodic testing of functions that are not automatically tested by the self-diagnostics, such as final actuation of safety components. Manual periodic tests can be conducted with the plant on-line and without jeopardy of spurious system level actuation due to single failures during testing.

(4) Safety Grade HSI System

The Safety Grade HSI system consists of conventional hardwired switches for manual actuation of Reactor Trip and ESF actuation signals, and Safety VDUs and Processors which provide Post Accident Monitoring indications and manual controls and status indications for all components in safety related process systems.

Each train of the Safety Grade HSI System interfaces with the corresponding trains of all other systems within the PSMS. There are Safety Grade HSI components for each train located on the Operator Console and the Remote Shutdown Console. The Safety VDUs

and switches for each train are isolated from each other. The Safety VDUs and switches at the Operators Console and the Remote Shutdown Console are also isolated from each other and from the controllers in the PSMS to ensure that HSI failures that may result from a fire in one location cannot adversely affect the HSI in the alternate location.

(5) Reactor Trip Breakers

When a limit is approached, the RPS initiates signals to open the Reactor Trip Breakers. This action removes power to the control rod drive mechanism coils permitting the rods to fall by gravity into the core. This rapid negative reactivity insertion will cause the reactor to shutdown.

Figure 4.1-6 illustrates the configuration of the reactor trip breakers. The breakers are located 2 separated rooms.

c. Plant Control and Monitoring System (PCMS)

The PCMS encompasses all non-safety related I&C systems in the plant with the exception of special purpose controllers (e.g. Alternate Generator engine controls). The PCMS interfaces with these other non-safety related systems and components so there is only one fully integrated HSI system in the MCR.

The following sections describe the major systems within the PCMS echelon:

(1) Reactor Control System

The Reactor Control System receives non-safety field sensor signals. This system also receives status signals from plant process components and manual operation signals from the Operator Console to control and monitor the NSSS process components. This system controls continuous control components, such as modulating air operated valves, and discrete state components such as motor-operated valves, solenoid-operated valves, pumps etc.

This is a microprocessor based system that achieves high reliability through segmentation of process system groups (e.g. pressurizer pressure control, feedwater control, rod control etc.), redundancy within each segment, and microprocessor self-diagnostics, including data communications.

(2) Radiation Monitoring System

The Radiation Monitoring System is a microprocessor based system that monitors plant process radio-activity and area radiation level.

(3) Rod Position Indication System

The Rod Position Indication System is a microprocessor based system that monitors control rod position. It detects dropped rods and misalignment of control rods. The system consists of processing equipment located in the I&C equipment room. For the US-APWR remote I/O is located inside the containment vessel. The location of remote I/O for other plants is described in Plant Licensing Documentation.

(4) Control Rod Drive Mechanism (CRDM) Control System

The CRDM Control System is a microprocessor based system that receives control rod direction and speed demand signals from the Reactor Control System and manual operation signals from the Operator Console. This system outputs signals to control the electro-magnetic coil sequencing within the CRDMs.

(5) In-Core Neutron Instrumentation System

The In-core Neutron Instrumentation System is a microprocessor based system that provides remote data acquisition for in-core detector signal monitoring.

The In-core Neutron Instrumentation is top-mounted. In-core detectors are inserted into the core through detector guide thimbles which lead to the fuel assemblies and cover the effective axial fuel length. The In-core detectors are horizontally distributed over the entire core at approximately 40 locations. The In-core detectors provide signals for the measurement of core power distribution.

(6) Turbine Protection System

The Turbine Protection System receives signals regarding the turbine-generator and provides appropriate trip actions when it detects undesirable operating conditions of the turbine-generator.

This is a microprocessor based system that achieves high reliability through redundancy within the system and microprocessor self-diagnostics.

(7) Turbine EHG (Electro-Hydraulic Governor) Control System

The Turbine EHG Control System consists of redundant microprocessors and several hardwired logic parts (servo controller etc.). The system has a speed control unit, a load control unit, an over-speed protection unit and an automatic turbine control unit. This system is used, either for control or for supervisory purposes.
This is a microprocessor based system that achieves high reliability through redundancy and microprocessor self-diagnostics.

(8) Balance of Plant Control System

The Balance of Plant (BOP) control system controls BOP systems such as service water, circulating water, feedwater, turbine control, HVAC, and non-essential component cooling water. The system receives inputs from field process instrumentation and manual operation signals from the Operator Console to control and monitor modulating control valves, and discrete components such as motor operated valves, solenoid operated valves, and pumps.

This is a microprocessor based system that achieves high reliability through segmentation of process systems groups, redundancy within each segment, and microprocessor self-diagnostics, including data communications.

(9) Turbine Supervisory Instrument System

The Turbine Supervisory Instrument system monitors important parameters of the turbine such as vibration, rotor position, etc.

(10) Electrical Control System

The Electrical Control System controls and monitors the electrical system and components.

This is a microprocessor based system that achieves high reliability through redundancy within the system and microprocessor self-diagnostics.

(11) Generator Transformer Protection System

The Generator Transformer Protection System provides a generator trip in case of receiving a turbine trip signal. This system also controls related components (breaker) in case of undesirable operating conditions of the generator and transformer.

(12) Auto Voltage Regulator (AVR)/Automatic Load Regulator (ALR) System

The AVR/ALR System provides regulation of generator voltage.

d. Diverse Actuation System

For coping with common cause failures (CCF) in the software of the PSMS and PCMS, the Diverse Actuation System (DAS) provides monitoring of key safety parameters and back-up automatic/manual actuation of the safety and non-safety components required to mitigate anticipated operational occurrences and accidents.

The DAS consists of hardwired or digital components which are diverse from the MELTAC Platform which is used in the PSMS and PCMS, so that a postulated CCF in these digital systems will not impair the DAS function.

The DAS is classified as a non-safety system. The DAS shares sensor inputs with the PSMS through analog interfaces that are not subject to the postulated CCF in the PSMS. Interfaces to safety process inputs and the Safety Logic System outputs are isolated within the safety systems through qualified conventional isolators.

The DAS provides manual system level actuation controls for critical safety functions. Where the time is insufficient for manual operator action, the DAS provides automatic actuation of the plant safety functions needed for accident mitigation.

The DAS is fully described in the Defense-in-Depth and Diversity Topical Report.

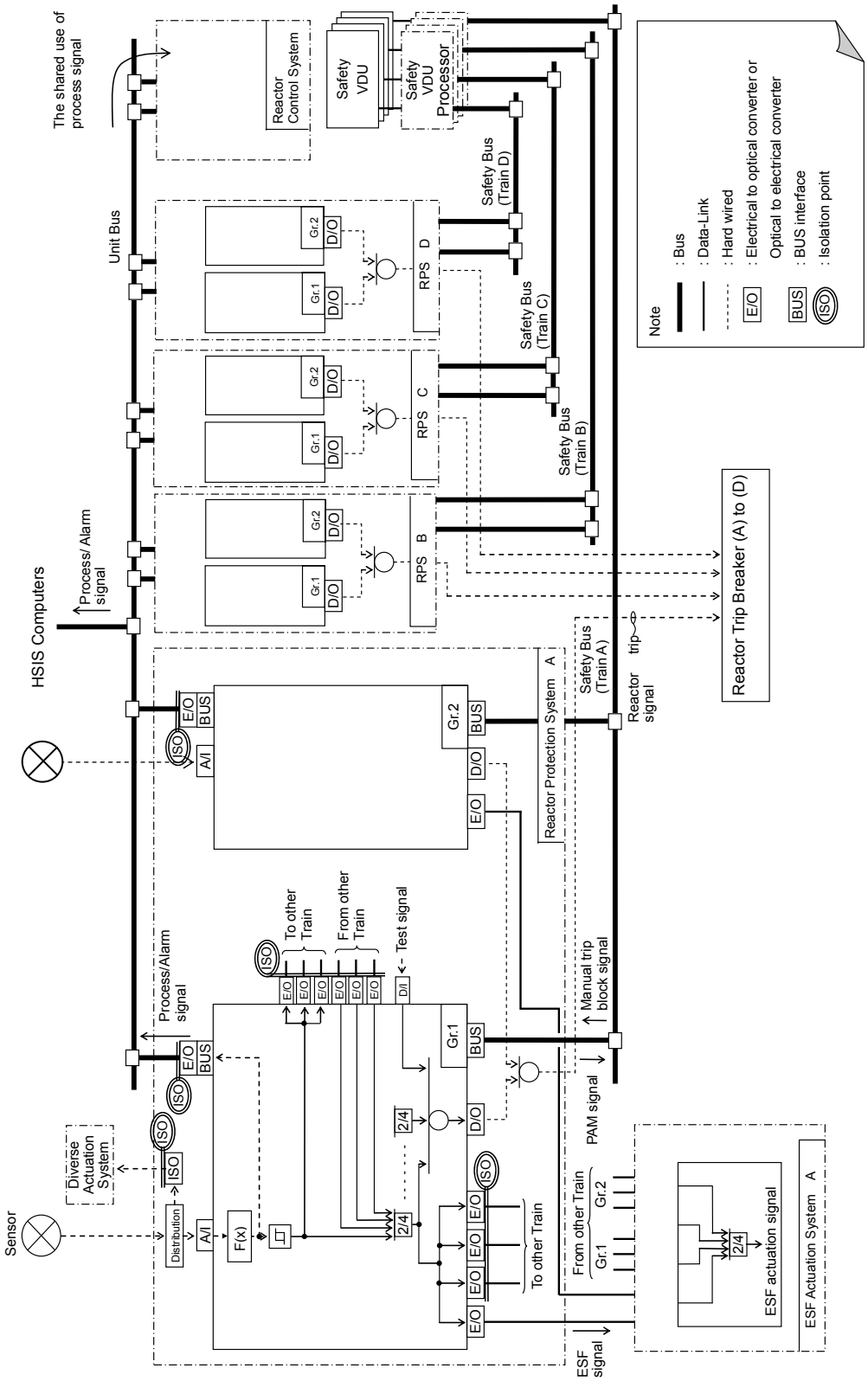


Figure 4.1-4 Configurations of the Reactor Protection System

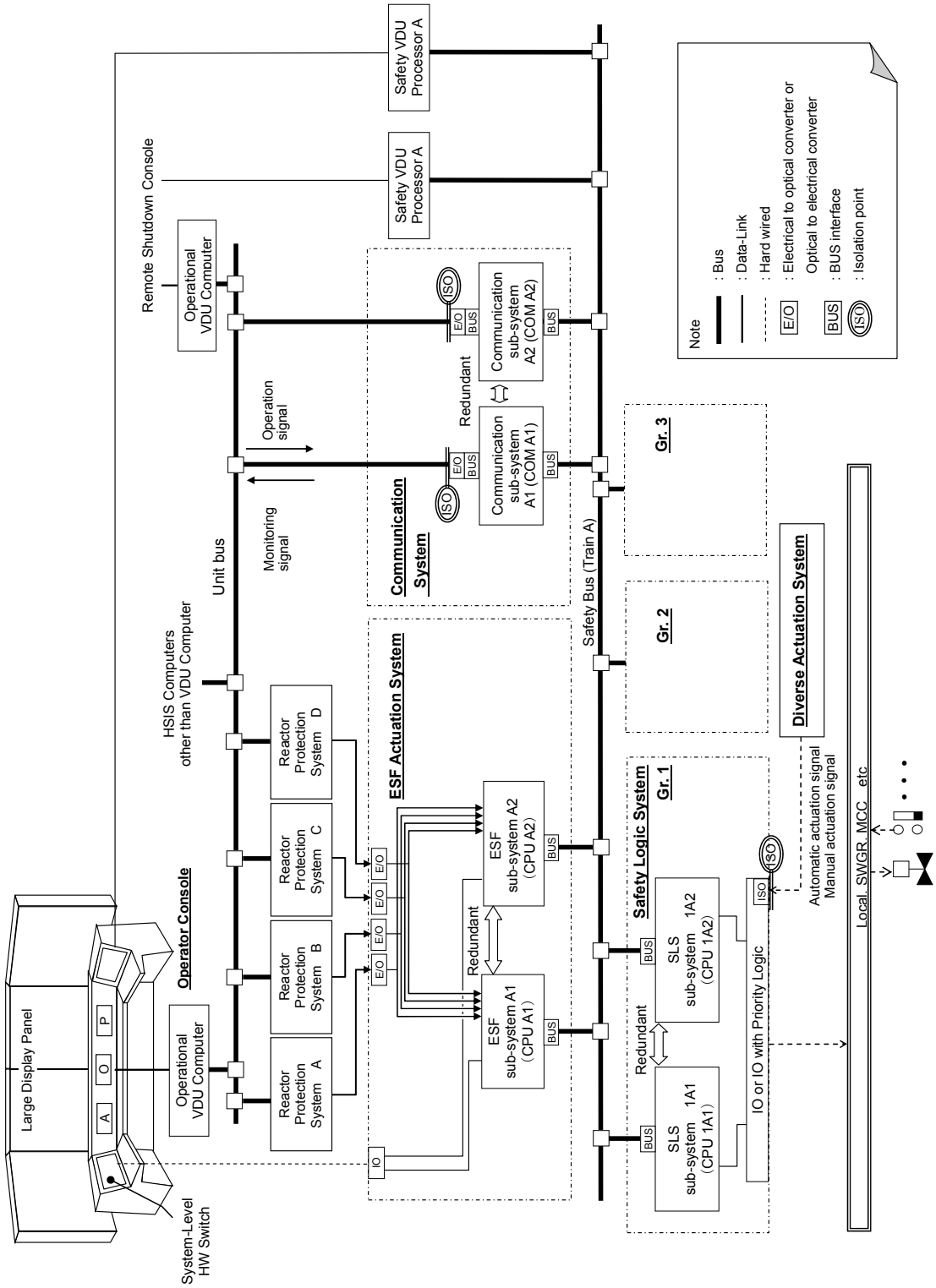


Figure 4.1-5 Configurations of the ESFAS, SLS, and Safety Grade HSI

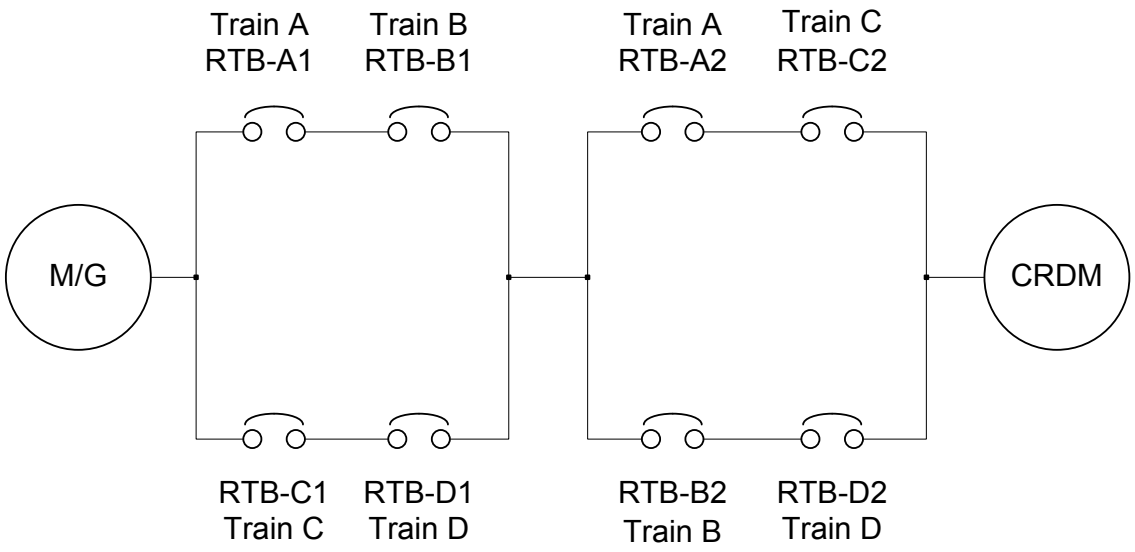


Figure 4.1-6 Configurations of the Reactor Trip Breakers

4.2 Detailed Description of Safety-Related Systems

4.2.1 Reactor Protection System (RPS)

a. Reactor Trip Function in RPS

The RPS automatically prevents operation of the reactor in an unsafe region by shutting down the reactor whenever the limits of the safe region are approached. The safe operating region is defined by several considerations such as mechanical/hydraulic limitations on equipment, and heat transfer phenomena. The RPS maintains surveillance of process variables which are direct measurements of equipment mechanical limitations, such as pressure and also on variables which are direct measurements of the heat transfer capability of the reactor (e.g. reactor coolant flow and reactor coolant temperatures). Other parameters utilized in the RPS are calculated indirectly from a combination of process variables, such as delta T. Whenever a direct process measurement or calculated variable exceeds a setpoint the reactor will be shutdown in order to protect against either gross damage to fuel clad or loss of system integrity which could lead to release of radioactive fission products into the containment vessel.

To initiate a reactor trip, the RPS interfaces to the following equipment:

- Sensors and manual inputs
- Reactor Trip Breakers

The RPS consists of four redundant and independent trains. Normally, four redundant measurements using sensors from the four separate trains are made for each variable used for reactor trip. Selected analog measurements are converted to digital form by analog-to-digital converters within the four trains of the RPS. Signal conditioning may be applied to selected inputs following the conversion to digital form. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a given parameter is generated if one train's measurement exceeds its limit. Processing on all variables for reactor trip is divided into two subsystems in each of the four redundant trains of the RPS. Each train sends its own partial trip signal to each of the other three trains over isolated serial data links. Each train will generate a reactor trip signal if two or more trains of the same variable are in the partial trip state.

Each train of the RPS consists of two separate digital controllers to achieve defense-in-depth through functional diversity. Functional diversity provides two separate methods of detecting the same abnormal plant condition. Each functionally diverse digital controller within a train can initiate a reactor trip. Generally, each functionally diverse digital controller monitors and processes inputs from different plant sensors. For most events there are at least two diverse sensor measurements for initiation of protection for each plant accident condition. Where two diverse sensor measurements are not available, analog splitters are used to interface the same analog sensor signals to the two functionally diverse controllers.

The reactor trip signal from each of the four RPS trains is sent to a corresponding Reactor Trip Actuation (RTA) train. Each of the 4 RTA trains consists of two Reactor Trip Breakers. The reactor is tripped when two or more RTA trains receive a reactor trip signal. This automatic trip demand initiates the following two actions: 1) it de-energizes the under-voltage trip attachments on the Reactor Trip Breakers, and 2) it energizes the shunt trip devices on the Reactor Trip Breakers. Either action causes the breakers to trip.

The PRA safety goals, the Single Failure Criterion, and GDC24 are met with only three trains in service. Therefore, these requirements are met even when one RPS train and its corresponding RTA train are bypassed. Therefore, bypass of one complete RPS/RTA train is permitted for a limited time period consistent with the reliability of the remaining three trains. Interlocks between RPS trains prevent bypassing two RPS trains or two RTA trains.

It is noted that the PSMS and PCMS share sensors. The method used to ensure this sensor sharing does not compromise conformance to the Single Failure Criterion or GDC 24 while a train is bypassed is discussed below.

b. Engineered Safety Features Actuation Function in RPS

In addition, to the requirements for a reactor trip for anticipated abnormal transients, adequate instrumentation and controls are provided to sense accident situations and initiate the operation of necessary Engineered Safety Features (ESF). The occurrence of a limiting fault, such as a loss of coolant accident (LOCA) or a steam line break, requires a reactor trip plus actuation of one or more ESF in order to prevent or mitigate damage to the core and reactor coolant system (RCS) components, and ensure containment vessel integrity.

In order to accomplish these design objectives, the RPS receives signals from various sensors and transmitters for actuation of ESF systems.

The RPS uses selected plant parameters to determine if predetermined safety limits are being exceeded. These parameters and safety limits are monitored in various combinations which are indicative of primary or secondary system boundary ruptures. Once the required logic combination is completed, the RPS sends the appropriate actuation signals to the ESFAS for event mitigation.

To actuate ESF systems the RPS interfaces with the following equipment:

- Sensors
- Engineered Safety Features Actuation System

Four sensors, each in separate trains, normally monitor each variable which is used for an engineered safety feature (ESF) actuation. (These sensors may be monitoring the same variable for a reactor trip function as well.) Analog measurements are converted to digital form by analog-to-digital converters within each of the four trains of the RPS. Following required signal conditioning or processing, the measurements are compared against the setpoints for the ESF to be generated. This signal conditioning, processing and comparison is done independently within each of the four trains of the RPS. When the measurement exceeds the setpoint, the output of comparison results in a partial actuation signal for that train. Each RPS train sends its own partial actuation signal to each of the other three RPS trains over isolated serial data links. Each RPS train will generate a system level ESF actuation signal if two or more redundant trains of a single variable are in the partial actuation state.

