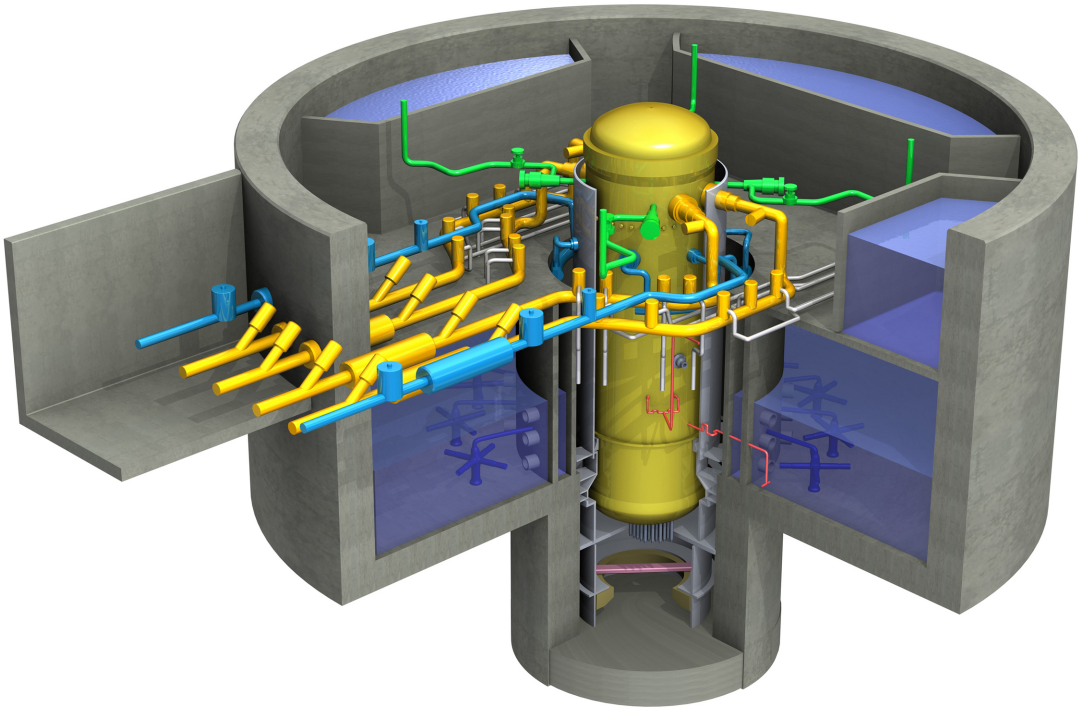
GE-Hitachi Nuclear Energy

26A6642AW
Revision 4
September 2007



ESBWR Design Control Document
Tier 2

Chapter 7
Instrumentation and Control Systems

Contents

7. Instrumentation and Control Systems 7.1-1

7.1 Introduction 7.1-1

7.1.1 Distributed Control and Information System 7.1-1
7.1.2 Q-DCIS General Description Summary 7.1-2
7.1.2.1 Q-DCIS Safety-Related Design Bases Summary 7.1-5
7.1.2.2 Q-DCIS Power Generation Design Bases Summary 7.1-5
7.1.2.3 Q-DCIS Safety Evaluation Summary 7.1-5
7.1.2.4 Q-DCIS Regulatory Requirements Conformance Summary 7.1-5
7.1.2.5 Q-DCIS Testing and Inspection Requirements Summary 7.1-6
7.1.2.6 Q-DCIS Operator Interface Requirements Summary 7.1-6
7.1.2.7 Q-DCIS Boundary Summary 7.1-6
7.1.2.8 Q-DCIS Major Systems Description Summary 7.1-6
7.1.3 Q-DCIS Specifics 7.1-11
7.1.3.1 Q-DCIS Design Bases 7.1-11
7.1.3.2 Q-DCIS Description 7.1-12
7.1.3.3 Q-DCIS Safety Evaluation 7.1-17
7.1.3.4 Q-DCIS Testing and Inspection Requirements 7.1-22
7.1.3.5 Q-DCIS Instrumentation and Control Requirements 7.1-22
7.1.3.6 Q-DCIS Boundaries 7.1-23
7.1.4 N-DCIS General Description Summary 7.1-23
7.1.4.1 N-DCIS Safety-Related Design Bases Summary 7.1-26
7.1.4.2 N-DCIS Nonsafety-Related Design Bases Summary 7.1-26
7.1.4.3 N-DCIS Safety Evaluation Summary 7.1-27
7.1.4.4 N-DCIS Regulatory Requirements Conformance Summary 7.1-27
7.1.4.5 N-DCIS Testing and Inspection Requirements Summary 7.1-27
7.1.4.6 N-DCIS Operator Interface Requirements Summary 7.1-28
7.1.4.7 N-DCIS System Boundaries 7.1-28
7.1.4.8 N-DCIS Major Systems Description Summary 7.1-28
7.1.5 N-DCIS Specifics 7.1-30
7.1.5.1 N-DCIS Design Bases 7.1-31
7.1.5.2 N-DCIS Description 7.1-34
7.1.5.3 N-DCIS Safety Evaluation 7.1-53
7.1.5.4 N-DCIS Testing and Inspection Requirements 7.1-56
7.1.5.5 N-DCIS Instrumentation and Control Requirements 7.1-56
7.1.5.6 N-DCIS Major System Interfaces 7.1-56
7.1.6 General DCIS Conformance with Regulatory Requirements and Industry Codes and Standards 7.1-60
7.1.6.1 Code of Federal Regulations 7.1-60
7.1.6.2 General Design Criteria 7.1-61
7.1.6.3 Staff Requirements Memorandum 7.1-61
7.1.6.4 Regulatory Guides 7.1-62
7.1.6.5 Branch Technical Positions 7.1-66
7.1.6.6 Industry Standards 7.1-68

7.1.7 COL Information 7.1-81
7.1.8 References 7.1-81
7.2 Reactor Trip System 7.2-1
7.2.1 Reactor Protection System 7.2-1
7.2.1.1 System Design Bases 7.2-1
7.2.1.2 System Description 7.2-3
7.2.1.3 Safety Evaluation 7.2-17
7.2.1.4 Testing and Inspection Requirements 7.2-23
7.2.1.5 Instrumentation and Control Requirements 7.2-24
7.2.2 Neutron Monitoring System 7.2-30
7.2.2.1 System Design Bases 7.2-30
7.2.2.2 System Description 7.2-35
7.2.2.3 Safety Evaluation 7.2-44
7.2.2.4 Testing and Inspection Requirements 7.2-49
7.2.2.5 Instrumentation and Control Requirements 7.2-50
7.2.3 Suppression Pool Temperature Monitoring 7.2-53
7.2.3.1 System Design Bases 7.2-53
7.2.3.2 System Description 7.2-54
7.2.3.3 Safety Evaluation 7.2-55
7.2.3.4 Testing and Inspection Requirements 7.2-59
7.2.3.5 Instrumentation and Controls Requirements 7.2-59
7.2.4 COL Information 7.2-59
7.2.5 References 7.2-59
7.3 Engineered Safety Features Systems 7.3-1
7.3.1 Emergency Core Cooling System 7.3-1
7.3.1.1 Automatic Depressurization System 7.3-1
7.3.1.2 Gravity-Driven Cooling System 7.3-10
7.3.2 Passive Containment Cooling System 7.3-22
7.3.3 Leak Detection and Isolation System 7.3-23
7.3.3.1 System Design Bases 7.3-23
7.3.3.2 System Description 7.3-24
7.3.3.3 Safety Evaluation 7.3-25
7.3.3.4 Testing and Inspection Requirements 7.3-30
7.3.3.5 Instrumentation and Controls Requirements 7.3-30
7.3.4 Control Room Habitability System 7.3-31
7.3.4.1 System Design Bases 7.3-31
7.3.4.2 System Description 7.3-31
7.3.4.3 Safety Evaluation 7.3-33
7.3.4.4 Testing and Inspection Requirements 7.3-37
7.3.4.5 Instrumentation and Control Requirements 7.3-37
7.3.5 Engineered Safety Features Safety System Logic and Control 7.3-37
7.3.5.1 System Design Bases 7.3-37
7.3.5.2 System Description 7.3-38
7.3.5.3 Safety Evaluation 7.3-41
7.3.5.4 Testing and Inspection Requirements 7.3-47

7.3.5.5 Instrumentation and Controls Requirements 7.3-47
7.3.6 COL Information 7.3-48
7.3.7 References 7.3-48
7.4 Safety-Related Safe-Shutdown and Nonsafety-Related Cold Shutdown Systems 7.4-1
7.4.1 Standby Liquid Control System 7.4-1
7.4.1.1 System Design Bases 7.4-1
7.4.1.2 System Description 7.4-2
7.4.1.3 Safety Evaluation 7.4-3
7.4.1.4 Testing and Inspection Requirements 7.4-7
7.4.1.5 Instrumentation and Control Requirements 7.4-8
7.4.2 Remote Shutdown System 7.4-8
7.4.2.1 System Design Bases 7.4-8
7.4.2.2 System Description 7.4-9
7.4.2.3 Safety Evaluation 7.4-11
7.4.2.4 Testing and Inspection Requirements 7.4-14
7.4.2.5 Instrumentation and Control Requirements 7.4-14
7.4.3 Reactor Water Cleanup/Shutdown Cooling System 7.4-14
7.4.3.1 System Design Bases 7.4-14
7.4.3.2 System Description 7.4-15
7.4.3.3 Safety Evaluation 7.4-17
7.4.3.4 Testing and Inspection Requirements 7.4-19
7.4.3.5 Instrumentation and Control Requirements 7.4-19
7.4.4 Isolation Condenser System 7.4-19
7.4.4.1 System Design Bases 7.4-19
7.4.4.2 System Description 7.4-20
7.4.4.3 Safety Evaluation 7.4-20
7.4.4.4 Testing and Inspection Requirements 7.4-24
7.4.4.5 Instrumentation and Control Requirements 7.4-24
7.4.5 COL Information 7.4-25
7.4.6 References 7.4-25
7.5 Safety-Related and Nonsafety-Related Information Systems 7.5-1
7.5.1 Post Accident Monitoring Instrumentation 7.5-1
7.5.1.1 System Design Bases 7.5-1
7.5.1.2 System Descriptions 7.5-2
7.5.1.3 Safety Evaluation 7.5-2
7.5.1.4 Testing and Inspection Requirements 7.5-9
7.5.1.5 Instrumentation and Controls Requirements 7.5-9
7.5.2 Containment Monitoring System 7.5-9
7.5.2.1 System Design Bases 7.5-10
7.5.2.2 System Description 7.5-11
7.5.2.3 Safety Evaluation 7.5-12
7.5.2.4 Testing and Inspection Requirements 7.5-15
7.5.2.5 Instrumentation and Control Requirements 7.5-16
7.5.3 Process Radiation Monitoring System 7.5-16
7.5.3.1 Design Bases 7.5-16

7.5.3.2 System Description 7.5-17
7.5.3.3 Safety Evaluation 7.5-17
7.5.3.4 Testing and Inspection Requirements 7.5-20
7.5.3.5 Instrumentation and Control Requirements 7.5-20
7.5.4 Area Radiation Monitoring System 7.5-20
7.5.4.1 Design Bases 7.5-20
7.5.4.2 System Description 7.5-20
7.5.4.3 Safety Evaluation 7.5-20
7.5.4.4 Testing and Inspection Requirements 7.5-22
7.5.4.5 Instrumentation and Control Requirements 7.5-22
7.5.5 Pool Monitoring Subsystems 7.5-22
7.5.5.1 System Design Bases 7.5-24
7.5.5.2 System Description 7.5-24
7.5.5.3 Safety Evaluation 7.5-24
7.5.5.4 Testing and Inspection Requirements 7.5-24
7.5.5.5 Instrumentation and Control Requirements 7.5-24
7.5.6 Wetwell-to-Drywell Vacuum Breaker Monitoring 7.5-24
7.5.7 COL Information 7.5-24
7.5.8 References 7.5-24
7.6 Interlock Systems 7.6-1
7.6.1 High Pressure/Low Pressure Interlock Systems 7.6-1
7.6.1.1 System Design Bases 7.6-1
7.6.1.2 System Description 7.6-1
7.6.1.3 Safety Evaluation 7.6-4
7.6.1.4 Testing and Inspection Requirements 7.6-7
7.6.1.5 Instrumentation and Control Requirements 7.6-7
7.6.2 Other Interlock Systems 7.6-7
7.6.2.1 Isolation – Between the Diverse Protection System and Safety-Related Systems 7.6-7
7.6.3 COL Information 7.6-7
7.6.4 References 7.6-7
7.7 Control Systems 7.7-1
7.7.1 Nuclear Boiler System 7.7-1
7.7.1.1 System Design Bases 7.7-2
7.7.1.2 System Description 7.7-3
7.7.1.3 Safety Evaluation 7.7-5
7.7.1.4 Testing and Inspection Requirements 7.7-7
7.7.1.5 Instrumentation and Control Requirements 7.7-8
7.7.2 Rod Control and Information System 7.7-8
7.7.2.1 System Design Bases 7.7-8
7.7.2.2 System Description 7.7-10
7.7.2.3 Safety Evaluation 7.7-24
7.7.2.4 Testing and Inspection Requirements 7.7-25
7.7.2.5 Instrumentation and Control Requirements 7.7-25
7.7.3 Feedwater Control System 7.7-26

7.7.3.1 System Design Bases 7.7-26
7.7.3.2 System Description 7.7-27
7.7.3.3 Safety Evaluation 7.7-28
7.7.3.4 Testing and Inspection Requirements 7.7-30
7.7.3.5 Instrumentation and Control Requirements 7.7-30
7.7.4 Plant Automation System 7.7-32
7.7.4.1 System Design Bases 7.7-32
7.7.4.2 System Description 7.7-32
7.7.4.3 Safety Evaluation 7.7-33
7.7.4.4 Testing and Inspection Requirements 7.7-34
7.7.4.5 Instrumentation and Control Requirements 7.7-34
7.7.5 Steam Bypass and Pressure Control System 7.7-35
7.7.5.1 System Design Bases 7.7-35
7.7.5.2 System Description 7.7-35
7.7.5.3 Safety Evaluation 7.7-37
7.7.5.4 Testing and Inspection Requirements 7.7-39
7.7.5.5 Instrumentation and Control Requirement 7.7-39
7.7.5.6 Major Instrument Interfaces with SB&PC System 7.7-39
7.7.6 Neutron Monitoring System - Nonsafety-Related Subsystems 7.7-41
7.7.6.1 System Design Basis 7.7-41
7.7.6.2 System Description 7.7-42
7.7.6.3 Safety Evaluation 7.7-44
7.7.6.4 Testing and Inspection Requirements 7.7-45
7.7.6.5 Instrumentation and Control Requirements 7.7-46
7.7.7 Containment Inerting System 7.7-46
7.7.7.1 System Design Bases 7.7-46
7.7.7.2 System Description 7.7-47
7.7.7.3 Safety Evaluation 7.7-47
7.7.7.4 Testing and Inspection Requirements 7.7-48
7.7.7.5 Instrumentation and Control Requirements 7.7-48
7.7.8 COL Information 7.7-50
7.7.9 References 7.7-50

7.8 Diverse Instrumentation and Control Systems 7.8-1

7.8.1 System Description 7.8-1
7.8.1.1 Anticipated Transients Without Scram Mitigation Functions 7.8-2
7.8.1.2 Diverse Instrumentation and Control 7.8-6
7.8.1.3 Diverse Manual Controls and Displays 7.8-9
7.8.2 Common Mode Failure Defenses Within Safety-Related System Design 7.8-10
7.8.2.1 Design Techniques for Optimizing Safety-Related Hardware and Software . 7.8-10
7.8.2.2 Defense Against Common Mode Failure 7.8-11
7.8.3 Safety Evaluation 7.8-12
7.8.3.1 Code of Federal Regulations 7.8-13
7.8.3.2 General Design Criteria 7.8-14
7.8.3.3 Staff Requirements Memorandum 7.8-14
7.8.3.4 Regulatory Guides 7.8-15
7.8.3.5 Branch Technical Position 7.8-16

7.8.4 Testing and Inspection Requirements 7.8-17
7.8.5 Instrumentation and Control Requirements 7.8-18
7.8.6 COL Information 7.8-18
7.8.7 References 7.8-18
7.9 Data Communication Systems - Deleted 7.9-1

7A. Automated Fixed In-Core Probe Subsystem for the Neutron Monitoring System - Deleted7A-1

7B. Software Quality Program for Software Design and Development – Deleted 7B-1

List of Tables

Table 7.1-1 Regulatory Requirements Applicability Matrix

Table 7.1-2 Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Table 7.2-1 Channels Used in Functional Performance of RPS

Table 7.2-2 SRNM Trip Function Summary

Table 7.2-3 SRNM Trip Signals

Table 7.2-4 APRM Trip Function Summary

Table 7.2-5 Outputs from SPTMs to Other Systems

Table 7.2-6 OPRM Trip Function Summary

Table 7.3-1 Automatic Depressurization System Parameters

Table 7.3-2 Safety Relief Valve Initiation Parameters

Table 7.3-3 Automatic Depressurization Valve Parameters

Table 7.3-4 Gravity Driven Cooling System Parameters

Table 7.3-5 LD&IS Interfacing Sensor Parameters

Table 7.5-1 Design and Qualification for Instrumentation - (Deleted)

Table 7.5-2 PAM Variable List – (Deleted)

Table 7.5-3 Type A Variables – (Deleted)

Table 7.5-4 CMS Testing and Inspection Requirements

Table 7.7-1 Major Plant Automation System Interfaces

Table 7B-1 Software Requirements Specification – (Deleted)

Table 7B-2 Software Architecture Description– (Deleted)

Table 7B-3 Software Design Specification– (Deleted)

Table 7B-4 Software Source Code Listings– (Deleted)

Table 7B-5 System Build Documents– (Deleted)

Table 7B-6 Installation Configuration Tables– (Deleted)

Table 7B-7 Operations-Maintenance Manuals– (Deleted)

Table 7B-8 Training Manuals– (Deleted)

List of Illustrations

Figure 7.1-1. ESBWR Instrumentation and Control Simplified Block Diagram

Figure 7.1-2. ESBWR Distributed Control and Information System (DCIS) Functional Network Diagram

Figure 7.1-3. ESBWR Distributed Power-Sensor Diversity Diagram

Figure 7.1-4. ESBWR Hardware/Software (Architecture) Diversity Diagram

Figure 7.2-1. RPS Functional Block

Figure 7.2-2. RPS Interfaces and Boundaries Diagram

Figure 7.2-3. Neutron Flux Monitoring Ranges

Figure 7.2-4. Basic Configuration of a Typical SRNM Subsystem

Figure 7.2-5. Basic Configuration of a Typical PRNM Subsystem

Figure 7.2-6. SRNM Detector Locations

Figure 7.2-7. LPRM Locations in the Core

Figure 7.2-8. Axial Distribution of LPRM Detectors

Figure 7.2-9. LPRM Assignments to APRM Channels

Figure 7.2-10. LPRM Assignment to OPRM Channels

Figure 7.3-1a. SRV Initiation Logics

Figure 7.3-1b. GDCS and DPV Initiation Logics

Figure 7.3-1c. DPS Initiation Logic

Figure 7.3-2. GDCS Equalizing Valve Initiation Logics

Figure 7.3-3. LD&IS System Design Configuration

Figure 7.3-4. SSLC/ESF Functional Block Diagram

Figure 7.3-5. SSLC/ESF System Interface Diagram

Figure 7.4-1. Remote Shutdown System Panel Schematic

Figure 7.4-2a. RWCU/SDC System Train A Differential Mass Flow Logic- Division 1

Figure 7.4-2b. RWCU/SDC System Train A Differential Mass Flow Logic- Division 2

Figure 7.4-2c. RWCU/SDC System Train A Differential Mass Flow Logic- Division 3

Figure 7.4-2d. RWCU/SDC System Train A Differential Mass Flow Logic- Division 4

Figure 7.4-2e. RWCU/SDC Line Break Outside Containment Train A Isolation Logic

Figure 7.4-3. Isolation Condenser System Initiation and Actuation

Figure 7.5-1. Containment Monitoring System Design

Figure 7.5-2. (Deleted)

Figure 7.5-3. Area Radiation Monitoring System Functional Block Diagram

Figure 7.7-1. Water Level Range Definition

Figure 7.7-2. RC&IS Block Diagram

Figure 7.7-3. Feedwater Control System Functional Diagram

Figure 7.7-4. Plant Automation System Simplified Functional Diagram

Figure 7.7-5. SB&PC Simplified Functional Block Diagram

Figure 7.7-6. SB&PC FTDC Block Diagram

Figure 7.8-1. Simplified DPS Block Diagram

Figure 7.8-2. ARI & FMCRD Run-In Logic

Figure 7.8-3. ATWS Mitigation Logic (SLC System Initiation, Feedwater Runback)

Figure 7.8-4. Diverse ESF Triple Redundant Logic

Abbreviations And Acronyms List

Term	Definition
10 CFR	Title 10, Code of Federal Regulations
A/D	Analog-to-Digital
AAS	Alarm Management and Annunciation
ABWR	Advanced Boiling Water Reactor
ABS	Auxiliary Boiler System
AC	Alternating Current
AC	Air Conditioning
ADS	Automatic Depressurization System
AFIP	Automated Fixed In-Core Probe
AHS	Air Handling Unit
ALWR	Advanced Light Water Reactor
AMS	Alarm Management System
ANS	American Nuclear Society
ANSI	American National Standards Institute
AO	Analog Output
AOF	Allocation of Functions
AOO	Anticipated Operational Occurrence
AOP	Abnormal Operating Procedures
APF	Automated Program Functions
APRM	Average Power Range Monitor
APR	Automatic Power Regulator
ARI	Alternate Rod Insertion
ARMS	Area Radiation Monitoring System
ASD	Adjustable Speed Drive
ASME	American Society of Mechanical Engineers
ATLM	Automated Thermal Limit Monitor
ATM	Analog Trip Modules
ATWS	Anticipated Transients Without Scram
ATWS/SLC	Anticipated Transients Without Scram and Standby Liquid Control
AUXB	Auxiliary Boiler
BiMAC	Basemat-Internal Melt Arrest Coolability
BISI	Bypass and Inoperable Status Indicator
BOP	Balance of Plant
BPU	Bypass Unit
BTP	NRC Branch Technical Position
BWR	Boiling Water Reactor
C&FS	Condensate and Feedwater System
CB	Control Building

Abbreviations And Acronyms List

Term	Definition
CCF	Common Cause Failure
CCTV	Closed Circuit Television
CIM	Communication Interface Module
CIRC	Circulating Water System
CIS	Containment Inerting System
CMF	Common Mode Failure
CMS	Containment Monitoring System
COL	Combined Operating License
COTS	Commercial-Off-The-Shelf
CP	Control Processor
CPS	Condensate Purification System
CPU	Central Processing Unit
CR	Control Rod
CRC	Cyclic Redundancy Checking
CRD	Control Rod Drive
CRDHS	Control Rod Drive Hydraulic Subsystem
CRDS	Control Rod Drive System
CRHA	Control Room Habitability Area
CRHAVS	Control Room Habitability Area Heating, Ventilation, and Air Conditioning Subsystem
CRHS	Control Room Habitability System
CS	Control System
CRT	Cathode Ray Tube
D/A	Digital-to-Analog
DAC	Design Acceptance Criteria
DBE	Design Basis Event
DC	Direct Current
DCD	Design Control Document
DCIS	Distributed Control and Information System
DOI	Dedicated Operator Interface
DPS	Diverse Protection System
DPV	Depressurization Valve
DTM	Digital Trip Module
ECCS	Emergency Core Cooling System
EFU	Emergency Filter Unit
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EOF	Emergency Operations Facility
EOP	Emergency Operating Procedures
EPDS	Electric Power Distribution System

Abbreviations And Acronyms List

Term	Definition
EPG	Emergency Procedures Guidelines
EPRI	Electric Power Research Institute
ERDS	Emergency Response Data System
ERICP	Emergency Rod Insertion Control Panel
ERIP	Emergency Rod Insertion Panel
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Activation Systems
FAPCS	Fuel and Auxiliary Pool Cooling System
FCM	File Control Module
FMCRD	Fine Motion Control Rod Drive
FMEA	Failure Mode and Effects Analysis
FRA	Functional Requirements Analysis
FTDC	Fault-Tolerant Digital Controller
FW	Feedwater
FWC	Feedwater Control System
FWRB	Feedwater Run Back
GDC	General Design Criteria
GDCS	Gravity-Driven Cooling System
GE	General Electric Company
GEH	GE-Hitachi Nuclear Energy
GLSOS	Generator Lube and Seal Oil System
GWSR	Ganged Withdrawal Sequence Restriction
HCU	Hydraulic Control Unit
HCW	High Conductivity Waste
HDVS	Heater Drain and Vent System
HFE	Human Factors Engineering
HFEITS	Human Factors Engineering Issue Tracking System
HGCS	Hydrogen Gas Control System
HP	High Pressure
HPCI	High Pressure Coolant System
HP/LP	High Pressure/Low Pressure
HPNSS	High Pressure Nitrogen Supply System
HVAC	Heating, Ventilation and Air Conditioning
IAS	Instrument Air System
I&C	Instrumentation and Control
I/O	Input/Output
IC	Isolation Condenser
IC/PCC	Isolation Condenser/Passive Containment Cooling
ICP	Instrumentation and Control Power Supply

Abbreviations And Acronyms List

Term	Definition
ICS	Isolation Condenser System
IEEE	Institute of Electrical and Electronic Engineers
ILRT	Integrated Leak Rate Test
IMC	Induction Motor Controller
IMCC	Induction Motor Controller Cabinet
INOP	Instrument Inoperative
IP	Implementation Plan
ISA	Instrument Society of America
ISO	International Standards Organization
ITAAC	Inspections, Tests, Analyses and Acceptance Criteria
ITS	Issue Tracking System
LBD	Licensing Basis Document
LCO	Limiting Conditions for Operation
LCW	Low Conductivity Waste
LD&IS	Leak Detection and Isolation System
LFCV	Low Flow Control Valve
LHGR	Linear Heat Generation Rate
LOCA	Loss-of-Coolant-Accident
LOPP	Loss of Preferred Power
LP	Low Pressure
LPCI	Low Pressure Coolant Injection
LPRM	Local Power Range Monitor
LPSP	Lighting and Service Power System
LSP	Low Power Setpoint
LTR	Licensing Topical Report
LWMS	Liquid Waste Management System
MBB	Motor Built-In Brake
MCPR	Minimum Critical Power Ratio
MCR	Main Control Room
MCRP	Main Control Room (MCR) Panel
MIL	Military
MLHGR	Maximum Linear Heat Generation Rate
MMI	Man-Machine Interface
MRBM	Multi-Channel Rod Block Monitor
MSIV	Main Steam Isolation Valve
MSL	Main Steamline
MSR	Moisture Separator Reheater System
MSV	Mean Square Voltage
MTBF	Mean Time Between Failure

Abbreviations And Acronyms List

Term	Definition
NBS	Nuclear Boiler System
NDL	Nuclear Data Link
N-DCIS	Nonsafety-related Distributed Control and Information System
NMS	Neutron Monitoring System
NQA	Nuclear Quality Assurance
NRC	Nuclear Regulatory Commission
NSS	Nuclear Steam Supply
NSSS	Nuclear Steam Supply System
NUMAC	Nuclear Measurement Analysis and Control
nV	Nano Volts
O&M	Operation and Maintenance
OBCV	Overboard Control Valve
OGS	Offgas System
OIS	Oxygen Injection System
OLMCPR	Operating Limit Minimum Critical Power Ratio
OLMLHGR	Operating Limit Minimum Linear Heat Generation Rate
OLP	On-Line Procedures
OLU	Output Logic Unit
OPRM	Oscillation Power Range Monitor
P&ID	Piping and Instrumentation Drawing
PAM	Post Accident Monitoring
PAS	Plant Automation System
PASS	Post Accident Sampling Subsystem of Containment Monitoring System
PCCS	Passive Containment Cooling System
PCD	Plant Configuration Database
PCF	Plant Computer Functions
PCV	Primary Containment Vessel
PGCS	Power Generation and Control Subsystem of Plant Automation System
PI	Proportional and Integral
PIP	Plant Investment Protection
PLC	Programmable Logic Controllers
PLU	Power-Load Unbalance
PMCF	Performance Monitoring and Control Functions
PMCS	Performance Monitoring and Control Subsystem of N-DCIS
PRA	Probabilistic Risk Assessment
PRMS	Process Radiation Monitoring System
PRNM	Power Range Neutron Monitoring
PROM	Programmable Read-Only Memory
PSS	Process Sampling System

Abbreviations And Acronyms List

Term	Definition
PSWS	Plant Service Water System
PSW	Plant Service Water
QA	Quality Assurance
Q-DCIS	Safety-related Distributed Control and Information System
RACS	Rod Action Control Subsystem
RAPI	Rod Action and Position Information
RAT	Reserve Auxiliary Transformer
RB	Reactor Building
RBC	Rod Brake Controller
RBCC	Rod Brake Controller Cabinet
RBS	Rod Block Setpoint
RCIC	Reactor Core Isolation Coolant
RC&IS	Rod Control and Information System
RCCWS	Reactor Component Cooling Water System
RCPB	Reactor Coolant Pressure Boundary
RDC	Resolver-to-Digital Converter
RFI	Radio Frequency Interference
RFP	Reactor Feed Pump
RG	Regulatory Guide
RMS	Root Mean Square
RMU	Remote Multiplexer Unit
ROM	Read-only Memory
RPS	Reactor Protection System
RPSM	Reactor Protective System Monitoring
RPV	Reactor Pressure Vessel
RRPS	Reference Rod Pull Sequence
RSM	Rod Server Module
RSPC	Rod Server Processing Channel
RSS	Remote Shutdown System
RSSM	Reed Switch Sensor Module
RTIF	Reactor Trip and Isolation Function(s)
RTS	Reactor Trip System
RWCU/SDC	Reactor Water Cleanup and Shutdown Cooling
RWM	Rod Worth Minimizer
S/DRSRO	Single/Dual Rod Sequence Restriction Override
SAD	Software Architecture Description
SAG	Severe Accident Guideline
SAS	Service Air System
SB&PC	Steam Bypass and Pressure Control

Abbreviations And Acronyms List

Term	Definition
SBO	Station Blackout
SCM	Software Configuration Management
SCMP	Software Configuration Management Plan
SCRRI	Selected Control Rod Run-in
SCRRI/SRI	Selected Control Rod Run-in / Select Rod Insert
SCWS	Stator Cooling Water System
SDP	Software Development Plan
SDC	Shutdown Cooling
SDS	System Design Specification
SECY	Secretary of the Commission, Office of the (NRC)
SIntP	Software Integration Plan
SIP	Software Installation Plan
SIU	Signal Interface Unit
SLC	Standby Liquid Control
SMP	Software Management Plan
SOE	Sequence of Events
SOMP	Software Operations and Maintenance Plan
SPDS	Safety Parameter Display System
SPTMS	Suppression Pool Temperature Monitoring Subsystem of Containment Monitoring System
SQA	Software Quality Assurance
SQAP	Software Quality Assurance Plan
SRI	Select Rod Insert
SRM	Staff Requirements Memorandum
SRNM	Startup Range Neutron Monitor
SRP	Standard Review Plan
SRS	Software Requirements Specification
SRV	Safety Relief Valve
SS	Safe Shutdown
SSE	Safe Shutdown Earthquake
SSLC	Safety System Logic and Control
SSLC/ESF	Safety System Logic and Control Engineered Safety Feature
SSP	Software Safety Plan
STP	Software Training Program
STRAP	Scram Time Recording and Analysis Panel
STrngP	Software Training Plan
STRP	Scram Time Recording Panel
SVVP	Software Verification and Validation Plan
SW	Software
TA	Task Analysis

Abbreviations And Acronyms List

Term	Definition
TAF	Top of Active Fuel
TASS	Turbine Auxiliary Steam System
TBS	Turbine Bypass System
TBV	Turbine Bypass Valve
TCCWS	Turbine Component Cooling Water System
TCS	Turbine Control System
TCV	Turbine Control Valve
TG	Turbine Generator
TGCS	Turbine Generator Control System
TLOS	Turbine Lube Oil System
TLU	Trip Logic Unit
TMI	Three Mile Island
TMSS	Turbine Main Steam System
TPM&D	Thermal Performance Monitor and Diagnostic
TR	Topical Report
TRA	Transient Recording and Analysis
TSC	Technical Support Center
TSM	Technical Specification Monitoring
TSV	Turbine Stop Valve
UAT	Unit Auxiliary Transformer
UPS	Uninterruptible Power Supply
USNRC	United States Nuclear Regulatory Commission
V&V	Verification and Validation
VAC	Volts Alternating Current
VDC	Volts Direct Current
VDU	Video Display Unit
VLU	Voter Logic Unit
WDP	Wide Panel Display
WRNMS	Wide Range Neutron Monitor System
ZNI	Zinc Injection System

7. INSTRUMENTATION AND CONTROL SYSTEMS

7.1 INTRODUCTION

This chapter presents specific detailed design and performance information for the Instrumentation and Control (I&C) systems that are significant for plant operation and are used throughout the plant. I&C systems are designated as either Safety-related Distributed Control and Information System (Q-DCIS) or Nonsafety-related Distributed Control and Information System (N-DCIS). A description of the system of classification can be found in Section 3.2.