4.2.2 ESF Actuation System (ESFAS)

The ESFAS consists of one train for each mechanical ESF train in the plant. For the US-APWR some ESF systems have four trains, others have two trains. Since the ESFAS is

common to all ESF systems, there are four ESFAS trains for the US-APWR. The number of ESF trains and corresponding ESFAS trains for other plants is described in Plant Licensing Documentation.

The system level ESF actuation signal from each of the four RPS trains is transmitted over isolated data links to an ESFAS controller in each of the ESFAS trains. If there are two ESF trains, the system level ESF actuation signal is transmitted to controllers in two ESFAS trains. If there are four ESF trains, the system level ESF actuation signal is transmitted to controllers in four ESFAS trains.

Each ESFAS controller consists of a duplex architecture using dual CPUs, to enhance reliability. In the Digital Platform TR this is referred to as a Redundant Parallel Controller configuration. Two-out-of-four coincidence voting logic is performed twice within each train through the redundant subsystems within each ESFAS controller. Each subsystem generates a train level ESF actuation signal, if the required coincidence of system level ESFAS actuation signals exists at its input, and the correct combination of system level actuation signals exist to satisfy logic sensitive to specific accident situations.

Train level ESF manual actuation signals generated from the Operator Console are also processed by the logic in each redundant subsystem of each ESFAS train to generate the same train level ESF actuation signals. Train level manual actuation signals are generated for each ESFAS signal from separate switches for each ESFAS train. To avoid spurious actuation from a single contact or signal path failure, each switch contains two contacts that are interfaced to two separate digital inputs. Each ESFAS subsystem processes these signals through two-out-two logic for redundant train level actuation.

Whether automatically or manually initiated, train level ESF actuation signals are transmitted from both subsystems of the ESFAS controller to the corresponding train of the Safety Logic System. The number of ESFAS trains which generate train level ESF actuation signals corresponds to the number of mechanical ESF trains being actuated.

ESF actuation function can be manually bypassed for manual testing or maintenance at train level. In addition, some function may be manually overridden at the train level by deliberate manual operator action to accommodate expected plant conditions after safety function actuation. These train level bypass or override logic are processed in ESFAS controller. Specific bypass or override logic are described in Plant Licensing Document.

The ESF Actuation System also provides automatic load sequencing for the Emergency Generators to accommodate the Loss of Offsite Power (LOOP) accident. Each ESFAS train monitors the loss of power condition for its respective train. Upon detecting a loss of power, the ESFAS starts the Emergency Generator for its train and disconnects the loads for its train from the electrical bus. Once the Emergency Generator is capable of accepting loads, the ESFAS sequences the loads for its train back onto the electrical bus in an order appropriate for the current train level ESF actuation signal(s). The ESFAS sequencing logic accommodates ESF actuation signals occurring prior to or during a loading sequence. The ESFAS load sequencing function is independent for each train.

4.2.3 Safety Logic System

The Safety Logic System (SLS) controls safety related plant components in all trains based on ESF actuation signals, process instrumentation and component level manual actions from the non-safety Operational VDUs and Safety VDUs.

The SLS consists of one train for each safety related mechanical train in the plant. For the US-APWR some safety related process systems have four trains, others have two trains. Since the SLS is common to all safety related process systems, there are four SLS trains for the US-APWR. The number of safety related process trains and corresponding SLS trains for other plants is described in Plant Licensing Documentation.

The SLS consists of multiple controllers in each train. Plant process systems are assigned to controllers based on consideration of maintenance, potential SLS equipment failures and optimization of controller performance. In general, complete plant process systems are assigned to one controller. Multiple process systems are assigned to the same controller or a single process system is assigned to multiple controllers only if the plant effects of controller failure and maintenance are demonstrated to be acceptable, based on the plant specific FMEA. The number and configuration of controllers in each SLS train is described in Plant Licensing Documentation.

To enhance reliability, each SLS controller consists of a duplex architecture using dual redundant CPUs operating in a redundant parallel configuration. In the Digital Platform TR this is referred to as a Redundant Parallel Controller configuration. Each controller of the duplex architecture receives ESF actuation signals and Load Sequencing signals from the corresponding duplex controller of the ESFAS.
The SLS also includes I/O modules mounted in I/O chassis. These I/O chassis can be located within the same cabinet as the controllers or remotely in separate cabinets that are distributed throughout the plant to reduce the length of cable from the process component or instrument to the I/O chassis. Signals from each SLS controller in the duplex architecture are combined in the output modules using 1-out-of-2 logic for control of plant components to the desired safety state.

The SLS I/O modules include contact input conversion devices and Power Interface (PIF) modules. The PIF module transforms the low level signals to voltage and currents commensurate with the actuation devices (such as, motor starters, switchgear, etc.) which they must operate. The actuation devices, in turn, control motive power to the final ESF component. Each train of the Safety Logic System thus interfaces the PSMS to each train of the plant process ESF equipment.

Each controller has multiple I/O chassis, each chassis has multiple I/O modules and each I/O module accommodates one or more process interfaces. The plant process interfaces are assigned to I/O modules/chassis with consideration of maintenance and potential SLS equipment failures. The plant specific FMEA demonstrates acceptable plant level effects for failure or maintenance of any I/O module or any I/O chassis. I/O modules are duplicated within a single SLS train if a single failure of the I/O module will cause a spurious reactor trip. For example I/O modules for the Main Steam Isolation valves are typically duplicated. The I/O configuration is described in Plant Licensing Documentation. PIF modules include logic and interfaces to combine signals from the SLS controllers with signals from the DAS. This interface and logic are also used in a few other cases where fast hardwired response is required, such as turbine trip from turbine protection system.

The primary functions performed by the SLS are described below:

a. Control of ESF Components

The ESFAS provides all system level ESF actuation logics including the automatic load sequence for the safety Emergency Generators. Whether automatically or manually generated, train level ESF actuation signals are transmitted from each ESFAS train to the corresponding train of the Safety Logic System (SLS).

Within the Safety Logic System, the train level ESF actuation signals are then broken down to component actuation signals to actuate each component associated with an ESF. For example, a single safety injection signal must start pumps, align valves, start diesel generators and so on. The logic within each train of the Safety Logic System accomplishes this function and also performs necessary interlocking to ensure that components are properly aligned for safety. The SLS also controls ESF components based on manual component level controls from Operational VDUs and Safety VDUs.

b. Control of Safe Shutdown Components

The systems necessary for safe shutdown perform two basic functions. First, they provide the necessary reactivity control to maintain the core in a sub-critical condition. Boration capability is provided to compensate for xenon decay and to maintain the required core shutdown margin. Second, these systems must provide residual heat removal capability to maintain adequate core cooling.

The Reactor Protection System and the Engineered Safety Features Actuation Systems are designed to mitigate accident conditions and achieve immediate stable hot shutdown conditions for the plant.

Manual controls through the Safety VDUs or Operational VDUs on the Operator Console in the Main Control Room or the Remote Shutdown Console allow operators to maintain longer term hot shutdown conditions and transition to and maintain cold shutdown conditions for the plant. All manual and automatic operation of plant safety systems is via the Safety Logic System. Non-safety systems are not required for safe shutdown of the plant.

c. Control of Interlocks Important to Safety

The SLS provides interlocks which operate to reduce the probability of occurrence of specific events or to verify the state of a safety system. These include interlocks to prevent over pressurization of low-pressure systems and interlocks to ensure availability of engineered safety features.

Typical examples of the Interlocks Important to Safety are as follows;

- Interlocks for Residual Heat Removal Heat Exchanger Inlet Isolation Valve
- Component Cooling Water isolation for non-safety components
- Interlocks for Accumulator Isolation Valves

The Safety Logic System controls these Interlocks Important to Safety through the application software in the SLS controllers. Non-safety systems are not required for Interlocks Important to Safety.

4.2.4 Safety Grade HSI System

All automated safety functions may be manually initiated and monitored by operators using the Safety Grade HSI System. The Safety Grade HSI System is also used to manually initiate other safety functions that are not automated, including safety functions credited for safe shutdown. The Safety Grade HSI System also provides all safety related plant information to operators, including critical parameters required for post accident conditions.

a. Control of Reactor Trip Switchgear

Operators can trip the Reactor Trip Breakers using conventional fixed position hardwired switches on the Operator Console. There is one switch for each Reactor Trip Actuation train.

b. Control of ESF Components

The ESF components are controlled from the Safety Grade HSI System on the Operator Console. There are two types of control.

- Soft control using touch screens on the Safety VDUs. Soft controls include component and system level functions. Most soft controls on the Safety VDU are duplicated on the non-safety Operational VDUs. Due to better graphics and better screen navigation features, the Operational VDUs are the preferred HSI for all normal and abnormal plant conditions. Therefore, the soft controls on the Safety VDU are considered backup controls.
- Hard control using conventional fixed position switches on the Operator Console. Hard controls are provided to initiate each system level ESF actuation signal. The switches are hardwired to the ESFAS.

c. Post Accident Monitoring (PAM)

The Safety Grade HSI system displays PAM parameters that are designated Type A, B or C in RG 1.97. The purpose of displaying these post-accident monitoring (PAM) parameters is to assist main control room personnel in evaluating the safety status of the plant. PAM parameters are direct measurements or derived variables representative of the safety status of the plant. The primary function of the PAM parameters is to aid the operator in the rapid detection of abnormal operating conditions. As an operator aid, the PAM variables represent a minimum set of plant parameters from which the plant safety status can be assessed.

The Type A and B PAM parameters are normally displayed continuously on the Safety VDUs on the Operator Console in the main control room. There is one or more Safety VDU for each train. The parameters are selected based on R.G. 1.97 and at least two channels of each parameter are available.

The PAM parameters are not visible on the Safety VDU when the Safety VDU is being used for back-up control functions. However, a summary of plant safety status, including display of Type A and B PAM parameters, is always continuously displayed on the non-safety Large Display Panel. Detail information for all PAM parameters can be displayed on the non-safety Operational VDUs.

d. Safe Shutdown from Outside the Main Control Room

The Remote Shutdown Console, located outside the Main Control Room fire zone, is installed so that safe shutdown can be achieved in the case that the operators can not stay within the Main Control Room.

In order to achieve and maintain the reactor in the cold shutdown condition (safe shutdown state), it is necessary to remove excess heat to control the temperature, pressure and volume of the reactor coolant, and to supply boric acid, etc. Therefore, the operating controls, of those plant systems necessary for the above mentioned operations, can be operated from the Remote Shutdown Console. The Remote Shutdown Console provides the equivalent functions of the Operational VDUs and the Safety VDUs in the Main Control Room.

These controls are switched over from the Main Control Room to the Remote Shutdown Console by MCR/RSC Transfer Switches. The configuration of MCR/RSC Transfer System is illustrated in Fig. 4.2-1.

Separate Transfer Switches to control each of the four PSMS trains and one for the PCMS are located just outside of the Main Control Room fire zone (five switches, one per each PSMS train and one for PCMS) and in the Remote Shutdown Room (five switches, one per each PSMS train and one for PCMS). When the transfer actions from the Main Control Room to Remote Shutdown Console are initiated from both sets of switches for any one train, HSI signals from the MCR are blocked and HSI signals at the RSC are enabled. Transfer is controlled separately for each of the four PSMS trains and separately for the PCMS. Any subsequent damage to MCR HSI devises, caused by the fire in the Main Control Room, does not affect the functions of the Remote Shutdown Console. Transfer from the RSC back to the MCR is activated separately for each of the four PSMS trains and the PCMS using the same transfer switches. Access to the Remote Shutdown Console, and the Transfer Switches near the MCR is administratively controlled through closed areas with key access.

This design ensures no single failure will prevent transfer of more than one train. In addition a single failure will not result in spurious transfer of any train. The design also limits unauthorized transfer by controlling physical access to the transfer switches and ensuring that switches in two separate locations must be actuated before a transfer will occur.

4.2.5 Plant Control and Monitoring System

The non-safety Plant Control and Monitoring System (PCMS) provides direct monitoring and control of non-safety plant systems. It also provides the preferred HSI for all plant systems, including safety systems. This section describes the interfaces of the PCMS to the safety related Protection and Safety Monitoring System (PSMS) and the HSI functions of the PCMS that support plant safety.

a. Instrumentation Shared with the Protection and Safety Monitoring System

In some cases, it is advantageous to employ control signals derived from instrumentation that is also used in the protection trains. This reduces the need for separate non-safety instrumentation which would require additional penetrations into reactor pressure boundaries and additional maintenance in hazardous areas. For each parameter where instrumentation is shared, the PCMS receives four redundant instrument signals from each train of the RPS. The signals are interfaced through fiber optic data networks. As such, an electrical fault in the PCMS cannot propagate to the protection channel.

The SSA ensures the PCMS does not take erroneous control actions based on a single instrument channel failure or single RPS train failure. As such, a single failure will not cause the PCMS to take erroneous control actions that challenge the PSMS, while the PSMS is in a degraded operability state due to the failed instrument channel or failed RPS train. This signal selection algorithm within the PCMS is one design feature that contributes to allowing the RPS to have one instrument channel inoperable or bypassed at all times while still complying with GDC24 and IEEE 603. Other design features that are also necessary for allowing continuous operation with only three RPS trains is described in other sections.

b. Important to Safety Indication

This section describes information provided to the plant operators from the PCMS for: (1) assessing plant conditions and safety system performance, and making decisions related to plant responses to abnormal events; and (2) preplanned manual operator actions related to accident mitigation. The PCMS also provides the necessary information from which appropriate actions can be taken to mitigate the consequences of anticipated operational occurrences.

(1) Post-Accident Monitoring (PAM)

A summary of plant safety status is always continuously displayed on the Large Display Panel and detail information for all PAM parameters can be displayed on the Operational VDUs.

(2) Bypassed or Inoperable Status Indication (BISI)

If a safety function of the PSMS is bypassed or inoperable at the train level, this is continuously indicated on the Large Display Panel. Other bypassed or inoperable conditions that do not result in inoperability of safety functions at the train level are indicated on Operational VDUs but not on the Large Display Panel. For example, if one redundant subsystem fails within an ESFAS or RPS controller the safety function of the controller is still maintained for that train, so this inoperable condition is only indicated on Operational VDUs. Alternately, if an instrument input to a train of the RPS is bypassed or inoperable, this is continuously indicated on the Large Display Panel because that RPS train can no longer perform its safety function for that parameter.

As a minimum BISI is provided for the following systems:

- RPS, ESFAS and SLS
- Interlocks for isolation of low-pressure systems from the reactor coolant system
- ECCS accumulator isolation valves
- Operability of components in ESF process systems

The BISI information is displayed on the Large Display Panel (LDP) in the main control room as alarm information. The alarm information on the LDP is spatially-dedicated and continuously visible. The redundant processing of alarm information is described below. Although the LDP itself is not redundant, the LDP screen can be displayed on any Operational VDU.

The LDP system and the alarm processors are not Class 1E. Isolation for inputs from the PSMS via fiber optic data-network interfaces ensures independence and separation of safety systems.

(3) Plant Alarms

The primary purpose of plant alarms is "to alert operators that the plant is in an abnormal status." Alarms are used not only to draw operator's attention, but also to identify the extent (such as where and what degree) of the abnormal status. The main purposes of alarms can then be summarized as following.

- Alert operators that the plant is in abnormal status.
- Provide operators with information relating to the abnormal status (where and what degree)
- Help operators in making judgments and taking countermeasures

The computers and data links used to process alarms are redundant. The data links from the safety cabinets (RPS, ESFAS, etc.) are physically and functionally isolated to not influence the safety system in case of failure of the alarm processing.

The plant alarms are also designed taking into consideration functional and ergonomic aspects, thereby ensuring appropriate fulfillment of operator roles at the time of an alarm.

The main features of the alarm system are as follows;

- Adequate display to acknowledge and recognize alarm information
- Application of alarm prioritization to avoid alarm avalanche
- Request functions from alarm display to relevant operation display and alarm response procedures.

These functions help operators to identify and diagnose transients.

(4) Safety Parameter Display System (SPDS)

The safety parameter display system (SPDS) provides a display of plant parameters from which the safety status of operation may be assessed in the main control room, TSC, and EOF. The primary function of the SPDS is to help operating personnel in the main control room make quick assessments of plant safety status. Duplication of the SPDS displays in the TSC and EOF improves the exchange of information between these facilities and the control room and assists corporate and plant management in the decision-making process. The SPDS is operated during normal operations and during all classes of emergencies. The SPDS has the flexibility to allow future modifications to be incorporated, such as the capability to handle operator interaction and diagnostic analysis.

The functions and design of SPDS in the main control room are realized as a part of the overall HSI design. The TSC and EOF are described in Plant Licensing Documentation.

c. Safety Systems and Components Controlled from Operational VDUs

Operational VDUs on the Operator Console provide controls for safety and non-safety systems and components in all trains. These controls are available by touch operation or other pointing device from the same screen. The common HSI of the multi-cannel Operational VDU provides the following operability benefits:

- A single operator can execute procedures that involve multiple safety and non-safety systems, simplifying task coordination.
- All soft control and monitoring, for safety system and non-safety functions, are executed on the same display. This reduces operator transitions between workstation and between display screens, thereby deducing operator work load.
- Computer based procedures allow operators to access relevant display formats which are hyper linked from the procedure and shown on the Operational VDU.

Therefore, even though the Safety VDUs provide HSI for all safety related control and monitoring functions, the multi-channel operator station (i.e. the Operational VDU) is the preferred HSI for all normal and abnormal plant conditions. Operation during degraded HSI conditions, such as failure of the Operational VDUs, is described in the HSI Topical Report.

To ensure there is no potential for the non-safety system to adversely affect any safety functions, the interface between the non-safety Operational VDUs in the PCMS and the PSMS is isolated as described below.

- Electrical independence
  Fiber optic interfaces between the PSMS and PCMS prevent propagation of electrical faults between divisions. The electrical independence features are shown in Fig. 4.2-2.

- Data processing independence
  The PSMS employs communication processors for the PCMS that are separate from the processors that perform safety logic functions. The safety processors and communication processors communicate via dual ported memory. This ensures there is no potential for communications functions, such as handshaking, to disrupt deterministic safety function processing. The data processing independence features are shown in Fig. 4.2-2.

- No ability to transfer unpredicted data
  There is no file transfer capability in the PSMS. Only predefined communication data sets are used between the PSMS and PCMS. Therefore any unknown data is rejected by the PSMS.

- No ability to alter safety software
  The software in the PSMS cannot be changed through the non-safety communication network, which is called the Unit Bus. The PSMS software is changeable only through the Maintenance Network which is key locked and alarmed.

- Additional protection against cyber threats
  The PCMS and PSMS will be controlled under the most stringent administrative controls for cyber security. There is only one-way communication to other systems that are not under these same controls.

- Acceptable safety function performance
  Manual controls from the Safety VDU can have priority over any non-safety controls from the PCMS.

- Failures of non-safety systems are bounded by the safety analysis
  Any plant condition created by the worst case erroneous/spurious non-safety data set (e.g. non-safety failure commanding spurious opening of a safety relief valve) is bounded by the plant safety analysis.

The Operational VDU and associated processors are not Class 1E. However, they are tested to the same seismic levels as the PSMS. During this testing the Operational VDU and associated processors have demonstrated their ability to maintain physical integrity and all functionality during and after an Operating Basis Earthquake and a Safe Shutdown Earthquake.

4.2.6 Diverse Actuation System

The non-safety Diverse Actuation System (DAS) provides monitoring and control of safety related and non-safety related plant systems to cope with abnormal plant conditions concurrent with a common cause failure (CCF) that disables all functions of the PSMS and PCMS. This section describes the interfaces of the DAS to the PSMS and PCMS and the HSI functions of the DAS that support plant safety. A more detailed description of the DAS is provided in the Defense-in-Depth and Diversity Topical Report.

Safety or non-safety sensors selected by the plant design are interfaced from within the PSMS or PCMS input modules. These input modules utilize analog splitters and isolators that connected the input signals to the DAS prior to any digital processing. Therefore, a software CCF within the PSMS or PCMS will not affect the DAS function. The input module design is described in the Digital Platform Topical Report.

Within the DAS manual actuation is provided for all critical functions at the train level (e.g. reactivity level, core heat removal, reactor coolant inventory and containment isolation). Automatic actuation is also provided for functions where time for manual operator action is inadequate.

The DAS interfaces to non-safety process systems and to redundant trains of safety process systems. Since the DAS is a non-safety system it does not need to meet the single failure criteria for actuation. However, the design typically includes redundant inputs and processors arranged in a two-out-of-two configuration to ensure the DAS can sustain one random component failure without spurious actuation of either manual or automatic functions at the system or train level. Spurious actuation of single plant components due to single DAS output failures is considered in the plant safety analysis.

The Diverse HSI Panel is typically located within the MCR fire zone. The DAS interface to the PSMS/PCMS output modules is disabled when the MCR is evacuated using the MCR/RSC Transfer Switches, describe above. This ensures that DAS failures that may result due to MCR fire damage, will not result in spurious actuation of DAS functions and plant components that could interfere with safety shutdown from the RSC. The DAS is not needed when the MCR is evacuated since a plant accident is not postulated concurrent with a MCR evacuation.

The DAS is a non-safety system, therefore it does not need to be tested during plant operation. During plant shutdown, the system can be tested by manually injecting input signals to confirm setpoints, and logic functions and system outputs.

In addition, test functions and indications are built into the system so there is no need to disconnect and termination or use external equipment for test monitoring. Any exceptions to this are described in Plant Licensing Documentation.

Figure 4.2-1 Configuration of RSC/MCR Transfer System

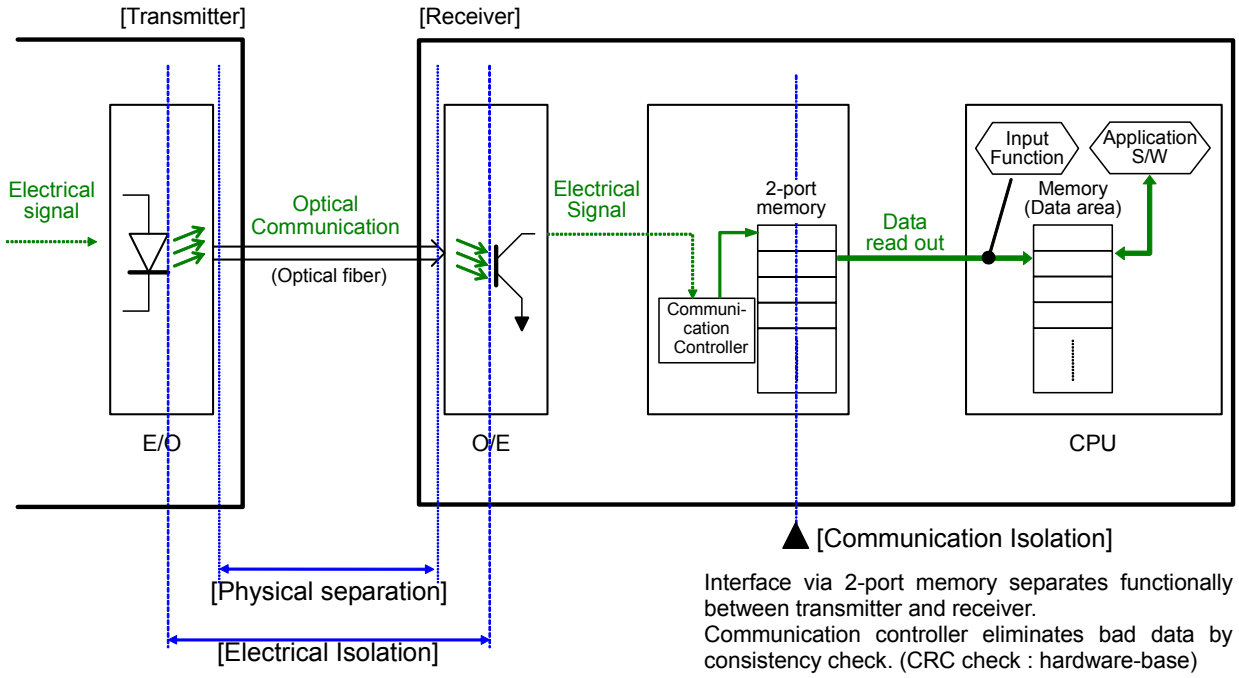


Figure 4.2-2 Electrical Independence Features between PCMS and PSMS

4.3 PSMS Self-diagnostics Features

The integrity of PSMS components is continuously checked by the platform self-diagnostic features, which are described in detail in the Digital Platform Topical Report. The platform self diagnostic features continuously check the integrity of processing and communication components as well as the range of process inputs. These self-diagnostic features allow early detection of failures, and allow easy and quick repair that improves system availability. Information about detected failures is gathered through system communication networks and provided to maintenance staff in a comprehensive manner. Alarms are generated in the MCR for any failures that effect system functionality. The platform self-diagnostic features control the redundant configuration to maintain all system functions for most single failures.

In addition to platform diagnostic features, the redundant system inputs from different trains are continuously compared to detect failed/drifting instrumentation or input modules. This comparison is performed continuously in the Unit Management Computer of the PCMS; deviations are alarmed in the MCR.

4.4 PSMS Manual Testing and Calibration Features

Continuous platform and system level self-diagnostic features allow elimination of most manual surveillances required for Technical Specification compliance. Manual testing and manual calibration is only provided for functions with no self-diagnostics.

4.4.1 Manual Testing

Manual test features are provided for system level manual actuation of Reactor Trip and ESF actuation signals, the Safety VDU touch screens, binary process inputs and final actuation of plant process components. An additional manual test is conducted to confirm the integrity of the PSMS software memory. Most manual tests may be conducted on-line without full system actuation and without plant disturbance. Each of these manual tests is described in the sections below.

- Manual Reactor Trip
  The manual Reactor Trip actuation signals are tested by actuating the conventional switches on the Operator Console and the Remote Shutdown Console, one train at a time. When the Reactor Trip function is tested one train of reactor trip breakers will open, but the plant will not trip, since breakers in two trains must open to de-energize the CRDMs.

  The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5. However, this test may be conducted more frequently, if required by the reliability of the reactor trip breakers. The test frequency for the reactor trip breakers is described in Plant Licensing Documentation.

- Manual ESF Actuation
  The manual ESF actuation signals are tested on-line by actuating the conventional switches on the Operator Console. Correct functionality is confirmed by status signals sent from the PSMS to the PCMS HSI. These status signals are generated by the PSMS controllers, so there is overlap between the manual test and the platform self-diagnostics. To prevent train level actuation during this test, a Bypass for Manual Test is activated prior

to the test. This blocks all manual actuation signals for one division within the ESFAS logic. In accordance with RG.1.47, the block is alarmed with SDCV display to indicate the ESFAS train is bypassed. Removal of the bypass is verified when the alarm has cleared. The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5.

- Safety VDU
  Safety VDU touch screens are tested by manually touching screen targets and confirming correct Safety VDU response.

  The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5.

- Binary Process Inputs
  Binary process inputs to the PSMS are tested periodically by manipulating the process to stimulate a state change in the process monitoring device. Correct functionality is confirmed by status signals sent from the PSMS to the PCMS HSI. These status signals are generated by the PSMS controllers, so there is overlap between the manual test and the platform self-diagnostics. To avoid spurious actuations during this test, the test is conducted with the train that receives the signal in a bypass mode. This prevents spurious actuation of this train and it prevents propagation of the input signal state change to other trains.

  The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5. However, these tests may be conducted more frequently, if required by the reliability of the process monitoring device. The test frequency for binary process monitoring devices is described in Plant Licensing Documentation.

- Final Actuation Outputs

  Either test, individual or group, also confirms the functionality of the SLS output module and the interface to the plant component. Since the control signals are generated by the SLS controllers, there is overlap between the manual test and the platform self-diagnostics. The Reliability Analysis method, which demonstrates the need to conduct manual tests of the SLS outputs no more frequently than once per 24 months, is described in Section 6.5. However, this test may be conducted more frequently, if required by the reliability of the plant process components. The test frequency for the plant process components is

described in Plant Licensing Documentation.

- Software Memory Integrity

The Reliability Analysis method, which demonstrates the need to conduct Software Memory Integrity Tests no more frequently than once per 24 months, is described in Section 6.5.

Figure 4.4-1 shows the overlap testability for Reactor Trip. Figure 4.4-2 shows the overlap testability for ESF Actuation. Figure 4.4-3 shows the overlap testability for the Safety VDU.

4.4.2 Manual Calibration

PSMS analog input modules and power supplies are continuously checked for failure by the platform self diagnostics. In addition, redundant analog input channels are continuously compared between trains to detect failures and unexpected drift, as discussed above.

However, to correct for expected time dependent drift that can commonly affect all redundant analog instruments and analog processing components, these components are periodically checked for accuracy and calibrated as needed. The calibration check for PSMS components is most easily conducted in conjunction with the calibration check for plant process instrument.

Plant process instruments are calibrated using various techniques that stimulate the instrument's sensing mechanism. During the calibration of the instrument, the analog signal generated by the instrument is monitored on an Operational VDU or Safety VDU. This monitoring ensures the functionality of the signal path from the sensor to the PSMS, and the accuracy of the signal processing within the PSMS, including the analog input module. Since the VDU signals are generated by the SLS controllers, there is overlap between the manual calibration and the platform self-diagnostics.

Process instruments are calibrated one train at a time. During the calibration the instrument channel is bypassed in the RPS. This prevents erroneous RPS or ESFAS actuation due to a single failure of another channel during the calibration.

The Accuracy Analysis method, described in Section 6.5, demonstrates the need to check the calibration of PSMS power supplies and analog input modules no more frequently than once per 24 months. However, this test may be conducted more frequently, if required by the reliability of the plant process instrumentation. The test frequency for the plant process instrumentation is described in Plant Licensing Documentation.

4.4.3 Response Time

The PSMS does not include any special built-in provisions to periodically test system response time. Response time is calculated and independently verified and validated during the system design process, as described in Section 6.5. The PSMS includes no components that have known aging or wear-out mechanisms that can impact response time. Therefore response time can only be affected by random failures or calibration discrepancies. All random failures and calibration discrepancies are detected by the testing and calibration methods described above.

4.5 PSMS On-line Maintenance

Components in the PSMS that require periodic age related replacement, such as power supplies, are described in the Platform Topical Report. Other components are replaced only when they are detected as failed either by self-diagnostics or manual surveillances.

Failures detected by platform self-diagnostics are automatically diagnosed to the replaceable module level. Alarms are provided on Operational VDUs and failed module identification is provided on the Engineering Tool. Failed processor modules in a Redundant Parallel Controller configuration and failed I/O modules may cause actuation or failure of components in a single train, depending on the application logic. The plant level effects of these failures are described in Plant Licensing Documentation.

Processor modules and I/O modules can be replaced while the PSMS controllers are powered. Other modules require power to be removed from the chassis, prior to module replacement. For failed processor modules in controllers configured for parallel or standby redundancy, the controllers will recover to their normal redundant configuration with no plant impact beyond the initial failure, as discussed above. Replacement of I/O modules must consider that some modules have more than one input or output. Therefore, if the initial failure was limited to a single channel on the module, removal of the failed module may impact more channels and therefore more plant interfaces. Failures and module replacement are considered in the assignment of plant process I/O to I/O modules during the system design, to minimize plant impact during module failure or maintenance. The plant level of effects of I/O modules failures and maintenance are described in Plant Licensing Documentation.

Figure 4.4-1 Overlap Testability for Reactor Trip

Figure 4.4-2 Overlap Testability for ESF Actuation

Figure 4.4-3 Overlap Testability for Safety VDU

5.0 DESIGN BASIS

This section puts special emphasis on the explanation of key technical issues and describes the general design features for compliance with seismic and fire protection requirements.

5.1 Key Technical Issue

This section summarizes the I&C system features that specifically address the following key technical issues.

- Multi-channel operator stations
- HSI to accommodate reduced operator staffing
- Operation under degraded conditions
- Integrated RPS/ESFAS with functional diversity
- Common cause failure modes for Defense-in-Depth and Diversity analysis
- Credit for leak detection in Defense-in-Depth and Diversity analysis
- Common output modules for PSMS/PCMS and DAS
- Control system failure modes for safety analysis
- Credit for self-diagnostics for technical specification surveillances
- Unrestricted bypassed of one safety instrument channel
- Minimum inventory of HSI
- Computer based procedures

5.1.1 Multi-Channel Operator Station

There is two-way communication between non-safety Operational VDUs and the PCMS and between the non-safety Operational VDUs and all trains of the PSMS. To ensure independence between redundant safety trains and between the non-safety and safety systems the following independence measures described in Section 4.2.5, above, are applied.

- Electrical independence
- Data processing independence
- No ability to transfer unpredicted data
- No ability to alter safety software
- Additional protection against cyber threats
- Acceptable safety function performance
- Failures of non-safety systems are bounded by the safety analysis

5.1.2 HSI to Accommodate Reduced Operator Staffing

There are several features of the I&C systems that support reduced operator staffing:

- The multi-channel Operational VDUs provide the primary operator interface for both the MCR and the RSR. The multi-channel Operational VDUs allows a single operator to execute Computerized Procedures and control all safety and non-safety systems and components from a single HSI device.
- Self-diagnostics and continuous automated calibration features reduce the need for

operator support of maintenance and testing activities.

- Most manual surveillance tests requiring operator support can be conducted from the MCR.

5.1.3 Operation under Degraded Conditions

In the event of complete failure of all Operational VDUs, the plant can be safely shut down using only the Safety VDUs. Also, the plant can be safely shut down using only the Safety VDUs in the event of a complete PCMS failure. Based on the high reliability of these non-safety components, complete failure of the PCMS or complete failure of the Operational VDUs, are considered to be very infrequent events.

5.1.4 Integrated RPS & ESFAS with Functional Diversity

Within the same subsystem of the RPS, RPS bistable and coincidence voting functions are also used for ESFAS, where both functions are actuated on the same parameters. The functions are combined because integration of RPS and ESFAS requires less hardware than if the functions were separated. Less hardware results in fewer failures and less testing. Fewer maintenance interactions with the system reduce the potential for human errors that can reduce system reliability or cause spurious actuations that threaten plant safety.

Instead of separating RPS and ESFAS, functional diversity is provided within the integrated RPS/ ESFAS through two separate subsystems in each train. For each DBA each subsystem processes diverse sensor inputs that can each detect the DBA and initiate protective actions. PRAs done for the MHI digital I&C design show significant benefit for this functional diversity. On the other hand, PRAs done for the MHI digital I&C show minimal benefit for additional RPS/ESFAS separation (with functional diversity).

5.1.5 Common Cause Failure Modes for Defense-in-Depth and Diversity analysis

BTP-19 requires consideration of CCFs that “disable” the protection system. Based on this, the coping analysis described in the Defense-in-Depth and Diversity Topical Report considers CCFs that result in a fail as-is condition in the PSMS and PCMS. The coping analysis does not consider CCFs that result in output state changes (i.e., spurious actuation to de-energized or energized state).

The basis for this is that both systems employ fixed cyclical deterministic processing with very simple application functions. These functions are tested through an extensive software QA program. As a result the systems will not react differently during a DBA than they react every day. Based on this, it can be concluded that the designs preclude CCFs induced by changing input conditions. Therefore it is reasonable to assume that for the PSMS and PCMS, the CCF postulated for BTP-19 is not induced by the DBA, but rather by an undetected hidden defect (i.e. a defect that results in a fail as-is condition). An undetectable hidden defect may still exist when a DBA occurs. However a hidden defect that results in output state changes is immediately detectable by operators. Operators can correct this CCF prior to a DBA, so it is not considered in the BTP-19 coping analysis.

5.1.6 Credit for Leak Detection in Defense-in-Depth and Diversity Analysis

The DAS includes diverse processing and display of leak measurement sensors. The Defense-in-Depth and Diversity Topical Report credits this diverse leak detection which allow operators to detect and mitigate the leak even if the PSMS and PCMS are not operating correctly due to an undetected latent CCF. This is consistent with BTP-19, the System 80+ Design Certification Document (DCD), and the NRC's SER of that DCD, NUREG-1462, which states "Credit for leak detection is accepted …because (1) LBLOCAs and MSLBs … in combination with a CCF … is highly unlikely (2) I&C equipment possesses sufficient diversity and simplicity including manual controls… and instrumentation…"
The details of the DAS leak detection functions are described in the Defense-in-Depth and Diversity Topical Report.

5.1.7 Output Module for PSMS/PCMS and DAS

Output Modules in the Safety Logic System and PCMS interface control signals to the plant components. These same output modules are used to interface control signals from the Diverse Actuation System. A common Output Module provides one power interface conversion device for control of one plant component. This reduces the maintenance that would be required for two separate devices and it reduces the complexity of combining the SLS/PCMS and DAS signals via relay logic. Reduced complexity results in improved reliability.

Control signals are interfaced from the Safety Logic System or PCMS controllers to the software part of the Output Module via the controller's I/O communication network. Control signals from the DAS are interfaced via conventional hardwired connections and conventional isolators (for the SLS only) to the hardware part of the Output Module. The isolators are part of the SLS (i.e. they are Class 1E devices). Therefore DAS output signals interface to plant components via only the hardware part of the Output Module, so CCF within the PSMS or PCMS digital platform will not affect DAS signals.
Figure 5.1-1 shows the signal interface between output module and SLS and DAS.

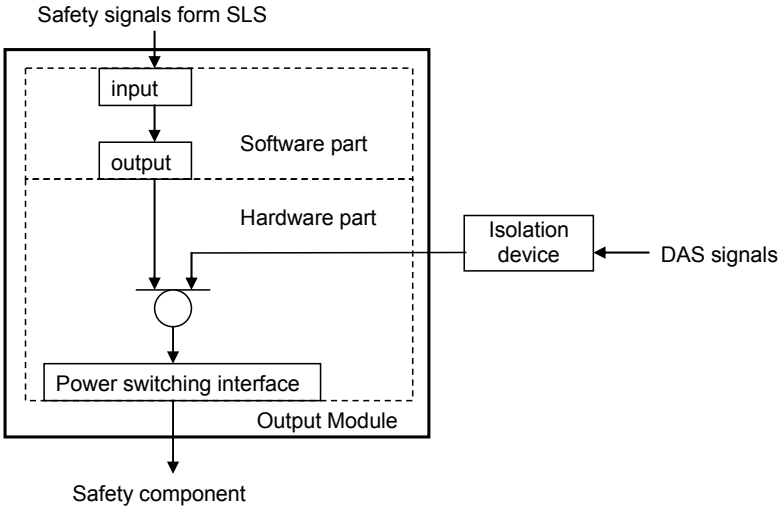


Figure 5.1-1 Signal Interface of Output Module

5.1.8 Control System Failure Mode

The non-safety PCMS has high reliability based on the following design features:

- The MELTAC platform that is applied to the PCMS is essentially the same as the MELTAC platform applied to the PSMS.
- The PCMS includes redundant controllers operating in a Redundant Standby Controller Configuration, as explained in the Digital Platform Topical Report. In this configuration a back-up standby controller changes into the active control mode if there is a failure of the primary controller.
- Non-safety control functions are partitioned in multiple redundant PCMS controllers to limit the effects of single failures.

Figure 5.1-2 shows the configuration example of the Reactor Control System.

5.1.9 Credit for Self-Diagnostics for Technical Specification Surveillance

Testing from the sensor inputs of the PSMS through to the actuated equipment is accomplished through a series of overlapping sequential tests. The majority of the tests are conducted automatically through self-diagnostics.

Figure 4.4-1 shows the overlap testability for Reactor Trip. Figure 4.4-2 shows the overlap testability for ESF Actuation. Figure 4.4-3 shows the overlap testability for the Safety VDU.

5.1.10 Unrestricted Bypass of One Safety Instrument Channel

The PSMS includes multiple trains from sensors to actuated device with complete electrical isolation and independence. For system functions with four instrument channels, one instrument channel may be bypassed continuously without violating any design criteria. The system adheres to all criteria with only three instrument channels in operation, as follows:

- Conformance to the single failure criteria is still maintained because if one instrument channel fails (with one instrument channel already inoperable), the 2/4 logic in the RPS and ESFAS is satisfied with the remaining two instrument channel, and all functions are actuated with the remaining two instrument channel.
- Even with sensors shared by the PSMS and PCMS, and one instrument channel inoperable, conformance to GDC 24 is still maintained. This is because the Signal Selection function in the PCMS prevents any erroneous control actions due to a shared sensor failure (or failure in the shared sensor signal path). This prevents challenges to the protection system. Since the PSMS is not challenged by a shared sensor failure, the sensor failure is considered the single failure. The PSMS remains fully functional with the remaining two trains. This method of compliance with GDC24 for shared sensors and a division continuously bypassed, is consistent with IEEE603 Section 5.6.3.3 and with the interpretation and approval for System 80+. Due to the importance of the Signal Selection logic it is designed using the same software QA program as the Safety Parameter Display System (SPDS) functions. This software QA program is described in the Design Process section below.
- With only three instrument channels in service the reliability of the safety function is sufficient to achieve the plant level PRA goals for CDF and LERF.