The following subsections, tables, and figures provide a synopsis of the Distributed Control and Information System (DCIS):

- Subsection 7.1.1 contains a brief description of the DCIS.
- Subsection 7.1.2 summarizes the safety-related DCIS (Q-DCIS).
- Subsection 7.1.3 contains a detailed description of the Q-DCIS.
- Subsection 7.1.4 summarizes the nonsafety-related DCIS (N-DCIS).
- Subsection 7.1.5 contains a detailed description of the N-DCIS.
- Subsection 7.1.6 discusses conformance of I&C systems with Regulatory Requirements, Guidelines, and Industry Codes and Standards.
- Table 7.1-1 is a Regulatory Requirements Applicability Matrix.
- Table 7.1-2 is a section roadmap of an evaluation of IEEE Std. 603 Specific Criteria Compliance.
- Figure 7.1-1 is a simplified functional block diagram of the I&C.
- Figure 7.1-2 is a functional network diagram of the DCIS.
- Figure 7.1-3 is a Distributed Power-Sensor Diversity Diagram.
- Figure 7.1-4 is a Hardware/Software (Architecture) Diversity Diagram.

7.1.1 Distributed Control and Information System

The DCIS is an arrangement of I&C networked components and individual systems that together provide the following capabilities and functions:

- Digital Processing and logic capability;
- Remote and local data acquisition;
- Gateways/datalinks between systems and components;
- Operator monitoring and control interfaces;

- Secure communications with Firewalls to external computer systems and networks;
- Alarm management functions; and
- Communications between the systems.

Figure 7.1-1 shows a simplified functional block diagram of the ESBWR Instrumentation and Control system. The DCIS is subdivided into the Q-DCIS and the N-DCIS. The data communication systems embedded in the DCIS perform the data communication functions that are part of or support the systems described in Sections 7.2 through 7.8. A network diagram of the DCIS appears as Figure 7.1-2, which is a functional representation of the current design

The Q-DCIS and N-DCIS architectures, their relationships, and their acceptance criteria are further described throughout Section 7.1.

The Q-DCIS and N-DCIS functions are implemented with diverse power and sensors as indicated in Figure 7.1-3 and diverse hardware and software architectures as shown in Figure 7.1-4. These are fully discussed in Reference 7.1-3, the Licensing Topical Report (LTR) "ESBWR I&C Defense-In-Depth And Diversity Report," NEDO-33251.

The software for the Q-DCIS and N-DCIS are designed and developed in accordance with the LTRs "ESBWR I&C Software Management Plan," NEDO-33226, NEDE-33226P, and "ESBWR I&C Software Quality Assurance Plan" NEDO-33245, NEDE-33245P. (References 7.1-12 and 7.1-10, respectively.) These plans describe the managerial, design, development, and software quality assurance requirements for the DCIS and addresses the Nuclear Regulatory Commission (NRC) review guidance provided in the Standard Review Plan (SRP).

7.1.2 Q-DCIS General Description Summary

The Q-DCIS comprises the safety-related portion of the DCIS, which performs the safety-related control and monitoring functions. The Q-DCIS is organized into four physically and electrically isolated divisions. Each division is segmented into systems; segmentation allows, but does not require, the systems to operate independently of each other. The Q-DCIS major cabinets, systems, and functions are:

- Reactor Trip and Isolation Function (RTIF) Cabinets (these cabinets include the following systems and functions):
  - Reactor Protection System (RPS) (Refer to Subsection 7.2.1);
  - Main Steam Isolation Valve (MSIV) Functions of the Leak Detection And Isolation System (LD&IS) (Refer to Subsection 7.3.3);
  - Anticipated Transient Without Scram/Standby Liquid Control (ATWS/SLC) Functions (Refer to Subsection 7.4.1); and
  - Suppression Pool Temperature Monitoring Functions for RPS and Containment Monitoring System (CMS) (Refer to Subsection 7.2.3).

- Neutron Monitoring System (NMS) (Refer to Subsection 7.2.2):
  - Startup Range Neutron Monitor (SRNM) functions;
  - Power Range Neutron Monitor (PRNM) functions that include:
    (1) Local Power Range Monitor (LPRM) functions;
    (2) Average Power Range Monitor (APRM) functions; and
    (3) Oscillation Power Range Monitor (OPRM) functions.
- Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) System (Refer to Subsection 7.3.5):
  - Emergency Core Cooling System (ECCS) functions that include:
    (1) Automatic Depressurization System (ADS) functions;
    (2) Gravity-Driven Cooling System (GDCS) functions;
    (3) Isolation Condenser System (ICS) functions;
    (4) SLC System ECCS functions;
    (5) LD&IS Functions (except the MSIVs functions); and
    (6) Control Room Habitability System (CRHS) functions.
  - Safety-related monitoring and manual control functions.

The Q-DCIS major components include:

- A fiber optic cable and hardwired network;
- System control processors;
- Non-microprocessor based logic;
- Remote Multiplexer Units (RMUs);
- Load drivers (discrete outputs);
- Communication Interface Modules (CIMs);
- Video Display Units (VDUs);
- Main Control Room (MCR) wide display panels/consoles that house the controls and monitoring;
- Hard controls/indicators (for monitoring); and
- Cabinets for housing devices such as power supplies.

The Q-DCIS provides most of the interface functions for the RPS, NMS, and SSLC/ESF protection systems. These include data acquisition, monitoring, communication, and control functions. As a safety-related system, Q-DCIS is qualified for the environments and conditions that exist before, during, and following the Design Basis Events (DBEs) identified in Chapter 15. Each division of the Q-DCIS is electrically isolated from other Q-DCIS divisions and from the N-DCIS. Data communication is controlled between the Q-DCIS divisions and between the Q-DCIS and the N-DCIS. Communication between Q-DCIS divisions and between the Q-DCIS and the N-DCIS is always by fiber optic cable. Data communication between the Q-DCIS and the N-DCIS is managed by isolation devices, which are safety-related components within the Q-DCIS, and by N-DCIS gateways/datalinks. The RPS, NMS, and SSLC/ESF protection systems are designed so that no safety-related function depends on any nonsafety-related component, data, or communication channel.

The Q-DCIS uses RMUs for data acquisition for the RPS, NMS, and SSLC/ESF protection systems and for safety-related displays in the MCR and Remote Shutdown System (RSS). These units may be distributed within the division or they may reside in specific chassis and not be dedicated to specific RPS, NMS, or SSLC/ESF systems (for example, GDCS, ICS, and ADS).

For added reliability and diversity, the architecture of the RPS and NMS protection systems is different from the architecture of the SSLC/ESF protection system (refer to Figure 7.1-3 and Figure 7.1-4). These systems normally operate automatically, without operator input.

The RPS and NMS status is monitored on the divisional Q-DCIS safety-related VDUs that are connected to the SSLC/ESF (and may also be independently monitored on N-DCIS VDUs after appropriate isolation). The RPS and NMS process data are sent per division through a one-way dedicated communication path (gateways/datalinks) for display on the corresponding divisional safety-related VDU. The RPS, NMS, and SSLC/ESF operate independently of the VDUs and continue to perform their safety-related functions if there is a failure of the VDU network. Safety-related VDUs are provided in the MCR and at the RSS and operate independently of one another. The safety-related VDUs provide data display capability for the RPS, NMS, and SSLC/ESF safety-related systems and manual control capability for the SSLC/ESF safety-related systems in a Human Factors Engineering (HFE) approved format.

The divisional Q-DCIS components outside of the MCR are located in physically separate DCIS divisional rooms or compartments in the Reactor Building (RB) and Control Building (CB) that have appropriate fire barriers between them.

The divisional Q-DCIS components are powered by redundant, independent, and separated uninterruptible power supplies dedicated to their division with battery backup (per division) for at least 72 hours. After 72 hours, the Q-DCIS can operate continuously on power from either of the two diesel generators or from off-site power (Refer to Subsection 8.1.5.2.1 for additional information about the power sources for the isolation load centers and safety-related Uninterruptible AC power.)

The Q-DCIS provides self-diagnostics that monitor communication, power, and processors to the replaceable card, module, or chassis level. Process diagnostics include system alarms and the ability to identify sensor failures. Process and self-diagnostic system alarms are provided to the MCR.

7.1.2.1 Q-DCIS Safety-Related Design Bases Summary

The safety-related design bases applicable to the Q-DCIS are found in IEEE Std. 603, Sections 4.1, 4.2, 4.5, 4.8, and 4.10. They specifically address reading signals; performing signal conditioning; transmitting data signals and commands; performing safety-related logic independently; providing alarms to N-DCIS; and isolating data communication.

7.1.2.2 Q-DCIS Power Generation Design Bases Summary

The power generation design basis for the Q-DCIS is to transmit safety-related system data through qualified isolation devices to N-DCIS gateways/datalinks for historical trending and analysis and alarm management functions.

7.1.2.3 Q-DCIS Safety Evaluation Summary

The Q-DCIS conforms with IEEE Std. 603 criteria.

The Q-DCIS is arranged into four divisions. The intra-divisional and safety-related to nonsafety-related fiber optic cable communication paths are redundant to support reliability and to allow self-diagnostics to be communicated in the presence of a single failure. Safety-related cabinets and chassis are powered by redundant uninterruptible sources for both reliability and diagnostic capability. For communications between divisions of safety-related systems, there is no single communication or power failure that results in the loss of a safety-related function. A dual communication or power failure can result in the loss of a single division but not in the loss of a safety-related function. A two-division failure that requires four communications or power failures does not result in the loss of a safety-related function.

Table 7.1-1 identifies the DCIS systems and the associated regulatory requirements, guidelines, and codes and standards applied in accordance with the SRP. The following subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.1.2.4 Q-DCIS Regulatory Requirements Conformance Summary

The Q-DCIS conforms with applicable portions of the following regulations, guidelines, and standards:

- 10 CFR 50.34, 10 CFR 50.55, 10 CFR 50.62, and 10 CFR 52.47;
- NUREGs 694, 718, 737, NUREG/CR-6083, and NUREG/CR-6303;
- IEEE Std. 7-4.3.2, 323, 344, 379, 338, 383, 384, 497, 518, 603, 828, 829, 830, 1008, 1012, 1028, 1042, 1050, and 1074;
- American National Standards Institute (ANSI)/Instrument Society of America (ISA) s67.02 and s67.04.01;
- General Design Criteria (GDC) 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 25, and 29;
- Staff Requirements Memorandum (SRM) II.Q and II.T to SECY 93-087;

- Regulatory Guides (RGs) 1.22, 1.47, 1.53, 1.62, 1.75, 1.97, 1.105, 1.118, 1.151, 1.152, 1.153, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173, 1.180, and 1.204; and
- Branch Technical Positions (BTPs) HICB-1, 8, 9, 11, 12, 14, 16, 17, 18, 19, and 21.

7.1.2.5 Q-DCIS Testing and Inspection Requirements Summary

The Q-DCIS integrated hardware and software functions, including the network parameters and data status, are checked and tested together. The Analog-to-Digital (A/D) converters (also the Digital-to-Analog (D/A) converters if used) in the RMUs are the only components requiring periodic calibration checks. Some of the key diagnostics include:

- The Central Processing Unit (CPU) status check;
- Parity checks, watchdog timer status;
- Voltage level in controllers;
- Data path integrity and data validation checks;
- Data cycling time; and
- Processor clock time.

7.1.2.6 Q-DCIS Operator Interface Requirements Summary

The Q-DCIS VDUs support operator monitoring and manual control of the safety-related systems. The VDUs present process and diagnostic alarm information. When one of the two power supplies or communications paths within a division fails, the division and VDU operation continues automatically, without operator intervention. Failures in three divisions are required before there is a loss of a safety-related function.

The following Q-DCIS indications and alarms, as a minimum, are provided in the MCR (IEEE Std. 603, Section 5.8):

- Q-DCIS MCR alarms for Division 1, 2, 3, and 4 trouble; and
- Q-DCIS MCR indications for Division 1, 2, 3, and 4 diagnostic displays.

7.1.2.7 Q-DCIS Boundary Summary

There are no Q-DCIS components in the N-DCIS. The Q-DCIS does not include the sensors or the sensor wiring to the RMUs or the RMU output wiring to the actuators.

7.1.2.8 Q-DCIS Major Systems Description Summary

The Q-DCIS systems and components are safety-related entities of the DCIS. The RPS is the designated reactor trip system. The SSLC/ESF is the designated ESF actuation system. The automatic decision-making and trip logic functions associated with the safety-related RPS and ESF actuation system are accomplished by independent, separate, and diverse protection logic

platforms, each using four logic processing divisions. Input signals from redundant channels of safety-related instrumentation are used to perform logic operations that result in decisions for safety-related action through the associated actuation devices (for example, pilot solenoid valves, squib valves, and air operated valves).

7.1.2.8.1 Reactor Protection System Description Summary

The RPS implements the reactor trip functions. The RPS is the overall complex of instrument channels, trip logics, trip actuators, manual controls and scram logic circuitry that initiates rapid insertion of control rods to shut down the reactor in situations that could result in unsafe reactor operations. This action prevents or limits fuel damage and system pressure excursions, minimizing the release of radioactive material.

The RPS also establishes appropriate logic for different reactor operating modes, provides monitoring, and control signals to other systems and actuates alarms.

The RPS overrides selected operator actions and process controls and is based on a fail-safe design philosophy. The RPS design provides reliable, single-failure-proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures. This is accomplished through the combination of fail-safe and fault tolerant equipment design and a two-out-of-four voting logic algorithm.

Note that although the RTIF cabinets house the RPS and the ATWS/SLC systems, the ATWS/SLC uses different hardware and is not a fail-safe design. The RPS sensors, hardware, and logic are diverse from SSLC/ESF logic, ATWS mitigation logic, and Diverse Protection System (DPS) logic.

7.1.2.8.2 Neutron Monitoring System Description Summary

The NMS monitors neutron flux in the reactor core from the startup source range to beyond rated power. The NMS provides logic signals to the RPS to automatically shut down the reactor when a condition necessitating a reactor scram is detected. The system provides indication of neutron flux that can be correlated with thermal power level for the entire range of flux conditions that can exist in the core. The NMS comprises the following systems:

- SRNM System - The Startup Range Neutron Monitoring (SRNM) system monitors thermal neutron flux levels from very low average power levels to a power level above 15% of rated power. At 15% of rated power the monitoring function is overlapped with Local/Average Power Range Monitoring (LPRM/APRM) systems to assure continuous monitoring of thermal neutron flux levels. The SRNM channel is able to provide local power information up to 100% of rated power. The SRNM system generates trip signals to prevent fuel damage resulting from abnormal positive reactivity insertions under conditions that are not covered by the APRMs. The SRNMs generate a high neutron flux trip and a high rate of neutron flux increase trip.

- PRNM System - The Power Range Neutron Monitoring (PRNM) system includes the LPRM, the APRM, and the Oscillation Power Range Monitoring (OPRM) functions.

The outputs of the individual LPRMs are averaged to provide the average power level of the reactor core, and the OPRM System provides monitoring of neutron flux and core thermal hydraulic instabilities. In the low end of the power range from 1% to 15% of rated power, the SRNM and PRNM monitoring functions overlap.

- The Automatic Fixed In-core Probe (AFIP) – This AFIP is a nonsafety-related component of the NMS system and does not provide information to the Q-DCIS. It calibrates the LPRM system by providing neutron flux information to 3D MONICORE.
- Multi-Channel Rod Block Monitor (MRBM) - The MRBM is a nonsafety-related component of the NMS system and is completely isolated from the Q-DCIS by one-way fiber optic cable communication. It provides control rod blocks to the Rod Control and Information System (RC&IS) to prevent core thermal limit violations.

7.1.2.8.3 SSLC/ESF System Description Summary

The SSLC/ESF is the overall complex of instrument channels, trip logics, trip actuators, manual controls, and actuation logic circuitry that initiates protective action to mitigate the consequences of DBEs. Input signals from redundant channels of safety-related instrumentation are used to make trip decisions and perform logic operations that result in accident mitigating actions. The SSLC/ESF provides the automatic decision-making and trip logic to initiate the following protection functions:

- The various ECCS;
- Leak detection, containment isolation and radioactivity release barrier defense actuation; and
- Control room habitability.

7.1.2.8.3.1 Emergency Core Cooling System Description Summary

The ECCS provides emergency core cooling for events that threaten reactor coolant inventory, such as a Loss of Coolant Accident (LOCA). The ECCS comprises the ADS, the GDCS, the ICS, and the SLC system. The ECCS function is discussed more fully in Subsection 7.3.1.

7.1.2.8.3.2 Automatic Depressurization System Description Summary

The ADS resides within the Nuclear Boiler System (NBS) and comprises Safety Relief Valves (SRVs), Depressurization Valves (DPVs), and associated I&C. The ADS depressurizes the reactor to allow the low head GDCS to provide make-up coolant to the reactor. The ADS logic resides in the SSLC/ESF portion of the Q-DCIS.

7.1.2.8.3.3 Gravity Driven Cooling System Description Summary

Following the receipt of an actuation signal, the GDCS provides emergency core cooling when the reactor has been depressurized. The GDCS is capable of injecting large volumes of water into the Reactor Pressure Vessel (RPV) to keep the core covered for at least 72 hours following a LOCA. The GDCS also performs a deluge function that drains the GDCS pools to the lower

drywell if a severe accident core melt sequence occurs. The GDCS deluge logic, which is nonsafety-related except for permissives to avoid inadvertent actuation, is separate and diverse from the Q-DCIS. The basic components of the GDCS are within the containment. The GDCS pools, piping, and valves are in the drywell. The suppression pool is on the outer periphery of the drywell within the containment envelope. The GDCS I&C is designed to:

- Automatically initiate the GDCS to prevent fuel cladding temperatures from reaching their limits;
- Respond to a need for emergency core cooling following reactor depressurization;
- Be completely automatic in operation. Manual initiation of the GDCS is possible at any time providing protective permissive conditions have been satisfied; and
- Prevent the inadvertent actuation of the deluge valves, thus preventing inadvertent draining of the GDCS pools.

7.1.2.8.3.4 Isolation Condenser System Description Summary

The ICS is a safety-related system that removes reactor decay heat following reactor shutdown and isolation. It also prevents unnecessary reactor depressurization and operation of the ECCS. The primary function of the ICS is to limit reactor pressure and prevent SRV operation following an isolation of the main steam lines. The ICS, together with the water stored in the RPV, provides sufficient reactor coolant volumes to avoid automatic depressurization caused by low reactor water level. The ICS passively removes excess sensible and core decay heat from the reactor, with minimal loss of coolant inventory from the reactor, when the normal heat removal systems are unavailable. The ICS logic resides in the SSLC/ESF portion of the Q-DCIS.

7.1.2.8.3.5 Standby Liquid Control System Description Summary

The SLC system performs dual functions. In its ECCS mode, it provides additional coolant inventory to respond to a LOCA. It is also a backup method for bringing the nuclear reactor to subcriticality and then maintaining subcriticality as the reactor cools.

The SLC system bases are discussed in Subsection 7.4.1. The SLC logic resides in the SSLC/ESF and the ATWS/SLC portions of the Q-DCIS.

7.1.2.8.3.6 Leak Detection and Isolation System Description Summary

The LD&IS monitors leakage sources from the Reactor Coolant Pressure Boundary (RCPB). It automatically initiates closure of the appropriate valves to isolate the source of the leak if monitored system variables exceed preset limits. This limits coolant release from the RCPB and, therefore, the release of radioactive materials into the environment.

The MSIV isolation logic of the LD&IS is fail-safe and therefore performed as part of the RTIF logic platform. The non-MSIV isolation logic of the LD&IS is performed as part of the SSLC/ESF logic platform.

7.1.2.8.3.7 Control Room Habitability System Description Summary

The primary function of the CRHS is to provide a safe environment for the operators to control the nuclear reactor and its auxiliary systems. The CRHS monitors the Control Room Habitability Area (CRHA) inlet ventilation air and actuates logic to isolate and filter the CRHA on detection of hazardous environmental conditions. The CRHS logic resides in the SSLC/ESF portion of the Q-DCIS.

7.1.2.8.3.8 Anticipated Transient Without Scram Standby Liquid Control Description Summary

The ATWS mitigation logic provides a diverse means of reducing power excursions from certain transients and a diverse means of emergency shutdown. The ATWS mitigation logic, which uses the soluble boron injection capability of the SLC system as a diverse means of negative reactivity insertion, is implemented as safety-related logic (designated as ATWS/SLC). The ATWS/SLC logic also provides a feedwater run-back signal to attenuate power excursions.

In the event that the control rods cannot provide sufficient negative reactivity insertion, the SLC system provides the capability of an orderly and safe shutdown by a diverse means. In addition to providing hot shutdown capability, the SLC is sized to counteract the positive reactivity that results from shutting down from rated power to a cold shutdown condition. The SLC system may be initiated manually, or automatically via the ATWS mitigation logic or the SSLC/ESF logic as an ECCS function. (Refer to Subsection 7.1.2.8.3.5.) The SLC logic resides on the SSLC/ESF and ATWS/SLC portions of the Q-DCIS.

The nonsafety-related ATWS mitigation logic is implemented in the (DPS). (Refer to Subsection 7.8.1.1.3.)

7.1.2.8.3.9 Passive Containment Cooling System Description Summary

The Passive Containment Cooling System (PCCS) cools the containment following a rise in containment pressure and temperature without requiring any component actuation. The PCCS does not need electric power and does not have instrumentation, control logic, or power actuated valves. This brief description is included here for completeness.

7.1.2.8.4 Containment Monitoring System Description Summary

The CMS provides the functions identified in Subsections 7.1.2.8.4.1 and 7.1.2.8.4.2. Refer to Subsection 7.5.2 for additional information.

7.1.2.8.4.1 Suppression Pool Temperature Monitoring System Function Description Summary

The safety-related Suppression Pool Temperature Monitoring System (SPTMS) is part of CMS and monitors suppression pool temperatures under all operating accident conditions. Should the suppression pool temperature exceed established limits, the SPTMS provides input for both a reactor scram and for automatic initiation of the suppression pool cooling mode of the Fuel Auxiliary Pool Cooling System (FAPCS) operation. The RTIF cabinet houses the equipment that performs the Suppression Pool Temperature Monitoring functions for the Containment Monitoring System (CMS) discussed in Section 7.5.2.

7.1.2.8.4.2 Other Containment Monitoring System Functions Description Summary

Other CMS functions, some of which are nonsafety-related, include monitoring several key containment parameters. These include fluid and radiation levels, pressures, hydrogen/oxygen concentrations, and dew point values. These parameters are monitored during normal reactor operations and post accident conditions to evaluate the containment integrity and other conditions. Abnormal measurements and indications initiate alarms in the MCR.

7.1.3 Q-DCIS Specifics

The Q-DCIS architecture, its relationships, and its acceptance criteria are described below. A simplified functional block diagram of the DCIS is shown as part of Figure 7.1-1. The Q-DCIS data communication systems are embedded in the DCIS; the DCIS performs the data communication functions that are part of or support the systems described in Sections 7.2 through 7.8. A network diagram of the DCIS appears as part of Figure 7.1-2, which shows the elements of the Q-DCIS and the N-DCIS. The figure is a functional representation of the design.

7.1.3.1 Q-DCIS Design Bases

7.1.3.1.1 Q-DCIS Safety-Related Design Bases

The safety-related design bases applicable to the Q-DCIS are found in IEEE Std. 603, Sections 4.1, 4.2, 4.5, 4.8, and 4.10. These sections specify that the Q-DCIS is to do the following:

- Read signals from the safety-related instrumentation locally and through RMUs;
- Perform required signal conditioning, if this function is required, and then digitize and format the input signals into messages for transmission on the Q-DCIS network or data path;
- Transmit the data signals and commands onto the Q-DCIS network or data path for interface with other safety-related systems and support safety-related system monitoring and operator input to/from the MCR and RSS VDUs;
- Support safety-related system monitoring and operator input to and from the MCR and RSS VDUs;
- Perform safety-related logic functions;
- Perform closed loop control and logic independently of the VDUs;
- Transmit the actuation signals to safety-related equipment as output from the RMUs;
- Provide self-diagnostic and process, alarm information to the operator; and
- Isolate data communication to and from the N-DCIS.

7.1.3.1.2 Q-DCIS Power Generation (Nonsafety-Related) Design Basis

The power generation design basis for the Q-DCIS is to transmit plant parameters and other safety-related system data through safety-related isolation devices to the gateways/datalinks to the N-DCIS that provide interfaces to nonsafety-related system logic and displays for power generation.

7.1.3.1.3 Q-DCIS Setpoint Methodology

To determine setpoints and select I&C, the following are considered: range, accuracy, resolution, instrument drift, environmental conditions at the sensor location, changes in the process, testability, and repeatability. The recommended test frequency is greater for instrumentation that demonstrates a stronger tendency to drift. Adequate margin between safety-related limits and instrument setpoints is provided to allow for instrument error. The response time of the instrument is assumed in the safety analysis and verified in plant-specific surveillance testing. The amount of instrument error is determined by test and experience. The setpoint is selected based on a known error; the Q-DCIS equipment is microprocessor based with discrete setpoints that do not drift.

The actual settings are determined from operating experience or conservative analyses when specific instrument operating experience is not available. The settings are far enough from the values expected in normal operation to preclude inadvertent initiation of the safety-related action. At the same time, they are far enough from the analyzed trip values to ensure that appropriate margins are maintained between the actual settings and the analyzed values. The margin between the limiting safety-related system settings and the actual safety-related limits include consideration of the maximum credible transient in the process being measured.

The periodic test frequency for each variable is determined from historical data on setpoint drift and from quantitative reliability requirements for each system and its components. Setpoints are established for the Q-DCIS systems in accordance with proven instrument error and setpoint calculation methodology described in “General Electric Instrument Setpoint Methodology", Reference 7.1-9.

7.1.3.2 Q-DCIS Description

The Q-DCIS provides the data processing and transmission network that encompasses the four independent and separate data multiplexing divisions, Divisions 1, 2, 3, and 4, corresponding to the four divisions of safety-related electrical and I&C equipment. Each Q-DCIS division consists of the RMUs, the fiber optic cable signal transmission path, the SSLC cabinets, the RTIF cabinets, the cabinet power supplies, the safety-related VDUs, and safety-related fiber optic CIMs.

The Q-DCIS contains multiple dual redundant fiber optic cable networks for each of the four divisions. The networks connect the RMUs with the following: divisional safety-related VDUs; the RPS and NMS Digital Trip Modules (DTMs); the SSLC/ESF CIMs; the RPS, the NMS, and the SSLC/ESF Test Cabinets located in the safety-related Q-DCIS equipment rooms in the RB and CB; and the N-DCIS through isolated digital gateways/datalinks.