5.1.11 Minimum Inventory of HSI

Class 1E HSI is provided by the Safety VDUs for all safety related indications and controls. Spatially Dedicated Continuously Visible (SDCV) displays are provided for all critical safety

function parameters and for bypassed or inoperable conditions. This data is obtained from the PSMS and PCMS. SDCV HSIs are provided for manual actuation of Reactor Trip and ESFAS. Additional SDCV HSIs may be provided to ensure timely operator actions for specific plant events. The complete minimum inventory of SDCV HSI is described in the HSI system Topical Report. These are also described in Plant Licensing Documentation.

5.1.12 Computer Based Procedures

Computer based procedure allows operators to access relevant display formats which are hyper linked from the procedure and shown no the Operational VDU. Operator accesses and operates the required control switch quickly from the linked display formats on the Operational VDU, if necessary.

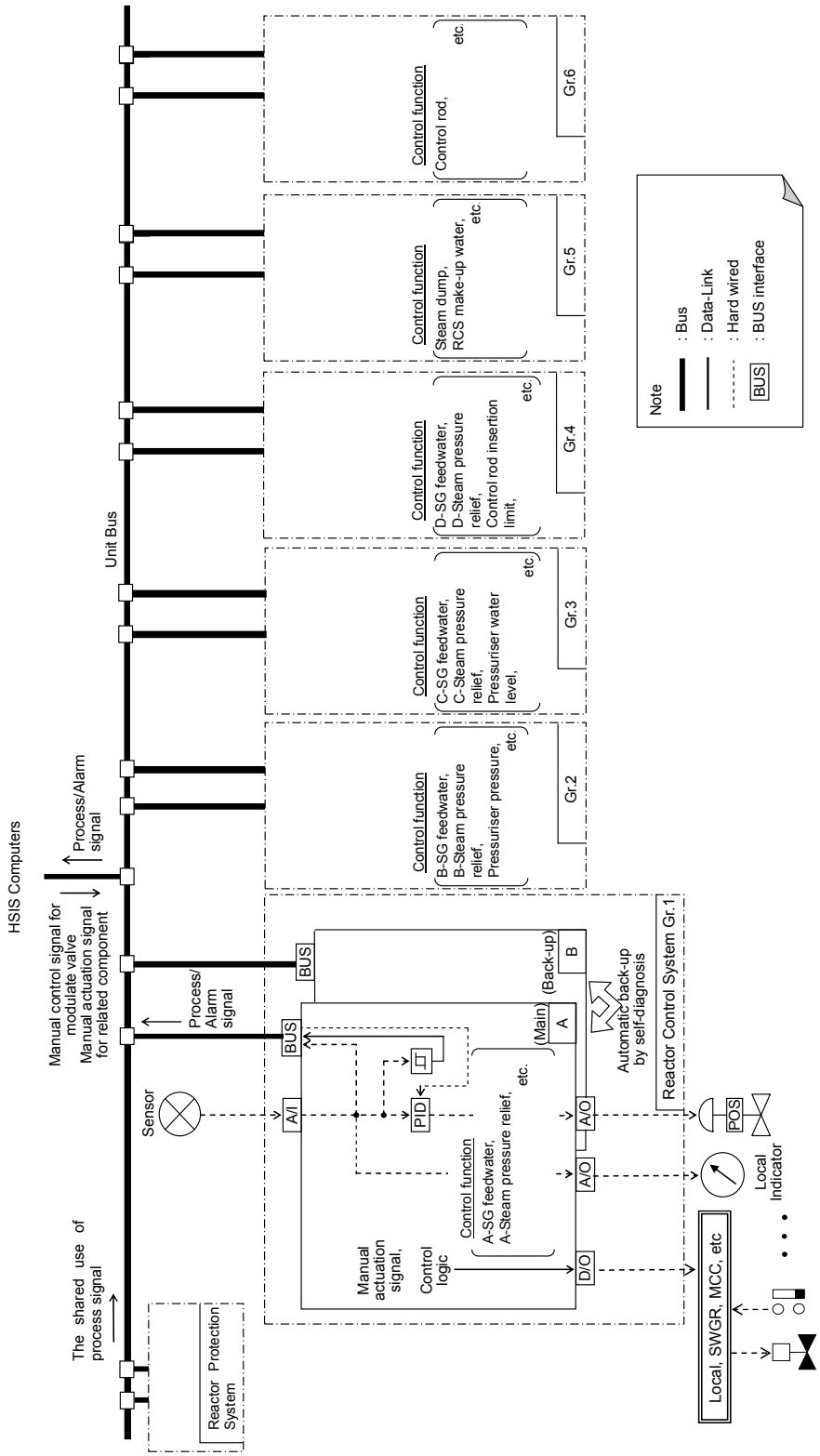


Figure 5.1-2 Configuration Example of Reactor Control System

5.2 General Design Features

5.2.1 Seismic

The PSMS, including the Safety VDU, is classified as Class 1E Seismic Category 1. The system is qualified to maintain physical integrity and all functionality during and after an Operating Basis Earthquake and a Safe Shutdown Earthquake.

5.2.2 Environmental Qualification

The PSMS is located in the main control room, remote shutdown room and I&C equipment rooms so that it is not influenced by external effects such as tornadoes, hurricanes and floods.

The PSMS operates in the following environmental conditions:

a. Temperature

68-79°F (20°C-26 ^{o}C) (This is the normal room ambient condition for continuous operation to maximize equipment life.)
50-122°F (10°C-50 ^{o}C) (when the protection function is required during SBO)

The PSMS cabinets, Operator Console and Remote Shutdown Console ensure no more than a 18 ^{o}F (10°C) heat rise between the temperature of cabinet air at the ventilation entry and exit, so that the ambient temperature at the platform components is no more than 100°F (40°C), which is the MTBF calculation basis of the MELTAC Platform components.
A cabinet temperature that exceeds the normal conditions, 97°F (36°C), is alarmed. A small margin for the alarm setpoint is provided to avoid nuisance alarms.

b. Humidity

Below 95% (non-condensing)

c. Radiation

The PSMS is located in areas where the radiation influence is negligible (i.e. up to 10^3 RADS).

d. Dust

The PSMS is located in areas where there is no dust influence (i.e. under 0.3mg/m^3). If the equipment is located in a high dust area, appropriate prevention for high dust influence must be provided. These preventions are discussed in Plant Licensing Documentation.

5.2.3 Fire Protection

The PSMS is made from nonflammable or flame resistance materials to minimize the potential source of fire and minimize the potential propagation of fire. The redundant trains of the PSMS are located in separate fire areas of the plant to ensure a fire that adversely affects one train does not affect other trains. The multiple trains of PSMS equipment located in the MCR fire area are isolated from the PSMS equipment located in the separate train equipment room fire

area. The multiple trains of PSMS equipment located in the Remote Shutdown Room (RSR) fire area are isolated from the PSMS equipment located in the separate train equipment room fire area. There are no connections between the multiple trains of PSMS equipment located in the MCR and the RSR. Therefore the multiple trains of PSMS equipment located in the MCR are inherently isolated from the multiple trains of PSMS equipment located in the RSR.
The MCR-RSR transfer switch logic is shown in Fig.4.2-1.

5.2.4 EMI/RFI Compatibility

The PSMS includes the following features to protect against Electro-Magnetic Interference (EMI) and Radio Frequency Interference (RFI), such as lightning, electrical surges, radiated and conducted interference from other plant equipment, wireless radio communications, etc.:

- Electrical isolators such as power line filters for input power sources and isolation amplifiers for analog input/outputs
- Optical fiber for multiplexed data communication lines and self-diagnostic of the multiplex data communication line to detect corrupted data transmission
- Two type of earth bars are installed in each cabinet, one for cabinet ground and one for internal circuits ground. The earth bar for the internal circuits is connected to a dedicated plant earth bar which is used only for sensitive instrumentation grounding (clean earth bar). The power line filters and I/O cable shields are connected to the cabinet ground earth bar.

5.2.5 Electrical Power

Each train of the PSMS is supplied from a safety related battery backed Uninterruptable Power Supply (UPS) through a DC to AC inverter. Each train of the PSMS is also supplied from a safety-related AC transformer power supply. The UPS and the AC transformer power supply provide redundant power to CPUs, I/O and VDU in the PSMS. Both power supplies are tied to the Emergency Generators. The safety UPS and AC transformer are shown in Fig. 5.2-1 and Fig. 5.2-2.

Each section of the PCMS is supplied from a non-safety battery backed UPS through a DC to AC inverter. Each section of the PCMS is also supplied from a backup non-safety UPS or a backup non-safety AC transformer power supply. The two power supplies provide redundant power to CPUs, I/O and VDUs in the PCMS. Both non-safety power supplies are tied to the Alternate Power Source. The primary and backup power supplies are shown in Fig. 5.2-3 and Fig. 5.2-4.

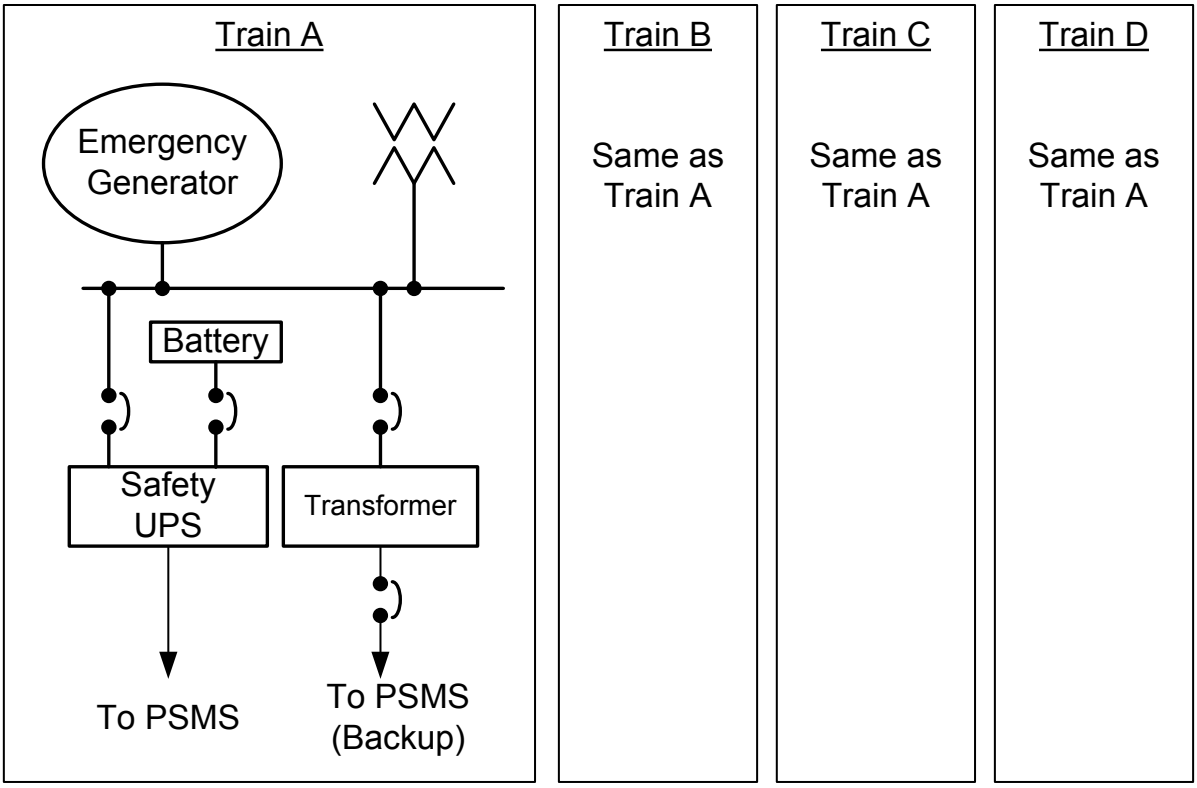


Figure 5.2-1 Safety UPS for PSMS

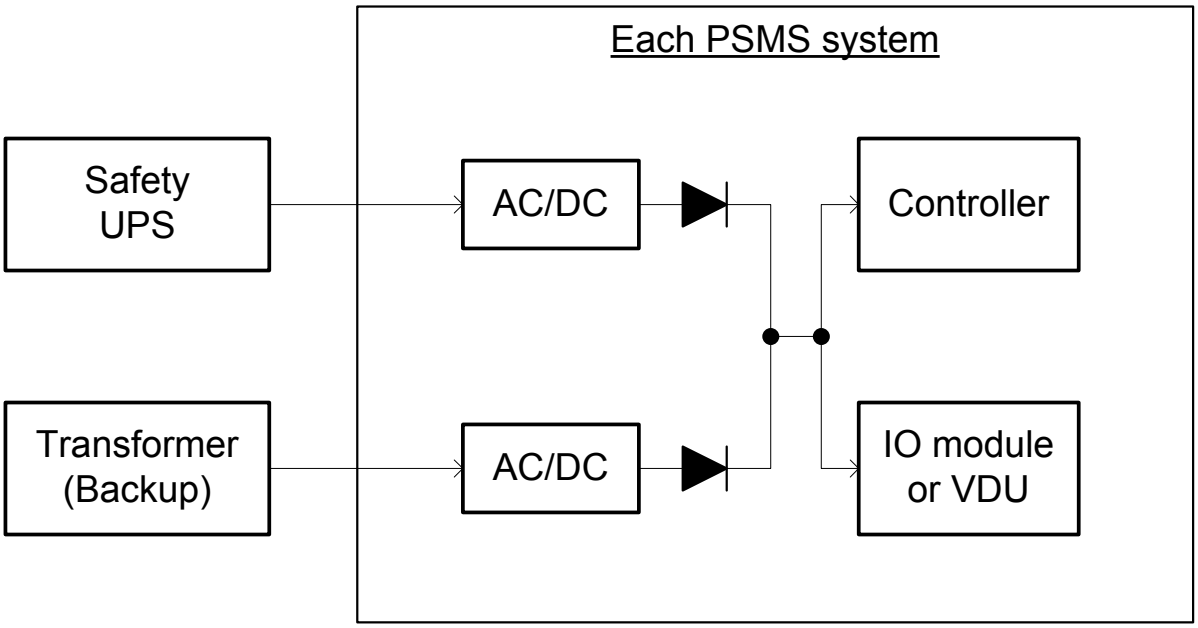


Figure 5.2-2 Electrical Power Source for PSMS

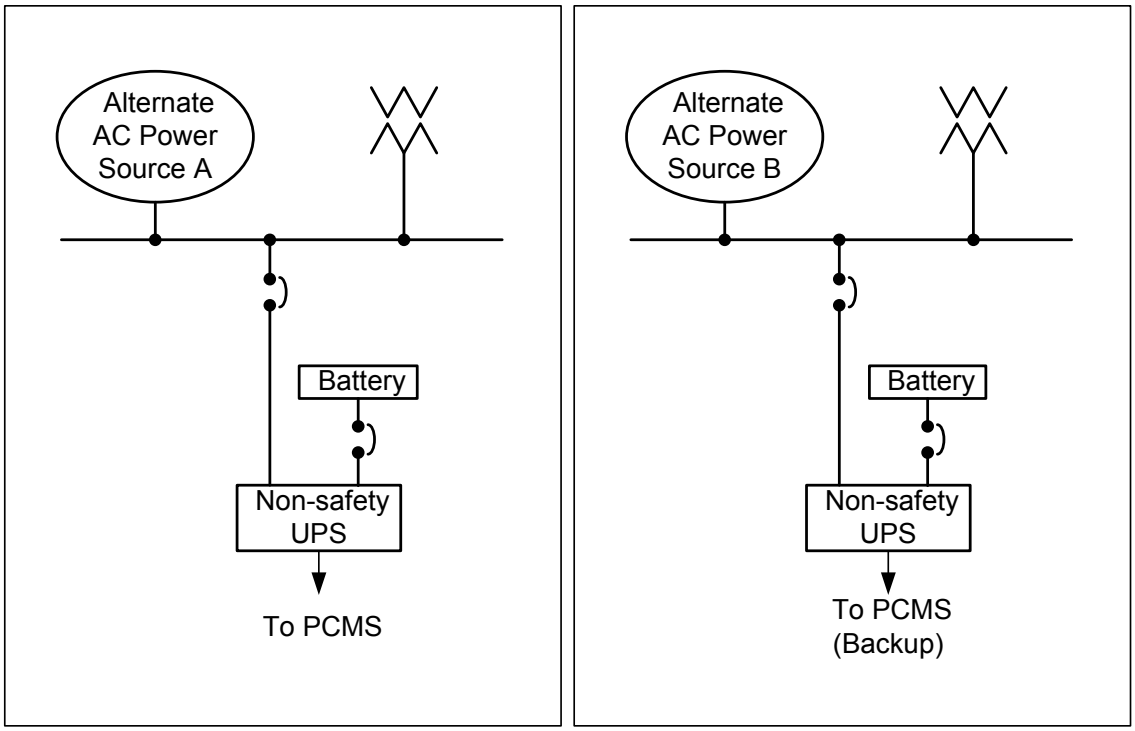


Figure 5.2-3 Non-safety UPS for PCMS

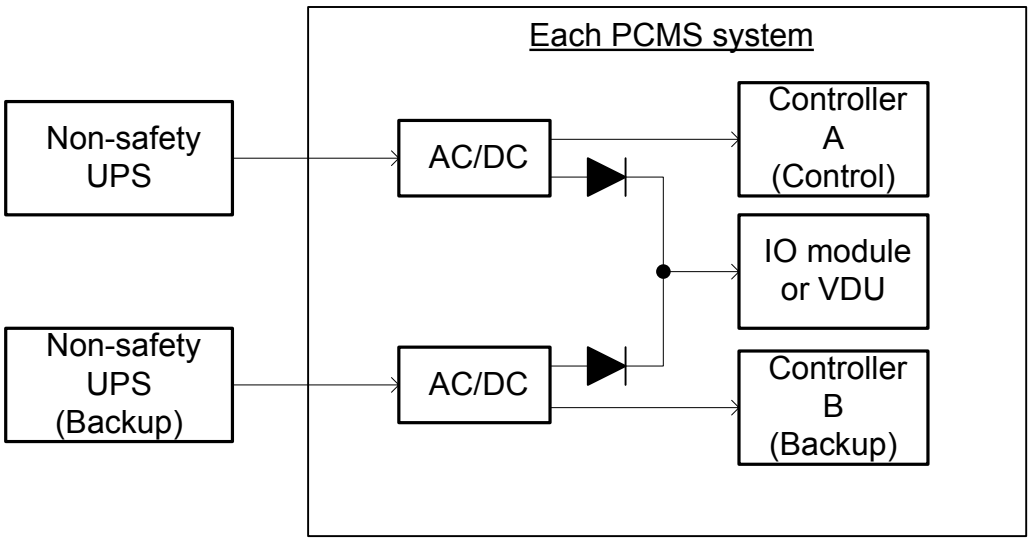


Figure 5.2-4 Electrical Power Source for PCMS

6.0 DESIGN PROCESS

This section describes key elements of the Design Process conducted by MHI to implement the PSMS, at the application level. The Design Process for the basic digital platform of the PSMS is described in the Digital Platform Topical Report.

This section describes the Design Process for both hardware and software. Section 6.1 provides an overview of the complete process, encompassing both hardware and software. Sections 6.2 and 6.3 describe the organization and processes used for application software development. Section 6.4 explains how the entire Design Process for both software and hardware is controlled. Section 6.5 describes the key analysis conducted during the Design Process which ensures the final system conforms to critical design basis requirements.

6.1 Design Process Overview

The safety system development process proceeds in the following phases as shown in Figure 6.1-1.

- Plant requirements
- System requirements
- Hardware/software requirements
- Hardware/software design and production
- Factory test
- Installation and commissioning
- Final documentation

The following discussion summarizes the activities undertaken and documents generated during each phase.

(1) Plant requirements phase

This phase defines the requirements and the key design aspects for all I&C systems that are critical to the plant's design basis for safety, performance and maintainability. This phase determines the industry regulations and standards that apply to the I&C systems and the Design Process for those systems. Key documents produced during this phase include Plant Licensing Documentation and quality program documents, such as the Software Life Cycle Process documents described in Section 6.3.1.

(2) System requirements phase

During this phase System Requirement Specifications are written for each I&C system. These specifications define performance, functional and HSI requirements, and system interfaces. The specifications also define the digital platform and basic architecture of each system using that platform.

(3) Hardware/software requirements phase

This phase produces specifications for hardware and software. Hardware specifications define the configuration of basic platform modules into chassis and cabinets. Electrical power, interface designs and application software specifications are documented in block

diagrams and elementary wiring diagrams. The software specification defines the functions and architecture of the software, including key partitions and interfaces. The functional design is documented primarily in logic diagrams and graphical screen layouts. The hardware and software specifications also define key requirements for Unit Testing and Integration Testing.

During this phase the analysis described in Section 6.5 are also conducted to confirm as much of the design as possible. Some aspects of the analysis may be based on assumptions that are confirmed, or revised as necessary, in later phases of the Design Process.

(4) Hardware/software design and production phase

During this phase the basic platform hardware is manufactured and configured in cabinets with all power and signal wiring. Application Software is also created for all controllers and HSI devices. Unit testing is conducted as required by the software specification. During this phase operations and maintenance manuals are created.

(5) Factory test phase

During this phase Basic Software and Application Software are integrated with the platform hardware for each system. A series of integration tests validates the designs first at the system level and then at the level of all I&C systems integration. Operations and maintenance manuals are also validated during this phase.

(6) Installation and commissioning phase

Activities in this phase are installation check and commissioning. During this phase controllers are connected with field equipment such as detectors, actuators, etc. Pre-operational tests are conducted to ensure all equipment has not been damaged during shipping or installation and that all interconnections are correct. Additional functional testing may be conducted as required by plant design requirements.

(7) Operation phase

During this phase the I&C systems are in operation. Self-diagnostics continuously monitor performance and calibration and manual tests are conducted periodically. Failed equipment is replaced. Software or hardware may be upgraded occasionally to accommodate new requirements, correct design errors or manage obsolescence.

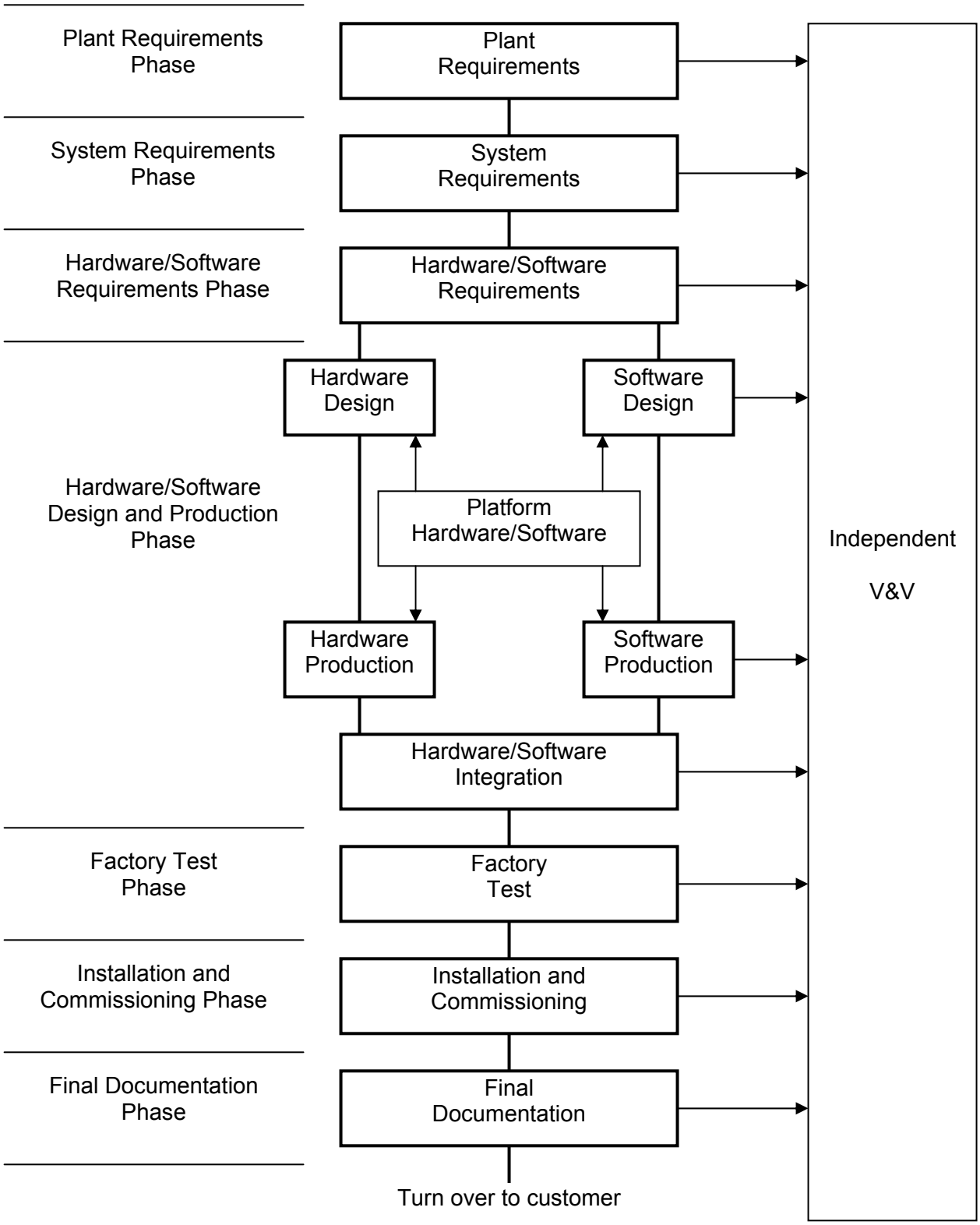


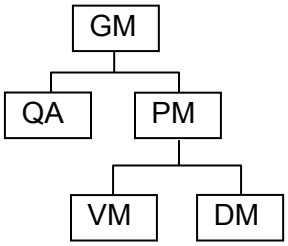
Figure 6.1-1 Safety System Development Process

6.2 Software Life Cycle Process Control

The organization, roles and responsibilities implemented to control the Application Software life cycle process for the PSMS are described in this section. The Software Life Cycle Process for the MELTAC Basic Software is described in the Digital Platform Topical Report.

6.2.1 Organization

The organizational structure to control the Software Life Cycle Process is shown in Fig. 6.2-1.



GM – general manager

QA – quality assurance organization
PM – project manager

VM – V&V team manager
DM – design team manager

Figure 6.2-1 Organizational Structure to Control the Software Life Cycle Process

6.2.2 Roles and Responsibilities

The roles and responsibilities for the key sections of the organization are described in this section.

(1) Project Manager (PM)

PM assures that process of design, V&V and quality assurance is appropriately implemented in accordance with Software Quality Assurance Plan.

(2) Design Team Manager (DTM)

The Design Team conducts all design activities for hardware and software. The DTM assures that the design team correctly performs the design for safety systems based on the technical requirements and the development process in accordance with Software Quality Assurance Plan.

(3) V&V Team Manager (VTM)

The V&V team performs software design verification and software validation to confirm that the requirements from the design specification are incorporated into the input and output documents for each phase of the software development process.

The V&V Team Manager is responsible for all activities of the V&V Team. He has sufficient resources (budget, staff, etc.) and authority to ensure V&V activities are not adversely affected by commercial and schedule pressures.

The V&V Team has technical competence equivalent to the Design team.

(4) QA Organization

The QA organization conducts independent audits of Design Team and V&V Team activities to confirm that requirements and implementation of the Software Life Cycle Process are appropriately planned and implemented in accordance with the Software Quality Assurance Plan.

The QA organization assures that any design or V&V activities subcontracted to other organizations also comply with the Software Quality Assurance Plan, This includes conformance of the suppliers' overall QA program.

6.3 Requirements, Implementation and Design Outputs for Software Life Cycle Process

In accordance with BTP HICB-14, a summary of the requirements, the implementation and the design outputs for the Software Life Cycle Process in Figure 6.1-1 are described in this section.

6.3.1 Software Life Cycle Process Requirements

This section describes the key contents of the documents that govern the Application Software life cycle process. These documents are generically applicable to Application Software for all systems and all projects. These plans are supplemented, as specified in these generic plans, by additional information that is documented in the Project Plan which is written uniquely for each project. Any deviations from the requirements in these generic plans are also documented in the Project Plan. The Project Plan also includes an assessment of the software project risk and the risk management plan.

(1) Software Management Plan

- Strategy for managing the software project.
- Method for monitoring progress against the software management plan
- Method for identifying any deviations from the software management plan in time to take corrective action
- Process for managing the project

(2) Software Development Plan

- Software life cycle used in the project including uniquely identifiable development, verification and support processes with well-defined inputs and outputs
- Strategy for managing the technical development effort
- Each life cycle activity is divided into well-defined tasks.
- Methods, techniques and tools to be used for software development
- Verification and configuration control requirements for software development environment and tools

- Standards and guidelines to be followed
- Requirements for the Project Plan to include schedule key work packages, milestones and hold points to avoid unexpected schedule delays

(3) Software Quality Assurance Plan

- Software quality assurance procedures for the entire software life cycle
- Traceability requirements to be maintained throughout the software life cycle
- Required reviews and audits by the QA organization
- Requirements and procedures for the software quality assurance records
- Method for ensuring that approved standards, methods and tools are applied throughout the software life cycle
- The method for establishing and maintaining the standards and methods for software V&V and software configuration management

(4) Software Integration Plan

- Procedures and controls for software integration, and for combined hardware/software integration
- Requirements for verifying the output products of the Engineering Tools

(5) Software Installation Plan

- Procedures for software installation, and for combined hardware/software installation
- Procedures and controls used to ensure the success of software/hardware integration

(6) Software Operation & Maintenance Plan

- Procedures necessary to start, operate and stop the software system
- Security requirements for the software system, such as prevention of unauthorized changes to hardware, software and system parameters,
- Timely evaluation of the effects of reported problems to support equipment operability determinations as required by plant technical specification
- Software, hardware and associated documentation required to maintain the delivered software
- Verification requirements for the output products of Engineering Tools or the results of Engineering Tool activities

(7) Software Training Plan

The Training Plan ensures that customers thoroughly understand the components, operation and maintenance of the PSMS.

- Description of the Training Program
- Methods, techniques and tools used to accomplish the training function
- Description of the Training System which is equivalent to the actual hardware/software system

(8) Software Safety Plan

The Software Safety Plan identifies critical plant requirements, such as trip function response time and fail-safe modes, that are assured through special attention throughout the software development process. This document describes the methods required to assure additional quality for these areas (e.g. design reviews, analysis, tests, etc).

(9) Software Verification and Validation Plan

- V&V applies to all PSMS software. The specific V&V activities are dependent on the safety significance of the software. The V&V Plan includes V&V requirements for each software category.
- Inputs and outputs for each phase of V&V activity
- Criteria to be used to verify the completion of each V&V task
- Methods for using a Requirements Traceability Matrix to confirm all requirements are addressed in each phase of the design
- Requirements for regression analysis and testing for changes after software baselining
- V&V reporting requirements including review documentation requirements, evaluation criteria and error reporting

(10) Software Configuration Management Plan

- Items requiring configuration control and procedures for placing these items under configuration control
- Procedures for tracking problem reports to ensure that each problem reported has been correctly resolved
- Control of all software design changes
- Approval process for authorizing all changes to baselines.

6.3.2 Software Life Cycle Process Implementation

Implementation outputs for the Software Life Cycle Process are described in this section.

(1) Safety Analysis

A Software Safety Analysis is performed to ensure that the safety system Application Software satisfies the plant's critical safety requirements. The Software Safety Analysis includes the following:

- Critical plant safety requirements are correctly indicated in the system requirement documents.
- Critical plant safety requirements are tracked throughout all phases of the development process.
- Software elements used to implement the critical plant safety requirements are identified. There is qualified evidence which demonstrates the quality of those elements.
- Problems identified by the Software Safety Analysis are documented and tracked to resolution

(2) V&V Analysis and Test Reports

V&V reports are provided for each V&V phase in accordance with the Software V&V Plan. V&V reports include review documentation requirements, evaluation criteria, error reporting.

(3) Configuration Management Reports

All changes to baselines are documented.

Problem reports are prepared to describe anomalous and inconsistent software and documentation.

Status accounting is performed for each set of life cycle activities prior to completion of those activities. The status accounting should document configuration item identifications, baselines, problem report status, change history and release status.

6.3.3 Software Life Cycle Process Design Outputs

Typical design outputs for the Software Life Cycle Process are described as follows.

(1) Requirement specification

- Safety system basic design requirement (including system performance requirements, system operational requirements, system design basis, etc.)
- Block diagram, Elementary wiring diagram (including technical description of software, interface of inputs/outputs, etc.)
- Setpoint list

(2) Design specification

- Specification for PSMS equipment

(3) Software document

- Software document for PSMS (Application Software hard copy)

(4) Operation & maintenance manuals

- User manuals

(5) Training manuals

- Training manuals

6.4 Life Cycle Process

Control methods of the life cycle process are described in this section.

6.4.1 Access Control

6.4.2 Design Change Management

All changes to the baselines in configuration management are performed in accordance with the following steps.

- Change Request is initiated by the relevant engineering section.
- Change Request is reviewed by the Design Team and the V&V Team.
- Change Request is approved by the Design Team and V&V Team Managers and the Project Manager.
- The design change is implemented.
- The revised baseline is documented.

6.4.3 Cyber Security Management

The following are cyber security control methods during the design phase.

- Access controls for the software tools which support software development are described in section 6.4.1.
- There is no communication between the Engineering Tool environment and other communication networks, such as the corporate Information Technology network, that would allow unintended changes or introduce malicious code.
- The Engineering Tool does not include virus protection, because there is no communication between this tool and other communication networks.
- Baselined software which is under configuration management, requires formal checkout and checkin to make changes. All changes are controlled by the Configuration Management procedures.
- The V&V Team specifically exams all software for unintended functions. This is accomplished by ensuring all specification requirements have been incorporated in the Application Software and ensuring the Application does not contain any unused functions.
- Final application software is transferred from the Engineering Tool to the PSMS controllers using software checks that confirm that no errors or changes have been introduced.

Plants are expected to follow the cyber security requirements of NEI 04-04, or equivalent. The following minimum cyber security control methods are required to ensure the integrity of software in the PSMS.

- Connections to the plant or corporate Information Technology network or to any other communication networks from the PSMS or PCMS are for outbound communication only.
- Engineering Tools are maintained under the same level of cyber security controls as the PSMS. As a minimum this includes administrative controls with key access or password to ensure configuration control, avoidance of unintended changes and avoidance of malicious code.
- Computers that run Engineering Tools are not connected to the corporate Information Technology network and to any other communication networks that are not under the same level of cyber security controls.

6.4.4 Life Cycle Management

(1) Quality Records Management

Quality records are collected and controlled in accordance with Quality Assurance Program (QAP) Description For Design Certification of the US-APWR, PQD-HD-19005.
This Quality Assurance Program requires records of completed items and activities affecting quality are appropriately stored. The records and their retention times are defined.

(2) Error and Corrective Action Reporting

Error and Corrective Action Reporting is performed in accordance with Quality Assurance Program (QAP) Description For Design Certification of the US-APWR, PQD-HD-19005.
This Quality Assurance Program requires reports for conditions adverse to quality. These reports are analyzed to identify trends. Significant conditions adverse to quality and significant adverse trends are documented and reported to responsible management. In the case of a significant condition adverse to quality, the cause is determined and actions to preclude recurrence are taken and the cause and corrective action are reported to management.

6.5 Analysis Method

6.5.1 FMEA Method

The Failure Modes and Effects Analyses (FMEA) demonstrates that:

- All credible PSMS failures are detectable (through self-diagnosis or manual surveillance tests).
- No credible single failure will prevent PSMS actuation.
- No credible single failure will result in spurious PSMS actuation.
- The PSMS will fail to the safe state for all credible failures. The safe state for RPS is trip. The safe state for ESFAS/SLS is as-is.
- Credible PCMS failures do not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the SAR.

This section describes the FMEA method.

Safety functions are designed with multiple divisions. Each safety division is independent from the other safety divisions and from the non-safety divisions. Independence ensures that credible single failures cannot propagate between divisions within the safety system or between safety and non-safety divisions. Therefore credible single failures can not prevent proper protective action at the system level. The credible single failures considered in the safety and non-safety divisions are described in the FMEA for each system. The FMEA follows the guidance of IEEE379, which is endorsed by RG1.53.

<u>Component</u>
The component being analyzed is identified by functional description (e.g. analog input module). Where there are multiple similar components additional descriptive information is added to ensure an unambiguous identification (e.g. chassis/slot location, specific module type, etc.)

<u>Failure Mode</u>
The failure modes of the component are defined in the terms of the component's output interface to other downstream components. Typical failure modes include High, Low, As-is. One row is included in the table for each credible failure mode.

<u>Method of Failure Detection</u>
The means by which the failure will come to the attention of the plant operation/maintenance staff are identified. This could be by automatic detection or manual testing.

Local Failure Effect
The consequent effect(s) of the failure on the component or on its adjunct components are described. Symptoms and local effects including dependent failure are also provided.

Effect on Protective Function or Plant
For safety systems the effect of the failure on the ability to complete the protective function or spurious actuation of the protective function is described, including identification of any degradation in performance or degree of redundancy. For non-safety functions the effect of the failure on the plant is described. Any plant challenges that are outside the boundary conditions of the Plant Safety Analysis are discussed. For safety and non-safety functions mitigating design features that prevent or limit the failure effects are discussed.

Fault Classification
Failures that are undetectable or result in effects that violate the system design basis are specifically highlighted. These failures are specifically justified or the system design is modified.

Table 6.5-1 Typical FMEA Table

Reactor Protection System

Component	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function	Fault Classification
Pressurizer pressure sensor	Fail low	Self-diagnostic alarm for input out of range	Partial reactor trip for one train	Remaining three trains provide safety function	A=acceptable design basis compliance

The FMEA for each I&C system is provided in Plant Licensing Documentation.

6.5.2 Reliability Analysis Method

The reliability of the safety I&C system to perform its safety functions is analyzed in the Probabilistic Risk Assessment (PRA).

This analysis starts with the simplified block diagram discussed above for the FMEA. This block diagram shows the major components that must operate correctly for actuation of the safety function. The Mean Time Between Failure (MTBF) is identified for each component. The MTBF for components of the MELTAC platform are provided in the Digital Platform Topical Report. The MTBF for other components is obtained from industry handbooks or manufacturers publications. The system reliability is calculated based on this system model and the MTBF of each component.

The reliability analysis credits internal redundancy within each train, and it credits all four available trains for each system.

However, the reliability analysis credits only three of four instrument channels for each measured parameter. This conservative approach ensures that the system meets the required PRA goals while operating in a degraded condition. Based on this there are no Limiting Conditions of operation expected for extended operation with an instrument channel out of service.

The reliability analysis credits the immediate detection of module failures that are tested by self-diagnostics. For failures in components that are manually tested and calibrated, the reliability analysis is based on a 24 month surveillance interval.

The reliability analysis for specific plant applications are discussed in Plant Licensing Documentation.