Each Q-DCIS system is housed in a set of uniquely identified cabinets. Separate cabinets are provided for each of the four divisions and the remotely mounted components within each division.

An RMU is an assembly of divisional Input/Output (I/O) equipment, power supplies and possibly some logic housed in one cabinet. The field sensors and process transmitters are hardwired to the divisional local RMUs in the RB and CB. At the input module of the field RMUs, the analog data is delivered to the analog input modules and discrete data is delivered to the digital input modules. The field sensors and wiring belong to the process system they are attached to and are not part of the Q-DCIS. Analog signal conditioning, A/D conversion, and digital signal conditioning such as filtering and voltage level conversion is performed at the input modules.

Each field RMU formats and transmits input signals as data messages to the dual network and then to the RPS, NMS, and SSLC/ESF components within its own division. The field RMUs receive the SSLC/ESF equipment control signals from the network for distribution by hardwired connection to the equipment actuators of the ESF functions.

The corresponding divisional Q-DCIS networks send data to the RPS, NMS, and SSLC/ESF components in separate RPS, NMS, and SSLC/ESF divisional cabinets. The data is also sent to other safety-related logic equipment such as the safety-related logic test cabinets for control of the functional tests, the CIMs, and the isolated divisional gateways/datalinks for communication with the N-DCIS.

The components of the Q-DCIS in the RB and CB are located in a controlled environment for safety-related equipment. The Q-DCIS components in the RB and safety-related logic cabinets located in the CB are provided with appropriate cooling to maintain the required environmental conditions; the cooling is active if either offsite or diesel generator power is available and is passive when the system is operating on battery power. The Q-DCIS components, including the fiber optic cable network, are not located in the primary containment or in high radiation areas. Signals from within these areas are hardwired by copper cable to the RMUs. Electromagnetic compatibility (EMC) of the RMUs and Q-DCIS equipment is ensured by conformance with the following program:

- The Q-DCIS components are designed to minimize susceptibility to and generation of Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI).
- The Q-DCIS components are subjected to tests for EMI, RFI, and surge conditions that conform with guidelines in RG 1.180.
- Grounding of RMU and Q-DCIS equipment follows the guidance given in IEEE Std. 518 and IEEE Std. 1050.

To minimize EMI effects, the Q-DCIS electrical equipment incorporates shielding and filtering. The equipment is mounted in grounded panels provided with isolated instrument grounds.

7.1.3.2.1 Reactor Trip Systems

7.1.3.2.1.1 Reactor Protection System

The safety-related RPS initiates an automatic reactor shutdown by rapid insertion of control rods (scram) if monitored system variables exceed pre-established limits. This action prevents fuel damage, limits system pressure, and, thus, minimizes the release of radioactive material. Refer to Subsection 7.2.1 for additional information.

7.1.3.2.1.2 Neutron Monitoring System

The safety-related NMS monitors the core thermal neutron flux from the startup source range to beyond rated power. The NMS provides logic signals to the RPS to automatically shut down the reactor when a condition necessitating a reactor scram is detected. Refer to Subsection 7.2.2 for additional information.

7.1.3.2.1.3 Suppression Pool Temperature Monitoring System Function

The safety-related SPTMS Subsystem of the CMS monitors suppression pool temperatures under all operating and accident conditions. The system operates continuously during reactor operation. If the suppression pool temperature exceeds established limits, the SPTMS provides input for a reactor scram and for automatic initiation of the suppression pool cooling mode of the FAPCS. Refer to Subsection 7.2.3 for additional information.

7.1.3.2.2 Engineered Safety Features Systems

7.1.3.2.2.1 Emergency Core Cooling System

The safety-related ECCS is an engineered safety feature that automatically initiates the following systems to mitigate LOCAs.

- ICS,
- ADS,
- GDCS, and
- SLC system.

Refer to Subsection 7.3.1 for additional information.

7.1.3.2.2.2 Isolation Condenser System

The safety-related ICS automatically limits reactor pressure and temperature within an acceptable range so that SRVs do not lift and emergency reactor depressurization action does not occur when the reactor becomes isolated during power operations. Over longer durations, the ICS also removes excess sensible and core decay heat from the reactor without the need for an external power supply. The ICS performs this function with minimal loss of coolant inventory

from the reactor when the normal heat removal systems are unavailable. Refer to Subsection 7.4.4 for additional information.

7.1.3.2.2.3 Leak Detection and Isolation System

The safety-related LD&IS monitors leakage sources from the RCPB. It automatically initiates closure of the appropriate valves to isolate the source of the leak if the monitored system variables exceed preset limits. This action limits the loss of coolant from the reactor coolant pressure boundary and the release of radioactive materials to the environment. Refer to Subsection 7.3.3 for additional information.

7.1.3.2.2.4 Control Room Habitability Systems

The CRHS is an ESF system that provides a safe environment within the control room that allows the operator(s) to:

- Control the nuclear reactor and its auxiliary systems during normal conditions;
- Safely shut down the reactor; and
- Maintain the reactor in a safe condition during abnormal events and accidents.

The CRHS includes CB shielding, area radiation monitoring and a CRHA Heating, Ventilation, and Air Conditioning (HVAC) System. The CRHS provides emergency food and water storage; emergency kitchen and sanitary facilities; protection from and removal of airborne radioactive contaminants; and the capability to remove smoke. The CRHA envelope, ventilation inlet/return isolation dampers, redundant Emergency Filter Units (EFUs) in the emergency HVAC system, and associated controls are safety-related. Refer to Subsection 7.3.4 for more information.

7.1.3.2.2.5 Safety System Logic and Control Engineered Safety Features System

The safety-related SSLC/ESF includes the control functions of the safety-related actuation devices of the safety-related plant systems. Input signals from redundant channels of safety-related instrumentation are used to perform logic operations that result in decisions for safety-related action. Trip logic outputs to the actuation devices, such as pilot solenoid valves and squib valves, initiate the appropriate plant protection actions. Refer to Subsection 7.3.5 for additional information.

7.1.3.2.2.6 Passive Containment Cooling System

The safety-related PCCS cools the containment following a rise in containment pressure and temperature without requiring any component actuation. The PCCS does not need electric power and does not have instrumentation, control logic, or power actuated valves. This brief description is included here for completeness. Refer to Subsection 7.3.2 for additional information.

7.1.3.2.3 Safe Shutdown Systems

7.1.3.2.3.1 Standby Liquid Control System

The safety-related SLC system provides a diverse means to shut down the reactor from full power to a subcritical condition, and then maintain the reactor subcritical using soluble boron injection. The SLC system can be manually initiated or initiated automatically for ATWS mitigation. The SLC system is also initiated automatically in response to LOCAs as part of the ECCS. Refer to Subsections 7.1.2.8.3.5, 7.1.2.8.3.8, and 7.4.1 for additional information.

7.1.3.2.3.2 Remote Shutdown System

The RSS has two redundant and independent panels located in two different areas in the RB. If the MCR becomes uninhabitable, all Division 1 and 2 safety-related parameters and all nonsafety-related parameters displayed or controlled at the MCR can be monitored and controlled from either of the RSS panels. Refer to Subsection 7.4.2 for additional information.

7.1.3.2.4 Safety-Related Information Systems

7.1.3.2.4.1 Post-Accident Monitoring Instrumentation

The Post-Accident Monitoring (PAM) instrumentation monitors variables and systems under accident conditions to ensure plant and personnel safety. An assessment of conformance with RG 1.97 is presented in Subsection 7.5.1.

7.1.3.2.4.2 Containment Monitoring System

CMS instrumentation measures and records radiation levels and the oxygen/hydrogen concentration levels in the primary containment under post-accident conditions. The CMS is designed to operate continuously during normal operation and is automatically put in service upon detection of LOCA conditions. Refer to Subsection 7.5.2 for additional information.

7.1.3.2.4.3 Process Radiation Monitoring System

Safety-related (for nonsafety-related, refer to Subsection 7.1.5.2.2.1) PRMS instrumentation monitors the following for radioactive materials: main steam lines, the drywell, discharges from the ICS, vent discharges, and liquid and gaseous effluent streams. The MCR display, recording, and alarm capabilities are provided along with controls that provide automatic trip inputs to the respective systems to prevent further radiation release. Refer to Subsection 7.5.3 for additional information.

7.1.3.2.5 Interlock Systems

The interlock functions are embedded in the DCIS logic, so that a separate interlock system is not required. Refer to Section 7.6 for additional information.

A reactor pressure interlock embedded in logic is provided to the GDCS to prohibit inadvertent manual initiation of the system during normal reactor operation.

Normally closed isolation valves are provided on the FAPCS Low Pressure Core Injection (LPCI) line to protect its low pressure piping from over-pressurization during reactor power operation and high-pressure transients and accidents. Redundant reactor pressure instruments provide a high-pressure signal to the FAPCS LPCI logic to prevent opening or to close, if open, the FAPCS injection valves when the reactor pressure exceeds the FAPCS low pressure setpoint. A HP/LP interlock is provided to prevent opening of the isolation valve when the reactor pressure is higher than the FAPCS design pressure.

Other than the isolation valves, the design does not have logic that isolates safety-related from nonsafety-related piping during a LOCA. It is not necessary because there are no piping interfaces separating the safety-related and nonsafety-related portions of piping systems.

7.1.3.2.6 Nuclear Boiler System Instrumentation

Redundant NBS safety-related instrumentation provides reactor vessel water level and reactor vessel pressure data for operator monitoring. The NBS instrumentation also provides inputs to safety-related systems during normal, transient, and accident conditions. Refer to Subsection 7.7.1 for additional information.

7.1.3.2.7 Data Communication Systems

The DCIS data communication functions are embedded within the Q-DCIS and the N-DCIS architectures. Safety-related Q-DCIS internal and external communication protocols are deterministic.

7.1.3.3 Q-DCIS Safety Evaluation

Communication from the Q-DCIS to the N-DCIS elements is through fiber optic cable. Fiber optic cable is also used:

- For limited communication between the Q-DCIS divisions (such as the two-out-of-four voting logic),
- For communication within a division,
- For providing data to the VDU monitors, and
- For transferring VDU outputs corresponding to manual initiation actions.

The use of fiber optic cable provides complete electrical isolation between components and noise free communication paths. The fiber optic communication module, which converts safety-related electrical signals to light on the sending side of the fiber optic cable, is physically located within and is powered by the division within which it is located. The fiber optic communication module is a qualified safety-related component.

The few cases of nonsafety-related to safety-related communication are also by fiber optic cable; the “receiving” fiber optic communication module is a qualified safety-related component. Safety-related system functions do not depend on the correctness or even the existence of the safety-related/nonsafety-related communications. The loss of this communication in either

direction only results in alarms and loss of data to the N-DCIS. Any single divisional data loss to N-DCIS does not affect power generation or safety. The loss of all safety-related data to N-DCIS can potentially affect power generation but only in a long-term situation such as core thermal limits monitoring.

The IEEE Std. 603, Sections 5.6 and 6.3, isolation occurs in the safety-related fiber optic communication transmitter or receiver module where the electrical signal is first converted to light. Although this standard applies to electrical cable, the fiber optic cables are sheathed in material that meets the IEEE Std. 383 standard addressing fire propagation mitigation.

The Q-DCIS is arranged into four divisions. The intra-divisional and safety-related to nonsafety-related fiber optic cable communication paths are redundant to support reliability and to allow self-diagnostics to be communicated in the presence of a single failure. Similarly, all safety-related cabinets and chassis are powered by redundant uninterruptible power supplies for reliability and self-diagnostics. For all safety-related to safety-related communication, safety-related functions continue to be initiated and executed in the presence of any single or dual communication or power failure. A single communication or power failure is tolerated. A dual communication or power failure may result in the loss of a single division but not in the loss of a safety-related function. A two-division failure, which requires four communications or power failures, does not result in the loss of a safety-related function.

Generally, a system of isolators within the safety-related systems described above and gateways/datalinks within N-DCIS transmit safety-related data to the N-DCIS. The gateways are specific to the communication link between the sending and receiving components. For example, the gateway between the SSLC/ESF and N-DCIS is different from the gateway between the RPS/NMS and the N-DCIS. The sending sources are different even though the receivers are the same.

Safety-related software is as simple as possible so that Q-DCIS components have no interrupts from nonsafety-related devices nor do they have to respond to nonsafety-related component queries for information. The Q-DCIS components simply put information on the safety-related networks in a known format so that other safety-related devices can retrieve what is needed for their function. Additionally self-diagnostic information is also put on the networks. The safety-related communications interfaces indiscriminately retrieve all of the divisional information from the network and send it one way to the nonsafety-related gateway. Time tags are described below.

The nonsafety-related gateway translates the safety-related information into a format that the N-DCIS can apply. The N-DCIS gateway responds to interrupts and queries and packages the safety-related information into the necessary message packets to support specific N-DCIS components for monitoring and alarm management purposes. Additionally, there are some safety-related to nonsafety-related communications paths that do not involve gateways. The receiver is designed to receive and extract the safety-related transmitter generated data/signal without the need for data conversion, for example, the NMS to Automated Thermal Limit Monitor (ATLM) and MRBM communication. The nonsafety-related gateways, when required, handle the data interface, but do not provide isolation for communications between the Q-DCIS and the N-DCIS. They do this by packaging the data for the various N-DCIS functions, responding to the N-DCIS requests for information and monitoring communication link status.

The physical communication between safety-related and safety-related systems and between safety-related and nonsafety-related systems is always by fiber optic cable. Within the safety-related system, the electrical to light interface is always safety-related. There is no credible seismic event, design basis accident, etc. that could cause a failure of the isolation barrier between the safety-related/safety-related or safety-related/nonsafety-related portions of the isolator (specifically, the components at each end of the fiber optic cable. Although unlikely, the worst-case failure is loss of communication. Therefore, the design complies with IEEE Std. 603, Section 5.6.

In addition to the assured electrical isolation, communication isolation enforces the design basis that no safety-related function depends on nonsafety-related communication. The safety-related Q-DCIS communications are governed by both hardware and software protocols. These protocols control the transmission and acceptance of data from outside the division so that these communications cannot adversely affect the operation or safety-related functions of that division. The communication protocols meet the design principles of the Q-DCIS communication interfaces described below. The most important design basis is that whether or not the communications interface is operable or whether there is anything functional on the nonsafety-related or safety-related side of the communications interface, the operation of the safety-related system is not affected.

The safety-related systems are designed not to depend on nonsafety-related communication for function; therefore, loss of communication is never a safety issue. More specifically, no feedback signals are sent from the nonsafety-related components to the safety-related components. Check back, time synchronization, or similar signals are sent from nonsafety-related components to safety-related components but only under the circumstances described below. Time signals are sent to the gateways for use by the Q-DCIS to allow time tagging of data sent to the nonsafety-related components. These time signals are used by the Q-DCIS only for VDU indication so that all displays have the same time. They are never used to synchronize logic nor is the safety-related logic dependent in any way on the absence, presence, or correctness of the time signal.

The single remaining instance of nonsafety-related to safety-related communication involves the calibration of the APRM and LPRM. As with the retrofit Nuclear Measurement Analysis and Control (NUMAC) PRNM systems already licensed for some U.S. nuclear power plants, the data originate in 3D MONICORE, but the information exchange is manual and is rigorously controlled. Before the NUMAC chassis can accept new calibration data, even if it has been sent by 3D MONICORE, the operator must use a keylock switch to make the particular chassis inoperable (INOP). If the operator has not additionally put the corresponding division in bypass, the INOP is interpreted as an NMS trip. It is not physically possible to simultaneously put more than one division in bypass. Both trips and bypasses are alarmed in the MCR.

After the chassis has been made INOP, the operator reviews the download received by the chassis to be calibrated. Additionally, the operator determines that the checkback signal interchange indicates that the NUMAC chassis correctly received the 3D MONICORE data. Only after the operator is satisfied that the calibration data are reasonable does he instruct the NUMAC chassis that it is acceptable to use the downloaded data. The process is equivalent, but more convenient and accurate, to carrying the calibration data to the NUMAC chassis and inputting by hand, a process, which is still possible. After the download is accepted by

NUMAC, the operator uses the keylock switch to make the instrument operable and then resets the bypass for the division.

The general data flow of the four divisions of the Q-DCIS is from the RMUs located in the CB, RB, and possibly Fuel Building in areas appropriate to their division; there are no safety-related RMUs in any other building. Data such as that from transducers and switches is acquired by the RMU, appropriately signal conditioned and, with diagnostic data, sent via the redundant fiber optic cable communication links to the RPS, NMS and the SSLC/ESF units. The RPS, NMS, and the SSLC/ESF units are either centralized Control Processors (CP) or are distributed throughout the various cabinets within the division to perform the logic required by the safety-related systems.

There are always RPS, NMS, and SSLC/ESF units located in the MCR back panel area where there are four Q-DCIS rooms, one per division. The back panel area is where the inter-divisional communication is physically performed to support the two-out-of-four voting that initiates safety-related action. Additionally RPS, NMS, and SSLC/ESF CIMs are used to operate the safety-related VDUs in that division and to provide isolation between the Q-DCIS and the N-DCIS. Finally, calculated outputs from the RPS, NMS, and SSLC/ESF units are sent via the redundant communication system to the RMUs that provide outputs to the safety-related actuator solenoids, explosive squib valves, etc. Note that some outputs are hardwired directly to the final actuators if higher speeds are required.

The dual redundant, fiber optic cable, data networks described above replace the many conventional, long length, copper conductor cables of existing nuclear power plants. This reduces the cost and complexity of divisional cable runs that connect components of the plant protection and safety-related systems such as the RPS, MSIV isolation logic functions, LD&IS containment isolation functions, SSLC/ESF, and safety-related VDUs. The Q-DCIS also provides an electrically noise free transmission path for plant sensor data and safety-related system control signals.

There are at least two safety-related VDUs per division in the MCR. Divisions 1 and 2 have another VDU located on each RSS panel. The VDUs are used to monitor safety-related information from their connected division and are used to provide manual operator inputs to the safety-related logic. The VDUs are also used for divisional self-diagnostics and divisional alarms.

The four VDU divisions allow checking, with a high degree of confidence, of the operational availability of each sense and command feature input sensor for the RPS, NMS, and SSLC/ESF systems by cross-checking between channels that bear a known relationship with each other (IEEE Std. 603, Section 6.5.).

The interconnections between Divisions 1, 2, 3, and 4 are used for two-out-of-four logic. The interconnections are provided by isolated fiber optic digital interfaces; there are no electrical connections between divisions. The four divisions operate asynchronously and do not depend on the interdivisional data link communication for correct operation of the safety-related logic or functions. Fail-safe systems like the RPS or the NMS interpret loss of interdivisional communication as a trip from that division. The trip counts toward the 2/4 logic initiations unless the failed division is bypassed. Fail as-is systems like the ECCS interpret loss of

communications as a non-trip. The plant design basis is N-2; therefore, more than two of these types of failure are required to disable the safety-related functions.

The dual redundant data communication channels per division and the four redundant divisions of the Q-DCIS satisfy the single failure criterion of IEEE Std. 603, Section 5.1. They also satisfy the independence, testing, and repair requirements outlined in IEEE Std. 603, Section 5.6, 5.7, and 6.5. The fiber optic transmitters, receivers, cable and network that are part of the Q-DCIS within and between the four redundant divisions satisfy the separation and independence requirements of division equipment. The cable routing separation meets the requirements of the SRP subsection 9.5.1, Fire Protection Programs.

The DCIS contains continuous online diagnostic functions that monitor transmission path quality and integrity as well as the integrity of most of the system components. Self-diagnostics extend down to the replaceable card or module level. Off-line tests with simulated input signals can also be used to verify the overall system integrity. Segments of Q-DCIS can be tested, and calibrated if needed, on-line when portions of safety-related logic are bypassed. These components and the dual redundant data communication channels are repairable on-line if one channel fails. Because of the redundant power supplies and communication channels, almost all self-diagnostic alarms can be viewed in the MCR with all single and most multiple failures. The Q-DCIS failures are alarmed in the MCR (IEEE Std. 603, Section 5.7 and 6.5).

The Q-DCIS components and cabinets have redundant power supplies that are supplied by redundant uninterruptible power feeds within each division. These power feeds support the Q-DCIS operation for 72 hours without either diesel-generator or offsite power. The loss of one power feed or power supply does not affect any safety-related system function (IEEE Std. 603, Section 8.1).

The Q-DCIS includes the safety-related hardware and software for the RPS, NMS, and SSLC/ESF protection functions and parallels the four-division design of those systems. No failure of any two divisions prevents a safety-related action, such as a detection or a trip, from being accomplished successfully. Component self-testing reconfigures the system to the approved safe state upon detection of uncorrectable errors. Off-line test and calibration of the Q-DCIS components is designed into the system. Individual divisions may be disconnected for maintenance and calibration through bypass within the safety-related logic division without compromising the operations of the other divisions. Only one division can be bypassed at any one time and the existence of a bypass is alarmed in the MCR.

The regulatory acceptance criteria and guidance applicable to each of the Q-DCIS systems identified in the "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants", NUREG-0800 (Reference 7.1-1) are in Table 7.1-1, Regulatory Requirements Applicability Matrix. Sections 7.2 through Section 7.8 contain regulatory conformance discussions for each specific system. The degree of applicability and conformance, along with any clarification or justification for exceptions, is presented in the evaluation sections for each specific system.

7.1.3.4 Q-DCIS Testing and Inspection Requirements

The testing and inspection requirements for each system within the Q-DCIS are presented in specific subsections in Chapter 7.

The components of the Q-DCIS are readily accessible for testing purposes. The continuous automatic online diagnostics of the Q-DCIS detect most data transmission errors and hardware failures at the replaceable card or module level. Continuous self-diagnostics in each RMU monitor the status of each module or card.

The DCIS functions are closely interfaced with the following:

- Safety-related logic functions,
- Integrated hardware and software functions of the Q-DCIS, and
- Safety-related logic including network parameters.

Data status of these functions are checked and tested together. Some of the key diagnostics include the following:

- CPU status check,
- Parity checks,
- Watchdog timer status,
- Voltage level in controllers,
- Data path integrity and data validation checks, and
- Data cycling time.

The DCIS functions are closely interfaced with the safety-related logic functions, the integrated hardware and software functions of the Q-DCIS and safety-related logic including network parameters and data status are checked and tested together. Some of the key diagnostics include the CPU status check, parity checks, watchdog timer status, voltage level in controllers, data path integrity and data validation checks, and data cycling time. The A/D converters (and the D/A converters if used) in the RMUs are the only components requiring periodic calibration checks, which can be performed automatically. In the Q-DCIS, online diagnostics are qualified as safety-related in conjunction with functional software qualification (IEEE Std. 603, Section 5.7).

Any detected hardware failure results in an alarm in the MCR. Corrupted data are detected through error detection functions in the network.

7.1.3.5 Q-DCIS Instrumentation and Control Requirements

The data transmission function delivers system data to all nodes in the network, such as distributed logics of the Q-DCIS RMUs and specific safety-related logic system components, and in certain safety-related systems through dedicated data paths. The Q-DCIS thus provides the necessary integrated support for the distributed control logic functions of the RMUs and

safety-related logic equipment. The data I/O and transmission functions do not require any manual operator intervention and have no operator controls.

The Q-DCIS operates continuously in all modes of plant operation to support the data transmission requirements of the interfacing systems. When one network of the dual network system fails, operation continues automatically without operator intervention. In the event that a channel failure occurs, the network alarms in the MCR indicate the failed component. The failed segment of the channel can be isolated from the operating segments and repaired on-line (IEEE Std. 603, Section 5.7, 5.10, and 6.5).

The following Q-DCIS displays and alarms, as a minimum, are provided in the MCR (IEEE Std. 603, Section 5.8).

- MCR Alarms:
  - Division 1 Q-DCIS trouble,
  - Division 2 Q-DCIS trouble,
  - Division 3 Q-DCIS trouble, and
  - Division 4 Q-DCIS trouble.
- MCR Indications:
  - Division 1 Q-DCIS diagnostic displays,
  - Division 2 Q-DCIS diagnostic displays,
  - Division 3 Q-DCIS diagnostic displays, and
  - Division 4 Q-DCIS diagnostic displays.

7.1.3.6 Q-DCIS Boundaries

The Q-DCIS does not include any N-DCIS components. In addition, the Q-DCIS does not include either the sensors or the sensor wiring to the RMUs nor the RMU output wiring to the actuators.

7.1.4 N-DCIS General Description Summary

The N-DCIS comprises the nonsafety-related portion of the DCIS. The N-DCIS components are redundant when they are needed to support power generation and are segmented into systems. Segmentation allows, but does not require, the systems to operate independently of each other. The N-DCIS major systems and functions follow. (See Subsection 7.1.5 and Figures 7.1-1 and 7.1-2 for more detail.)

- GE-Hitachi Nuclear Energy (GEH) Systems which include:
  - Rod Control and Information,

  - Diverse Protection,
  - 3D MONICORE,
  - Nonsafety-related Gateways/Datalinks, and
  - Neutron Monitoring (nonsafety-related portion).
- PIP Systems (Train A and Train B) which include:
  - Control Rod Drive (CRD),
  - Reactor Component Cooling Water,
  - Fuel and Auxiliary Pools Cooling,
  - Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC),
  - Drywell Cooling,
  - Instrument Air,
  - Plant Service Water,
  - Plant Service Water Cooling Towers,
  - Diesel Generators,
  - Nuclear Island Chillers, and
  - 6.9 KV Plant Electric Power.
- Balance of Plant (BOP) Systems which include:
  - Steam Bypass and Pressure Control (SB&PC),
  - Feedwater Control,
  - Plant Automation,
  - Condensate and Feedwater,
  - Condensate Purification, and
  - Turbine-Generator Control.
- Plant Computer Systems Group which includes:
  - Plant Computer Functions (PCFs),
  - MCR and RSS VDUs,
  - Transient Recording,
  - Core Thermal Power/Flow,

- Data Historian,
- Alarm Systems, and
- On-Line Procedures (OLP).

The N-DCIS major components include:

- A fiber optic cable and hardwired network;
- System control processors;
- Workstations;
- Dedicated network switches;
- RMUs;
- Gateways, datalinks, signal isolators, and I/O modules;
- MCR consoles and display panels;
- Fiber optic modems and media converters; and
- Computer peripherals, such as printers and plotters.

Although the N-DCIS is larger and more complex than the Q-DCIS, it is designed with a segmented architecture that allows the different portions of the system to operate independently of one another. Redundant automatic network switches manage the network so that during normal operation the segments appear seamless to the MCR operator; the network is designed to tolerate a single hardware failure (and many dual hardware failures) without loss of power generation capability or challenge to a safety-related system. The N-DCIS cannot control any Q-DCIS component. The N-DCIS accepts one-way communication from the Q-DCIS so that the safety-related information can be monitored, archived and alarmed seamlessly with the N-DCIS data.

The N-DCIS performs control functions with logic processing modules using signals acquired by the RMUs. The N-DCIS logic processing may be found in the N-DCIS cabinets dedicated to specific system logic functions, such as SB&PC and turbine-generator control, and in cabinets where several system logic functions are combined. The N-DCIS logic is implemented in triple redundant control systems for core nonsafety-related key systems, such as the Feedwater Control System (FWCS), SB&PC, and Plant Automation System (PAS). The N-DCIS logic is always at least redundant for systems required for power generation, so that no single failure of an active DCIS component can cause or prevent a BOP trip or reactor scram.

The N-DCIS provides the control and monitoring operator interface on the N-DCIS nonsafety-related VDUs in the MCR and RSS panels. The VDUs operate independently of one another yet each can normally access any component in the N-DCIS. This gives the RSS panels the same control and monitoring capability as the displays in the MCR. The N-DCIS provides gateways/datalinks as necessary to allow vendor supplied or prepackaged ("foreign") control

systems to be integrated into the DCIS. Examples may include the Condensate Purification System (CPS) and the Area Radiation Monitoring System (ARMS).

The N-DCIS components that support power generation are provided with two or three sources of uninterruptible power with battery backup for at least two hours. For loss of offsite power events or after DCIS battery backup power is lost, the N-DCIS operates continuously from either of the two diesel generators.

The N-DCIS provides extensive self-diagnostics that monitor communication, power, and other failures to the replaceable card, module or chassis level. Process diagnostics include system alarms and the ability to identify sensor failures. All of the process and self-diagnostic system alarms are provided in the MCR.

7.1.4.1 N-DCIS Safety-Related Design Bases Summary

The N-DCIS does not perform or support performance of any safety-related function. It is classified as a nonsafety-related system, and has no safety-related design basis.

7.1.4.2 N-DCIS Nonsafety-Related Design Bases Summary

The design bases for the N-DCIS include the following requirements:

- Provide functional/operational independence of nonsafety-related divisions important to power generation.
- Perform closed loop control and system logic.
- Tolerate a single failure of an N-DCIS component without loss of power generation capability or challenge to a safety-related system.
- Receive selected signals from the Q-DCIS and send them to nonsafety-related devices.
- Collect and archive data for transient analysis, data trending, sequence of events recording, display of Safety Parameter Display System (SPDS) and accident monitoring information, and managing the annunciation of alarm conditions in the MCR.
- Provide secure data communication to the Technical Support Center (TSC), Emergency Operating Facility (EOF), the Emergency Response Data System (ERDS) and generally provide information to other external users.
- Provide gateway interfaces to control and logic processing equipment supplied by parties other than the primary N-DCIS equipment supplier.
- Perform various PCF that includes calculations, displays, and alarms.
- Provide for report generation.
- Provide for a Plant Configuration Database (PCD).

7.1.4.3 N-DCIS Safety Evaluation Summary

The N-DCIS is classified as a nonsafety-related system. It is used as the primary control, monitoring, and data communication system with power production applications. The N-DCIS is not required for safety-related purposes, nor is its operability required during or after any DBE. The system is required to operate in the normal plant environment and is relied on for data communications and power production applications. The N-DCIS provides an isolated alternate path for safety-related data to be presented to the plant operators. The N-DCIS network that supports the dual/triplicate, fault-tolerant digital controllers and communication scheme is diverse from the Q-DCIS network design in both hardware and software.

The N-DCIS equipment is located throughout the plant and is subject to the environment of each area. RMUs are typically located throughout the plant and auxiliary buildings. Computer equipment and peripherals are typically located mainly in the CB (MCR and Back Panel areas), Radwaste Building, TSC, EOF, and other auxiliary buildings.

The N-DCIS panels and components are designed to maintain structural integrity, during and after a DBE, and do not prevent any safety-related equipment in their area from performing its safety-related function.

Table 7.1-1 identifies the DCIS systems and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.1.4.4 N-DCIS Regulatory Requirements Conformance Summary

The N-DCIS meets applicable sections of the following regulations, guidelines, and industry standards as shown in Table 7.1-1 and/or described in subsection 7.1.6.

- 10 CFR 52.47;
- NUREG 0694, 0718, and 0737;
- IEEE Std. 7-4.3.2, 323, 344, 338, 383, 384, 497, 518, 603, 828, 829, 830, 1008, 1012, 1028, 1042, 1074;
- ANSI/ISA S67.04.01;
- GDC 1, 2, 4, 13, 19, and 24;
- SRM II.Q and II.T to SECY 93-087;
- RGs 1.97, 1.152, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173, 1.180, and 1.204; and
- BTPs HICB-10, 11, 12, 14, 16, 17, 18, 19, and 21.

7.1.4.5 N-DCIS Testing and Inspection Requirements Summary

The N-DCIS components and critical components of interfacing systems are tested to ensure that the specified performance requirements are satisfied (Reference 7.1-10). Factory, construction,

and preoperational testing of the N-DCIS elements are performed before fuel loading and startup testing to ensure that the system functions as designed and that actual system performance is within specified criteria.

The N-DCIS controllers, displays, monitoring and input and output communication interfaces function continuously during normal power operation. Abnormal operation of these components can be detected during plant operation. In addition, the controllers are equipped with on-line diagnostic capabilities to identify and isolate failure of I/O signals, buses, power supplies, processors, and inter-processor communications. These on-line diagnostics can be performed without interrupting the normal operation of the N-DCIS.

7.1.4.6 N-DCIS Operator Interface Requirements Summary

The N-DCIS VDUs allow operator control and monitoring of the N-DCIS systems. However, they only allow monitoring of safety-related system data, through appropriate isolation. The VDUs are also segmented so that the network segments can be monitored and controlled independently. During normal operation the segments are not apparent to the operators. The N-DCIS supplies alarm and annunciation information to the operator and a permanent overview mimic display for important plant information.

7.1.4.7 N-DCIS System Boundaries

The N-DCIS includes no Q-DCIS components. The N-DCIS does not include the sensors or the sensor wiring to the RMUs or the RMU output wiring to the actuators.

7.1.4.8 N-DCIS Major Systems Description Summary

The N-DCIS systems and components are nonsafety-related entities of the DCIS. The N-DCIS major system summary descriptions follow.

7.1.4.8.1 GE-Hitachi Nuclear Energy Systems Description Summary

GEH systems include:

- 3D MONICORE that calculates three dimensional power distribution and thermal limits for the reactor core;
- Systems that control and monitor the Control Rod Motion, including Rod Control and Information System (RC&IS), ATLM, Rod Worth Minimizer (RWM), MRBM, and Signal Interface Unit (SIU);
- The logic for SPDS;
- The DPS that provides a subset of reactor scram and the ECCS functions;
- The nonsafety-related gateways/datalinks that translate and distribute data from the Q-DCIS to the N-DCIS;
- Operator control and monitoring from the MCR VDUs; and

- The nonsafety-related portion of the NMS that provides data to the AFIP subsystem and the MRBM subsystem.

7.1.4.8.2 Plant Investment Protection Systems (Train A and Train B) Description Summary

The N-DCIS for the Plant Investment Protection (PIP) Systems (Train A and Train B) provides the logic to control the following plant systems:

- CRD,
- RWCU/SDC,
- FAPCS,
- Reactor Component Cooling Water System (RCCWS),
- Plant Service Water System (PSWS),
- PSWS cooling towers,
- Chillers,
- Drywell cooling nonsafety-related electrical systems,
- Instrument air,
- Diesel generators, and
- 6.9 KV Plant Electric Power.

The N-DCIS segments in PIP A and PIP B allow for operator control and monitoring from the MCR nonsafety-related VDUs and the RSS VDUs. The A and B segments can operate independently of one another.

During loss of offsite power events, the N-DCIS for PIP A and PIP B is powered by diesel generators in the Standby AC On-Site Power Supply System and can therefore operate without offsite power.

7.1.4.8.3 Balance Of Plant Systems Description Summary

The BOP segments provide the logic for systems involved in power generation. These systems control/protect the following:

- Reactor pressure;
- RPV water level;
- Plant Automation System (PAS);
- The turbine and generator;
- The main condenser and normal heat sink;

- The nonsafety-related plant electrical systems that are non-PIP;
- Power generation components such as the Moisture Separator Reheater (MSR) and the CPS; and
- The Condensate and Feedwater System (C&FS), including extraction and level control.

Segments in the BOP systems allow for operator control and monitoring from the MCR nonsafety-related VDUs.

7.1.4.8.4 Plant Computer Systems Group Description Summary

The Plant Computer Systems Group provides:

- PCF distributed throughout the N-DCIS segments in redundant workstations and/or controllers. PCF provide Performance Monitoring and Control (PMC), prediction calculations, visual display control, point log and alarm processing, surveillance test support, and automation;
- The plant alarm management system that alerts the operator to process deviations and equipment/instrument malfunctions;
- The Historian function, that stores data for later analysis and trending;
- Control of the main mimic on the MCR Wide Panel Display (WDP);
- Support functions for printers and the secure data communications to the TSC, EOF, ERDS, and potential links to the Simulator;
- OLP to guide the operator during normal and abnormal operations, and to verify and record compliance;
- Report generators to allow the operator, technician, or engineer to create historical or real time reports for performance analysis and maintenance activities;
- The PCD to document, manage, and configure components of the N-DCIS; and
- Gateways to vendor-supplied nonsafety-related systems such as seismic, meteorological, and radiation monitoring.

7.1.5 N-DCIS Specifics

The N-DCIS is one of two functional units of the DCIS and is nonsafety-related. The second functional unit, the Q-DCIS is safety-related.

A simple functional block diagram of the DCIS is shown as part of Figure 7.1-1. The N-DCIS data communication systems are embedded in the DCIS that performs the data communication functions that are part of and support the nonsafety-related systems described in Sections 7.2 through 7.8 and support the Q-DCIS to N-DCIS communications for the safety-related systems described in Sections 7.2 through 7.8. A functional network diagram of the DCIS appears as part of Figure 7.1-2, which indicates the elements of the N-DCIS and the Q-DCIS.

The N-DCIS architecture, its relationships, and its acceptance criteria are further described in this section.

7.1.5.1 N-DCIS Design Bases

7.1.5.1.1 N-DCIS Safety-Related Design Bases

The N-DCIS does not perform or ensure any safety-related function. It is classified as a nonsafety-related system, and has no safety-related design basis.

7.1.5.1.2 N-DCIS Nonsafety-Related Design Bases

The N-DCIS is used as the primary control, monitoring, and data communication system for power production applications. The design bases for the N-DCIS include the requirements to:

- Segment the N-DCIS display and control of the two PIP Systems (A&B) and the BOP systems so they can operate independently of one other;
- Segment the major reactor control systems (FWCS, SB&PC, Turbine-Generator Control System [TGCS] and PAS) so they can operate independently of one another and from the DPS;
- Perform closed loop control and system logic independently of the MCR VDUs and Ethernet networks. Operability of the remote shutdown panels, and their VDUs is independent of the operation or existence of the MCR displays;
- Ensure that no single failure of an N-DCIS component affects power generation;
- Provide a communication path for nonsafety-related data gathered and distributed throughout the plant, including data link interfaces to control systems. The communication paths are redundant and include both the “native” control systems and “foreign”, vendor supplied or prepackaged control systems (condensate purification, offgas, radwaste, area radiation monitoring, and meteorological monitoring, for example);
- Reliably transfer to or from the plant areas, in digital format, analog or binary information that has been collected and digitized from nonsafety-related RMUs. The RMUs include transmitters, contact closures and other sensors or process activation signals, generated elsewhere for the control of remote devices such as pumps, valves or solenoids;
- Receive selected safety-related signals from the Q-DCIS through gateway devices, or workstations and then transmit the signals to nonsafety-related VDUs and other nonsafety-related systems for control, monitoring and alarming purposes;
- Replace a majority of conventional, long-length, copper-conductor cables that connect components of the nonsafety-related plant instrumentation systems and control systems with fiber optic cable data networks to reduce cost and complexity;

- Provide an electrically noise-free transmission path for plant sensor data and control signals;
- Collect and archive data for transient analysis and data trending, sequence of events recording, display of SPDS and RG 1.97 information in the MCR, processing, and annunciation of alarm conditions to plant operational staff;
- Perform various PCF including PMC by providing Nuclear Steam Supply System (NSSS) performance and prediction calculations, visual display control, point log and alarm processing, surveillance test support, automation and the BOP performance calculations;
- Provide a permanent record and historical perspective for plant operating activities and abnormal events;
- Provide a secure communications interface with external computer and monitoring systems (one-way communication, no control capabilities). This includes the plant simulator (for training and for development and analysis of operational techniques), TSC, EOF, and the ERDS;
- Provide reactor core performance information;
- Provide a SPDS of critical plant operating parameters. The parameters include power, water level, temperatures, pressures, flows, and the status of pumps, and valves. The SPDS allows the MCR operators to follow the Plant Emergency Operating procedures (EOPs) to shut down the reactor, maintain adequate core cooling, cool down the reactor to cold shutdown conditions and maintain primary containment integrity as required by NUREG-0737, Supplement 1. Specific SPDS displays are available in the MCR and SPDS parameters are available on the main plant mimic on the MCR WDP;
- Provide the MCR overview displays, navigational/top level displays, and system level displays**;**
- Provide TSC and EOF displays;
- Provide an Alarm Management System (AMS) designed to alert the operator to an alarm condition, informing the operator of its priority, guiding the operator's response, and confirming whether the response was effective;
- Display normal, abnormal and EOPs on operator workstations and other workstations where display of operating procedures is permitted;
- Warn the operator to document that a Technical Specification limit, such as, Limiting Condition of Operation (LCO), is being approached or violated when such conditions are detectable;
- Provide a 3D MONICORE system interface with the operator and with other systems;
- Provide time tagging of all measured points to facilitate Transient Recording and Analysis (TRA), Sequence of Events (SOE) recording, and first out determination;

- Provide real-time core thermal power and flow calculations from critical to 100% of rated power;
- Provide on-line diagnostics and monitoring of plant individual thermal heat cycle components, normalized to current plant conditions;
- Provide hard copy reports of current and historical plant operating data with pre-defined and custom formats to suit the needs of operations, maintenance, and engineering;
- Provide overall configuration management functions for the N-DCIS PCD;
- Provide manual and automatic DPS Selected Control Rod Run-in (SCRRI) initiation and Select Rod Insertion (SRI);
- Provide the Alternate Rod Insertion (ARI) initiation signal;
- Initiate Fine Motion Control Rod Drive (FMCRD) and Emergency Rod Insertion (ERI) condition signals;
- Acquire process measurement and equipment status signals from the process sensors and discrete monitors of the plant's nonsafety-related systems;
- Perform signal conditioning and A/D conversion for continuous process (analog) signals and perform signal conditioning and change-of-state detection for discrete signals;
- Provide data message formatting and data transmission from remote locations in the plant to the MCR through fiber optic cable and hardwire network connections;
- Receive command and control signals from the redundant controllers in the MCR area, and transmit the signals from the MCR area to remote locations in the plant where the N-DCIS distributes the signals to the final actuating devices;
- Provide data link interfaces to all control and logic processing equipment supplied by parties other than the primary N-DCIS equipment supplier; and
- Provide data support functions through a secure communications interface with the TSC, EOF, and the ERDS, and provide operator aids provided by the plant computer system of the N-DCIS, such as safety parameter displays, transient data recording, analysis, archiving, alarm processing, and SOE processing.

7.1.5.1.3 N-DCIS Setpoint Methodology

To select instrumentation and controls and to determine setpoints, the design considers instrument drift, environmental conditions at the sensor location, changes in the process, testability, and repeatability. Adequate margin between limits and instrument setpoints is provided to allow for instrument error. The amount of instrument error is determined by test and experience. The setpoint is selected based on a known error; most of this error is in the transducer to the measurement channel and A/D converters of the RMU. The remaining equipment is microprocessor based with discrete setpoints that do not drift. The recommended test frequency is greater for instrumentation that demonstrates a stronger tendency to drift.

Ideally, the actual settings are determined by operating experience. However, in cases where operating experience is not available, settings are determined by conservative analysis. The settings are far enough from the values expected in normal operation to preclude inadvertent initiation of certain actions and far enough from the analyzed values to ensure that appropriate margins are maintained between the actual settings and analyzed values. The margin between the limiting system settings and the actual limits includes consideration of the maximum credible transient in the process being measured.

The periodic test frequency for each variable is determined from historical data on setpoint drift and from quantitative reliability requirements for each system and its components. A formal process is followed to establish key N-DCIS setpoints.

7.1.5.2 N-DCIS Description

The N-DCIS is a nonsafety-related network that is segmented into parts that can work independently of one another if failures occur. The segments are not visible to the operator during normal operation. The N-DCIS uses hardware and software platforms that are diverse from the Q-DCIS. The N-DCIS is a network that is dual redundant and at least redundantly powered so no single failure of an active component can affect power generation.

The individual N-DCIS segments are the:

- GEH network,
- PIP A network,
- PIP B network,
- BOP network, and
- Plant Computer network.

The segments are redundant, managed network switches (sometimes called “level 3” switches) into which the data acquisition, control and displays associated with that segment are connected. Each network switch can have up to several hundred “nodes” and several “uplink” ports that are connected to the other switches; all connections to these switches are through the fiber optic cable network. Fiber optic cables used for nonsafety-related applications are sheathed in material that meets the IEEE Std. 383 standard that addresses fire propagation mitigation.

The switches allow the various controllers, data acquisition and displays associated with a segment to communicate with each other by almost instantaneous virtual connections that end when the communication is finished. The switches’ “backbone” capacity determines how many simultaneous two-way connections can be made, but the capability is much higher than actually required. Only when a switch determines that an information data packet is destined for a node on another switch is the information put on an uplink to another switch. The network switches learn and maintain their own forwarding tables containing a list of all the nodes and hosts on their respective network segment. When a network switch receives a data communication packet, it forwards only that particular data packet to the segment to which that receiving host is

connected. This mechanism prevents data traffic between devices on the network from impacting devices on other segments of the network.

The uplink ports on the switches are connected together radially and in a ring because multiple interconnections increase reliability. Specifically the switches use a "spanning tree protocol" to automatically enable and disable ports so there is normally only one path from the nodes of one switch to another. Should a path become disabled, the switches automatically reconfigure to establish another path through the remaining switches and fiber optic cable paths. Reconfiguration requires no operator input and is usually accomplished in seconds.

Each switch "node" (workstation, display, and controller) is connected to redundant switches of the segment. These connections support normal plant operation. The switches have Mean Times Between Failure (MTBF) of greater than 100,000 hours. Each switch has redundant power feeds and can work from either power source. The switches and connected controllers support extensive component and data self-diagnostics, and failures are alarmed.

The above text and Figure 7.1-2 show that the N-DCIS is not a single network. It is redundant and segmented to support the DCIS with very high reliability. A single failure of one of the redundant switches in a segment or multiple failures that involve no more than one switch per segment has no effect on plant operation or data. The failure is alarmed and can be repaired online. In the highly unlikely event of both switches of a segment simultaneously failing, that particular segment is lost. However, the remaining segments are unaffected and individual nodes connected to the failed switches may continue to function. The remaining switches then automatically reconfigure their uplink ports such that the remaining segments automatically find data paths between themselves.

The major N-DCIS functions are segmented as defined below:

- GEH
  - Safety-related system gateways,
  - DPS (triple redundant processors),
  - 3D MONICORE,
  - ATLM,
  - MRBM,
  - RWM,
  - AFIP,
  - RC&IS, and
  - MCR displays.
- PIP A (includes the "A" segment of) and PIP B (includes the "B" segment of):
  - FAPCS,

  - CRD,
  - RWCU/SDC,
  - Diesel generator,
  - 6.9 KV electrical system (including protective relaying),
  - Low voltage electrical system (including protective relaying),
  - Uninterruptible power,
  - DC power,
  - Instrument and control power,
  - RCCW,
  - PSW,
  - PSW cooling towers (if applicable),
  - Instrument air,
  - Chillers,
  - Drywell cooling,
  - HVAC supporting above systems,
  - MCR displays, and
  - Remote shutdown panel displays.
- BOP:
  - TGCS (triple redundant processors),
  - SB&PC (triple redundant processors),
  - FWCS (triple redundant processors),
  - PAS (triple redundant processors),
  - Condensate/feedwater,
  - Heater drains and vents,
  - Main condenser,
  - Normal heat sink,
  - Makeup water system,
  - Moisture separator/reheater,

  - Turbine auxiliaries,
  - Generator auxiliaries,
  - Turbine Component Cooling Water System (TCCWS),
  - Service air,
  - Breathing air,
  - Chillers,
  - HVAC supporting above systems,
  - Auxiliary boiler,
  - Plant electrical system (including protective relaying),
  - Vendor supplied BOP systems/controllers (condensate polishing, offgas, condensate storage and transfer), and
  - MCR displays.
- Plant computer functions (PCF):
  - Core thermal power/flow,
  - Performance monitors (BOP, Bypass, Technical Specification Monitoring [TSM]),
  - Alarm/management,
  - On-line and alarm response procedures,
  - SPDS,
  - Nonsafety-related post accident (per RG 1.97) displays,
  - WDP (mimics, etc.),
  - Report generators,
  - Secure communications interfaces (TSC, EOF, ERDS),
  - Printers,
  - Historian function,
  - Fire protection system (through gateways/datalinks),
  - Area radiation monitoring,
  - Seismic monitoring, and

– Meteorological monitoring.

7.1.5.2.1 Nonsafety-Related Shutdown Systems

Descriptions of nonsafety-related shutdown systems follow.

7.1.5.2.1.1 Remote Shutdown System

Each RSS panel has the ability to operate all of the nonsafety-related PIP equipment and the BOP equipment, either automatically or manually. Refer to Subsection 7.4.2 for additional information.

7.1.5.2.1.2 Reactor Water Cleanup/Shutdown Cooling System

The nonsafety-related RWCU/SDC maintains reactor water purity during operation. It also provides normal shutdown cooling by taking suction from the RPV, pumping the flow through heat exchangers, and returning the cooled water to the vessel through the feedwater line. The system is segmented and allows the train A and B components to operate independently. Refer to Subsection 7.4.3 for additional information.

7.1.5.2.1.3 Fuel and Auxiliary Pools Cooling System

The nonsafety-related FAPCS maintains the fuel, PCCS/ICS and GDCS pools, by pumping pool water through heat exchangers and demineralizers into two 100% cooling and cleaning trains. They also maintain suppression pool temperatures and cleanliness during operation. The FAPCS can also initiate a "LPCI" mode following an accident and after the reactor has been depressurized to provide reactor makeup water for accident recovery. In this mode the FAPCS pump takes suction from the suppression pool and pumps it into the RPV through RWCU/SDC Loop B and Feedwater Loop A. The system is segmented and allows train A and B components to operate independently. Refer to Subsection 7.5.5 for additional information.

7.1.5.2.1.4 Control Rod Drive System

The nonsafety-related CRD usually maintains the Hydraulic Control Unit (HCU) accumulators at the required pressure to provide cooling water flow to the FMCRDs and to provide various high-pressure purge flows. The CRD can also provide a "high pressure injection" mode capable of supplying inventory to the reactor vessel at elevated pressures. The system is segmented and allows Train A and B components to operate independently. Refer to Section 4.6 for additional information.

7.1.5.2.2 Nonsafety-Related Information Systems

7.1.5.2.2.1 Process Radiation Monitoring System

Nonsafety-related PRMS instrumentation monitors the main steam lines, in the drywell, discharges from the ICS, vent discharges and liquid and gaseous effluent streams that may contain radioactive materials. The safety-related PRMS is discussed in Subsection 7.1.3.2.4.3.

MCR display, recording, and alarm capabilities are provided along with controls that provide automatic trip inputs to the respective systems to prevent further radiation release. Refer to Subsection 7.5.3 for additional information.

7.1.5.2.2.2 Area Radiation Monitoring System

Nonsafety-related ARMS instrumentation continuously monitors the gamma radiation levels within designated areas of the plant. It provides early warning to operating personnel when predetermined dose rates are exceeded. Refer to Subsection 7.5.4 for additional information.

7.1.5.2.3 Control Systems

7.1.5.2.3.1 Nuclear Boiler System Instrumentation

Nonsafety-related NBS instrumentation provides indication of reactor coolant and vessel temperatures, RPV water level, and reactor vessel pressure. Refer to Subsection 7.7.1 for additional information.

7.1.5.2.3.2 Rod Control and Information System

The nonsafety-related RC&IS is able to control reactor power level by controlling the movement of the control rods in the reactor core during manual, semi-automated, and automated modes of plant operations. The ATLM automatically enforces fuel operating thermal limits Minimum Critical Power Ratio (MCPR) and Maximum Linear Heat Generation Rate (MLHGR) when reactor power is above the Low Power Setpoint (LPSP). Refer to Subsection 7.7.2 for additional information.

7.1.5.2.3.3 Feedwater Control System

A highly reliable and triple redundant nonsafety-related FWCS automatically and manually regulates the flow of feedwater into the reactor pressure vessel. This maintains predetermined water level limits for all modes of reactor operation, including heatup and cooldown. Refer to Subsection 7.7.3 for additional information.

7.1.5.2.3.4 Plant Automation System

The nonsafety-related PAS:

- Provides automatic startup/shutdown algorithms and controls,
- Regulates reactivity during criticality control,
- Provides heatup and pressurization control,
- Regulates reactor power, and
- Provides automatic power generation control during power operation. Refer to Subsection 7.7.4 for additional information.

The PAS does not involve safety-related systems. The PAS is the first of two automation schemes implemented by the N-DCIS, plant-wide automation and system level automation. The PAS coordinates the action of multiple systems for plant-wide automation using system level controllers to automate the operation, maintenance, testing, and inspection functions. It uses Automated Program Functions (APF) to coordinate the Automatic Power Regulator (APR) and the Power Generation and Control Systems (PGCS) of the PAS.

The PAS provides the capability for supervisory control of the entire plant by supplying set-point commands to independent nonsafety-related automatic control systems as changing load demands and plant conditions dictate. Safety-related systems are never controlled or tasked by the PAS. The automation system covers the tasks involved in criticality, heat-up and pressurization, turbine roll and synchronization, and plant power control.

The APR and PGCS Subsystems of PAS automatically run the plant, with operator supervision from cold non-critical conditions to 100% rated temperature, pressure, and power and back to cold non-critical conditions.

The PAS establishes several broad automation sequences:

- Pre-startup check sequence,
- Approach to criticality and reactor pressurization sequence,
- One button startup and synchronization sequence,
- Power operations sequence (increase turbine load to rated power), and
- One button shut down sequence.

Prior to initiating the "one button startup and synchronization sequence," prerequisite and continually operating equipment must be in a satisfactory pre-defined condition. There is a complete list of prerequisite conditions for each system. Some plant systems are never shut down, even during refueling outages and their operating conditions are independent of plant power.

7.1.5.2.3.5 Turbine Generator Control System

Functions of the TGCS include:

- Turbine speed/acceleration control (including ability to navigate 100% load rejection/ Turbine Island Mode);
- Turbine over-speed protection;
- Turbine control interface with SB&PC;
- Turbine load control;
- Turbine valve testing;
- Interface with condensate/feedwater;

- Related surveillance tests, checks, and inspections;
- Automatic response to alarm conditions, system faults, and plant transients;
- Related generator control functions; and
- Related Turbine Generator (TG) auxiliary support control functions.

7.1.5.2.3.6 Steam Bypass and Pressure Control System

A highly reliable and triple redundant nonsafety-related SB&PC controls reactor pressure during plant startup, power generation, and the shutdown modes of operation. This is accomplished through control of the turbine control valves and/or turbine bypass valves so susceptibility to reactor trip, turbine generator trip, main steam isolation and safety relief valve opening is minimized. Refer to Subsection 7.7.5 for additional information.

7.1.5.2.3.7 Neutron Monitoring System - Nonsafety-related Systems

The nonsafety-related AFIP provides a signal proportional to the axial thermal neutron flux distribution at the radial core locations of the LPRM detectors. The signal facilitates fully automated, precise, reliable calibration of the LPRM gains. The signal also provides axial power measurement data for three dimensional core power distribution determinations. The nonsafety-related MRBM logic issues a control rod block demand to the RC&IS logic to prevent fuel damage. It assures that the MCPR and MLHGR do not violate fuel thermal safety-related limits. Refer to Subsection 7.7.6 for additional information.

7.1.5.2.3.8 Containment Inerting System

The nonsafety-related containment inerting system establishes and maintains an inert atmosphere within the Primary Containment Volume (PCV). It operates during all plant operating modes, except during plant shutdown for refueling and/or equipment maintenance and during limited periods of time to permit access for inspection at low reactor power. Refer to Subsection 7.7.7 for additional information.

7.1.5.2.3.9 Diverse Instrumentation and Controls

Although not required for safety, diverse I&C is provided to address BTP HICB-19 on Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems. This is in addition to the ATWS mitigation features, which provide alternate control rod insertion, boron injection, and feedwater runback. The safety-related ATWS mitigation function using liquid boron injection is a part of the diverse I&C functions. This diverse I&C function, called DPS, is implemented in a highly reliable triple redundant control system whose sensors, hardware and software are different from any of the safety-related I&C platforms.

The following diverse actuation functions are provided in the DPS:

- A set of protection logics that provide a diverse means to scram the reactor via control rod insertion using sensors, hardware and software that are separate and independent of the primary RPS.

- A set of initiation logics that provide a diverse means to initiate certain ESF functions using sensors, hardware and software that are separate and independent of the primary ESF systems.
- A set of ARI and associated logics, such as control rod run-in, through control rod insertion through an alternate means by opening the three sets of air header dump valves of the CRD system. This is also part of the ATWS mitigation function.

The DPS provides both manual and automatic initiation of the above functions. Refer to Subsection 7.8.1 for additional information.

7.1.5.2.3.10 Selected Control Rod Run-In / Select Rod Insert

The N-DCIS accepts the redundant loss of feedwater heating signals from the FWCS and the turbine trip and load rejection signals from the turbine control system, performs two-out-of-three voting on each, and then combines them as an "OR" function to become the automatic SRI and SCRRI command signals. The SRI and SCRRI can also be initiated manually from the MCR, which is part of the DPS and RC&IS system's scope. The manual SCRRI function is independent of the N-DCIS equipment scope. The SRI and SCRRI can also be initiated by the DPS.

The redundant N-DCIS SCRRI command signals are sent to the RC&IS. In the RC&IS each of the dual Rod Action and Position Information (RAPI) channels performs a two-out-of-three vote and initiates RAPI channel logic associated with accomplishing the SCRRI function. When activated, the SCRRI function inserts control rods using the FMCRD motors to pre-defined positions to reduce reactor thermal power to a target power level. This logic is implemented in a highly reliable redundant control system. The SCRRI command signal is also used in the emergency rod insertion control logic of the N-DCIS, as discussed below.

The redundant SRI command signals are sent from DPS to the nonsafety-related scram timing panel. This panel is electrically isolated from the divisional panels that contain the switches in the 120 VAC return from each HCU scram solenoid. When commanded to open (using two-out-of-three voting logic) for either a full DPS scram, a single HCU scram timing test or for predefined rod groups the affected HCUs scram their associated rods. Because the scram timing switches are in the solenoid return, the RPS load drivers are in the solenoid 120 VAC supply, and the switches and solenoids are in a "series" circuit, there is no credible failure of the scram timing panel that can prevent or affect an RPS scram.

7.1.5.2.3.11 Alternate Rods Insertion

The N-DCIS accepts the redundant ARI signals from the DPS and performs two-out-of-three voting of these signals to become the N-DCIS scope ARI initiation signal. Redundant ARI command signals are sent to the RC&IS where each of the dual RAPI channels perform a two-out-of-three vote and initiate the RAPI channel logic associated with accomplishing the ARI (motor run-in) function.

When activated, ARI inserts all operable control rods using their FMCRD motors in the normal full-in position. This acts as a backup means for the hydraulic safety-related scram function of the CRD system. This logic is implemented in a highly reliable redundant control system.

The ARI command signal is also used in the emergency rod insertion logic of the N-DCIS, as discussed below.

The DPS does not issue an ARI command without issuing a simultaneous scram command.

7.1.5.2.3.12 Emergency Rod Insertion

The N-DCIS combines the N-DCIS SCRRI command signal and the N-DCIS ARI command signal by an "OR" function to become an FMCRD emergency insertion signal. Redundant FMCRD emergency insertion signals are sent to the ERI control panel of the RC&IS, which performs two-out-of-three voting. It initiates associated emergency insertion condition signals in the ERI panels of the RC&IS that provide inputs to the Induction Motor Controllers (IMCs) of the RC&IS.

For the SCRRI or ARI motor run-in function of the RC&IS equipment to be initiated, the emergency insertion signals to the IMCs must also be activated concurrent with the IMCs receiving the SCRRI or ARI related command signals transmitted from the RAPI logic. This logic is implemented in a highly reliable redundant control system.

7.1.5.2.4 Plant Computer Functions

All PCF are an integral part of the HFE process (Refer to Chapter 18). The allocation of functions accommodates human capabilities and limitations, fault detection and recovery capabilities are provided, and an acceptable operator workload is not exceeded. Additionally, PCF (like the plant controllers) are powered with uninterruptible power supplies so that they are available to the operator for as long as the N-DCIS is powered.