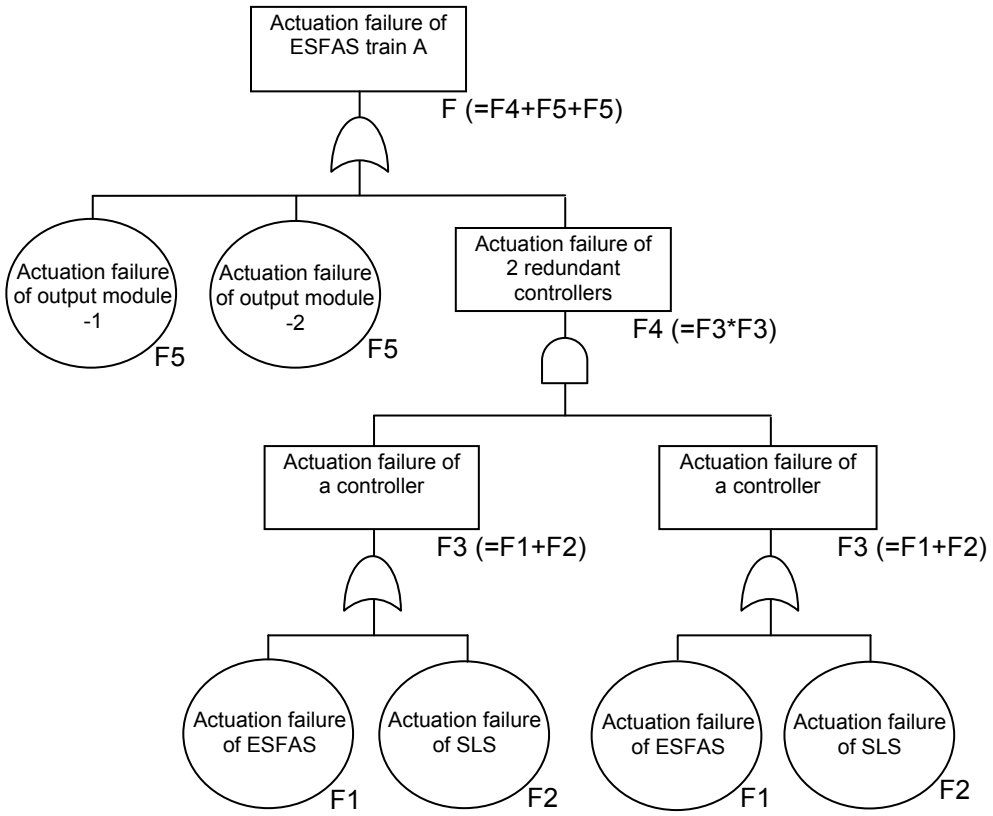


Figure 6.5-1 Typical FTA for Failure of ESFAS Actuation

6.5.3 Response Time Analysis Method

The response time of the safety functions is used in the plant safety analysis. The response time of each safety function is calculated by adding the response time of each component that makes up the system, from the process measurement to the actuation of the final component.

To illustrate the response time analysis method, the following configuration is the response time model for reactor trip.

Figure 6.5-2 Breakdown Response Time for Reactor Trip

6.5.4 Accuracy Analysis Method

The accuracy of each instrumentation loop for safety function is analyzed to determine the instrument channel set points. A typical loop consists of the following components:

- Sensor
- Analog input module

Loops that include an interface to the DAS would have an additional analog splitter/isolator.

The accuracy of the complete channel is calculated by combining the accuracy of each component in the loop using statistical methods. A square root of the sum of the squares (SRSS) method is applied. The accuracy of each component consists of the nominal accuracy plus uncertainty due to temperature effects and time dependent drift.

The typical formula for SRSS uncertainty calculation for one component in the loop takes the form:

$$A = \pm (B^2 + C^2 + D^2)^{1/2}$$

where

A = resultant uncertainty for one component
B, C, D = random and independent terms for each uncertainty element (e.g. temperature, time, etc).

The method is based on the guidance, ISA-RP67.04.02 -2000, “Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation.” The guidance provides the recommended practice for ISA-S67.04.01-2000 that is equivalent to ANSI/ISA-S67.04, Part I -1994 endorsed by RG 1.105.

To illustrate the accuracy analysis method, the uncertainty of the loop shown in the following figure is calculated below. The typical calculation model and calculation formula for the channel uncertainty of the instrumentation loop is described.

Figure 6.5-3 Typical Calculation Model for Channel Uncertainty of the Instrumentation Loop

6.5.5 Heat Load Analysis Method

The heat load of the components within each PSMS enclosure (i.e. cabinet or console in which PSMS equipment is mounted) is calculated to establish room Heating Ventilating and Air Conditioning (HVAC) sizing requirements. Proper HVAC sizing ensures the room ambient temperature stays within expected boundaries. The heat load for each PSMS enclosure is determined by the total consumption of electricity of the PSMS modules within the cabinet. The power consumption for each module is based on the MELTAC platform specifications for each module. Total electric power consumption is converted to total heat load.

The maximum temperature of the components within a PSMS enclosure is also calculated to ensure components operate below their maximum normal temperature (97°F [36°C]), and below their maximum qualified temperature (140°F [60°C]). To establish the internal cabinet operating temperature the temperature rise within the cabinet is calculated. The forced ventilation airflow within the cabinet is increased as necessary to ensure the normal and qualification limits are maintained. The heat rise calculations for each PSMS enclosure are confirmed by actual measurements during integration testing.

6.5.6 Seismic Analysis Method

Plant structures, systems, and components important to safety are required by GDC 2 to withstand the effects of earthquakes without loss of capability to perform their safety functions.

The seismic analysis method for the PSMS is based on Regulatory Guide 1.100, which endorses IEEE 344-1987.

The MELTAC platform (i.e. digital components and cabinet) is qualified by generic seismic type testing. The type testing method for the MELTAC platform is described in the Digital Platform Topical Report. This section explains the analysis methods used to confirm that the type tests bound the in plant conditions to which the MELTAC components will actually be exposed.

Seismic analyses, using the equivalent static acceleration method, and the mode superposition time-history method, are performed for the Safe Shutdown Earthquake (SSE). The analyses are performed to determine the seismic force distribution for use in the design of the nuclear island structures, and to develop in-structure seismic responses (accelerations,

displacements, and floor response spectra) for use in the analysis and design of seismic subsystems.

The seismic qualification methods for different configurations of MELTAC equipment within the PSMS are described as follow.

(1) Seismic Qualification for MELTAC components mounted within MELTAC cabinets

The seismic analysis confirms that the floor acceleration for each PSMS cabinet location in the plant is lower than the seismic acceleration value during type testing. The seismic analysis also confirms the total mass and distribution of equipment mounted within each cabinet is equivalent or less than the mass and distribution of the equipment mounted in the cabinet during type testing.

(2) Qualification of non-MELTAC enclosures

Special non-MELTAC enclosures, such as the Operator Console and Remote Shutdown Console are computer modeled using techniques such as the Finite Element Method (FEM). The computer model includes the mass and distribution of the equipment mounted within the enclosure. The model is computer stimulated with the floor response spectra for its specific location within the plant. The computer analysis confirms the structural integrity of the enclosure, including the maximum enclosure deflection, and the specific seismic accelerations at the mounting locations for MELTAC components (for use in item c., below).

(3) Qualification of MELTAC components mounted within non-MELTAC enclosures

The seismic accelerations at the equipment mounting locations (from item b. above) are compared to the seismic accelerations recorded at the equipment mounting locations during the MELTAC platform type tests. The analysis confirms that the type testing bounds the accelerations that will be seen by the MELTAC components in these special non-MELTAC enclosures.

6.5.7 EMI Analysis Method

The EMI qualification of the MELTAC platform is based on RG 1.180. The test is performed with a cabinet fully equipped with a typical configuration of components required for a safety system. The details of the EMI qualification testing are described in the Digital Platform Topical Report.

The EMI qualification analysis confirms that the type tested conditions bound the in plant conditions to which the MELTAC components will actually be exposed. This includes the configuration of the MELTAC components, and the wire routing, shielding and grounding. The EMI qualification analysis also confirms that the characteristics of the EMI environment for the type test bounds the EMI environment of the plant.

6.5.8 Fire Protection Analysis

Most components within the PSMS are manufactured from fire retardant materials to minimize the combustible load. The combustible load from the PSMS considered in the fire analysis is estimated based on the total content of flammable materials.

The fire protection analysis demonstrates the ability to achieve safe shutdown with a fire in one fire zone of the plant and the following failures of I&C equipment within that fire zone:

- The failures considered in the fire analysis include short circuits, open circuits and application of worst case credible faults in both common mode and transverse mode.
- The four trains of the PSMS and the PCMS are in five separate fire zones. The fire analysis considers the worst case spurious actuations that can result from the failures identified above for the equipment in the one zone with the fire.
- The MCR and RSC contain only HSI for multiple trains of the PSMS and the PCMS (DAS HSI is discussed below). The HSI is enabled in only one location at a time. A fire occurring in the RSC will have no impact on the plant because the HSI in this location is normally disabled. A fire occurring in the MCR will result in failures (as described above) initially in only one train (safety or non-safety), due to physical and electrical separation between trains. The fire will ultimately cause these failures in all trains. However, prior to this the MCR/RSC Transfer Switches will be activated to disable all MCR HSI. Therefore there will be no adverse effects on other trains.
- The DAS HSI is also located in the MCR. This HSI interfaces to all four PSMS trains. The DAS HSI is disabled if the MCR/RSC Transfer Switch is in the RSC position. The DAS HSI contains two circuits (1) permissive circuits and (2) system / component switch circuits. Permissive and switch circuits must both actuate to generate control actions in the PSMS. These two circuits are physically and electrically separated, including a fire barrier. In addition, most components within the DAS are manufactured from fire retardant materials to minimize the combustible load. If a fire starts in one DAS circuit, it will be detected by MCR operators, since the DAS is in a continuously manned location. Therefore, there is sufficient time for activation of the MCR/RSC Transfer Switch so that the DAS interfaces are disabled in the PSMS, before spurious DAS signals, which may be generated due to propagation of the fire, can cause adverse PSMS control actions.
- The automated section of the DAS contains two subsystems, which must both actuate to generate any control signals to the PSMS or PCMS. These two subsystems are in separate fire area so that a fire in one area may spuriously actuate only one PSMS division.

Figure 6.5-4 shows this fire protection configuration of DAS.

Figure 6.5-4 Configuration of Fire Protection for Diverse Actuation System

7.0 FUTURE LICENSING SUBMITTALS

The complete MHI digital I&C design is described in four Topical Reports:

- Safety I&C System Description And Design Process (this report)
- Digital Platform
- Human Systems Interface
- Defense in Depth and Diversity

Table 7-1 summarizes the additional information related to this Topical Report to be submitted for NRC approval in future Plant Licensing Documentation. Table 7-1 summarizes all items identified in previous sections of this report. This Plant Licensing Documentation, in combination with the contents of this Topical Report, the contents of the other Topical Reports identified above, and any items for Plant Licensing Documentation described in those other Topical Reports is expected to be sufficient to allow the NRC to make a final safety determination. Other documentation generated during the design process is available for NRC audit, as may be needed to allow the NRC to fully understand the MHI design and design process. These documents will be made available in the MNES office, which is in close proximity to the US NRC office.

Table 7-1 Future Licensing Submittals

Description	Section
Changes in implementation detail, as needed	1.0
Non-safety system descriptions	2.0
Specific buildings and equipment locations	3.1 GDC 2
Sharing of this Equipment between multiple units, as needed	3.1 GDC 5, A.5.13
Specific reactor trip functions	3.1 GDC 12. A.4.4
Specific instrumentation and control functions	3.1 GDC 13
Electric power sources for this Equipment	3.1 GDC 17, A.8
Specific protection system functions	3.1 GDC 20, A.4.4
Specific features to limit Reactivity Control Malfunctions	3.1 GDC 25
Specific functions to meet the Post-TMI requirements	3.1 10CFR50.34
Qualification of this instrumentation	3.1 10 CFR 50.49
Conformance to the requirements in items iv thru vii	3.1 10 CFR 52.47
Inspections, tests, analyses and acceptance criteria	3.1 10 CFR 52.79
FMEA for specific plant applications	3.3 RG 1.53, 4.5, 6.5.1
System level manual initiation switches at the RSP, as needed	3.3 RG 1.62
Specific accident monitoring instrumentation	3.3 RG 1.97
Conformance to seismic qualification type test envelope	3.31 RG 1.100
Process instrumentation uncertainties and the resulting safety related setpoints	3.3 GDC15, RG 1.105
Instrument Sensing Lines	3.3 RG 1.151
Conformance to lightning protection requirements	3.3 RG 1.204
Compliance with BTP HICB 1 thru 6	3.4
Anticipatory trips, as needed	3.4 BTP 9
Methods used for verifying the accuracy and response time of RTDs	3.4 BTP 13
Design Acceptance Criteria, Level of detail	3.3 RG 1.206
CCF coping for all DBAs	3.4 BTP 19
System response time for conformance with the plant design basis	3.4 BTP 21

Description	Section
Descriptions of specific plant systems	3.5 NUREG-0800
Cables for interfaces to/from this Equipment	3.6 IEEE 383
Design and qualification of other enclosures	3.6 IEEE 420
MCR layout design	4.1.a
Number of operators for other plants (not US-APWR)	4.1.a.1
Safe shutdown condition for other plants (not US-APWR)	4.1.a.14
Number of SLS trains for other plants (not US-APWR)	4.1.b.3, 4.2.3
Location of SLS I/O for other plants (not US-APWR)	4.1.b.3
Location of PCMS I/O for other plants (not US-APWR)	4.1.c.3
Number of ESF/ESFAS trains for other plants (not US-APWR)	4.2.2
Specific bypass or override function of ESF actuation	4.2.2
Number and configuration of controllers in each SLS train	4.2.3
SLS I/O configuration	4.2.3
TSC and EOF description	4.2.5.b
External test equipment for DAS, as needed	4.2.6
Test frequency for the reactor trip breakers	4.4.1
Test frequency for binary process monitoring devices	4.4.1
Test frequency for the plant process components	4.4.1, A.5.7
Test frequency for the plant process instrumentation	4.4.1
Additional spatially dedicated fixed position controls, as needed	5.1.11
Prevention for high dust influence, as needed	5.2.2.d
Reliability analysis for specific plant applications	6.5.2, A.5.15
Plant safety analyses (not I&C specific)	A.4.1 , A.4.2
Credit for manual actions and associated HSI	A.4.5.1, A.4.5.4, A.5.8.1, A.6.1
HSI for discretionary manual actions	A.4.5.4
Number, locations and processing method for spatially dependent variables	A.4.6
Equipment protective provisions	A.4.11
Security system for access control in the plant	A.5.9
Color coding for labels and name tags	A.5.11
Description of auxiliary features (e.g. electrical power sources, building HVAC)	A.5.12
Direct process measurements and algorithms for calculated functions	A.6.4
Automatically initiated Operating Bypasses	A.6.6
Parameters with multiple setpoints that are automatically or manually disabled	A.6.8.2
Plant components with Execute Feature Manual Controls	A.7.2

8.0 REFERENCES

In this section, references referred in this topical report except for applicable codes and standards and regulatory guidance in section 3 are enumerated.

1. MUAP-07005, “Safety System Digital Platform -MELTAC-” (attached JEXU-1012-1002)

2. MUAP-07006, “Defense-in-Depth and Diversity”

3. MUAP-07007, “HSI System Description and HFE Process”

4. PQD-HD-19005, “Quality Assurance Program (QAP) Description For Design Certification of US-APWR”

5. ISA-RP67.04.02-2000,“Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation”

6. “Cyber Security Program for Nuclear Power Reactors”, NEI 04-04,February 2005.

7. System 80+ Design Certification Document (DCD)

Appendix A Conformance to IEEE 603-1991

This appendix describes conformance of the PSMS to the requirements of IEEE 603. The section numbers follow the sections in IEEE603. All sections pertain to the 1991 version of this standard unless specifically noted.

A.1. Scope

This conformance section addresses the PSMS, which is the instrumentation and control portion of the safety system.

A.2. Definitions

The definitions are applicable to the PSMS.

A.3. References

The PSMS conforms to all referenced standards, as explained below.

A.4. Safety System Designation

A.4.1 Design Basis Events

The PSMS is designed to protect the health and safety of the public by limiting the release of radioactive material during accident conditions to acceptable limits The safety analyses described in Plant Licensing Documentation demonstrate that even under conservative critical conditions for design basis accidents, the safety systems provide confidence that the plant is put into and maintained in a safe state following accident conditions. The events considered in the safety analysis and limits of plant conditions are described in Plant Licensing Documentation.

A.4.2 Safety Functions and Corresponding Protective Actions

The functions of the PSMS credited in the plant safety analysis are described in Plant Licensing Documentation.

A.4.3 Permissive Conditions for Each Operating Bypass Capability

In the PSMS protective functions are initiated and accomplished during various reactor operating modes. Automatic or manual block of a protective function is provided during specific plant modes if that protective action would spuriously actuate due to normally expected plant conditions. Permissive interlocks are provided for manual blocks and both manual and automatic blocks are automatically removed whenever the appropriate plant conditions are not met. Hardware and software used to initiate an automatic block, provide a permissive for a manual block, and achieve automatic removal of the automatic or manual blocks are part of the PSMS and, as such, are designed in accordance with the criteria in this

report. Initiation of manual blocks may be by either the Operational VDUs or Safety VDUs. In either case the PSMS provides the necessary safety permissive and automatic removal.

A.4.4 Variables Required to be Monitored for Protective Action

The specific variables monitored for reactor trips are described in Plant Licensing Documentation. The information provided in this section is typical.

(1) Reactor Trip Signals
- Source Range Neutron Flux High
- Intermediate Range Neutron Flux High
- Power Range Neutron Flux High
- Power Range Neutron Flux Rate High
- Emergency Core Cooling System Actuation Signal
- Over Temperature Delta-T High
- Over Power Delta-T High
- Pressurizer Pressure High
- Pressurizer Pressure Low
- Reactor Coolant Flow Low
- Reactor Coolant Pump Speed Low
- Steam Generator Water Level Low
- Steam Generator Water Level High
- Pressurizer Water Level High
- Manual Actuation

Table A.4.4-1 lists the ranges for each reactor trip variable, except for the ECCS actuation signal trip. Those variables for the ECCS actuation signals are described in Table A.4.4-2

The specific variables monitored for engineered safety features (ESFs) actuation are described in Plant Licensing Documentation. The information provided in this section is typical.

(2) Emergency Core Cooling System (ECCS) Actuation Signals
- Pressurizer Pressure Low-Low
- Main Steam Line Pressure Low
- Containment Vessel Pressure High
- Manual Actuation

(3) Main Steam Line Isolation Signals
- Containment Vessel Pressure High-High
- Main Steam Line Pressure Low
- Main Steam Line Pressure Rate High
- Manual Actuation

(4) Containment Vessel Spray Actuation Signals
- Containment Vessel Pressure High-High-High
- Manual actuation

(5) Containment Vessel Isolation Signals

- ECCS Actuation Signal
- Containment Vessel Spray Actuation Signal
- Manual Actuation

(6) Emergency Feed Water Signals
- Steam Generator Water Level Low
- ECCS Actuation Signal
- Manual Actuation

Table A.4.4-1 lists typical ranges for the variables used in Engineered Safety Features actuation.

The Plant Technical Specifications specify the allowable values for the limiting conditions for operation (LCOs) and the trip setpoints for the reactor trip and ESF actuation.

Table A.4.4-1 Reactor Trip Variables, Ranges
(Design Basis for Reactor Trip) (Nominal)

Protective Functions	Variables to be Monitored	Range of Variables
Source Range Neutron Flux High	Neutron flux	6 decades of neutron flux
Intermediate Range Neutron Flux High	Neutron flux	Approximately 8 decades of neutron flux overlapping source range by 2 decades and including 100% rated power
Power Range Neutron Flux High	Neutron flux	1 to 120% of rated power
Power Range Neutron Flux Rate High	Neutron flux	1 to 120% of rated power
Over Temperature Delta-T High Level High	Delta-T	
	Reactor coolant inlet temp. (Tcold)	510 to 630°F (270 to 330°C)
	Reactor coolant outlet temp. (Thot)	530 to 650°F (280 to 340°C)
	Pressurizer pressure	1700 to 2500psig (11 to 17.5MPa[gage])
	Neutron flux (difference between top and bottom power range detectors)	-60 to +60% (Δψ)

Table A.4.4-1 Reactor Trip Variables, Ranges
(Design Basis for Reactor Trip) (Nominal)

Protective Functions	Variables to be Monitored	Range of Variables
Over Power Delta-T High	Delta-T	
	Reactor coolant inlet temp. (Tcold)	510 to 630°F (270 to 330°C)
	Reactor coolant outlet temp. (Thot)	530 to 650°F (280 to 340°C)
	Neutron flux (difference between top and bottom power range detectors)	-60 to +60% (Δψ)
Pressurizer Pressure High	Pressurizer pressure	1700 to 2500psig (11 to 17.5MPa[gage])
Pressurizer Pressure Low	Pressurizer pressure	1700 to 2500psig (11 to 17.5MPa[gage])
Reactor Coolant Flow Low	Reactor coolant flow	0 to 120% of rated flow
Reactor Coolant Pump Speed Low	Reactor coolant pump speed	0 to 120% of rated speed
Steam Generator Water Level Low	Steam generator water Level	0 to 100% of span (narrow range taps)
Steam Generator Water Level High	Steam generator water Level	0 to 100% of span (narrow range taps)
Pressurizer Water Level High	Pressurizer water level	0 to 100% of span
Manual	Switch position	N/A

Table A.4.4-2 Engineered Safety Features Actuation, Variables, Ranges (Nominal)		
ESF Functions	Variable to be Monitored	Range of Variable
Emergency Core Cooling System (ECCS) Actuation Signals		
Pressurizer Pressure Low-Low	Pressurizer pressure	1700 to 2500psig (11 to 17.5MPa[gage])
Main Steam Line Pressure Low	Main steam line pressure	0 to 1400psig (0 to 9.5MPa[gage])
Containment Vessel Pressure High	Containment vessel pressure	-7 to 80psig (-0.05 to 0.55MPa[gage])
Manual	Switch position	N/A
Main Steam Line Isolation Signals		
Containment Vessel Pressure High-High	Containment vessel pressure	-7 to 80psig (-0.05 to 0.55MPa[gage])
Main Steam Line Pressure Low	Main steam line pressure	0 to 1400psia (0 to 9.5MPa[gage])
Main Steam Line Pressure Rate High	Main steam line pressure	0 to 1400psig (0 to 9.5MPa[gage])
Manual	Switch position	N/A
Containment Vessel Spray Actuation Signals		
Containment Vessel Pressure High-High-High	Containment vessel pressure	-7 to 80psig (-0.05 to 0.55MPa[gage])
Manual	Switch position	N/A
Containment Vessel Isolation Signals		
Containment Vessel Spray Actuation Signal	Containment vessel pressure	-7 to 80psig (-0.05 to 0.55MPa[gage])
Manual	Switch position	N/A
Emergency Feed Water Signals		
Steam Generator Water Level Low	Steam generator water Level	0 to 100% of span (narrow range taps)
ECCS Actuation Signal	Same as ECCS Actuation Signal	Same as ECCS Actuation Signal
Manual Actuation	Switch position	N/A

A.4.5 The Minimum Criteria for Each Action Controlled by Manual Means

Means are provided in the MCR for manual initiation of protective functions at the system level. Manual control of safety systems at the component level is provided from the MCR and the Remote Shutdown Room.