The PCF increase the efficiency of plant performance by:

- Performing the functions and calculations defined as being necessary for the effective evaluation of nuclear power plant operation.
- Providing a permanent record and historical perspective for plant operating activities and abnormal events.
- Providing analysis, evaluation and recommendation capabilities for startup, normal operation, and plant shutdown.
- Providing the capability to monitor plant performance through presentation of video displays in the MCR and elsewhere throughout the plant and providing the ability to directly control certain nonsafety-related plant equipment through on-screen technology.
- Providing secure data communication with all external computer and monitoring systems (for example, one-way communication, no control capabilities) including the TSC, EOF, and ERDS.

- Performing core thermal power and core flow calculations from reactor heat balances. Iterative computational methods are used to establish a compatible relationship between the core coolant flow rate and core power distribution. The results are subsequently interpreted in the NSSS performance module as power in specified axial segments for each fuel bundle in the core.

The calculations performed by the N-DCIS include process validation and conversion, combination of points, NSSS performance calculations, and the BOP performance calculations.

The Performance Monitoring and Control (PMC) system provides the NSSS performance and prediction calculations, visual display control, point log and alarm processing and BOP performance calculations.

7.1.5.2.4.1 Safety Parameter Display System

The SPDS provides critical plant operating parameters such as power, water level, temperatures, pressure flows, and status of pumps and valves. The SPDS system allows the MCR operators to follow plant EOPs to shut down the reactor, maintain adequate core cooling, cool down the reactor to cold shutdown conditions and maintain primary containment integrity as required by NUREG-0737, Supplement 1. Specific SPDS parameters are available in the MCR and on the main plant mimic.

7.1.5.2.4.2 MCR Displays

The MCR panel equipment is part of the MCR Panels (MCRP) System. Information for the displays is presented with the following functional configuration arrangement.

- Level 0: Integrated overview display;
- Level 1: Navigational/top level display;
- Level 2: System level display;
- Integrated Overview Display (sometimes called the main plant mimic) provided on the WDP.
- The fixed-position portion of the large display panel provides critical plant operating information, such as power, water level, temperature, pressure, flows, status of major equipment, and availability of safety-related systems. There is a mimic in the MCR during plant normal, abnormal and emergency operating conditions. The dynamic display elements of the fixed-position displays are driven by dedicated microprocessor-based controllers that are independent of the N-DCIS.
- The large variable display portion of the WDP can indicate any display format available on a nonsafety-related VDU; the plant operator initiates the chosen format.
- Appropriately isolated safety-related information is available on the nonsafety-related Integrated Overview Display and various nonsafety-related VDUs.

- Navigational or Top Level Displays - The plant computer function provides the following navigational or top level displays:
  - Main Menu;
  - Safety Parameter Displays;
  - Post Accident Monitoring (RG 1.97) Displays;
  - Alarms;
  - Power Generation Control;
  - OLP;
  - Technical Specification Monitor/RPS Monitor;
  - 3D MONICORE;
  - Historian Function;
  - TRA;
  - Thermal Performance Monitor and Diagnostic (TPM&D);
  - Report Generator;
  - Bypass and Inoperable Status Indication (BISI); and
  - System Level Displays (P&IDs, alarms).

The PCF control displays provide direct control and parameter monitoring of nonsafety-related equipment and systems through the use of the VDUs and various input devices, which are part of the MCR panels.

The RC&IS dedicated operator interface provides control and monitoring of the RC&IS. This interface is not part of the PCF scope. The RC&IS interface is described in Subsection 7.7.2.

7.1.5.2.4.3 Alarm Management System

The plant AMS is available in the MCR, VDUs, and, indirectly at the TSC and EOF.

The plant AMS is designed to alert the operator to a deviation from normal conditions. It informs the operator of the deviation's priority, guides the operator's response, and confirms whether the response was effective.

To fulfill these basic functions, the system must:

- Detect and, in some cases, predict the occurrence of changes in the plant;
- Alert users to changes significant to the current operating situation, such that:
  - Only operationally relevant changes are alarmed;

- The demands imposed on users' attention to recognize the changes are considered with the demands of other concurrent control room tasks;
- Operators are alerted to additional plant information needed to understand and respond to changes;

To accomplish the above, the AMS uses the following design bases:

- Alert the operators to off-normal conditions which require them to take action;
- Reduce the number of alarms to be consistent with the total operator workload;
- Guide the operators to the appropriate response (linking alarms to alarm response procedures);
- Assist the operators in determining and maintaining an awareness of the state of the plant and its systems or functions;
- Minimize distraction and unnecessary workload placed on the operators by the alarm system – especially during transient and accident conditions;
- Satisfy the dark panel concept: no alarm signal is shown to the operator when the process is operating normally;
- Determine system level alarms based on function and task analysis;
- Include the means to provide the operator with information in different views including sorting, filtering, and grouping of alarms;
- Generate basic alarms and high-level, composite, alarms. The generated alarms are subject to potential filtering, alarm suppression, and alarm prioritization techniques. The plant Historian maintains an alarm log whether or not they are presented to the operator. Alarms are then presented in the MCR either audibly (annunciator), visually (display), or both;
- Create temporary operator-defined alarms and associated alarm setpoints; and
- Integrate with other information systems, such as the OLP and TSM, to facilitate operator tasks; in general the alarm management system and TSM provide the suggested operator response to the various alarm and monitoring function events.

7.1.5.2.4.4 On Line Procedures

OLP provide for:

- Display of normal, abnormal and EOPs on operator and other workstations;
- Display of operating procedures in logic, flowchart, and text formats;

- Hardcopy output of operating procedures from all workstation locations with the displayed format and content, considering potential alternative uses for study guides, and procedure maintenance;
- Maintenance (that is, addition, deletion, and modification) of operating procedures;
- Manual, semi-automated (selected procedures), or fully automated (selected procedures) implementation of operating procedures from the operator workstations;
- Access to controls from the displayed operating procedures;
- Continuous update of the display of parameters, to include embedded dynamic indication status (normal, warning, and alarm conditions), necessary for the plant operator to monitor and/or perform operating procedure steps;
- Confirmation of operator decisions and actions while retaining the operator as the final authority in the execution of procedures;
- Logs of the discrepancies between operator action and procedure execution options;
- Logs of the execution of sequences of steps (selected procedure sequences), not including actions taken by the operator to control components, to ensure that the proper status of components or systems is maintained (this may require manual operator input of steps that cannot be monitored by the N-DCIS); and
- Validation for each operating procedure using the plant Simulator.

7.1.5.2.4.5 Technical Specification Monitoring

TSM, when conditions are detectable, does the following:

- Warns the operator when a technical specification limit, LCO, is being approached;
- Warns the operator when the LCOs are being violated;
- Determines the approach to an LCO based on equipment status information, core limits and margins and other data;
- Indicates, to the extent practical, appropriate action(s) to avoid violating the LCOs;
- Acquires and processes available information to determine the approach to and existence of an LCO;
- Automatically acquires required information;
- Determines, given available information, any automatic testing that could impact the LCOs;
- Indicates, to the extent practical, the action needed to recover from an LCO;
- Provides a log of LCO violations;

- Acquires or calculates as necessary, reactor and core parameters required for monitoring LCOs, such as thermal limit margins, power distribution, and heat generation rates;
- Shows the results of calculations of reactor and core parameters on operator displays;
- Provides manual input capability for LCOs that cannot be monitored automatically by the TSM function;
- Sends alarms to the AMS, which provides for an acknowledgment function for alarm conditions;
- Shows the operator the availability status of the RPS and safety-related systems;
- Provides RPS and safety-related System Monitoring (RPSM) as a sub-function;
- Monitors, through RPSM, support services (for example, voltages, cooling water, oil pressure and levels) that can affect the availability of the RPS and other safety-related systems;
- Monitors, through RPSM, the availability of the initiating equipment (sensors and control systems) and the implementing equipment (for example, pumps, and valves);
- Monitors, through RPSM, the availability of primary and backup sources of services;
- Monitors, through RPSM, process parameters (reactor pressure, water storage tank levels, and environment) that can affect the successful operation of the RPS or other safety-related systems; and
- Provides manual and automatic entry, through the RPSM, of the maintenance, calibration, and test data needed to establish RPS and other safety-related system operability.

7.1.5.2.4.6 Report Generator

The Report Generator is a general-purpose report definition and execution utility program that allows the user to create reports within the PCF. It generates various required custom output reports in the MCR and indirectly to the TSC, and EOF.

The data sources for the Report Generator include any measured or calculated data stored either in the Historian or in a real-time database (measured and calculated points) that enables the report program to locate and retrieve data for pre-configured reports used by operators, engineers and maintenance personnel.

The Report Generator can process algorithms to support plant-wide equipment logs and reports.

7.1.5.2.4.7 Plant Configuration Database

The PCD provides overall configuration and management functions for the N-DCIS PCF at an engineering workstation for the PCF.

7.1.5.2.4.8 3D MONICORE

3D MONICORE provides core performance information. It has two major components, the Monitor and the Predictor. Both components use a three-dimensional core model code as the main calculation engine. 3D MONICORE provides the logic in the input preparation file that interfaces with the core model code that calculates the key reactor state information such as axial and radial power, moderator void and core flow distributions. From these calculations, other parameters such as the magnitude and location of minimum margin to thermal limits (such as MCPR, peak fuel rod linear powers and average planar heat generation rates), fuel exposure and operating envelope data can be determined.

The 3D MONICORE Monitor periodically tracks current reactor parameters automatically with live plant data. Typically, the tracking interval is once per hour, although the automation system may automatically initiate 3D MONICORE more often.

The 3D MONICORE Predictor runs upon user request with live data overlaid with user input. It predicts core parameters for reactor states either in steady or operational transient states other than the present one. This allows the user to study the effects of different rod patterns, core flows and fuel burnups before performing reactor maneuvers to support plant operation.

For accuracy improvement, 3D MONICORE has several adaptation modes, which use in-core neutron flux measurements and AFIP data to calculate nodal fit coefficients that can be input to later Monitor and Predictor cases. The choice of mode depends on the method used to adapt the results of the core model code to in-core detector measurements.

The 3D MONICORE function automatically provides data to other systems including the ATLM and RC&IS automatically, and to PRNM with rigorous manual controls. The data needed by these systems is detailed in their respective system specifications.

7.1.5.2.4.9 Historian

The Historian is the repository for all measured and calculated point data for the plant. It receives input from sources of point data, stores this data and presents it to the report generator, the display driver, and other applications needing historical point data. The Historian provides the following functions:

- Stores point data, plant operating activities, and abnormal event sequences, along with their time-tags, for retrieval and analysis;
- Stores third-party generated data, such as 3D MONICORE data, in a format compatible with the display and report system;
- Stores RG 1.97 variables for current trending or later analysis; and
- Provides on-line data storage capability dependent on plant history and events that is nominally for one fuel cycle. The system warns the system operator about remaining disk storage space, giving the operator time for download to an off-line archiving device. The preferred archiving device uses optical disks.

7.1.5.2.4.10 Transient Recording and Analysis and Sequence of Events Recording

Time tagging at the millisecond level is a function of the TRA and the SOE recording. Time tagging is accomplished as closely as possible to the origin of the data. The required resolution of time tagging is based on the speed of the monitored process variable, the origin of the data (that is, the N-DCIS, the Q-DCIS, or other gateway), and the available technology.

The capability of first-out determination and event analysis is provided by the combination of TRA, SOE, and the Historian.

The time tagging synchronizes all stored data provided by a central master clock.

The TRA utilities are largely reports of current point and historical point data. The TRA utilities may be used to analyze plant events and to support plant startup tests.

Some analysis functions are triggered by plant events and others are performed periodically based on the wall clock (for example hourly, shift, daily logs and reports).

7.1.5.2.4.11 Core Thermal Power and Core Flow Calculation

Real time core thermal power from critical to 100% of rated power is calculated almost continuously. The calculation is supported by multiple, validated parameter measurements and eliminates "constants," previously used for some heat balance inputs, so bias in the calculation is eliminated. At low thermal power levels, the Low Flow Control Valve (LFCV) feedwater flow measurement increases accuracy. The core flow is calculated by the heat balance core flow methodology using the core inlet temperature measurement as input to determine core inlet enthalpy.

7.1.5.2.4.12 Thermal Performance Monitor and Diagnostic

The Thermal Performance Monitor and Diagnostic (TPM&D) provides an on-line diagnostic and monitoring program for the thermal heat cycle. It calculates the deviations of the calculated performance of individual system components from the actual measured performance when the plant is above some threshold power. The trends of the performance data can be used by utility personnel to identify components contributing to thermal efficiency loss.

The TPM&D is a plant model that is normalized to current plant conditions such as reactor power, core flow, reactor pressure and circulating water temperature. The output of the model is a detailed calculation (for example, flows, enthalpies, pressures, and temperatures) of the plant individual heat cycle components with predicted (design basis) and actual performance parameters under that condition. These actual and predicted parameters are compared, and their differences are used to calculate a figure of merit. An example is an equivalent system parameter such as normalized heat exchanger cleanliness.

7.1.5.2.5 N-DCIS Hardware

The flow of data in the N-DCIS is similar to that in the Q-DCIS. Generally, data is acquired in the nonsafety-related RMUs, sent to nonsafety-related controllers, and then to workstations and displays for monitoring, alarming and recording purposes. The N-DCIS has the following major equipment:

- RMUs are located throughout plant buildings such as the RB, CB, Fuel Building (FB), circulating water system (CIRC) pumphouse, switchyard, Electric Building, Turbine Building, and Radwaste Building. The RMUs acquire and output the same signal types as the Q-DCIS RMUs but are nonsafety-related. The RMUs are connected either to the network switch cabinets or directly to the controller cabinets appropriate to the segment and located in the back panel areas of the CB. The links are always by redundant fiber optic cable.

- CP cabinets house the dual/triple redundant control processors, which process the control logic of nonsafety-related NSSS and most BOP systems. The CP cabinets receive plant process data multiplexed at the RMUs and transmitted either directly or through the network switch cabinets to the CP. The CP cabinets then transmit the resulting data to the RMUs where their output signals are used for control of nonsafety-related actuators. The CP cabinets also provide data to the MCR VDUs for operator interface displays or plant-level applications. Note that closed loop control takes place within a network segment so this control is not dependent on signals routed from another network switch segment.

- Network switch cabinets contain the redundant, managed switches for Ethernet switching and provide segmentation, and connection between the N-DCIS components connected to the redundant high-speed fiber optic cable networks.

- Workstation cabinets, depending on the application, support redundant or single workstations that, in turn support the VDUs. The workstations are used for dedicated logic functions where the use of a control processor is not appropriate, such as for the Historian, core thermal power or alarm management.

- The N-DCIS gateways/datalinks provide the N-DCIS communication with the Q-DCIS, vendor-supplied controllers, the secure communication with the TSC/EOF/ERDS, and other nonsafety-related packaged systems such as area radiation monitoring.

- Cabinets that house vendor supplied control or monitoring systems such as seismic monitoring, area radiation monitoring, and integrated leak rate testing.

- Gateway cabinets that collect selected safety-related signals through isolated divisional interfaces for archiving and for nonsafety-related control and monitoring purposes. These gateways or workstations are always interconnected by fiber optic cable to support the electrical isolation requirements between the Q-DCIS and the N-DCIS components. The N-DCIS has no control-related inputs to the safety-related systems with the exception of the NMS for LPRM and APRM calibration functions, for further detail on this communication and transmission of time synchronization signals see subsection 7.1.3.3. Otherwise, communication is one-way from the Q-DCIS to the N-DCIS.

- The MCR consoles and its MCR monitoring and control equipment is the main operator interface with the various plant processes. Example, flat panels with soft controls, or hard controls, page/party phone, meters, silence/acknowledge, recorders, main generator synchronizing inset, PAX phone, radio handsets, keyboards/trackballs.
- The display panels' components and functions include alarm display, mimic, flat panel displays, Closed Circuit Television (CCTV) monitors, large variable display, and the components' associated computer processors.
- Signal isolators isolate signals for RMU internal buses and the redundant fiber optic cable links in the field
- I/O modules provide interfaces between process sensors/actuators
- Fiber optic modems and media converters transmit and receive data through the redundant fiber optic cable links in the field to the redundant control processors
- Computer peripherals, such as printers and plotters, provide output data capabilities

7.1.5.2.6 N-DCIS Functions

The N-DCIS has no safety-related function and it is not required to be operable during or after any DBE. The N-DCIS provides distribution and controls data communication networks that support the monitoring and control of interfacing nonsafety-related plant I&C systems. The N-DCIS also processes data from safety-related systems that are originally acquired by the Q-DCIS. Such data are always transmitted through fiber optic cable to provide the required isolation between the Q-DCIS and the N-DCIS.

Safety-related and nonsafety-related data, once acquired for any reason, are available for any other reason including monitoring, alarming, and recording. Data can be organized for displays and reports in any combination. This ability demonstrates that there are no "dedicated" data. For example, data for RG 1.97, SPDS, alarms, a specific system, or for the mimic are not dedicated. Data from all sources can be combined to form any coherent function.

N-DCIS controllers perform closed loop control and system automatic logic independently of operator inputs from the control room N-DCIS VDUs. The remote shutdown panels operate independently of the MCR displays.

The system includes electrical devices and circuitry such as RMUs, control processors, network switches, data communication paths, and interfaces. These connect field sensors, display devices, controllers, power supplies, and actuators, which are part of the nonsafety-related systems. The N-DCIS also includes any associated data acquisition and communications software, if required, that supports its data distribution and control function. The N-DCIS replaces most conventional, long-length, copper-conductor cables with a dual or triple redundant, fiber optic cable, data network. The fiber optic cable data network reduces the cost and complexity of cable runs and provides an electrically noise-free transmission path for plant sensor data and nonsafety-related control signals.

Triple redundant controllers and data acquisition systems are used for the DPS, FWC, SB&PC, TGCS and PAS. As a minimum, dual redundant controllers and data acquisition are used for all power generation functions including non-control functions (such as 3D MONICORE) that support power generation and core thermal power and flow calculations. The nonsafety-related data from sensors are multiplexed at nonsafety-related RMUs and then transferred through the N-DCIS data network to components of the N-DCIS. Selected signals from the nonsafety-related instrumentation are transmitted to the N-DCIS input cabinets through dedicated hardwired connections as required for faster transmission rates of signals, such as SB&PC to TGCS control. Similarly, output signals to actuators and controls that require faster transmission rates, such as manual turbine trip signals, also use dedicated hardwired connections. The RMUs and the data communication network for such nonsafety-related data processing and transmission are part of the N-DCIS.

Divisionally separated redundant isolated digital gateways provide one-way communications from safety-related systems to the N-DCIS. The electrical and data isolation functions are part of the Q-DCIS, and the gateway functions (data conversion and packaging) are part of the N-DCIS. The communications from nonsafety-related systems to the Q-DCIS are limited to communication from the 3D MONICORE function of the N-DCIS to the PRNM (LPRM and APRM) function of the NMS and time tagging, for further detail on this communication and transmission of time synchronization signals see subsection 7.1.3.3.

The local N-DCIS RMUs perform signal conditioning and A/D signal conversion for continuous process signals. They also perform signal conditioning and change-of-state detection for discrete signals such as contact closures and openings. The RMU function performs both I/O signal-processing functions. The RMU formats the acquired signals into data messages and transmits the data through the data network to N-DCIS components for logic processing. The RMU with a system logic function receives logic commands, such as trip commands and control signals, from the data network N-DCIS logic processors. The RMU then provides terminal points for distributing the signals to the final actuating devices of the nonsafety-related systems.

Operator interfaces for control and display are realized through multiple, non-dedicated VDUs, each of which is connected to the segmented network switches.

The N-DCIS's on-line diagnostic functions monitor transmission path quality and integrity. The dual redundant data communication paths are repairable on-line if one path fails. The N-DCIS failures are alarmed in the MCR. Periodic surveillance, using off-line tests with simulated input signals, verifies the overall system integrity.

The N-DCIS networks and components are distributed throughout the plant and are powered by redundant internal power supplies fed from two 120 volt AC Uninterruptible Power Systems (UPS). Some systems, such as DPS, TGCS, FWCS, SB&PC, and PAS, are triple redundant and are powered by three nonsafety-related UPS load groups.

7.1.5.3 N-DCIS Safety Evaluation

The N-DCIS is classified as nonsafety-related and is not required for safety-related purposes. Its operability is not required during or after any DBE. The N-DCIS is required to operate in the normal plant environment and is significant for power production applications. The N-DCIS

does not perform any safety-related functions as a part of its design; however the N-DCIS does provide an isolated alternate path for safety-related data from Q-DCIS to N-DCIS that is presented in the MCR. The N-DCIS network that supports the dual/triplicate, fault-tolerant controllers of the process control systems uses a proven technique for high speed transfer of data different from Q-DCIS and thus provides diversity in design.

The N-DCIS equipment is located throughout the plant and is subject to the environment of each area. Specifically:

- RMUs are located throughout the plant and auxiliary buildings.
- Computer equipment and peripherals are located mainly in the CB in the MCR and Back Panel areas. They are also located in other areas such as the EOF, Radwaste Building, TSC, Auxiliary Fuel Building, Auxiliary Fuel Building roof area, or alternate building designations specific to the plant design.

The N-DCIS panels and components are designed to retain their structural integrity during and after DBEs so that proximate safety-related equipment is not prevented from performing its safety-related function.

Table 7.1-1 identifies the N-DCIS elements and the associated regulatory requirements, guidelines, and codes and standards applied, in accordance with the SRP. The following subsections address conformance with regulatory requirements, guidelines, and industry standards.

Additional regulatory requirements, guidelines, and industry standards not found in the following subsections may be found in subsection 7.1.6.

7.1.5.3.1 Code of Federal Regulations

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety-Related Issues

- Conformance: The N-DCIS is nonsafety-related and conforms so that there are no unresolved issues for the N-DCIS.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications

- Conformance: Inspection, Test, Analyses, and Acceptance Criteria (ITAAC) for the N-DCIS are identified in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements

- Conformance: There are no interface requirements for this section.

7.1.5.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, and 24:

- Conformance: The N-DCIS conforms with the GDCs identified above. Refer to Subsections 3.1.2 and 3.1.3 for a general discussion of each GDC.

7.1.5.3.3 Staff Requirements Memorandum

SRM, SECY-93-087, Item II.Q, Defense Against Common Mode Failures in Digital Instrumentation and Control Systems:

> Conformance: SRM for SECY 93-087, II.Q, states that if a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. The N-DCIS has diverse functionality.

SRM, SECY-93-087, Item II.T, Control Room Alarm Reliability:

> Conformance: The N-DCIS AMS follows guidance in the above document for redundancy, independence, and separation so that the "alarm system" is considered redundant, has its own redundant processors and uses signals from distributed and redundant controllers. Alarm points are sent through a dual network to redundant processors that have dual power feeds. The alarm processors are dedicated, redundant, and conservatively sized. The alarms can be displayed on multiple independent VDUs, each with dual power supplies. Alarms are driven by redundant data links to the AMS. The alarm processors are redundant. There is one horn and one voice speaker. Test buttons test the horn and the lights.

7.1.5.3.4 Regulatory Guides

RG 1.151 - Instrument Sensing Lines:

- Conformance: Not applicable to the N-DCIS. The N-DCIS receives signals from sensors in various systems in the plant that are from instrument sensing lines from nonsafety-related instrumentation but the N-DCIS itself does not contain instrument sensing lines.

- For details on conformance to those Regulatory Guides listed in subsection 7.1.4.4, refer to subsection 7.1.6.4.

7.1.5.3.5 Branch Technical Positions

BTP HICB-14: Guidance on Software Reviews for Digital Computer-based I&C Safety-related systems:

- Conformance: The N-DCIS conforms with the intent of this guideline as outlined in ISO 17799 for Security Management of the N-DCIS Control Network.

BTP HICB-16: Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail is commensurate with this BTP.

From the foregoing analyses, it is concluded that the N-DCIS meets its regulatory and industry design bases.

7.1.5.4 N-DCIS Testing and Inspection Requirements

The testing and inspection requirements for each system within the N-DCIS are presented as specific subsections in Chapter 7.

The N-DCIS controllers, displays, monitoring and I/O communication interfaces continuously function during normal power operation. Abnormal operation of these components can be detected. In addition, the controllers are equipped with on-line diagnostic capabilities for identifying and isolating failure of I/O signals, buses, power supplies, processors, and inter-processor communications. On-line diagnostics are performed without interrupting the normal control operation of the N-DCIS.

The N-DCIS components and critical components of interfacing systems are tested to ensure that the specified performance requirements are satisfied. Factory, construction, and preoperational testing of the N-DCIS are performed before fuel loading and startup testing to ensure that the system functions as designed and that tested system performance is within specified criteria.

7.1.5.5 N-DCIS Instrumentation and Control Requirements

7.1.5.5.1 Uninterruptible Nonsafety-Related AC Power Supply

The N-DCIS components and cabinets that are key to power generation are supplied with either dual redundant or triple redundant power supplies and power feeds. The sources of this power are three independent UPS inverters, normally supported by AC power. If off-site power fails and the diesel generators fail, the N-DCIS inverters receive power from three independent battery systems. All of these AC power feeds are well regulated and supply 120 ±10% volt AC, 60 Hz. Inverter operation. Frequency, voltages, currents, and battery and charger operation are monitored and alarmed. The N-DCIS panel is designed so that the loss of one power supply or incoming power source does not affect the N-DCIS or its functional or plant operation.

7.1.5.5.2 Lighting and Service Power System

The LSP supplies 120 VAC power to the N-DCIS for lighting and maintenance equipment. This includes internal cabinet lighting and convenience outlets.

7.1.5.6 N-DCIS Major System Interfaces

The N-DCIS has interfaces with almost all of the I&C and electrical nonsafety-related plant systems. Safety-related system information acquired by the Q-DCIS is available to N-DCIS through qualified isolation devices that are part of the Q-DCIS. System interfaces with nonsafety-related systems, or portions of systems, and systems acquiring Q-DCIS data through isolation devices/gateways/datalinks include:

- ARMS;
- Auxiliary Boiler System (ABS);
- C&FS;
- Chilled Water System;
- CIRC;
- Condensate Storage and Transfer System;
- Containment Inerting System;
- CMS;
- CB HVAC;
- CPS;
- CRD;
- Direct Current Power Supply;
- DPS;
- Drywell Cooling System;
- Electrical Power Distribution System (EPDS);
- Electric Equipment Building HVAC;
- Equipment and Floor Drain System;
- Extraction System;
- FAPCS;
- FPS;
- Flammability Control System;
- Fuel Building HVAC;
- Fuel Transfer System (FTS);
- FWCS;
- GDCS;
- Generator;
- Generator Lube and Seal Oil System (GLSOS);
- Heater Drain and Vent System (HDVS);

- High Pressure Nitrogen Supply System (HPNSS);
- Hydrogen Gas Control System (HGCS);
- Hydrogen Water Chemistry;
- Instrument Air System (IAS);
- ICS;
- I&C Power Supply;
- LD&IS;
- Lighting and Servicing Power Supply;
- Liquid Waste Management System (LWMS);
- Low Voltage Distribution System;
- Main Condenser and Auxiliaries;
- Main Turbine;
- Makeup Water System;
- Medium Voltage Distribution System;
- Meteorological Observation Station;
- MSR;
- NBS;
- NMS;
- Offgas System (OGS);
- Oil Storage and Transfer System;
- Oxygen Injection System (OIS);
- PAS;
- PCCS;
- PSWS;
- Process Sampling System (PSS);
- The Q-DCIS;
- Radwaste Building HVAC;
- RC&IS;

- RB HVAC;
- RCCWS;
- RWCU/SDC;
- RPMS;
- RPS;
- RSS;
- The SB&PCS;
- Service Air System (SAS);
- Service Building HVAC;
- Service Water Building HVAC;
- SLC;
- Solid Waste Management System;
- SSLC/ESF;
- Standby On-Site AC Power Supply;
- Stator Cooling Water System (SCWS);
- Turbine Auxiliary Steam System (TASS);
- Turbine Building Cooling Water System;
- Turbine Building HVAC;
- Turbine Bypass System (TBS);
- TGCS;
- Turbine Gland Seal System;
- Turbine Lube Oil System (TLOS);
- Turbine Main Steam System (TMSS);
- Uninterruptible AC Power Supply:
- Yard Miscellaneous Drain System; and
- Zinc Injection System (ZNI), an optional system.

7.1.6 General DCIS Conformance with Regulatory Requirements and Industry Codes and Standards

NUREG 0800, Table 7.1 lists the Code of Federal Regulations, GDC, SRM, RGs, and Instrumentation and Controls Branch Memoranda (HICB) that provide acceptance criteria or guidelines for each subsection of Chapter 7.

The specific regulatory acceptance criteria and guideline requirements applicable to each of these systems (safety-related or nonsafety-related but significant for plant operation) identified in the SRP are identified and tabulated in Table 7.1-1. The regulatory requirements applicability matrix for Table 7.1-1 is followed in Sections 7.2 through 7.8 by a regulatory conformance discussion for each specific system. The degree of applicability and conformance, along with any clarifications or justification for exceptions, are presented in the evaluation sections for each specific system. General Q-DCIS and N-DCIS conformance is discussed in the following subsections.

7.1.6.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety.10 CFR 50.55a(h) Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: The Q-DCIS complies with the above requirements.

10 CFR 50.34(f), Conformance with Three Mile Island (TMI) Action Plan Requirements:

- Response to TMI related matters is generally addressed in Chapter 1, Appendix 1A. TMI action plan requirements are identified for the systems in Table 7.1-1. The applicable systems are generally designed to conform. However, because of the design features, several of these requirements are not applicable. These are identified as follows:
  - II.K.3.13 – HPCI and RCIC Initiation Levels,
  - II.K.3.15 - Isolation of HPCI and RCIC (Turbine Driven),
  - II.K.3.21 - Automatic Restart of LPCS and LPCI, and
  - II.K.3.22 - RCIC Automatic Switchover of Suction Supply.

The TMI action items applicable to the I&C systems are:

- 10 CFR 50.34(f)(2)(v) [I.D.3], Bypass and Inoperable Status Indication,
- 10 CFR 50.34(f)(2)(xvii) [II.F.1], Accident Monitoring Instrumentation,
- 10 CFR 50.34(f)(2)(xviii) [II.F.2], Inadequate Core Cooling Instrumentation,
- 10 CFR 50.34(f)(2)(xiv) [II.E.4.2], Containment Isolation Systems,
- 10 CFR 50.34(f)(2)(xix) [II.F.3], Instruments for Monitoring Plant Conditions Following Core Damage,
- 10 CFR 50.34(f)(2)(xxiv) [II.K.3.23], Central Reactor Vessel Water Level Recording,

10 CFR 50.62 (ATWS)

- Conformance: The design has ATWS mitigation functions, as described in Section 7.8.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements

- Conformance: There are no interface requirements for this section

10 CFR 52.47(a)(2), Level of Detail

- Conformance: The level of detail provided for the RPS within the DCD conforms with this regulation.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.1.6.2 General Design Criteria

In accordance with Table 7.1-1, the following GDC are addressed for the Q-DCIS:

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 25, and 29.

- Conformance: The Q-DCIS is in compliance with these GDC. Specific conformance of the I&C systems themselves is addressed in Sections 7.2 through 7.8.

7.1.6.3 Staff Requirements Memorandum

SRM to SECY 93-087 II.Q (Defense Against Common-Mode Failures):

- The digital I&C is designed with defense-in-depth and diversity for defense against common-mode failures. Section 7.8 includes the description of the diverse I&C systems that specifically addresses the requirements of this SRM.

SRM to SECY 93-087 II.T (Control Room Annunciator/Alarm Reliability):

- The AMS follows guidance in the above document for redundancy, independence, and separation because the "alarm system" is considered redundant. Alarm points are sent through dual networks to redundant message processors on dual power supplies. The processors are dedicated and only do alarm processing. The alarms are displayed on multiple independent VDUs that each have dual power supplies. The alarm tiles, or their equivalent, are driven by redundant data links (dual power). There are redundant alarm

processors. There are no alarms that require manually controlled actions for safety-related systems to accomplish their function. Thus the requirements for safety-related equipment and circuits are not applicable.

7.1.6.4 Regulatory Guides

A discussion of the general conformance of the I&C equipment with RGs is provided below.

RG 1.22 - Periodic Testing of Protection System Actuation Functions. Safety-related systems have provision for periodic testing. Proper functioning of analog sensors is verified by channel cross-comparison and is done continuously by the PCFs. Some actuators and digital sensors, because of their locations, cannot be fully tested during actual reactor operation. Such equipment is identified and provisions for meeting the guidance of Paragraph D.4 (per BTP HICB-8) are discussed in the Safety Evaluation subsections within Sections 7.2 through 7.8.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems. Bypass indications are designed to satisfy the guidance of IEEE Std. 603, Paragraph 5.8.3, and RG 1.47. The design of the bypass indications allows testing during normal operation and is used to supplement administrative procedures by providing indications of safety-related systems status.

Bypass indications use isolation devices that preclude the possibility of any adverse electrical effect of the bypass indication circuits on the plant safety-related system.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems. The safety-related system designs conform with the single failure criterion; additionally the design meets N-2 conditions.

RG 1.62 - Manual Initiation of Protective Actions**.** Manual initiation of the protective action is provided at the system level for safety-related systems conditions.

RG 1.75 **-** Physical Independence of Electric Systems**.** The safety-related system designs conform with RG 1.75. See chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for a discussion of how the design meets the requirements of RG 1.75.

RG 1.97 - Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident. I&C is designed to meet the guidance of RG 1.97. Details of design implementation are discussed in Section 7.5.

RG 1.105 - Instrument Setpoints for safety-related Systems**.** The I&C systems are consistent with the guidance of RG 1.105. The applicable analytical or design basis limit (technical specification limit), as well as the nominal trip setpoint (instrument setpoint) and any "as-found tolerance" and, "as left tolerance" are provided in separate documentation. These parameters are appropriately separated from each other based on instrument accuracy, calibration capability and design drift (estimated) allowance data. The setpoints are within the instrument best-accuracy range. The established setpoints provide margin to satisfy safety-related requirements and plant availability objectives.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems. The I&C systems are consistent with the guidance of RG 1.118.

RG 1.151 - Instrument Sensing Lines. The instrument sensing lines are designed to satisfy the guidance of RG 1.151. These lines are used to perform safety-related and nonsafety-related functions. There are four redundant, separate sets of instrument lines, each having safety-related instruments associated with one of the four electrical safety-related divisions. The RPS logic requires any two-out-of-four signals to Scram. If a channel is bypassed, the logic is two-out-of-three. Also, emergency core cooling functions are redundant throughout the four divisions and the feedwater system is designed with fault-tolerant triple digital controllers that use sensors separate from the safety-related sensors. Therefore, the systems are designed so that no single failure or two-division failure can cause an event and at the same time, the systems prevent mitigating action for the event.

RG 1.152 - Computer Software Used in Safety-related Systems. Criteria and guidelines stated in this Regulatory Guide are a basis for design procedures established for programmable digital equipment. As the principal RG for digital computers in safety-related systems in nuclear power plants, it endorses and refers to IEEE Std. 603 for specific criteria details. This RG also contains discussions on digital I&C equipment common mode failure issues. The concern is related to the possibility that a design error in the software in redundant channels of a safety-related system could lead to common-cause or common-mode failure of the safety-related system function. It is possible for conditions to exist where some form of diversity is necessary that provides additional assurance beyond that which is provided by the design and Quality Assurance (QA) programs that incorporate software QA and Verification and Validation (V&V). The design techniques of functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defense-in-depth can be applied as defense against common-cause failures. The justification for equipment diversity, or for the diversity of related system software such as a real-time operation system, must extend to equipment components to ensure that actual diversity exists. Claims for diversity based on different manufacturers are insufficient without consideration of the above. Other considerations such as functional and signal diversity, that lead to different software requirements form a stronger basis for diversity. The following sections are noted in IEEE Std. 7-4.3.2 as specifically addressed by the NRC in RG 1.152:

- The main text portions of IEEE Std. 7-4.3.2 are similar to the 1993 version, with more extensive requirements incorporated for software development, V&V, software configuration management, equipment qualification, self-diagnostics, independence, and reliability. There is no specific detail on diverse method requirements.

- Annex B "Diversity Requirements Determination“ is essentially unchanged from the 1993 version. This annex provides a methodology for determining the need for diversity. RG 1.152 does not endorse Annex B.

- Annex C "Dedication of existing commercial computers" is similar to the 1993 version.

- Annex E, "Communication Independence" is similar to the annex in the 1993 version. The NRC does not endorse Annex E.

- Annex F, "Computer reliability": This is similar to the annex in 1993 version. The NRC states that quantitative reliability goals are not the only means, and does not endorse this method as the sole means of meeting the regulations for reliability of digital computers. The NRC acceptance is based on deterministic criteria.

- Safety I&C System compliance with IEEE Std. 7-4.3.2

Additionally RG 1.152 also includes guidance applicable to the Q-DCIS. Compliance is summarized as follows:

Defense against software common mode failures: GEH has evaluated BTP-HICB-19 guidelines including the acceptance criteria on defense-in-depth and diversity and defense against common mode failures, on the four echelons of defense against common-mode failures. The four echelons are control systems, reactor trip system, Engineered Safety Features Actuation System (ESFAS), and monitoring and indicator functions. To fully address the guidelines of BTP HICB-19 on defense-in-depth and diversity and defense against common mode failures, the DPS backs up the primary safety-related I&C system protection functions. The DPS is implemented with hardware and software that is totally separate and independent from the primary safety-related I&C protection systems (RPS and SSLC/ESF). The DPS is implemented in addition to the ATWS/SLC system function. A detailed description of the DPS and the description of defense-in-depth and diversity and defense against common mode failure are included in Section 7.8.

Software development process: The software development process of the Q-DCIS (including control systems key for plant operation) follows the guidelines of BTP HICB-14. Software development process plans for the DCIS design implementation include the Software Management Plan (SMP), Software Development Plan (SDP), Software Verification and Validation Plan (SVVP), Software Configuration Management Plan (SCMP), Software Safety Plan (SSP), as required by guidance in BTP HICB-14 and are described in References 7.1-10 and 7.1-12. Actual detailed hardware and software design implementation follows the guidelines specified by these plans as part of the Design Acceptance Criteria (DAC) process.

Equipment qualification, self-diagnostics, independence, and reliability: IEEE Std. 603 states that these requirements are applicable to safety-related I&C system equipment. The Q-DCIS meets the requirements of IEEE Std. 603, and the above requirements in areas applicable to digital computer-based equipment.

Security: The security guidelines included in RG 1.152 are evaluated and incorporated as appropriate and necessary in the DCIS design, both on plant hardware security measures and software security measures. The software development process plans are developed with the security requirements incorporated for actual detailed design implementation.

RG 1.153 - Criteria for Safety Systems. Safety-related systems are designed to satisfy the requirements of IEEE Std. 603, as endorsed by RG 1.153.

RG 1.168 - Verification, Validation, Reviews, and Audits For Digital Computer Software Used In Safety Systems of Nuclear Power Plants: This RG endorses IEEE Std. 1012, IEEE Standard for SVVPs, and IEEE Std. 1028, IEEE Standard for Software Reviews and Audits. IEEE Std. 1012 is acceptable for providing high functional reliability and design quality in software used in safety-related systems. IEEE Std. 1028 is acceptable for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions. Safety-related systems use the guidance in these standards, as discussed in Reference 7.1-10, to develop portions of the overall SDP and thus comply with this RG.

RG 1.169 - Configuration Management Plans For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants: This RG endorses IEEE Std. 828, IEEE Standard for SCMPs, and ANSI/IEEE Std. 1042, IEEE Guide to Software Configuration Management. These standards, with the clarifications provided in the Regulatory Position, describe acceptable methods for providing high functional reliability and design quality in software used in safety-related systems. Safety-related systems use the guidance in these standards, as discussed in Reference 7.1-10, to develop portions of the overall SDP and thus comply with this RG.

RG 1.170 - Software Test Documentation For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants: The guidance contained in IEEE Std. 829, IEEE Standard for Software Test Documentation, provides an acceptable approach for meeting the requirements of 10 CFR Part 50 as they apply to the test documentation of safety-related system software subject to the provisions in this guide. Safety-related systems use the guidance in these standards to develop portions of the overall SDP and thus comply with this RG.

RG 1.171 - Software Unit Testing For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants: This RG endorses IEEE Std. 1008, IEEE Standard for Software Unit Testing, subject to the provisions in this guide. This standard defines an acceptable method for planning, preparing for, conducting, and evaluating software unit testing. Safety-related systems use the guidance in this standard to develop, as discussed in Reference 7.1-10, portions of the overall SDP and, thus, comply with this RG.

RG 1.172 - Software Requirements Specifications For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants: This RG endorses IEEE Std. 830, Recommended Practice for Software Requirements Specifications, as amended in the Regulatory Position. This standard describes current practices for writing software requirements specifications for a wide variety of systems. It is not specifically aimed at safety-related applications; however, it does provide guidance on the development of software requirements specifications that exhibit characteristics important for developing safety-related system software. This is consistent with the goal of ensuring high-integrity software in reactor safety-related systems. Safety-related systems use the guidance in this standard, as described in the References 7.1-10 and 7.1-12, to develop portions of the overall software development plan and thus comply with this RG.

RG 1.173 - Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants: This RG endorses IEEE Std. 1074. The standard describes, in terms of inputs, development, verification or control processes, and outputs, a set of processes and constituent activities that are commonly accepted as composing a controlled and well-coordinated software development process. It describes inter-relationships among activities by defining the source activities that produce the inputs and the destination activities that receive the outputs. The standard specifies activities that must be performed and their inter-relationships; it does not specify complete acceptance criteria for determining whether the activities themselves are properly designed. Therefore, the standard should be used in conjunction with guidance from other appropriate RGs, standards, and software engineering literature. Safety-related systems use the guidance in this standard, as described in References 7.1-10 and 7.1-12, to develop portions of the overall SDP and thus comply with this RG.

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems: Electrical and electronic components in the I&C safety-related

systems are qualified for anticipated levels of EMI at their as-installed locations. EMC of I&C equipment is verified through factory testing and site-specific testing for both individual equipment and interconnected systems to meet EMC requirements for protection against the following:

- EMI,
- RFI,
- Electrostatic Discharge, and
- Electrical Surge.

EMI qualifications follow the requirements defined in Mil Std. 461E and IEC 61000-4. Q-DCIS equipment is qualified to perform continuously within specified ranges even when exposed to EMI environmental limits at the hardware mounting location. To that end, EMI qualifications for safety-related systems meet the proposed requirements of RG 1.180, Rev 1 "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems."

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants: The surge withstanding capability of the safety-related I&C design conforms with IEEE Std. 1050. See Subsection 8A.1.2 for detailed information about conformance with RG 1.204 and the lightning protection system.

7.1.6.5 Branch Technical Positions

BTPs that are applicable to the I&C systems are identified relative to the I&C systems in Table 7.1-1. BTPs are guidance documents; the I&C systems are generally designed to conform with the BTPs. The degree of conformance, along with any clarifications or exceptions, is discussed in the safety evaluation subsections of Sections 7.1 through 7.8.

BTP HICB-1: Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System.

For details see subsection 7.3.1.2.3.5.

BTP HICB-8: Guidance on Application of RG 1.22. The Q-DCIS is fully functional during reactor operation and is tested in conjunction with the SSLC/ESF. Therefore, the Q-DCIS meets this BTP.

BTP HICB-9: Guidance on Requirements for RPS Anticipatory Trips.

The Q-DCIS conforms with this BTP.

BTP HICB-10: Guidance on Application of Regulatory Guide 1.97. I&C is designed to meet the guidance of HICB-10. Details of design implementation are discussed in Section 7.5.

BTP HICB-11: Guidance on Application and Qualification of Isolation Devices. The Q-DCIS conforms with this BTP.

BTP HICB-12: Guidance on Establishing and Maintaining Instrument Setpoints. The Q-DCIS conforms with this BTP.

BTP HICB-14: Guidance on Software Reviews for Digital Computer-based I&C Safety Systems. Refer to Subsections 7.1.2.4, Reference 7.1-10 and 7.1-12 discussions. The Q-DCIS conforms with the guidance of this BTP.

The Q-DCIS and N-DCIS follow a development process that is in accordance with BTP HICB-14. As part of the Certification activity, the software development process plans require NRC review and approval.

Safety-related I&C systems (RPS and SSLC/ESF) use computers for their logic functions. A description of the Q-DCIS design, together with the description of the DPS is included in Section 7.8, and specifically addresses the issues of defense-in-depth and diversity and defense against common mode failures.

BTP HICB-16: Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52. This BTP is applicable to all sections of the Design Control Document.

BTP HICB-16 states that the application should do the following:

- Describe the resolution of unresolved and generic safety issues applicable to the I&C systems,
- Describe the interface requirements to be met by portions of the plant for which the application does not seek certification and which are necessary to ensure proper functioning of the I&C system;
- Identify and describe the validation of innovative means of accomplishing I&C system safety-related functions.

Applications that propose the use of computers for systems with safety-related uses should describe the computer system development process. Applications that propose the use of computers for RTS and ESFAS functions should also describe the design of the overall I&C systems with respect to defense-in-depth and diversity requirements.

The I&C design has no unresolved or generic safety-related issues applicable to I&C systems. In Section 1.11, unresolved and generic safety-related issues are discussed. There are several new generic issues that are related to I&C systems, such as failure of protective devices on safety-related equipment, electromagnetic pulse, identification of protection system instrument sensing lines, and protection system testability. These issues either are not applicable to safety-related I&C systems or are addressed by the safety-related I&C design. Within the scope of the DCD submitted for certification application, there are no interface requirements described here that fall into this category.

The design uses the voluminous data available from operating plants and from the testing and licensing efforts performed to license the predecessor designs and individual plants. The I&C design does not use innovative means for accomplishing safety functions.

BTP HICB-17: Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based I&C Systems. Refer to Subsection 7.2.1.3.5 and 7.3.4.3 discussions. The Q-DCIS conforms with this BTP.

BTP HICB-18: Guidance on Use of Programmable Logic Controllers in Digital Computer-based I&C System. The Q-DCIS conforms with this BTP.

BTP HICB-19: Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (Item II.Q of SECY-93-087). The Q-DCIS conforms with this BTP.

BTP HICB-21: Guidance on Evaluation of Digital System Architecture and Real-Time Performance. The Q-DCIS conforms with this BTP.

7.1.6.6 Industry Standards

The safety evaluation subsections throughout Chapter 7 address the RGs are identified by the SRP. The IEEE standards that are endorsed by RGs are not addressed separately.

Some codes or standards that are not mentioned in the SRP are used in specific system applications. These are identified in the system description and the corresponding reference section. Some IEEE standards applicable to the I&C equipment are addressed in other chapters in accordance with the SRP format. These are identified as follows:

IEC 61000-4 – The design conforms to this series of standards.

IEEE Std. 323 – "Qualifying safety-related Equipment for Nuclear Power Generating Stations". Safety-related systems are designed to meet the requirements of IEEE Std. 323. Environmental qualification is addressed in Section 3.11.

IEEE Std. 344 – "Recommended Practices for Seismic Qualification of Safety-related Equipment for Nuclear Power Generating Stations". Safety-related I&C equipment is classified as Seismic Category I and designed to withstand the effects of the Safe Shutdown Earthquake (SSE). It remains functional during normal and accident conditions. Qualification and documentation procedures used for Seismic Category I equipment and systems satisfy the provisions of IEEE Std. 344 as indicated in Section 3.10.

IEEE Std. 383 – "IEEE Standard for Type Test of Safety-related Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations." Electric cable conforms with this standard. Fiber optic cable insulation/covering/jacketing also conforms with the requirements for flame tests in this standard.

IEEE Std. 384 – "IEEE Standard Criteria for Independence of Safety-related Equipment and Circuits". See the discussion of RG 1.75 in Subsection 7.1.6.4. IEEE Std. 497 – "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations." Accident monitoring instrumentation is discussed in Section 7.5.

IEEE Std. 518 – "IEEE Guide for the Installation of Electrical Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources". The design conforms to this standard.

IEEE Std. 603 – "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations". Conformance with this standard is discussed in Subsection 7.1.6.6.1.

IEEE Std. 1050 – "IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations". The design conforms to this standard.

7.1.6.6.1 IEEE Std. 603 – IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

The scope of IEEE Std. 603 includes safety-related I&C systems and is described in Sections 7.1 through 7.8. IEEE Std. 603 does not directly apply to nonsafety-related systems, other than to require independence between nonsafety-related systems and safety-related systems. For convenience, some of these requirements may also be adopted as design bases for some nonsafety-related I&C components and systems such as for accident monitoring instrumentation, in accordance with RG 1.97. Conformance with the requirements of IEEE Std. 603 is also identified as conformance with the requirements and guidance contained within the federal regulations GDC, SRM, and RGs, as described throughout Section 7.1. The safety-related I&C design comprises the Q-DCIS, RPS, NMS, and SSLC/ESF. The design conforms with IEEE Std. 603. ITAACs are provided for the major attributes for compliance with IEEE Std. 603 and are not intended to limit the scope of compliance.

7.1.6.6.1.1 Safety System Designation (IEEE Std. 603, Section 4, et al)

IEEE Std. 603, Section 4, requires that a specific basis be established for the design of each safety-related system. The DBEs applicable to the safety-related control systems are shown in Table 15.0-2. DBEs comprise Anticipated Operational Occurrences (AOO), infrequent events, accidents, and special events. The plant operating conditions applicable to each DBE are shown in Tables 15.1-2 and 15.1-3. The safety-related analysis acceptance criteria for the AOOs, infrequent events, and accidents are shown in Tables 15.0-3, 15.0-4, 15.0-5, and 15.0-6. Special events are evaluated in Subsections 15.5.1 through 15.5.7. Credited systems, interlocks, and functions for each DBE are described in Sections 15.2, 15.3, 15.4, and 15.5. Additional details about the specific safety-related or nonsafety-related interfacing system design bases, interlocks, and functions are found in Sections 4.6, 5.2, 5.4, 6.2, 6.3, 8.3, 9.1, 9.3, 9.4, 10.2, 10.3, and 10.4. Information provided for each design basis item enables the detailed design of the system to be carried out. Safety-related system design basis descriptions are included in the various sections of this chapter as indicated below.

- Reactor Trip System:
  - RPS (Subsection 7.2.1) and
  - NMS (Subsection 7.2.2).
- Suppression Pool Temperature Monitoring (Subsection 7.2.3)
- ESF
  - ECCS (Subsection 7.3.1),

  - ADS (Subsection 7.3.1.1),
  - GDCS (Subsection 7.3.1.2),
  - PCCS (Subsection 7.3.2),
  - LD&IS (Subsection 7.3.3),
  - CR Habitability (Subsection 7.3.4), and
  - SSLC/ESF (Subsection 7.3.5).
- SLC (Subsection 7.4.1)
- RSS (Subsection 7.4.2)
- RWCU/SDC (Subsection 7.4.3)
- ICS (Subsection 7.4.4)
- CMS (Subsection 7.5.2)
- Interlock Systems (Section 7.6)

7.1.6.6.1.2 Single Failure Criterion (IEEE Std. 603, 5.1)

The safety-related control systems include sufficient redundancy, diversity, and independence to meet system performance requirements if the system is degraded by any single credible failure. In the RPS logic controller (reactor and SSLC/ESF), two-out-of-four redundancy and trip logic prevent a single failure from inhibiting a scram or reactor core cooling safety-related function. They also prevent a single failure from causing either an inadvertent reactor trip or an emergency core cooling action. Redundancy begins with the sensors monitoring the variables and continues through the signal processing, output devices, and actuators. More than one diverse sensor and control system initiates most protective actions. No single failure or two division failure within the safety-related system causes an AOO to degrade to an Infrequent Event or an Infrequent Event to degrade to an Accident.

Communication between redundant divisions or between safety-related control systems and nonsafety-related control systems is electrically isolated and one-way. Communication is typically by optical couplers and fiber optic cabling.

Each division is sufficiently independent from the other divisions so that no one division is dependent on information, timing data, or communication from any other division to initiate a safety-related trip signal. The failure of a single division does not prevent the initiation of a safety-related trip. Each safety-related logic controller evaluates the data from its own division's sensors and continuously broadcasts the result of its evaluation to the other divisions as either a "trip" or "no trip" signal.

A safety-related trip is initiated whenever any two working divisions sense conditions that require a safety-related trip. Each division receives input data from its own set of diverse and/or redundant sensors connected to the same process source and separately transmits trip signals to

the other divisions. The trip actuators go to their trip state whenever they receive concurrent, like parameter trip signals from any two safety-related logic controller transmissions. The two-out-of-four voting logic treats the absence of an interdivisional trip signal as a signal. The signal isolators are qualified to withstand all credible faults, such as short circuits or high voltage, so that faults cannot propagate and degrade the performance of any safety-related control function.

Reference 7.1-4 describes the type of diversity that exists among the four echelons of defense-in-depth and identifies the dependency, redundancy, and independence among the echelons.

An analysis of the redundancy and independence of the safety-related protection systems and a block level Failure Mode and Effects Analysis (FMEA) is performed of the complete safety-related reactor protection, ESF, and DPS designs. In addition, the platform specific LTRs for the safety-related system architectures include analysis summaries of the architecture's conformance with the requirements of IEEE Std. 603.

7.1.6.6.1.3 Completion of Protective Action (IEEE Std. 603, Sections 5.2 and 7.3)

After initiation by either automatic or manual means, the protective actions go to completion in conformance with IEEE Std. 603, Section 5.2. They go to completion by using one of the following: seal-in logic, non-resettable squib valves, manually reset valves, diverse functions, or a combination of logic, valves and functions. Deliberate operator action is required to return the safety-related systems to normal. Control rod insertion is performed hydraulically if there is loss of power to both scram pilot valve solenoids, the three scram air header dump valves, or both pairs of ARI solenoid valves. The loss of power mode is latched at the load drivers by seal-in logic or by a maintained-open switch. The FMCRD mechanism provides a diverse means to hold the control rods in the fully inserted position if the loss of power signal is maintained long enough to allow the FMCRD to reach the fully inserted position. Specific descriptions are included in Subsection 7.2.1.1 and in other subsections as shown in Table 7.1-2.

7.1.6.6.1.4 Quality (IEEE Std. 603, 5.3)

All equipment is provided under the GEH 10 CFR 50, Appendix B quality assurance program. The NRC accepted GEH Quality Assurance Program with its implementing procedures, constitutes the Quality Assurance system that is applied to the Q-DCIS design. It satisfies all applicable requirements of the following: 1) 10 CFR 50 Appendix B; 2) ANSI/ASME NQA-1; and 3) ISO 9001. ESBWR safety-related I&C systems employing digital computers, software, firmware, and software tools conform with the quality requirements described in IEEE Std. 7-4.3.2 as described in the software plans described in LTR, "ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan," NEDO-33217 (Reference 7.1-13). Software tools used to support software development processes and verification and validation (V&V) processes are controlled under a configuration management program. The software tool configuration management process ensures that software tools are part of a test tool validation process. The software test tool validation process confirms by one or both of the following methods that software tools are suitable for use:

- Software tools are subjected to a test tool validation program.

- Software tools are used in a manner such that defects not detected by the software tool are detected by V&V activities.

7.1.6.6.1.5 Equipment Qualification (IEEE Std. 603, Section 5.4)

It is required that safety-related equipment be designed to meet the safety-related functional performance requirements over the range of normal, abnormal, and Design Basis Accident environmental conditions for the area in which it is located. Equipment qualification typically includes EMI qualification, seismic qualification, and other environmental condition qualification such as temperature, humidity, radiation, and pressure. The Q-DCIS systems are designed to meet the equipment qualification requirements set forth in 10 CFR 50.49, RG 1.209, RG 1.89, RG 1.100, IEEE Std. 603 IEEE Std. 323, and IEEE Std. 344. The qualification is established using qualification methods set forth in "General Electric Environmental Qualification Program", NEDE-24326-1-P (Reference 7.1-2). The Q-DCIS components are designed to be qualified to operate in the normal, abnormal, and DBA environments in which they are located.

For environmental qualification, the following areas are addressed:

Temperature and Humidity: The Q-DCIS components are designed to be qualified using type testing as preferred method and analysis to demonstrate that the components perform all specified functions correctly when operated within the specified temperature range and relative humidity range. Pressure: The Q-DCIS components are designed to be qualified (by analysis) to perform safety-related functions for any absolute pressure in the range specified.

Radiation: The Q-DCIS components are designed to be qualified (by analysis) to perform safety-related functions over their service life under the specified radiation conditions. The design ensures that the maximum radiation levels at the equipment locations do not exceed the allowed limits.

Seismic Qualification: The Q-DCIS components are designed to be qualified, by type testing and analysis, to perform safety-related functions correctly when operated within the specified seismic limits, and when mounted in accordance with the specified methods. The Q-DCIS components are qualified in accordance with the requirements of RG 1.100 (IEEE Std. 344). The design ensures that the maximum seismic accelerations at the mounting locations of the equipment do not exceed the allowed limits.

EMI Qualification: The Q-DCIS components are designed to be qualified by type testing and analysis to perform all safety-related functions when operated within the specified EMI limits. The Q-DCIS components are qualified in conformance with RG 1.180, when mounted in accordance with the specified methods. The Q-DCIS equipment is designed to not be susceptible to electromagnetic disturbances from neighboring modules or cause electromagnetic disturbances to neighboring modules. The EMI qualification design follows the requirements specified in Mil Std. 461E and IEC 61000-4, depending on the specific requirement conditions. The Q-DCIS equipment is qualified to perform within its specifications continuously while exposed to EMI environmental limits at the hardware mounting location. The EMI susceptibility and emissions testing is performed by type testing. In addition to the equipment design

considerations, plant-specific actions are required to establish practices to control emission sources, maintain good grounding practices, and maintain equipment and cable separation.

7.1.6.6.1.6 System Integrity (IEEE Std. 603, Section 5.5)

The Q-DCIS systems are required to accomplish their safety-related functions under the full range of applicable conditions enumerated in the design bases. Other areas addressed as requirements include adequate system real-time performance for digital computer-based systems to ensure completion of protective action, evaluation of hardware integrity and software integrity (software safety-related analysis, as part of BTP HICB-14 requirements), failure to a safe state upon loss of energy or adverse environmental conditions, and the requirements for manual reset.

The Q-DCIS meets the integrity requirements described in IEEE Std. 603, Section 5.5. The RPS functions fail in the tripped state. The SSLC/ESF fails to a state where the actuated component remains "as-is" to prevent a control system induced LOCA. Hardware and software failures detected by self-diagnostics cause a trip signal to be generated in the division in which the failure occurs in RPS and no signal is generated if the failure occurs in a SSLC/ESF division. Failure of hardware and software does not inhibit manual initiation of protective functions. More details of system integrity design considerations are included in the system description subsections of the respective safety-related systems as outlined in Table 7.1-2.

7.1.6.6.1.7 Independence (IEEE Std. 603, Section 5.6)

The independence requirements address the independence between redundant portions of a safety-related system, between safety-related systems and the effects of DBEs, and between safety-related systems and other systems. Three aspects of independence are addressed in each case: physical independence, electrical independence, and communication independence. Q-DCIS meets these requirements.

The Q-DCIS systems have four redundant and independent channels (divisions) that are physically independent and separated and that have independent electrical power sources applied to each channel. Unless fiber optic cable is used, there are no common switches shared by the four channels. The sensors used for each of the four channels, are independent and physically separated from one another. Communication directly between the four channels is limited to the minimum, such as channel trip signals and bypass status signals, and is through proper isolation devices, such as qualified CIMs and fiber optic cables.