A.4.5.1 Emergency actuation of reactor trip and/or ESFAS is automatically provided by the PSMS, immediately after an accident is automatically detected. The automated systems allow the plant to achieve a safe stable state with no credited manual operator actions. Operators can detect abnormal conditions by monitoring plant instrumentation and can manually initiate the same protective actuations at any time. In general, manual actuation of reactor trip or ESFAS is not required or credited in the plant safety analysis. Any deviation from this is explained in Plant Licensing Documentation. Whether or not these manual actions are credited, there are no interlocks that prevent manual actuation.

To maintain the safe stable state, some manual operator actions are needed.
In general, the PSMS is designed so the earliest operator actions are not required for certain time period defined in the safety analysis from the onset of the accident. Earlier manual operator actions for specific events (e.g. Boron Dilution) are described in Plant Licensing Documentation, including appropriate HFE justification.

Interlocks ensure that operator actions cannot defeat an automatic safety function during any plant condition where that safety function may be required. In addition, when safety functions are automatically initiated, interlocks ensure that opposing manual actions cannot be taken until acceptable plant conditions are achieved.

A.4.5.2 Manual actuation of one protective action does not interfere with subsequent automatic actuation of other protective actions. There is no capability to completely block or bypass the initiation of any automatic actuation, except when plant condition interlocks permit this blocking as discussed in Section A.4.3, above.

A.4.5.3 The safety related ventilation system provides cooling, heating, humidity control, filtration, pressurization, ventilation, and air conditioning service to the MCR. This ventilation system and its support systems consist of four redundant trains, while the emergency systems consist of two trains, and provide these functions in a reliable and failure tolerant fashion. If offsite power is not available, each onsite safety Emergency Generator provides backup power. In case of accident, the MCR is isolated to protect operators from invading radioactivity, and the emergency ventilation system which consists of two redundant trains is activated.

A.4.5.4 The manual operator actions credited in the safety analysis for accident mitigation, and the variables displayed in the MCR specifically for this purpose are described in Plant Licensing Documentation. The variables used by operators to monitor the plant and take discretionary manual actions are also discussed in Plant Licensing Documentation. The HSI for all of these manual functions is available on Safety VDUs and multi-channel Operational VDUs.

A.4.6 Spatially Dependent Variables

The minimum number, locations and processing method for spatially dependent variables is described in Plant Licensing Documentation. The description below is typical.

Thermowell-mounted resistance temperature detectors (RTDs) installed in each reactor coolant loop provide the hot and cold leg temperature signals required for input to the protection and control functions. The hot leg temperature measurement in each loop is accomplished using three fast-response, dual-element, narrow-range RTDs. The three thermowells in each hot leg are mounted approximately 120 degrees apart in the cross-sectional plane of the piping, to obtain a representative temperature sample. The temperatures measured by the three RTDs are different due to hot leg temperature streaming and vary as a function of thermal power. The PSMS averages these signals to generate a hot leg average temperature.

Radially varying cold leg temperature is not a concern because the RTDs are located downstream of the reactor coolant pumps. The pumps provide mixing of the coolant so that radial temperature variations do not exist.

Radial neutron flux is not a spatially dependent concern because of core radial symmetry. Calculations involving overtemperature and overpower deltaT use axial variation in neutron flux. Excore detectors furnish this axially-dependent information to the overtemperature and overpower calculations in the RPS.

A.4.7 Range of Conditions for Safety System Performance

The PSMS is located in a mild environment. The equipment is seismically qualified to meet safe shutdown earthquake (SSE) levels. The equipment is also qualified for electromagnetic and radio frequency interference.

The Emergency Power Supply system (EPS), from emergency busses and generators, and the Uninterruptible Power Supply system (UPS), from plant batteries and inverters, supplies electrical power to the PSMS. The PSMS performs its safety functions within the range of voltage and frequency provided by EPS and UPS.

A.4.8 Functional Degradation of Safety Functions

The PSMS is located in plant areas that provide protection from accident related hazards such as missiles, pipe breaks and flooding. The redundant trains of the PSMS are isolated from each other and isolated from non-safety systems. Isolation ensures functional and communications independence and independence for fires and electrical faults. The design life of PSMS components is maximized when operated continuously in a controlled ventilation environment. The PSMS will operate reliably for extended periods with loss of ventilation.

A.4.9 Reliability

The reliability analysis methods for the PSMS are described in Section 6.5.2. This analysis ensures that the PSMS meets the reliability requirements assumed in the Probabilistic Risk Assessment (PRA). The PSMS includes either N trains or N+1 trains, depending on the application. N is the number of trains needed to meet the single failure criterion and the number of trains needed to meet the PRA goals.

A.4.10 The Critical Points in Time or the Plant Conditions

The PSMS automatically initiates appropriate protective actions when a plant condition monitored by the system reaches a preset level. The critical points in time are determined by the PSMS response time modeled in the accident analysis. The PSMS is designed and tested to meet the response times assumed in the accident analysis.

The operator can reset the PSMS system level actuation signal using two distinct and deliberate actions. There are no automatic resets of the system level actuation signals.

A.4.11 Equipment Protective Provisions

No credible single failure of an equipment protective device prevents the initiation or accomplishment of a safety function at the system level.

The PSMS continuously checks internal conditions such as power supply and digital component operability. Components are automatically shut down under component failure conditions that may lead to unpredictable system performance. These checks are conducted independently within each train of the PSMS, therefore a spurious shutdown of PSMS equipment will only affect one train.

The equipment protective features are designed to place the safety systems in a safety state, or into a state that has been demonstrated to be acceptable, if the safety equipment fails or the equipment protective device operates. Each protection function has different characteristics and therefore different techniques are used to achieve a fail-safe design. Examples of protective features for selected functions include:

- Reactor trip circuits are designed to fail in the tripped state.

- Engineered safety features actuated components are designed to fail into a de-energized state. This state that has been demonstrated to be acceptable if conditions such as disconnection, loss of power source, or postulated adverse environments are experienced.

- Sensor circuits are designed, where possible, so that a loss of power will produce a safe signal or will produce an off-scale value or a signal that can be identified by the protection system as bad. Digital protective equipment input circuits are designed to recognize off-scale or bad values and take appropriate action (alarm, actuate or use redundant signal or equipment where available, etc.)

- Actuation signals from multiple PSMS trains are provided for selected actuated equipment to improve the reliability of the protection system and minimize the impact of equipment protective provisions.

Equipment protective provisions may also be included in the instrumentation monitored by the PSMS and the plant components controlled by the PSMS. Provisions such as electrical fault and thermal overload protection are common in safety related plant components. Any provisions of this type are described in Plant Licensing Documentation. Since all equipment protective provisions are independent within each train of the safety systems, a spurious shutdown of plant equipment will only effect one train.

A.4.12 Other Special Design Basis

The PSMS complies with all applicable regulatory and industry criteria as described in Section 3. A non-safety DAS is included to provide the functions necessary to reduce the risk associated with postulated common cause failures of critical PSMS functions. The DAS is separate, independent and isolated from the PSMS. The DAS is diverse from the PSMS in all design aspects, including software, hardware, function and HSI.

A.5. Safety System Criteria

A.5.1 Single Failure Criterion

A credible single failure within the PSMS does not prevent the initiation or accomplishment of a protective function at the system level, even when a channel is intentionally bypassed for test or maintenance.

The safety system includes sufficient redundancy to meet system performance requirements even if the system is degraded by a single failure. Redundancy begins with the sensors monitoring the variables and continues through the signal processing and actuation electronics. Redundant actuations are also provided.

Connections between redundant divisions or connections that carry signals to or from non-safety systems are designed to ensure that faults or erroneous data originating in one division cannot propagate and cause failure of another division. The design ensures that any erroneous operation that may be caused by signals from other safety divisions, including the non-safety divisions, is within the boundaries of the safety analysis and is mitigated by other protective actions.

One design goal of the PSMS is to minimize inadvertent reactor trips and ESF actuations. Redundancy is provided for critical circuits which could malfunction and give an erroneous trip or ESF actuation signal. The reactor trip breaker arrangement prevents a single failure from causing a reactor trip. The two-out-of-four actuation logic for reactor trip requires trip signals from two-out-of-four divisions.

The design to reduce the likelihood of inadvertent trips or engineered safety features actuations does not negate the ability of the safety system to meet the single failure criterion, even when channels are bypassed for test or maintenance.

A.5.2 Completion of Protective Action

Once initiated, either automatically or manually, protective functions proceed to completion. In addition, system level signals cannot be manually reset until the plant condition is restored to a pre-determined setpoint. Any exception to this is described in Plant Licensing Documentation. The operator can override ESF actuation, after the protective function proceeds to completion. The override can be initiated only on a component-by-component basis by deliberate intervention using two distinct manual actions.

A.5.3 Quality

The quality of PSMS components and modules and the quality of the PSMS design process is controlled by a program that meets the requirements of ASME NQA-1-1994.

Conformance to ASME NQA-1-1994 is described in the QA Topical Report.

A.5.4 Equipment Qualification

Section 5.2 describes the environmental and seismic qualification of the PSMS.

A.5.5 System Integrity

PSMS is located in plant areas that provide protection from natural phenomena related hazards such as tornadoes, and accident related hazards such as missiles, pipe breaks and flooding. The equipment is environmentally and seismically qualified and qualified for input power variations.

A.5.6 Independence

A.5.6.1 Between Redundant Portions of a Safety System

Division independence is carried throughout the PSMS as well as the sensors and the devices actuating the protective function. Physical separation is used to achieve separation of all redundant train components. Wiring for redundant trains uses physical separation or barriers to provide independence of the circuits. Separation of wiring is achieved using separate wireways, cable trays, and containment penetrations for each train. Separation distances and barriers conform to regulatory guides or industry standards. Where this is not possible due to physical constraints, such as for HSI devices on control panels, analysis and testing is used to

demonstrate the adequacy of the isolation method. Separate power feeds energize each redundant protection division.

Where redundant equipment communicates, such as between the trains of the RPS, fiber optic cables are employed to preserve electrical independence of the divisions. Communications independence is achieved by communication modules that are separate from the safety function processing modules. Functional independence is achieved by coincidence voting logic.

A.5.6.2 Between Safety Systems and Effects of a Design Basis Event

The PSMS is qualified to maintain its functional capability during and after a design basis earthquake. The PSMS is protected against other design basis events by other plant structures.

A.5.6.3 Between Safety Systems and Other Systems

A.5.6.3.1 Interconnected Equipment

Signals from the PSMS are transmitted to the PCMS and DAS through conventional analog/binary isolation devices or fiber optic cables. Conventional analog/binary isolators are part of the safety system and are tested to confirm that credible failures on the non-safety side of the isolation device do not prevent the PSMS from meeting its performance requirements. Credible failure tests include short circuits; open circuits; grounds; and the application of the maximum transverse or common cause AC or DC potentials that may be present in any cabinet where the isolation device is located or in any wireway where its electrical or optical lines run.

A.5.6.3.2 Equipment in Proximity

Non-safety wiring is separated from safety wiring or separated with barriers. Analyses or tests are used to verify the adequacy of wire routing where separation distances are less than those suggested by regulatory guides or industry standards.

A.5.6.3.3 The Effects of a Single Random Failure

There are no single failures that can result in a design basis event and also prevent proper action of any portion of the PSMS. Although sensors are shared between the PCMS and PSMS, the PCMS includes Signal Selection Algorism which prevents erroneous control system actions due to single sensor failures. So if a shared sensor were to fail, one train of the PSMS is degraded, but there would be no resulting design basis event that would require protective action.

A.5.6.4 Detailed Independence Criteria

IEEE 384-1981, Regulatory Guide 1.75

Cables of one train are run in separate raceway and physically separated from cables of other trains. Group N raceways are separated from safety groups A, B, C and D. Raceways from group N are routed in the same areas as the safety groups according to spatial separation stipulated in Regulatory Guide 1.75-2005 and IEEE 384-1992

The exceptions to the guidance in Regulatory Guide 1.75 are based on test results used to support exceptions to the separation guidance for operating nuclear power plants. For example, minimum separation distance of Teflon-wire is 5mm based on test. This exception is used in the diverse HSI Panel.

Non-Class 1E circuits are electrically isolated from Class 1E circuits, and Class 1E circuits from different separation groups are electrically isolated. Isolation is by qualified isolation devices, shielding and wiring techniques, physical separation (in accordance with Regulatory Guide 1.75 for circuits in raceways), or an appropriate combination thereof.

When isolation devices are used to isolate Class 1E circuits from non-Class 1E circuits, the isolation devices are identified as Class 1E and are treated as such. Beyond the isolation device(s) these circuits are identified as non-Class 1E and are separated from Class 1E circuits in accordance with the above separation criteria.

A.5.7 Capability for Test and Calibration

Testing from the sensor inputs of the PSMS through to the actuated equipment is accomplished through a series of overlapping sequential tests. The majority of the tests are conducted automatically through self-diagnostics. Most remaining manual tests may be performed with the plant at full power. Manual and automatic tests are described in Section 4.4.

The test frequency for manual tests is based on a reliability analysis. This analysis demonstrates the need to conduct manual tests for PSMS equipment no more frequently than once per 24 months, which is no more than once per fuel cycle. Therefore conducting manual tests for PSMS equipment on-line or off-line, during refueling shutdown, is at the discretion of the plant owner.

A.5.8 Information Displays

A.5.8.1 Displays for Manually Controlled Actions

In general, there are no manually controlled actions credited in the plant safety analysis. All actions credited for accident mitigation are automated. Any exception to this is described in Plant Licensing Documentation.

Should manual actions be required by the safety analysis the Safety VDUs provide the following HSI functions:

- Plant process indications that would lead operators to take those actions
- Required manual controls
- Indications to confirm the manual controls have been executed (i.e. component status feedback)

The non-safety PCMS provides the following HSI functions:

- Plant process indications that would lead operators to take those actions
- Prompting alarms
- Indications to confirm the effectiveness of the manual control actions

The HSI Topical Report provides a description of all PCMS HSI functions.

A.5.8.2 System Status Indication

The actuation of a protective action is indicated at the train level and component level by the PCMS using data received from the PSMS.

The following information is generated by the PSMS for display by the PCMS:

- Parameter values that lead to trip/actuations
- Pre-trip and trip alarms signals indicating status of partial trip signal paths
- Status indication for system level actuation signal paths and train level actuation signal paths
- Actuated equipment status – This status is displayed at the component level and also at the train level. Train level displays use logic to show the successful or unsuccessful actuation of all required components.

In addition the Safety VDU provides actuated equipment status at the component level.

A.5.8.3 Indication of Bypasses

The PSMS provides the operator with indications of bypassed status, as described in Section 4.2.5-b. The display of the status information for RPS and ESFAS allows the operator to identify the specific bypassed functions, and to determine if the trip/actuation logic has reverted to a condition that accommodates the inoperable equipment (i.e. two-out-of-three, two-out-of-two, one-out-of-two). In addition to the status indication, an alarm is sounded in the MCR if more than one bypass is attempted for a given protection function.

SDCV indications for each train are automatically provided for inoperable or bypassed conditions that adversely affect the function of the train. SDCV indications can also be manually actuated for conditions that are not automatically monitored. For example, for

unmonitored components, such as hand-wheel valves, the component's status is manually entered in the PCMS data base. The component status is displayed on Operational VDU displays. In addition, if that status adversely affects the operability of the train, the train level SDCV indication is automatically activated. The train level SDCV indication can also be manually actuated directly for other unexpected conditions that may have no manual data entry capability in the PCMS data base.

A.5.8.4 Location of Displays

All PSMS controls and indications are located on the Operator Console or the Remote Shutdown Console. These consoles are ergonomically designed for easy operator access to information and controls. Displays for normally used Operational VDUs include controls and associated information and alarms. Safety VDUs, which provide backup HSI, normally provide information displays. Screen navigation is required to switch to control displays. The indications and alarms on the MCR Large Display Panel are easily viewable from the Operational VDUs, Safety VDUs, or conventional system level PSMS controls.

Detailed descriptions of the HSI are provided in the HSI Topical Report.

A.5.9 Control of Access

The PSMS controllers and I/O are located within cabinets with key locks. Cabinet doors are expected to be normally locked. Each train of PSMS cabinets are expected to be located in physically separate equipment rooms, that are also accessible only with the appropriate security access (e.g. key or security card). Plant Licensing Documentation describes the security system and physical arrangement.

Access to controls within the PSMS cabinets is required to access any controls that can disable or change the functional configuration of the system. This includes access to setpoint adjustments, channel calibration adjustments, test points, and software change points.

A.5.10 Repair

The PSMS facilitates the recognition, location, replacement, repair and adjustment of malfunctioning components or modules. The built-in diagnostics, along with the Operational VDU alarms and Engineering Tool provide a mechanism for rapidly identifying and locating malfunctioning assemblies.
Channel bypass permits replacement of malfunctioning sensors or PSMS components, without jeopardizing plant availability, and while still meeting the single failure criterion.

A.5.11 Identification

Equipment within each redundant train of the PSMS has distinct color coded labels. Cabinets are marked on their exterior with labels clearly visible from cabinet entry doors. Equipment, within a cabinet, that is the same train as the cabinet marking, is not marked. However, any equipment that is not the same train as the cabinet marking, is marked to show its different train assignment. For cabinets or control panels that contain multiple trains of equipment, such as the Operator Console, all PSMS equipment is distinctly marked by train. Non-cabinet mounted PSMS equipment, such as the RSC and Transfer Switch Panel are also marked.

Plant Licensing Documentation describes distinct train color coding for labels and name tags. The color-coding described below is typical.

Division	Color Coding
Train A	RED with WHITE lettering
Train B	GREEN with WHITE lettering
Train C	BLUE with WHITE lettering
Train D	YELLOW with BLACK lettering
Non-Train N	White with Black Lettering

A.5.12 Auxiliary Features

The PSMS is built on the digital platform described in the Digital Platform Topical Report. All components of this platform, with the exception of the Engineering Tool Personal Computer, are safety related and conform to the requirements for safety systems. Other auxiliary features such as electrical power sources and building HVAC are described in Plant Licensing Documentation.

The PSMS includes safety related functions such as reactor trip and ESF actuation. It also typically includes the following associated non-safety related functions:

- Alarm signal generation
- Indications for RG 1.97 Rev.3 Type D and E variables
- Indications for system actuation status
- Cabinet temperature monitoring
- Door open monitoring
- Input power monitoring

These associated non-safety functions are not isolated from the PSMS. Therefore they are considered part of the safety system. The Software Quality Assurance Plan, Verification & Validation Plan and Configuration Management Plan impose sufficient requirements to ensure these associated non-safety functions do not degrade the safety system below an acceptable level.

A.5.13 Multi-Unit Stations

In general, there is no sharing of PSMS components between units. Any sharing of components is discussed in Plant Licensing Documentation.

A.5.14 Human Factors

The Human Factors Engineering program applied to the PSMS functions is described in the HSI Topical Report.

A.5.15 Reliability

The PSMS reliability is used in the Probabilistic Risk Assessment (PRA). That analysis is described in Plant Licensing Documentation. The component level reliability which is the basis for the PRA analysis is described in the Digital Platform Topical Report. The system level reliability method which is the basis for the PRA analysis is described in Section 6.5.2.

A.5.16 Common Cause Failure (IEEE 603-1998)

The following features of the PSMS minimize the potential for Common Cause Failure:

- Isolation of redundant divisions
- Conformance to the single failure criterion
- Equipment qualification to preclude external influence
- A digital platform with many years of operation in nuclear power applications
- Simple deterministic software processing
- Graphic based software design tools
- Graphic based maintenance tools for calibration, test and repair
- Segmentation of diverse reactor trip functions into separate RPS controllers (discussed in more detail below)
- A rigorous design process for systems, software and hardware that meets the requirements for safety related systems
- A rigorous independent Verification and Validation process that meets the requirements for safety related systems

For each design basis accident addressed in the plant safety analysis, two diverse parameters are used to detect the event and initiate protective actions. These diverse parameters are processed in two separate Controller Groups within each train of the RPS. The following table shows typical examples of this diversity.

Table A.5.16-1 Diverse Parameters in Two Separate Controller Groups

The plant safety analysis describes the two parameters and how they are credited in the safety analysis.

The two diverse parameters are monitored by two separate sensors which interface to two separate digital controllers within the RPS. The two controllers each process these inputs to

generate reactor trip and/or ESF actuation signals. This two fold diversity is duplicated in each redundant RPS train. The processing of diverse parameters results in functional redundancy within each RPS train. This functional redundancy helps to minimize the potential for CCF.

Regardless of the minimum potential for CCF achieved through the design features described above, the Defense-in-Depth and Diversity Topical Report describes the potential effects of a CCF and features of the Overall I&C Design which allow coping with a CCF concurrent with plant accidents. The Defense-in-Depth and Diversity Topical Report also describes the coping analysis for a typical plant accident.

A.6. Sense and Command Features - Functional and Design Requirements

The Sense and Command Features of the safety system are encompassed by the PSMS, including the RPS, ESFAS, SLS and Safety Grade HSI System.

A.6.1 Automatic Control

The PSMS is designed to automatically initiate reactor trip and actuate the engineered safety features necessary to mitigate the effects of anticipated operational occurrences and design basis accidents. The PSMS automatically initiates appropriate safety functions whenever a variable measured by the PSMS reaches a trip or actuation setpoint. In general, the earliest operator actions are not required for certain time period defined in the safety analysis. Any exception to this is described in Plant Licensing Documentation.

A.6.2 Manual Control

Manual initiation of reactor trip is provided at the train level. Manual initiation of ESF is also provided at the train level. Fixed-position controls are provided for use as a manual backup to the automatic protection signals provided by the PSMS. Manual initiation of a protective function performs all actions performed by automatic initiation, such as providing the required action sequencing functions and interlocks.

Manual initiation of reactor trip bypasses all PSMS controllers, as shown in Fig.A.6.2-1. Manual initiation of ESF bypasses the RPS controllers as shown in Fig.A.6.2-1. Manual initiation depends on the operation of the minimum of equipment and, once initiated, proceeds to completion unless deliberate operator intervention is taken. No single failure in either the automatic portion, manual portion, or shared portion prevents manual or automatic initiation of a protective function at the division level. This capability is achieved through the redundant structure of the PSMS.

Redundant manual controls and indications are also provided by redundant PSMS trains to maintain safe stable plant conditions after the protective actions are completed. In addition, the PSMS provides redundant manual controls and indications to achieve and maintain safe shutdown.

All manual controls and indication discussed above are located in the MCR and are easily accessible to the operator. Manual controls and indications to achieve safe shutdown are also located on the Remote Shutdown Console.

Figure A.6.2-1 Manual Control

A.6.3 Interaction between the Sense and Command features and other Systems

Certain information derived from PSMS channels is used by the PCMS to control the plant. This reduces the number of penetrations into critical pressure boundaries, such as into the reactor coolant loops, pressurizer and steam generators. It also helps reduce congestion and enhance separation.

A control system Signal Selection Algorithm within the PCMS is used so that a malfunctioning PSMS channel does not cause the control system to take erroneous control actions that would result in a challenge to the PSMS. Therefore, where protection signals are used for control, functional isolation is provided between the control and protection systems.

A.6.4 Derivation of System Inputs

To the extent feasible and practical, protection system inputs are derived from signals that are direct measures of the desired variables. The PSMS calculates some variables where direct measurement is not feasible. These are the thermal overtemperature delta-T reactor trip and the overpower delta-T reactor trip. Direct process measurements for protective actions and algorithms for calculated functions is described in Plant Licensing Documentation.

A.6.5 Capability for Testing and Calibration

Input sensors from each PSMS are compared continuously in the PCMS to detect abnormal deviations. This comparison occurs after the analog to digital conversion in the PSMS so it also checks the accuracy of PSMS components. PSMS sensors are periodically stimulated to calibrate the sensor for expected time dependent drift. The readout for this calibration also occurs after the analog to digital conversion in the PSMS, so it also checks the accuracy of PSMS components.

The PSMS facilitates the diagnosis, location, and repair or adjustment of malfunctioning components.

A.6.6 Operating Bypasses

Test and maintenance bypasses are described in Section A.6.7. Several Operating Bypasses are described in this section.

Some Operating Bypasses automatically block certain protective actions that would otherwise prevent modes of operations such as start-up. These Operating Bypasses are automatically initiated separately within each PSMS division when the plant process permissive condition is sensed by the PSMS input channel(s). Automatically initiated Operating Bypasses are described in Plant Licensing Documentation. The following is a list of typical automatically initiated Operating Bypasses:

- Source Range Neutron Flux High Trip is bypassed automatically by Power Range Neutron Flux High (P-10)
- Reactor Coolant Flow Low 2-out-of-4 Trip is bypassed automatically by Power Range Neutron Flux High (P-7)

Other Operating Bypasses must be manually initiated. These Operating Bypasses can be manually initiated separately within each PSMS division when the plant process permissive condition is sensed by the PSMS input channel(s). Manually initiated Operating Bypasses are described in Plant Licensing Documentation. The following is a list of typical manually initiated Operating Bypasses:

- Source Range Neutron Flux High Trip is bypassed manually with Intermediate Range Neutron Flux High (P-6)
- Intermediate Range Neutron Flux High Trip is bypassed manually with Power Range Neutron Flux High (P-10)
- Pressurizer Pressure Low ECCS actuation is bypassed manually with Pressurizer Pressure (P-11)
- Main Steam Line Pressure Low ECCS actuation is bypassed manually with Pressurizer Pressure (P-11)

All Operating Bypasses, either manually or automatically initiated, are automatically removed when the plant moves to an operating regime where the protective action is required if an accident occurred. Status indication is provided in the control room for all Operating Bypasses.

A.6.7 Maintenance Bypass

a. Input Channel Bypass

The safety system is designed to permit the unrestricted bypass for maintenance, test, or repair of any one protection input channel in the group of channels monitoring a selected variable. This bypass is accomplished during power operation without causing initiation of a protective function. The system also meets the single failure criterion while permitting power operation for an indefinite period of time with one channel of the selected variable bypassed. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

With one channel bypassed, the RPS does not permit the bypass of a second channel in the group monitoring the same variable. An attempt to apply multiple bypasses is blocked, and trip/actuation is not triggered by the attempt.

Generally, there are four protection channels for each actuation function. Accident and reliability analyses assume that one of these channels is in the bypass mode at the time of the accident. This assumption precludes potential limitations that might have otherwise been placed on the use of the bypass feature.

For each input, the technical specifications limit the period allowed for two channels to be out of service (i.e. either two failed in a non-trip state or one in bypass and one failed in a non-trip state). The time specified in the technical specifications is determined by considering the probability of the event the significance of the input to event mitigation.

b. Train Level RPS Bypass

Each RPS train takes inputs from one or more input process sensors, performs compensation or other calculation which terminates in one or more bistable functions where the process variable is compared against setpoints. The coincidence logic portion of the RPS receives the partial trip outputs from these comparisons and combines them with the partial trip status of the other channels to initiate a Reactor Trip or ESF actuation.

Each RPS train has the ability to bypass all partial trip input signals from the other trains. This function is useful if an entire RPS train is taken out of service. When an entire RPS train is bypassed each individual channel for that train is bypassed and therefore subject to the alarms and interlocks described above for individual input channels. Therefore, if input channels are previously bypassed the RPS train level bypass may be blocked or alarmed. Similarly, if an RPS bypass is already active, any attempt to put additional input channels in bypass is alarmed / blocked.

Each ESFAS train also has the ability to bypass all system level ESF actuation input signals from any one RPS train. This function is useful if an entire RPS train is taken out of service. When an RPS train is bypassed, interlocks are generated to block bypassing additional RPS trains.

There are four RPS channels for each ESF actuation function. Accident and reliability analyses assume that one of these channels is in the bypass mode at the time of the accident. This assumption precludes potential limitations that might have otherwise been placed on the use of the bypass feature.

For each ESF actuation function, the technical specifications limit the period allowed for an RPS train to be bypassed or out of service. The time specified in the technical specifications is determined by considering the degree of redundancy provided for the function and the importance of the function.

c. ESF Actuation Bypass

Bypasses are provided in each SLS train to block the automatic actuation of one or more ESFAS functions (e.g. SI, EFW, MSI, etc.). The purpose of this bypass is to allow maintenance on an EFS process system or to accommodate an ESFAS controller failure. For example if you bypass SI-A, SI will not actuate for Train A, but Train B, C and D are not affected. There are alarms for ESFAS or SLS out of service conditions that would block functionality at the train level.

A.6.8 Setpoint

A.6.8.1 Setpoint Uncertainties

Three values applicable to reactor trip and ESF actuations are specified:

- Safety analysis limit
- Allowable value
- Nominal setpoint

The safety analysis limit is the value assumed in the accident analysis and is the least conservative value.

The allowable value is the Technical Specification value and is obtained by subtracting a safety margin from the safety analysis limit. The safety margin accounts for instrument error, process uncertainties such as flow stratification and transport factor effects etc. The method used for combining all process measurement effects to determine the total process measurement uncertainty is described in Section 6.5.4.

The nominal setpoint is the value set into the equipment and is obtained by adding or subtracting allowances for instrument drift from the allowable value. The nominal setpoint allows for the normal expected instrument loop drift between calibration intervals, such that the Technical Specification allowable value setpoint limit is not exceeded under normal operation. The method used for combining the drift of all analog devices in a process loop to determine the resulting total instrument loop drift is described in Section 6.5.4.

As described above, allowance is made for process uncertainties, instrument error, instrument drift, and calibration uncertainty to obtain the nominal setpoint value that is actually set into the equipment. The only requirement on the instrument's accuracy is that, over the instrument span, the error must always by less than or equal to the error value allowed in the accident analysis. The instrument does not need to be the most accurate at the setpoint value as long as it meets the minimum accuracy requirement. The accident analysis accounts for the expected errors at the actual setpoint.

A.6.8.2 Multiple Setpoints

Multiple trip setpoints are used for some reactor trip parameters. Some of these trip setpoints are automatically enabled or disabled based on setpoints for other plant parameters which are indicative of different modes of plant operation. These plant mode monitoring parameters provide positive means to ensure that the more restrictive trip setpoint is used.

Other trip setpoints are manually enabled or disabled based on administrative controls. To manually disable a setpoint a permissive interlock must be reached. This interlock can be based on the same process parameter or an alternate process parameter. If the interlock permissive condition is no longer satisfied the manually disabled setpoint is reenabled.

The hardware and software used to prevent improper use of less restrictive trip settings are considered part of the PSMS.

Parameters with multiple setpoints that are automatically or manually disabled are described in Plant Licensing Documentation. For example Power Range Neutron Flux High is used typically to manually enable/ disable the Low or High setpoint.

A.7. Executive Features - Functional and Design Requirements

The Execute Features of the safety system include the Reactor Trip Breakers, the breakers and motor starters for ESF components and all ESF components (e.g. pumps, valves etc.). The Sense and Command Features of the Safety System, which are encompassed by the PSMS, actuate these Execute Features. The Reactor Trip Breakers are actuated directly by the PSMS. Some plant components are also actuated directly by the PSMS, such as solenoid operated valves. Other plant components, such as pumps and motor operated valves, are actuated by the PSMS via breakers and/or motor starters.

A.7.1 Automatic Control

The Execute Features respond to control signals from the PSMS. The PSMS output signals may be the result of automatic or manual control signals. The priority between automatic and manual controls, and between manual controls at different operating locations is based on logic that resides within the PSMS.

A.7.2 Manual Control

Manual controls that are an integral part of the Execute Features typically include conventional control switches located on breakers or motor starters, or in proximity to plant process components. These are referred to as Execute Feature Manual Controls. These manual controls are typically provided for maintenance of the plant process component. The Execute Feature Manual Controls are not part of the PSMS (i.e. the Sense and Command Features). These manual controls are not required for any design basis event, including safe shutdown from outside the MCR.

During normal operation, the Execute Feature Manual Controls are in a passive state which allows automatic/manual controls from the PSMS to control the plant component. If an Execute Feature Manual Control is activated it can block or override control from the PSMS. Should this occur, the component is considered inoperable and appropriate train level inoperable indications are provided in the MCR, as described in Section A.4.11, above. The Execute Feature Manual Controls are located in security controlled access areas, or behind key locked cabinet doors.

Plant components with Execute Feature Manual Controls are described in Plant Licensing Documentation.

A.7.3 Completion of Protective Action

The protective actions are latched in the Sense and Command Features of the PSMS to ensure protective actions go to completion. This latching within the PSMS compensates for Execute Features that do not inherently latch, as described below.

Once actuated the breakers inherently remain in their actuated position. A deliberate opposite control signal is needed to reposition the breaker. This applies to the reactor trip breakers and breaker controlled plant components. Therefore when a breaker is actuated (open or close) from the PSMS, the protective action inherently goes to completion.

Motor-starters, motor-operated valves and solenoid valves also inherently remain in their actuated position, if the actuated position is the de-energized position. If the PSMS requires the component to energize for the protective action, the component will respond to the PSMS, but will reposition to its deenergized state, when the PSMS actuation signal is removed. Therefore the PSMS latches the protective action signal to ensure completion of the protective action. A deliberate automatic or manual control action is required to unlatch the PSMS control logic.

It is noted that once travel for a motor-operated valve is competed, the valve will remain in its position even after the PSMS control signal is removed. A deliberate automatic or manual control action is required to reposition a motor-operated valve.

A.7.4 Operating Bypass

There are no Operating Bypasses in the Execute Features.

A.7.5 Maintenance Bypass

The Execute Feature Manual Controls, discussed above, may be considered Maintenance Bypasses. These controls have access controls. In addition, if Execute Feature Manual Controls disable a safety system, plant administrative controls ensure this occurs in only one safety division at a time. Plant Technical Specifications limit the amount of time plant systems may be in an inoperable condition.

A.8. Power Source Requirements

Power sources are described in Plant Licensing Documentation.

Appendix B Conformance to IEEE 7-4.3.2 -2003

This appendix describes conformance of the digital PSMS to the requirements of IEEE 7-4.3.2. The section numbers follow the sections in IEEE 7-4.3.2. All sections pertain to the 2003 version of this standard unless specifically noted.

B.1. Scope

This conformance section addresses the computer portions of the PSMS.

B.2. References

The PSMS conforms to all referenced standards, as explained below.

B.3. Definitions and abbreviations

The definitions are applicable to the PSMS.

B.4. Safety System Design Basis

No requirements beyond IEEE Std 603-1998 are necessary.

B.5. Safety System Criteria

B.5.1 Single Failure Criterion

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.2 Completion of Protective Action

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.3 Quality

B.5.3.1 Software Development

The software development process for the PSMS application software is described in section 6.

B.5.3.1.1 Software quality metrics

The process for establishing software quality metrics for the PSMS application software is described in section 6.

B.5.3.2 Software tools

The software tools are described in the Digital Platform Topical Report.
The use of these tools for developing application software is described in section 6.3 of this Topical Report.

B.5.3.3 Verification and Validation

The verification and validation for the digital platform software is described in the Digital Platform Topical Report. The verification and validation for the system application software is described in section 6.

B.5.3.4 Independent V&V (IV&V) requirements

The independent verification and validation requirements for the digital platform software are described in the Digital Platform Topical Report. The basic organization of independent verification and validation for the safety I&C system is described in section 6.2.

B.5.3.5 Software configuration management

The software configuration management for the digital platform software is described in the Digital Platform Topical Report. The software configuration management for the system application software is described in section 6.

B.5.3.6 Software project risk management

The software project risk management for the digital platform software is described in the Digital Platform Topical Report. The software project risk management for the system application software is controlled by software life cycle process activities described in section 6.3.

B.5.4 Equipment Qualification

B.5.4.1 Computer system testing

The computer system testing for the digital platform software is described in the Digital Platform Topical Report.

B.5.4.2 Qualification of existing commercial computers

There are no commercial computers in the PSMS.

B.5.5 System Integrity

B.5.5.1 Design for computer integrity

The computer integrity for the digital platform software is described in the Digital Platform Topical Report. The computer integrity for the system application software is described in section 6.1.

B.5.5.2 Design for test and calibration

The design for test and calibration for the system application software is described in section 5.1.9.

B.5.5.3 Fault detection and self-diagnostics

The fault detection and self-diagnostics is described in the Digital Platform Topical Report.

B.5.6 Independence

The methods used to ensure independence between computers in different safety divisions and between computers in safety and non-safety systems is described above. The methods include:

a. Electrical independence
Data communications between computers in different safety divisions or between safety and non-safety computers are transmitted through fiber optic cables. The fiber optic cables provide inherent isolation for electrical faults.

b. Data processing independence
The PSMS employs communication processors that are separate from the processors that perform safety logic functions. The safety processors and communication processors communicate via dual ported memory. This ensures there is no potential for communications functions, such as handshaking, to disrupt deterministic safety function processing.

c. No ability to transfer unpredicted data
There is no file transfer capability in the PSMS. Only predefined communication data sets are used between the PSMS trains and between the PSMS and PCMS. Therefore any unknown data is rejected by the PSMS.

d. No ability to alter safety software
The software in the PSMS cannot be changed through the communication interface between PSMS trains or the communication interface for the PCMS. The PSMS software is changeable only through the Maintenance Network which is key locked and alarmed. The Maintenance Network is used only within the same train.

e. Additional protection against cyber threats
The PCMS and PSMS will be controlled under the most stringent administrative controls for cyber security. There is only one-way communication to other systems that are not under these same controls.

The following additional design features are specific to the interface between Operational VDUs in the PCMS and the PSMS.

f. Acceptable safety function performance
Signals from the PCMS are enabled or disable in the SLS logic through manual controls on the Safety VDUs. Therefore manual controls from the Safety VDU can have priority over any non-safety controls from the PCMS. In addition, the logic in the SLS blocks non-safety signals from the PCMS when any safety function signal is present, such as a safety interlock or ESFAS signal.

g. Failures of non-safety systems are bounded by the safety analysis
Any plant condition created by the worst case erroneous/spurious non-safety data set (e.g. non-safety failure commanding spurious opening of a safety relief valve) is bounded by the plant safety analysis. This analysis is based on spurious communication of a single data set (i.e. one erroneous control command) because spurious communication of multiple erroneous control commands is not considered credible. The basis for this credible failure mode is described in Appendix C.

Figure B.5.6-1 Software Isolation (Non-Safety VDU / Safety System)

B.5.7 Capability for Test and Calibration

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.8 Information Displays

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.9 Control of Access

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.10 Repair

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.11 Identification

The identification for the digital platform software is described in the Digital Platform Topical Report. The identification for the system application software is described in section 6.1

B.5.12 Auxiliary Features

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.13 Multi-Unit Stations

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.14 Human Factors

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.15 Reliability

The reliability for the digital platform is described in the Digital Platform Topical Report. The reliability method for the system is described in section 6.5.2.

B.6. Sense and Command Features - Functional and Design Requirements

No requirements beyond IEEE Std 603-1998 are necessary.

B.7. Executive Features - Functional and Design Requirements

No requirements beyond IEEE Std 603-1998 are necessary.

B.8. Power Source Requirements

No requirements beyond IEEE Std 603-1998 are necessary.

Appendix C Prevention of Multiple Spurious Commands and Probability Assessment

C.1. Prevention of Multiple Spurious Commands

C.2. Probability Assessment

Figure C.2-1 Probability Assessment Flow