Independence between the safety-related systems and the effects of DBEs is achieved through proper equipment qualification. Safety-related equipment is qualified for continuous functional capability in the environment at the equipment location, for which DBE conditions are considered. Safety-related systems are totally separated and independent from nonsafety-related systems.

Communication from safety-related systems to nonsafety-related systems is carried out with proper signal isolation devices, such as CIMs and fiber optic cable wired network, and data path gateway. Communication from nonsafety-related systems to safety-related systems is prohibited, with one exception. LPRM calibration gain adjustment factors, which are calculated in the nonsafety-related plant computer function of the N-DCIS, are transmitted to the safety-related

LPRM/APRM equipment using proper signal isolation. However, this data transmission can only be implemented and accepted by the safety-related equipment with the operator's acknowledgment for further detail on this communication and transmission of time synchronization signals see subsection 7.1.3.3. The RPS and SSLC/ESF protection functions have priority over data transmissions, so that data transmissions do not interfere with the RPS or SSLC/ESF protection functions. More details of safety-related system independence design are included in the system description subsections of the respective safety-related systems as outlined in Table 7.1-2.

7.1.6.6.1.8 Capability for Testing and Calibration (IEEE Std. 603, Section 5.7)

The capability for testing and calibration of safety-related system equipment is provided during power operation and duplicates the performance of the safety-related function as closely as practicable, as discussed in Sections 7.2 through 7.8. Tests can be performed in overlapping segments when testing one safety-related function. Maintenance bypasses of individual functions are provided in the safety-related system channels when it is not practical to perform a test during power operation without the bypasses. For example, the safety-related functions of each safety-related channel can be tested on-line with the tested channel bypassed from the two-out-of-four voting trip logic. The I&C equipment has built-in self-diagnostic functions to identify critical failures such as loss of power and data errors. The Q-DCIS meets the requirements outlined in this section. More details of system testing and calibration are included in the system description subsections of the respective safety-related systems as outlined in Table 7.1-2.

7.1.6.6.1.9 Information Displays (IEEE Std. 603, Section 5.8)

The information display design is part of the HFE design process described in Chapter 18. This process includes the steps to ensure compliance with regulatory requirements. It also includes guidance offered in RG 1.47 for bypassed and inoperable status indication and in RG 1.97 for accident monitoring instruments as discussed in Section 7.5.

Displays for manually controlled actions: Type A variables provide the primary information required for the control room operators to take the specified manual actions safety-related systems during DBEs, and there is not an automatic control. Additional discussion on this subject is included in Subsection 7.5.1.

System Status Indication: The safety-related and nonsafety-related I&C systems are provided with system status information that meets the requirements of IEEE Std. 603, Section 5.8. All pertinent system trip/logic status, parameter data values, equipment functional status and ESF actuator status are displayed to the operator upon request. For safety-related systems, this information is available for each division/channel. Certain information, key to plant operation and status monitoring, is permanently displayed on the large WDP in the MCR. Alarm and annunciation indications are also available in the MCR in accordance with system design requirements. Other than the post-accident safety-related display, the system status information is not safety-related.

Indication of Bypasses: For safety-related system protection functions, bypass status is continuously displayed to the operator. Bypass status information is available to be displayed in

accordance with system design requirements; certain bypass information is accompanied with an alarm. More details of system bypass and alarm conditions are included in the system description subsections of the respective safety-related systems as outlined in Table 7.1-2.

Location of Display: The locations of displays in the MCR are either on the main control console or on the large WDP visible and accessible to the operator. The man machine interface system design (man machine interface) includes design requirements and specifications on the classification of locations of various displays in the MCR. More detailed descriptions of requirements for the location of displays are included in Chapter 18 and its associated references.

7.1.6.6.1.10 Control of Access (IEEE Std. 603, Section 5.9)

There are several ways to implement access control to plant I&C equipment, particularly safety-related systems. Administrative control is used to implement access control so that qualified plant personnel are allowed to have access to keys to doors, cabinets, and keylock switches and passwords to obtain access to safety-related systems and equipment. Only qualified plant personnel are allowed to exercise operations such as change of setpoints, instrument calibration, equipment testing, and logic bypass operation. Only qualified plant personnel are allowed to access other plant operation switches. Keys, passwords, and other security devices (per the guidance of RG 1.152) are used by qualified plant personnel to enter specific rooms; open specific equipment cabinets; obtain permission to enter specific electronic instruments for calibration, testing, and setpoint changes; gain access to safety-related system software and data, and so forth. However, software of safety-related systems is typically not changeable at the plant site.

The safety-related and nonsafety-related DCIS cabinets have alarms in the MCR indicating that a cabinet door is open. There is no access to safety-related system equipment and control through the network from nonsafety-related system equipment. Computer-related access controls and authorization are part of the cyber-security program plan, which is described in the LTRs, "ESBWR Cyber Security Program Plan," NEDO-33295, (Non-Proprietary); and "ESBWR Cyber Security Program Plan," NEDE-33295-P, (Proprietary), Reference 7.1-8.

7.1.6.6.1.11 Repair (IEEE Std. 603, Section 5.10)

The Q-DCIS systems provide timely recognition of location, replacement, repair, and adjustment of malfunctioning equipment. Periodic self-diagnostic functions locate the failure to the component level. Through individual channel bypassing, the failure component is replaced or repaired on line without affecting the safety-related system protection function. During repairs the trip logic is amended from two-out-of-four to two-out-of-three. The single failure criterion is still met. Although it is not possible to bypass more than one division at a time, the Q-DCIS systems support dual divisional failures and provide all safety-related functions.

7.1.6.6.1.12 Identification (IEEE Std. 603, 5.11)

The Q-DCIS system equipment conforms with the identification requirements specified in IEEE Std. 603, Section 5.11. Color-coding is used as one of the major methods of identification. Safety-related system equipment is distinctly identified for each redundant portion of a safety-related system with identifying markings. Hardware component or equipment units have an

identification label or nameplate. For digital computer-based system equipment, versions of computer hardware, programs, and software are distinctly identified. Configuration management formalizes system component and software identification.

7.1.6.6.1.13 Auxiliary Features (IEEE Std. 603, 5.12)

Safety-related I&C system auxiliary supporting features satisfy the requirements of IEEE Std. 603, 5.12 where applicable, such as safety-related electrical system equipment including batteries, and inverters. The Q-DCIS is supported by four divisions of safety-related uninterruptible power, and by four divisions of instrument power supply. DC batteries supply power if there is a loss of off-site and on-site AC power.

HVAC, whether active or passive is a key auxiliary supporting system that maintains the necessary environmental conditions for both the safety-related and nonsafety-related I&C equipment. Under normal operating conditions when offsite power is available or when diesel generators are running, HVAC controls the temperature and humidity of all I&C equipment in all buildings. Under a loss of power condition, including Station Blackout (SBO), batteries provide continuous safety-related I&C operation for 72 hours, and continued operation of the nonsafety-related I&C equipment for two hours. However, during a loss of power active HVAC is not available to the safety-related CB or RB equipment, except the MCR habitability area as noted below. The Q-DCIS and its safety-related battery operated support equipment remain powered and the heat generated is removed passively (except possibly by small chassis mounted fans); the Q-DCIS and support equipment is qualified for the expected temperature rise. Battery-backed N-DCIS equipment is only powered for two hours if offsite and diesel generator power is lost; during that interval the same batteries supplying the N-DCIS also power nonsafety-related HVAC in the MCRA. If the nonsafety-related redundant HVAC is not available, safety-related temperature sensors with two-out-of-four logic trip the control room power that feeds the nonsafety-related I&C. The safety-related I&C that remains operable is qualified for the resulting temperature rise using passive heat removal. This scheme protects the equipment and maximizes operator comfort. Additional description of the HVAC design is included in Chapter 9.

Other auxiliary features that support the Q-DCIS functions prevent the safety-related system from degrading below an acceptable level.

7.1.6.6.1.14 Multi-Unit Stations (IEEE Std. 603, Section 5.13)

The Multi-Unit Station criteria do not apply to the standard design. The standard design submitted for NRC certification is for a single unit plant however for multiple unit designs only the N-DCIS would have common network components as necessary to control and monitor common hardware and systems. The Q-DCIS of multiple units would not have shared components nor shared divisions.

7.1.6.6.1.15 Human Factors Considerations (IEEE Std. 603, Section 5.14)

The I&C system design includes a HFE design process that is consistent with the requirements outlined in NUREG-0711, "Human Factors Engineering Program Review Model." The overall design and implementation process is described in Chapter 18. The HFE process defines a

comprehensive, iterative design approach for the development of a human-centered control and information infrastructure.

7.1.6.6.1.16 Reliability (IEEE Std. 603, Section 5.15)

The degree of redundancy, diversity, testability, and quality of the safety-related I&C design achieves the necessary functional reliability. Safety-related equipment is provided under GEH's 10 CFR 50 Appendix B quality program. The BTP-14 guidance followed for software development processes achieves reliable software design and implementation. To achieve defense against common mode failure, the design includes many defense-in-depth and diversity measures including the incorporation of the DPS described in Section 7.8. Reference 7.1-4, provides specific information on the redundancy and diversity used in safety-related I&C systems. Q-DCIS is included in the consideration of the Probabilistic Risk Assessment (PRA). (Refer to Chapter 19.)

7.1.6.6.1.17 Automatic Control (IEEE Std. 603, Sections 6.1 and 7.1)

The RPS and SSLC/ESF logic automatically initiates reactor scram trip and actuates the engineered safety features to mitigate the consequences of the AOOs and DBEs. These automatic protection actions are implemented through two-out-of-four voting logic whenever one or more process variables reach the scram or ESF actuation setpoint. Variables are monitored and measured by each of the RPS and SSLC/ESF divisions.

Plant-specific setpoint analyses evaluate whether the protection systems' precision is adequate. Instrument setpoints are determined by setpoint and safety-related analyses described in Reference 7.1-9. The GEH Setpoint Methodology uses plant-specific setpoint analyses to ensure that the characteristics of the instruments such as range, accuracy and resolution meet the performance requirements assumed for the safety-related control system components and systems of the safety-related I&C analyses in Chapter 15. The response times of the I&C systems are assumed in the safety-related analyses and verified by plant specific surveillance testing or system analyses. The Q-DCIS internal and external communication system design ensures that the real-time performance of the safety-related control systems is deterministic.

7.1.6.6.1.18 Manual Control (IEEE Std. 603, Sections 6.2 and 7.2)

Each protective action can be manually initiated at the system level, in conformance with RG 1.62, and at the division level in conformance with IEEE Std. 603, Sections 6.2 and 7.2. The manual initiation satisfies divisional rules for independence and separation. Two manual actions, each in a separate division, are required in order to satisfy the two-out-of-two system logic or the two-out-of-four division logic that initiates a reactor trip in the RPS and ESF functions of the SSLC/ESF system.

The operator can manually initiate the ESF functions by actuating manual switches in two-out-of-four divisions; thus, satisfying the two-out-of-two system initiation logic. The ESF functions that use squib valves use a redundant two-step arm and fire sequence. This prevents single failures from firing or from inhibiting the firing of the squib valves. The squib valves are the GDCS pool injection valves, the suppression pool injection valves, the GDCS deluge valves, the ADS DPV, and the SLC injection valves. To manually initiate the GDCS short-term and long-

term injection systems, a low-pressure signal must be present in the RPV. This prevents inadvertent manual initiation of the system during normal reactor operation.

The operator can manually initiate reactor emergency shutdown, reactor trip, with control rods using any of three different methods using redundant or diverse controls. The reactor trip occurs independently of the automatic trip logic and sensor status.

The two manual scram switches, the Reactor Mode Switch, and each of the four divisional manual trip switches (per protective system) are located in the MCR and are easily accessible to the operator.

The two MCR manual scram switches, the RSS manual scram switches, and the ATWS DPS manual scram switches share a minimum of equipment with the automatic controls. The MCR and RSS manual scram switches are directly connected to the power feed for the load drivers that are, in turn, connected directly to the scram pilot valve solenoids. The ATWS DPS manual scram switches are directly connected to the scram air header dump valves. An exception to RG 1.62, Regulatory Positions C.4 and C.5 is taken for the two or four divisional manual trip switches, for ADS (SRV and DPV), GDCS, ICS, and SLC manual initiation. These switches are indirectly connected to the squib valve load drivers or valve solenoids through the SSLC/ESF. The DPS manual trip switches are independently connected to the squib valve load drivers or valve solenoids, through a low reactor pressure interlock.

After manual initiation, the protective actions go to completion in conformance with IEEE Std. 603, Section 5.2 as described in Subsection 7.1.6.6.1.3. The manual initiation of a protective action performs all actions carried out by automatic initiation.

The manual controls are designed so that the information provided, display content and location are taken into consideration for easy operator access and action in the MCR. Further information about the design of manual controls and HFE considerations, as well as plant manual operation procedure requirements, are included in Chapter 18 and its associated references. Additional details of automatic and manual controls at system levels (RPS and SSLC/ESF) are included in Subsections 7.2.1 and 7.3.5.

7.1.6.6.1.19 Interaction Between the Sense and Command Features and Other Systems (IEEE Std. 603, Section 6.3)

The Q-DCIS protection systems are totally separate and independent from the nonsafety-related control systems. Any failure of nonsafety-related systems does not affect safety-related protection systems or prevent them from performing their safety-related functions. If one safety-related channel fails, any nonsafety-related control system can be isolated from the channel failure by using data validation techniques to select a valid control input from the three other remaining channels. ·The communication path broadcasts one way - from the protection system to the N-DCIS. A failure of the communication channel does not affect the protection function. The protection system does not rely on communication from the nonsafety-related channels; therefore, providing additional redundancy to isolate the protection system from communication failure is not required and not applied.

Sensors used by safety-related I&C systems are not shared with nonsafety-related control systems. Calculated safety-related signals such as APRMs can be used, after isolation, by

nonsafety-related control systems. The Q-DCIS meets the requirements of GDC 24. Additional descriptions of the Q-DCIS (RPS and SSLC/ESF) are included in Subsections 7.2.1 and 7.3.5.

The only interface from nonsafety-related systems to safety-related I&C is the data transmission of APRM and LPRM gain adjustment factor data from the plant computer system to the LPRM units. However such data transmission to the LPRM units needs operator acknowledgment for implementation, and does not interfere with the reactor protection function or ESF actuation function, for further detail on this communication and transmission of time synchronization signals see subsection 7.1.3.3.

7.1.6.6.1.20 Derivation of System Inputs (IEEE Std. 603, Section 6.4)

To the extent feasible, the protection system inputs are derived from signals that directly measure the designated process variables. The two RPS sensing inputs that are not direct measures of the variables are the RPV water level and the loss of feedwater flow in the RPS scram logics. The RPV water level is measured by the differential pressure derived from the sensing line with a reference point. This method is a proven technology in the BWR applications. The loss of the feedwater flow variable is represented by the loss of the power generation bus signal. When the power to the feedwater pump motor is lost, the feedwater flow is also immediately lost. The use of loss of power generation bus signals to represent the loss of feedwater flow signal meets the requirements of the safety-related analysis of Chapter 15, because it is the only credible way that all feedwater flow can be lost. The RPS initiating circuits and SSLC/ESF logics are described in Subsections 7.2.1 and 7.3.5.

7.1.6.6.1.21 Capability for Testing and Calibration (IEEE Std. 603, Section 6.5)

The operational availability of the protection system sensors can be checked by perturbing the monitored variables, by cross-checking between redundant channels that have a known relationship with each other and that have read-outs available, or by introducing and varying a substitute input to the sensor of the same nature as the measured variable. The four channel RPS, NMS, and SSLC/ESF logic provides at least two other valid channels for crosschecking of monitored variables. The third channel can also be available for crosschecking, depending on the maintenance bypass status. When one channel is placed into maintenance bypass mode, the condition is alarmed in the MCR and automatically causes the channel logic to be amended from a two-out-of-four voting scheme to a two-out-of-three voting scheme. Most sensors and actuators are provisioned for actual testing and calibration during power operation with the exceptions described in Sections 7.2 through 7.8.

7.1.6.6.1.22 Operating Bypasses (IEEE Std. 603, Sections 6.6 and 7.4)

Operating bypasses are implemented in the Q-DCIS. One example of such operating bypasses is associated with the trip function dependence on reactor operating mode. Requirements of IEEE Std. 603 are met by the safety-related I&C operating bypass design. Specific descriptions of safety-related system operating bypasses are included in Subsections 7.2.1.5.2.1 and 7.3.5.2. Operating bypasses are automatically removed as described in Subsections 7.2.1.5.2.1 and 7.3.5.2.

7.1.6.6.1.23 Maintenance Bypass (IEEE Std. 603, Sections 6.7 and 7.5)

Maintenance bypass capability is incorporated in the design of the Q-DCIS. This permits equipment maintenance, testing, and repair of one individual division/channel with the plant operating and without initiating any protection functions. The single failure criterion is met under this bypass condition. Although it is possible to bypass only one division at a time, the Q-DCIS design is able to supply its safety-related functions even with a two-division failure. Maintenance bypass is always alarmed or indicated in the MCR. Maintenance bypass for safety-related I&C systems is typically applied through a joystick bypass switch with exclusive logic that allows only one channel, out of four, to be bypassed at any given time. Maintenance bypasses are initiated manually by the plant operator per administrative control. Specific descriptions of safety-related system maintenance bypasses are included in Subsections 7.2.1.5.2.2 and 7.3.5.2.

7.1.6.6.1.24 Setpoints (IEEE Std. 603, Section 6.8)

Instrument setpoints are determined by setpoint and safety-related analyses using Reference 7.1-9. The GEH Setpoint Methodology uses plant-specific setpoint analyses to ensure that the instruments' range, accuracy, and resolution meet the performance requirements assumed for the safety-related control system components and systems in the safety-related analyses in Chapter 15. This methodology meets the requirements of IEEE Std. 603, Section 6.8. The response times of the I&C systems are assumed in the safety-related analyses and verified by plant specific surveillance testing or system analyses.

7.1.6.6.1.25 Electrical Power Sources (IEEE Std. 603, Section 8.1)

The Q-DCIS protection system cabinets and components are supported by two independent power sources. Each division of safety-related I&C is powered by two uninterruptible power supplies that can supply 120 VAC from either offsite power, diesel generator power, or safety-related batteries (for 72 hours). Either of the two power sources allows Q-DCIS operation. Two divisions of the uninterruptible 120 VAC are also used as the power sources for the solenoids of the scram pilot valves. Two divisions of power sources are used for the backup scram valves solenoids, for scram reset permissive logic. Specific descriptions of safety-related system power sources are included in Subsections 7.2.1.2.3 and 7.2.2.2.3, as well as in Chapter 8.

7.1.6.6.1.26 Non-electrical Power Sources (IEEE Std. 603, Section 8.2)

To perform the scram protection function, each Hydraulic Control Unit (HCU) furnishes pressurized water for the hydraulic scram, following a signal from the RPS. With low CRD HCU Accumulator Charging Pressure, the CRD system sounds an alarm in the MCR. A loss of nitrogen decreases the nitrogen pressure and actuates a pressure switch. Additionally, a float type level switch actuates an alarm if water leaks past the piston barrier and collects in the accumulator instrumentation block. An alarm is issued for low CRD charging header pressure that keeps the individual accumulators charged; if the CRD pressure decreases further the reactor is automatically scrammed while there is still pressure to do so.

The SLC system injection status is provided by the MCR indication of accumulator pressure. Operation of the accumulator nitrogen charging and makeup to accommodate small losses is

manual. MCR alarms are provided for high, low, and low-low conditions of accumulator pressure and low and low-low conditions of accumulator solution level.

7.1.6.6.1.27 Maintenance Bypass (IEEE Std. 603, Section 8.3)

The Q-DCIS components are powered by redundant, independent, and separated uninterruptible power supplies appropriate to their division with battery backup (per division) for at least 72 hours. The uninterruptible power supplies have both an automatic static transfer switch and a manual maintenance switch and either supply (per division) can operate its Q-DCIS division. Using the inverter's automatic or manual bypass and shutting down either the associated batteries, chargers or inverters technically makes the division inoperable but, in fact the division remains fully functional, only losing the ability to operate for 72 hours should offsite or diesel power be lost (it operates for approximately 36 hours under those circumstances). Operation of the Q-DCIS when one of its power supplies is in maintenance bypass is appropriately alarmed. In the very unlikely event that an entire division is without powered the fail safe RPS/NMS interprets it as a trip (unless bypassed) and the SSLC/ESF does not assume a trip. Since only two divisions are necessary to satisfy the safety requirements, no functionality is lost. An without powered division triggers an alarm. Further discussion of the safety-related power supplies is provided in Chapter 8.

7.1.6.6.1.28 Cyber Security (IEEE Std. 7-4.3.2)

The security requirements included in RG 1.152 are evaluated and incorporated in the Q-DCIS design and include plant hardware and software security measures. The software development process plans are developed with the security requirements.

The comprehensive cyber security program plan (Reference 7.1-8) identifies security risks and outlines appropriate procedures. The plant ensures that hardware, controls, and data networks comprising the control network cannot be disrupted, interrupted, or negatively affected by unauthorized users or external systems. It documents the design commitments, which meets the applicable requirements of RG 1.152, Section C.2, and Positions 2.1 through 2.9.

Inspections, tests, analyses, and acceptance criteria (ITAAC) associated with the cyber-security program plan are provided in Tier 1 together with the SDP.

7.1.7 COL Information

None

7.1.8 References

7.1-1 USNRC, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," NUREG-0800.

7.1-2 General Electric Company, "General Electric Environmental Qualification Program," NEDE-24326-1-P, Revision 1, Class III (Proprietary), January 1983.

7.1-3 Deleted

7.1-4 GE Energy Licensing Topical Report (LTR) entitled, "ESBWR I&C Defense-In-Depth and Diversity Report." NEDO-33251, Class I (Non-proprietary), Revision 0, July 2006.

7.1-5 Deleted

7.1-6 Deleted

7.1-7 Deleted

7.1-8 GE Energy, "ESBWR Cyber Security Program Plan," NEDO-33295, Class I (Non-Proprietary); and "ESBWR Cyber Security Program Plan," NEDE-33295-P, Class III (Proprietary).

7.1-9 GE Nuclear Energy, "General Electric Instrument Setpoint Methodology," NEDC 31336P-A, Class III (Proprietary), September 1996.

7.1-10 GE Energy Nuclear, "ESBWR I&C Software Quality Assurance Plan," NEDO-33245, Class I (Non-proprietary); and "ESBWR I&C Software Quality Assurance Plan," NEDE-33245P, Class III (Proprietary), Revision 2, July 2007.

7.1-11 Deleted

7.1-12 GE Energy Nuclear, "ESBWR I&C Software Management Plan," NEDO-33226, Class I (Non-proprietary); and "ESBWR I&C Software Management Plan," NEDE-33226P, Class III (Proprietary), Revision 2, July 2007.

7.1-13 GE Energy Nuclear, "ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan," Revision 3, NEDO-33217.

Table 7.1-1

Regulatory Requirements Applicability Matrix

System																												
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	Reference Standard	RPS (Q)	NMS (Q)	SPTM Function (Q)	ADS (Q)	GDCS (Q)	LD&IS (Q)	CRHS (Q)	SSLC /ESF (Q)	SLC (Q)	RSS (Q & N)	RWCU /SDC (N)	ICS (Q)	PAM (Q & N)	CMS (Q &N)	PRMS (Q &N)	ARMS (N)	Interlock Systems (Q & N) †	NBS (Q)	RC&IS (N)	FWCS (N)	PAS (N)	SB&PC (N)	NMS (N)	CIS(N)	DPS(N) ATWS/SLC (Q)	Q-DCIS (Q)	N-DCIS (N)
10 CFR																												
50.55a(a)(1)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X							X	X	
50.55a(h)	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X							X	X	
50.34(f)(2)(v)(I.D.3)		X	X	X	X	X	X	X	X	X			X	X	X	X		X	X								X	
50.34(f)(2)(xvii)(II.F.1)														X	X	X	X											
50.34(f)(2)(xviii)(II.F.2)														X														
50.34(f)(2)(xiv)(II.E.4.2)					X	X	X	X	X																			
50.34(f)(2)(xix)(II.F.3)														X	X	X	X											
50.34(f)(2)(xxiv)(II.K.3.23)														X														
50.44(c)(4)															X													
50.62										X										X	X					X#	X	
52.47(a)(1)(iv)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(a)(1)(vi)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(a)(1)(vii)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(a)(2)		X	X	X	X	X	X	X	X	X	X		X	X	X	X		X	X							X	X	
52.47(b)(2)(i)		X	X	X	X	X	X	X	X	X	X		X	X	X	X		X	X								X	
50.34(f)(2) xii [II.E.1.2]		N/A																										
50.34(f)(2) xx [II.G.1]		N/A																										
50.34(f)(2) xxii [II.K.2.9]		N/A																										
50.34(f)(2) xxiii [II.K.2.10]		N/A																										
52.79(c)		N/A																										

Table 7.1-1

Regulatory Requirements Applicability Matrix

System																												
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	Reference Standard	RPS (Q)	NMS (Q)	SPTM Function (Q)	ADS (Q)	GDCS (Q)	LD&IS (Q)	CRHS (Q)	SSLC /ESF (Q)	SLC (Q)	RSS (Q & N)	RWCU /SDC (N)	ICS (Q)	PAM (Q & N)	CMS (Q &N)	PRMS (Q &N)	ARMS (N)	Interlock Systems (Q & N) †	NBS (Q)	RC&IS (N)	FWCS (N)	PAS (N)	SB&PC (N)	NMS (N)	CIS(N)	DPS(N) ATWS/SLC (Q)	Q-DCIS (Q)	N-DCIS (N)
General Design Criteria																												
1		X	X	X	X	X	X	X	X	X	X		X	X	X	X		X	X							X	X	X
2	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								X	X
4	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								X	X
13	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
19		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
20	IEEE Std. 603	X	X	X	X	X	X	X	X																		X	
21	IEEE Std. 603 & IEEE Std. 338	X	X	X	X	X	X	X	X																		X	
22	IEEE Std. 603	X	X	X	X	X	X	X	X																		X	
23	IEEE Std. 603	X	X	X	X	X	X	X	X					X													X	
24	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
25	IEEE Std. 603	X	X	X														X									X	
29	IEEE Std. 603	X	X	X																X							X	
SRM to SECY 93-087																												
II.Q	BTP HICB-19	X	X	X	X	X	X	X	X										X							X	X	X
II.T														X	X	X											X	X
Regulatory Guides (RG)																												
1.22		X	X	X	X	X	X	X	X	X			X													X	X	
1.47	IEEE Std. 603	X	X	X	X	X	X	X	X	X			X		X	X		X									X	
1.53	IEEE Std. 379 IEEE Std. 603	X	X	X	X	X	X	X	X	X	X		X		X	X		X									X	
1.62	IEEE Std. 603	X		X	X	X	X	X	X	X			X													X	X	

Table 7.1-1

Regulatory Requirements Applicability Matrix

System																												
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	Reference Standard	RPS (Q)	NMS (Q)	SPTM Function (Q)	ADS (Q)	GDCS (Q)	LD&IS (Q)	CRHS (Q)	SSLC /ESF (Q)	SLC (Q)	RSS (Q & N)	RWCU /SDC (N)	ICS (Q)	PAM (Q & N)	CMS (Q &N)	PRMS (Q &N)	ARMS (N)	Interlock Systems (Q & N) †	NBS (Q)	RC&IS (N)	FWCS (N)	PAS (N)	SB&PC (N)	NMS (N)	CIS(N)	DPS(N) ATWS/SLC (Q)	Q-DCIS (Q)	N-DCIS (N)
1.75	IEEE Std. 384	X	X	X	X	X	X	X	X	X	X		X		X	X		X	X							X	X	
1.97	IEEE Std. 497		X	X										X													X	X
1.105	ANSI/ISA S67.04.01	X	X	X	X	X	X	X	X	X			X		X	X		X	X							X	X	
1.118	IEEE Std. 338	X	X	X	X	X	X	X	X	X	X		X		X	X		X								X	X	
1.151	ANSI/ISA-S67.02									X								X	X		X					X	X	
1.152*	IEEE Std. 7-4.3.2	X	X	X	X	X	X	X	X				X		X	X		X	X							X	X	X
1.153	IEEE Std. 603	X	X	X	X	X	X	X	X	X	X		X		X	X		X	X							X	X	
1.168*	IEEE Std. 1012 IEEE Std. 1028	X	X	X	X	X	X	X	X				X		X	X		X	X							X	X	(1)
1.169*	IEEE Std. 828	X	X	X	X	X	X	X	X				X		X	X		X	X							X	X	(1)
1.170*	IEEE Std. 829	X	X	X	X	X	X	X	X				X		X	X		X	X							X	X	(1)
1.171*	IEEE Std. 1008	X	X	X	X	X	X	X	X				X		X	X		X	X							X	X	(1)
1.172*	IEEE Std. 830	X	X	X	X	X	X	X	X				X		X	X		X	X							X	X	(1)
1.173*	IEEE Std. 1074	X	X	X	X	X	X	X	X				X		X	X		X	X							X	X	(1)
1.180	IEEE Std. 1050	X	X	X	X	X	X	X	X	X	X††	X††	X	X††	X††	X††	X††	X††	X	X††	X††	X††	X††	X††	X††	X††	X	X††
1.204	IEEE Std. 1050	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Branch Technical Positions (BTP)																												
BTP HICB-1	IEEE Std. 603					X												X									X	
BTP HICB-3	IEEE Std. 603	N/A																										
BTP HICB-6	IEEE Std. 603	N/A																										
BTP HICB-8	Refer to RG 1.22	X	X	X	X	X	X	X	X	X			X													X	X	
BTP HICB-9	Refer to RG 1.153	X																									X	

Table 7.1-1

Regulatory Requirements Applicability Matrix

System																												
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	Reference Standard	RPS (Q)	NMS (Q)	SPTM Function (Q)	ADS (Q)	GDCS (Q)	LD&IS (Q)	CRHS (Q)	SSLC /ESF (Q)	SLC (Q)	RSS (Q & N)	RWCU /SDC (N)	ICS (Q)	PAM (Q & N)	CMS (Q &N)	PRMS (Q &N)	ARMS (N)	Interlock Systems (Q & N) †	NBS (Q)	RC&IS (N)	FWCS (N)	PAS (N)	SB&PC (N)	NMS (N)	CIS(N)	DPS(N) ATWS/SLC (Q)	Q-DCIS (Q)	N-DCIS (N)
BTP HICB-10	Refer to RG 1.97		X	X										X														X
BTP HICB-11	Refer to RG1.75 RG 1.153	X	X	X	X	X	X	X	X	X	X		X		X	X		X	X							X	X	X
BTP HICB-12	Refer to RG 1.105	X	X	X	X	X	X	X	X	X			X		X	X		X	X							X	X	X
BTP HICB-13	Refer to RG 1.153	N/A																										
BTP HICB-14*	Refer to RG 1.152	X	X	X	X	X	X	X	X		X		X		X	X		X	X							X	X	X
BTP HICB-16		X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X
BTP HICB-17*	Refer to RG 1.22, 1.47, 1.53, 1.118, 1.152 & 1.153	X	X	X	X	X	X	X	X		X		X		X	X		X	X							X	X	X
BTP HICB-18*	Refer to RG 1.152	X	X	X	X	X	X	X	X		X		X		X	X		X	X							X	X	X
BTP HICB-19*	NUREG/CR-6303	X	X	X	X	X	X	X	X										X		X					X	X	X
BTP HICB-21*	NUREG/CR-6083	X	X	X	X	X	X	X	X		X		X		X	X		X	X							X	X	X

Notes:
Q=Q-DCIS, N=N-DCIS
X = The code or regulation is applicable to the specified system.
N/A = The code or regulation is not applicable to the ESBWR design.
(1) = Parts or all of this code or regulation are voluntarily invoked for the specified system..
*These criteria are addressed with the digital computer-related functions of the Q-DCIS
†Interlocks are embedded within system logic
††N-DCIS hardware uses industrial methods for EMI/EMF compliance
#Initiates the 10 CFR 50.62 ARI, SLC and FW runback and trip functions as described in Section 7.8.

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Subject		Instrumen-tation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumen-tation and Control Systems
IEEE Std. 603 Section	**Functions [1]**	**Q-DCIS, N-DCIS**	**RPS, NMS [2], SPTMS [3], MSIV (for LD&IS)**	**SSLC/ESF ECCS [4] (that is, ADS, GDCS, ICS, SLC), PCCS [5], LD&IS (except MSIV) CRHS**	**Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)**	**Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)**	**HP/LP SI (Q)**	**NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)**	**ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), SD* against CMF (N)**
4	Safety System Designation	7.1.2.1 7.1.3.1.1 7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3 NEDO-33251	7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3 NEDO-33251	7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3 NEDO-33251	7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3 NEDO-33251	7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3 NEDO-33251	7.1.6.6.1.1	7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3 NEDO-33251	7.1.6.6.1.1 Table 15.0-2 Table 15.1-2 Table 15.1-3 NEDO-33251
4.1 4.2 4.3 4.4 4.5	DBE, safety-related functions, permissive conditions for operating bypasses, monitored variables, analytical limits, minimum criteria for manual actions	7.1.6.6.1 7.1.2.1 7.1.3.1.1	7.2.1.1 (RPS) 7.2.1.2.4.1 7.2.1.2.4.2 Table 15.0-2 NEDO-33251	7.3.1.2.1 (GDCS) 7.4.4.1 (ICS) 7.4.4.5 7.4.1.1 (SLC)	7.4.1.1 (SLC) 7.4.1.2 7.4.2.2.2 (RSS) 7.4.3.1.2 (RWCU/SDC) 7.4.4.1 (ICS) 7.4.4.5	7.5.2.1 (CMS)	7.6.1.3	7.7.1.1.1 (NBS)	
4.6	Spatially dependent variables, identification, number and location	7.1.6.6.1.1	-	-	-	-	-	-	-
4.7	Range of transient and steady-state conditions	-	-	-	-	-	-	-	-

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Subject		Instrumen-tation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumen-tation and Control Systems
IEEE Std. 603 Section	Functions [1]	Q-DCIS, N-DCIS	RPS, NMS [2], SPTMS [3], MSIV (for LD&IS)	SSLC/ESF ECCS [4] (that is, ADS, GDCS, ICS, SLC), PCCS [5], LD&IS (except MSIV) CRHS	Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)	Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)	HP/LP SI (Q)	NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)	ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), SD* against CMF (N)
4.8	Adverse environmental conditions	7.1.2.1 7.1.3.1.1	-	7.4.4.3 (ICS) 7.4.1.1 (SLC) 7.4.1.3	7.4.1.1 (SLC) 7.4.1.3 7.4.4.3 (ICS)	-	7.6.1.2.11	7.7.1.1.1 (NBS) 7.7.1.3	-
4.10	DBE critical times / conditions	7.1.2.1 7.1.3.1.1	-	-	7.4.1.1 (SLC) 7.4.4.3 (ICS)	-	7.6.1.2.1	7.7.1.1.1 (NBS)	-
4.12	Special design basis	-	-	7.3.1.1.4 (ADS) 7.4.4.2 (ICS)	7.4.4.2 (ICS)	-	7.6.1.2.10	-	-

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Subject		Instrumen-tation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumen-tation and Control Systems
IEEE Std. 603 Section	**Functions [1]**	**Q-DCIS, N-DCIS**	**RPS, NMS [2], SPTMS [3], MSIV (for LD&IS)**	**SSLC/ESF ECCS [4] (that is, ADS, GDCS, ICS, SLC), PCCS [5], LD&IS (except MSIV) CRHS**	**Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)**	**Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)**	**HP/LP SI (Q)**	**NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)**	**ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), SD* against CMF (N)**
5.1	Single failure criterion	7.1.3.3 7.1.6.6.1.2	7.1.6.6.1.2 7.2.1.1 (RPS) 7.2.1.2.4 7.2.1.3.4 7.2.2.2.4.3 (NMS) 7.2.2.2.4.6 7.2.2.2.6.4	7.1.6.6.1.2 7.3.1.1.2 (ADS) 7.3.1.1.3 7.3.1.1.3.4 7.3.1.2.1 (GDCS) 7.3.1.2.2 7.3.1.2.3 7.3.1.2.3.4 7.3.3.1 (LD&IS) 7.3.3.2 7.3.4.2 (CRHS) 7.3.5.2.2 (SSLC/ESF) 7.3.5.3.4 7.4.4.3 (ICS)	7.1.6.6.1.2 7.4.1.3 (SLC) 7.4.2.2.1 (RSS) 7.4.2.3.1 7.4.2.3.3 7.4.4.3 (ICS)	7.1.6.6.1.2	7.1.6.6.1.2 7.6.1.2.4	7.1.6.6.1.2 7.7.1.3 (NBS)	7.1.6.6.1.2
5.2	Completion of protective action	7.1.6.6.1.3	7.1.6.6.1.3 7.2.1.1 (RPS) 7.2.1.3.4	7.1.6.6.1.3 7.3.1.1.2 (ADS) 7.3.1.2.2 (GDCS) 7.3.3.1 (LD&IS) 7.3.3.3 7.3.5.2.2 (SSLC/ESF)	7.1.6.6.1.3 7.4.1.2.2 (SLC)	7.1.6.6.1.3	-	7.1.6.6.1.3	7.1.6.6.1.3

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Subject		Instrumen-tation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumen-tation and Control Systems
IEEE Std. 603 Section	**Functions [1]**	**Q-DCIS, N-DCIS**	**RPS, NMS [2], SPTMS [3], MSIV (for LD&IS)**	**SSLC/ESF ECCS [4] (that is, ADS, GDCS, ICS, SLC), PCCS [5], LD&IS (except MSIV) CRHS**	**Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)**	**Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)**	**HP/LP SI (Q)**	**NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)**	**ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), SD* against CMF (N)**
5.3	Quality	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4
5.4	Equipment qualification	7.1.6.6.1.5	7.1.6.6.1.5 7.2.1.3.5 (RPS)	7.1.6.6.1.5 7.4.4.2 (ICS)	7.1.6.6.1.5 7.4.1.3 (SLC) 7.4.4.2 (ICS)	7.1.6.6.1.5	7.1.6.6.1.5 7.6.1.2.11	7.1.6.6.1.5	7.1.6.6.1.5 7.8.2.3 (CMF defenses within SSD)
5.5	System Integrity	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6 7.3.4.2 (CRHS)	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6
5.6	Independence	7.1.6.6.1.7 7.1.3.3	7.1.6.6.1.7 7.2.1.1 (RPS) 7.2.1.2.4.1 7.2.1.3.1 7.2.1.3.4 7.2.2.2.4.3 (NMS) 7.2.2.2.5.3 7.2.2.2.6.4 7.2.2.3.1 7.2.3.3.1 (SPTM)	7.1.6.6.1.7 7.3.1.2.3.1 (GDCS) 7.3.3.1 (LD&IS) 7.3.3.2 7.3.3.3.1 7.3.4.2 (CRHS) 7.3.5.2.2 (SSLC/ESF)	7.1.6.6.1.7 7.4.1.3 (SLC) 7.4.2.2.1 (RSS) 7.4.2.3.1 7.4.2.3.3 7.4.4.3.1 (ICS)	7.1.6.6.1.7 7.5.2.2 (CMS) 7.5.2.3.1 7.5.3.3.1 (PRMS)	7.1.6.6.1.7 7.6.1.2.9	7.1.6.6.1.7 7.7.2.2.7.4 (RC&IS) 7.7.3.1.2 (FWCS) 7.7.4.2 (PAS) 7.7.5.1.2 (SB&PC)	7.1.6.6.1.7 7.8.2.3 7.8.3.1

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Subject		Instrumen-tation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumen-tation and Control Systems
IEEE Std. 603 Section	**Functions [1]**	**Q-DCIS, N-DCIS**	**RPS, NMS [2], SPTMS [3], MSIV (for LD&IS)**	**SSLC/ESF ECCS [4] (that is, ADS, GDCS, ICS, SLC), PCCS [5], LD&IS (except MSIV) CRHS**	**Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)**	**Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)**	**HP/LP SI (Q)**	**NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)**	**ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), SD* against CMF (N)**
5.7	Capability for test and calibration	7.1.6.6.1.8 7.1.2.6 7.1.3.5 7.1.6.4	7.1.6.6.1.8 7.2.2.4 (NMS) 7.2.1.3.4 (RPS) 7.2.1.4.1	7.1.6.6.1.8 7.3.1.1.4 (ADS) 7.3.1.2.4 (GDCS) 7.3.3.1 (LD&IS) 7.3.3.4.2 7.3.5.4 (SSLC/ESF) 7.4.4.4 (ICS) 7.4.4.5 7.4.1.3 (SLC) 7.4.1.4	7.1.6.6.1.8 7.4.1.3 (SLC) 7.4.1.4 7.4.3.4 (RWCU/SDC) 7.4.4.4 (ICS) 7.4.4.5	7.1.6.6.1.8 7.5.3.4 (PRMS)	7.1.6.6.1.8 7.6.1.2.10	7.1.6.6.1.8 7.7.1.4 (NBS)	7.1.6.6.1.8

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Subject		Instrumen-tation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumen-tation and Control Systems
IEEE Std. 603 Section	**Functions [1]**	**Q-DCIS, N-DCIS**	**RPS, NMS [2], SPTMS [3], MSIV (for LD&IS)**	**SSLC/ESF ECCS [4] (that is, ADS, GDCS, ICS, SLC), PCCS [5], LD&IS (except MSIV) CRHS**	**Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)**	**Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)**	**HP/LP SI (Q)**	**NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)**	**ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), SD* against CMF (N)**
5.8	Information displays	7.1.6.6.1.9	7.1.6.6.1.9 7.2.1.2.4.2 (RPS) 7.2.1.3.1 7.2.1.3.4 7.2.2.3.1 (NMS) 7.2.2.5.1	7.1.6.6.1.9 7.3.1.1.2 (ADS) 7.3.1.1.5 7.3.1.2.1 (GDCS) 7.3.1.2.2 7.3.1.2.3.1 7.3.1.2.5 7.3.3.3.1 (LD&IS) 7.3.4.2 (CRHS) 7.3.5.3.1 (SSLC/ESF) 7.4.4.5 (ICS) 7.4.1.3 (SLC) 7.4.1.5	7.1.6.6.1.9 7.4.1.3 (SLC) 7.4.1.5 7.4.2.2.1 (RSS) 7.4.4.5 (ICS)	7.1.6.6.1.9 7.5.2.1 (CMS)	7.1.6.6.1.9 7.6.1.5	7.1.6.6.1.9 7.7.1.5 (NBS)	7.1.6.6.1.9
5.9	Control of Access	7.1.6.6.1.10	7.1.6.6.1.10 7.2.1.1 (RPS)	7.1.6.6.1.10 7.3.3.1 (LD&IS)	7.1.6.6.1.10 7.4.2.2.1 (RSS)	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10
5.10.	Repair	7.1.3.5 7.1.6.6.1.11	7.1.6.6.1.11 7.2.1.2.4.4 (RPS) 7.2.2.2.4.6 (NMS) 7.2.2.2.6.6	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Subject		Instrumen-tation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumen-tation and Control Systems
IEEE Std. 603 Section	**Functions [1]**	**Q-DCIS, N-DCIS**	**RPS, NMS [2], SPTMS [3], MSIV (for LD&IS)**	**SSLC/ESF ECCS [4] (that is, ADS, GDCS, ICS, SLC), PCCS [5], LD&IS (except MSIV) CRHS**	**Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)**	**Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)**	**HP/LP SI (Q)**	**NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)**	**ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), SD* against CMF (N)**
5.11	Identification	7.1.3.3 7.1.6.6.1.7 7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12
5.12	Auxiliary features	7.1.6.6.1.13	7.1.6.6.1.13 7.2.1.1 (RPS)	7.1.6.6.1.13	7.1.6.6.1.13 7.4.1.2.1 (SLC)	7.1.6.6.1.13	7.1.6.6.1.13 7.6.1.2.2	7.1.6.6.1.13	7.1.6.6.1.13
5.13	Multi-unit stations	7.1.2.6 7.1.3.5 7.1.6.4 7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14
5.14	Human factors considerations	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15
5.15	Reliability	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16
6.1	Automatic Control	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17 7.3.1.1.2 (ADS) 7.3.3.1 (LD&IS)	7.1.6.6.1.17	7.1.6.6.1.17	7.6.1.2.4	7.1.6.6.1.17	7.1.6.6.1.17

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Subject		Instrumen-tation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumen-tation and Control Systems
IEEE Std. 603 Section	**Functions [1]**	**Q-DCIS, N-DCIS**	**RPS, NMS [2], SPTMS [3], MSIV (for LD&IS)**	**SSLC/ESF ECCS [4] (that is, ADS, GDCS, ICS, SLC), PCCS [5], LD&IS (except MSIV) CRHS**	**Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)**	**Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)**	**HP/LP SI (Q)**	**NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)**	**ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), SD* against CMF (N)**
6.2	Manual control	7.1.6.6.1.18	7.1.6.6.1.18 7.2.1.1 (RPS) 7.2.1.3.4	7.1.6.6.1.18 7.3.1.1.2 (ADS) 7.3.1.2.1 (GDCS) 7.3.1.2.2 7.3.3.2 (LD&IS) 7.3.4.2 (CRHS) 7.3.5.3.1 (SSLC/ESF) 7.4.4.5 (ICS)	7.1.6.6.1.18 7.4.4.5 (ICS)	7.1.6.6.1.18	7.6.1.2.4	7.1.6.6.1.18	7.1.6.6.1.18
6.3	Interaction between the sense and command features and other systems	7.1.3.3 7.1.6.6.1.19	7.1.6.6.1.19 7.2.1.3.1 (RPS) 7.2.2.3.1 (NMS)	7.1.6.6.1.19	7.1.6.6.1.19 7.4.2.2.1 (RSS) 7.4.2.3.1 7.4.2.3.3 7.4.4.3.1 (ICS)	7.1.6.6.1.19	7.1.6.6.1.19 7.6.1.2.4	7.1.6.6.1.19	7.1.6.6.1.19
6.4	Derivation of system inputs	7.1.6.6.1.20	7.1.6.6.1.20	7.1.6.6.1.20	7.1.6.6.1.20	7.1.6.6.1.20	7.1.6.6.1.20	7.1.6.6.1.20	7.1.6.6.1.20

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Subject		Instrumen-tation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumen-tation and Control Systems
IEEE Std. 603 Section	**Functions [1]**	**Q-DCIS, N-DCIS**	**RPS, NMS [2], SPTMS [3], MSIV (for LD&IS)**	**SSLC/ESF ECCS [4] (that is, ADS, GDCS, ICS, SLC), PCCS [5], LD&IS (except MSIV) CRHS**	**Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)**	**Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)**	**HP/LP SI (Q)**	**NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)**	**ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), SD* against CMF (N)**
6.5	Capability for testing and calibration	7.1.3.3 7.1.3.5 7.1.6.6.1.21	7.1.6.6.1.21 7.2.1.3.4 (RPS) 7.2.1.4.1	7.1.6.6.1.21 7.3.1.1.4 (ADS) 7.3.1.2.4 (GDCS) 7.3.3.4.2 (LD&IS) 7.3.5.4 (SSLC/ESF) 7.4.4.4 (ICS) 7.4.4.5 7.4.1.3 (SLC)	7.1.6.6.1.21 7.4.1.3 (SLC) 7.4.3.4 (RWCU/SDC) 7.4.4.4 (ICS) 7.4.4.5	7.1.6.6.1.21 7.5.2.4 (CMS) 7.5.3.4 (PRMS)	7.1.6.6.1.21 7.6.1.2.10 7.6.1.4	7.1.6.6.1.21	7.1.6.6.1.21
6.6	Operating bypasses	7.1.6.6.1.22	7.1.6.6.1.22 7.2.1.5.2.1 (RPS)	7.1.6.6.1.22	7.1.6.6.1.22	7.1.6.6.1.22	-	7.1.6.6.1.22	7.1.6.6.1.22
6.7	Maintenance bypass	7.1.6.6.1.23	7.1.6.6.1.23 7.2.1.2.4 (RPS) 7.2.1.5.2.2	7.1.6.6.1.23	7.4.1.3 (SLC)	-	-	-	-
6.8	Setpoints	7.1.6.6.1.24	7.1.6.6.1.24 7.2.2.1.1.1 (NMS) 7.2.2.2.4.5 7.2.2.2.4.6	7.1.6.6.1.24 7.3.3.1 (LD&IS)	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Subject		Instrumen-tation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumen-tation and Control Systems
IEEE Std. 603 Section	**Functions [1]**	**Q-DCIS, N-DCIS**	**RPS, NMS [2], SPTMS [3], MSIV (for LD&IS)**	**SSLC/ESF ECCS [4] (that is, ADS, GDCS, ICS, SLC), PCCS [5], LD&IS (except MSIV) CRHS**	**Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)**	**Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)**	**HP/LP SI (Q)**	**NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)**	**ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), SD* against CMF (N)**
7.1	Automatic Control	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17 7.3.1.1.2 (ADS)	7.1.6.6.1.17	7.1.6.6.1.17	7.6.1.2.4	7.1.6.6.1.17	7.1.6.6.1.17
7.2	Manual control	7.1.6.6.1.18	7.1.6.6.1.18	7.1.6.6.1.18 7.3.1.1.2 (ADS) 7.3.1.2.1 (GDCS) 7.3.1.2.2 7.3.3.2 (LD&IS) 7.3.4.2 (CRHS) 7.3.5.3.1 (SSLC/ESF) 7.4.4.5 (ICS)	7.1.6.6.1.18 7.4.4.5 (ICS)	7.1.6.6.1.18		7.1.6.6.1.18	7.1.6.6.1.18
7.3	Completion of protective action	7.1.6.6.1.19	-	7.3.1.2.1 (GDCS)	-	-	-	-	-
7.4	Operating bypass	7.1.6.6.1.22	7.1.6.6.1.22 7.2.1.5.2.1 (RPS)	7.1.6.6.1.22	7.1.6.6.1.22	7.1.6.6.1.22		7.1.6.6.1.22	7.1.6.6.1.22
7.5	Maintenance bypass	7.1.6.6.1.23	7.1.6.6.1.23 7.2.1.2.4 (RPS) 7.2.1.5.2.2	7.1.6.6.1.23	-	-	-	-	-

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std. 603 Specific Criteria Compliance

Subject		Instrumen-tation & Control Systems	Reactor Trip Systems	Engineered Safety Features	Safe Shutdown Systems	Information Systems	Interlock Systems	Control Systems	Diverse Instrumen-tation and Control Systems
IEEE Std. 603 Section	**Functions [1]**	**Q-DCIS, N-DCIS**	**RPS, NMS [2], SPTMS [3], MSIV (for LD&IS)**	**SSLC/ESF ECCS [4] (that is, ADS, GDCS, ICS, SLC), PCCS [5], LD&IS (except MSIV) CRHS**	**Q and N SS (that is, SLC, RSS, RWCU / SDC (N), ICS)**	**Q and N IS (that is, Q IC Displays, PAM (QN), CMS (QN), PRMS (N), ARMS (N), PMS (QN), WTDVBM)**	**HP/LP SI (Q)**	**NBS (QN), RC&IS (QN), FWCS (N), PAS (N), SB&PC (N), NMS [(2)] (N) CIS (N)**	**ATWS (N), DIC* (N), DMCD* (N), CMF* defenses within SSD* (N), SD* against CMF (N)**
8.1	Electrical power sources	7.1.3.3 7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25 7.4.4.3 (ICS) 7.4.1.2.1 (SLC)	7.1.6.6.1.25 7.4.1.2.1 (SLC) 7.4.4.3 (ICS)	7.1.6.6.1.25	7.1.6.6.1.25 7.6.1.2.2	7.1.6.6.1.25	7.1.6.6.1.25
8.2	Non-electrical power sources	7.1.6.6.1.26	-	-	7.4.1.2.1 (SLC)	-	7.6.1.2.8	-	-
8.3	Maintenance Bypass	7.1.6.6.1.27	-	-	-	-	-	-	-

1. All systems are safety-related (Q) unless shown as nonsafety-related (N)
2. NMS has Q and N parts. The Q parts are SRNM, LPRM, APRM, and OPRM. The N parts are AFIP and MRBM.
3. SPTMS is part of the RTS, ref. 7.2.3.
4. The SSLC/ESF ECCS resides within the NBS, ref. 7.3.1.1.2.
5. Passive system which does not require any control system interface to perform its safety-related function

* CMF: Common Mode Failure
DIC: Diverse Instrumentation and Control
DMCD: Diverse Manual Controls and Displays
SSD: Safety-Related System Design
SD: System Defense

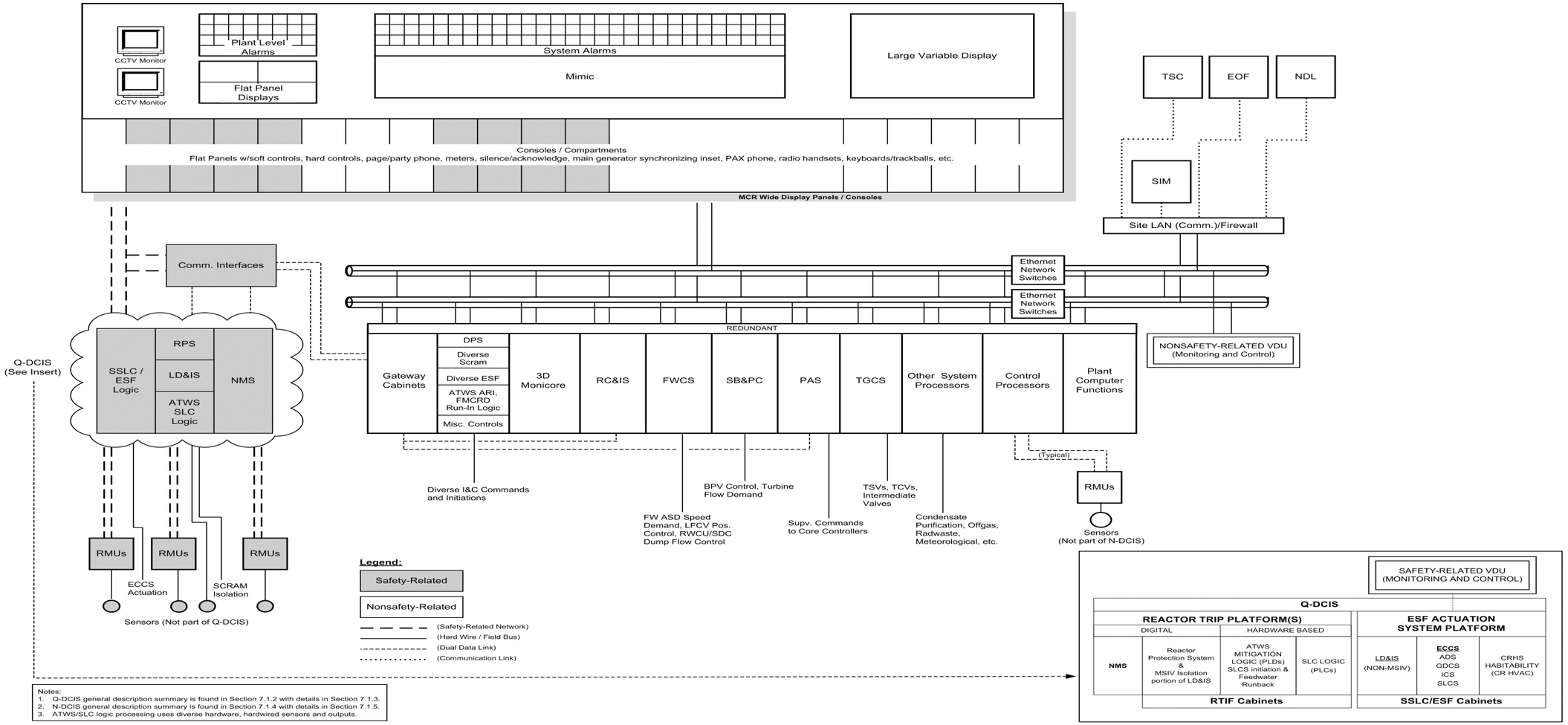


Figure 7.1-1. ESBWR Instrumentation and Control Simplified Block Diagram

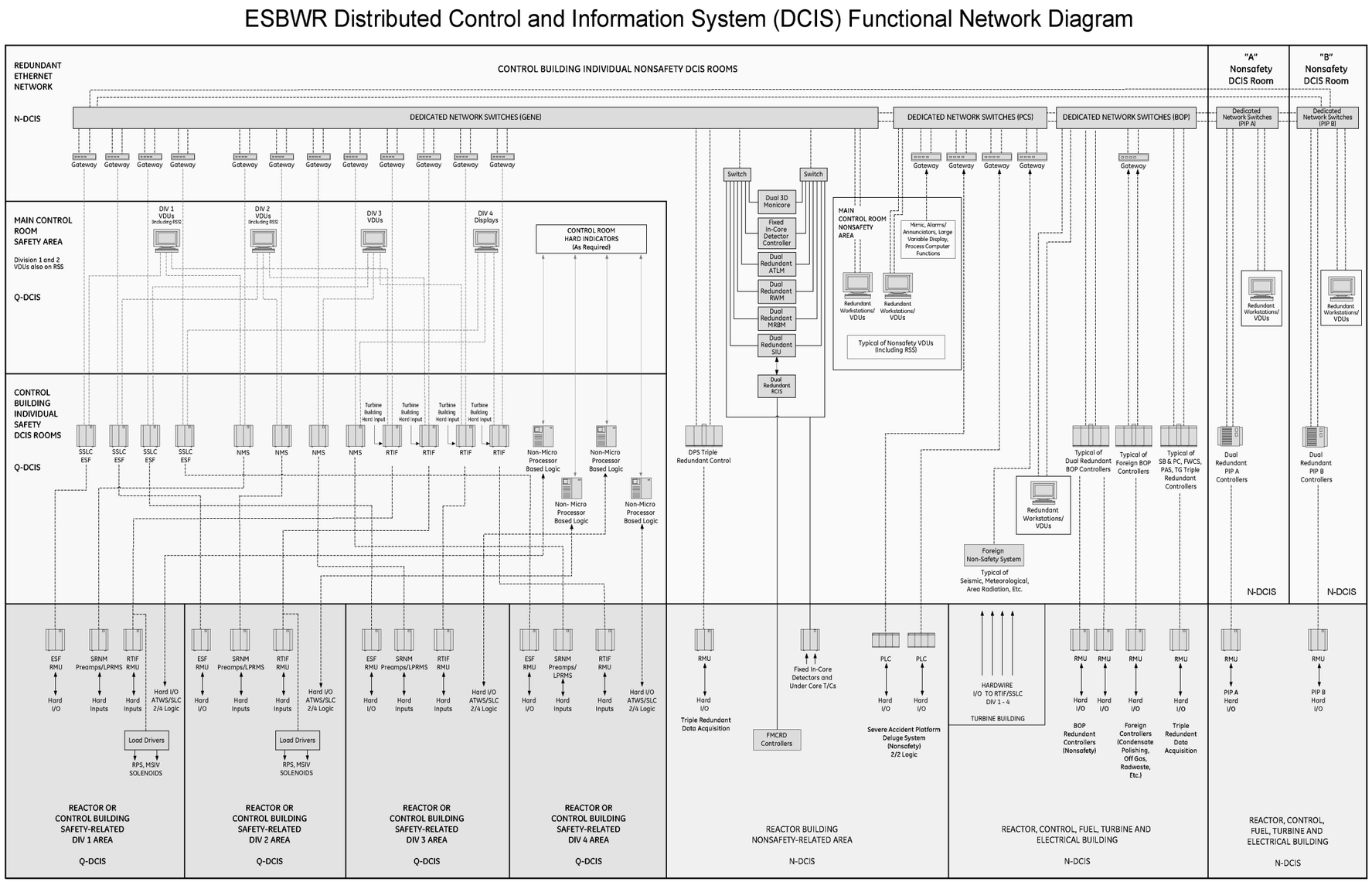
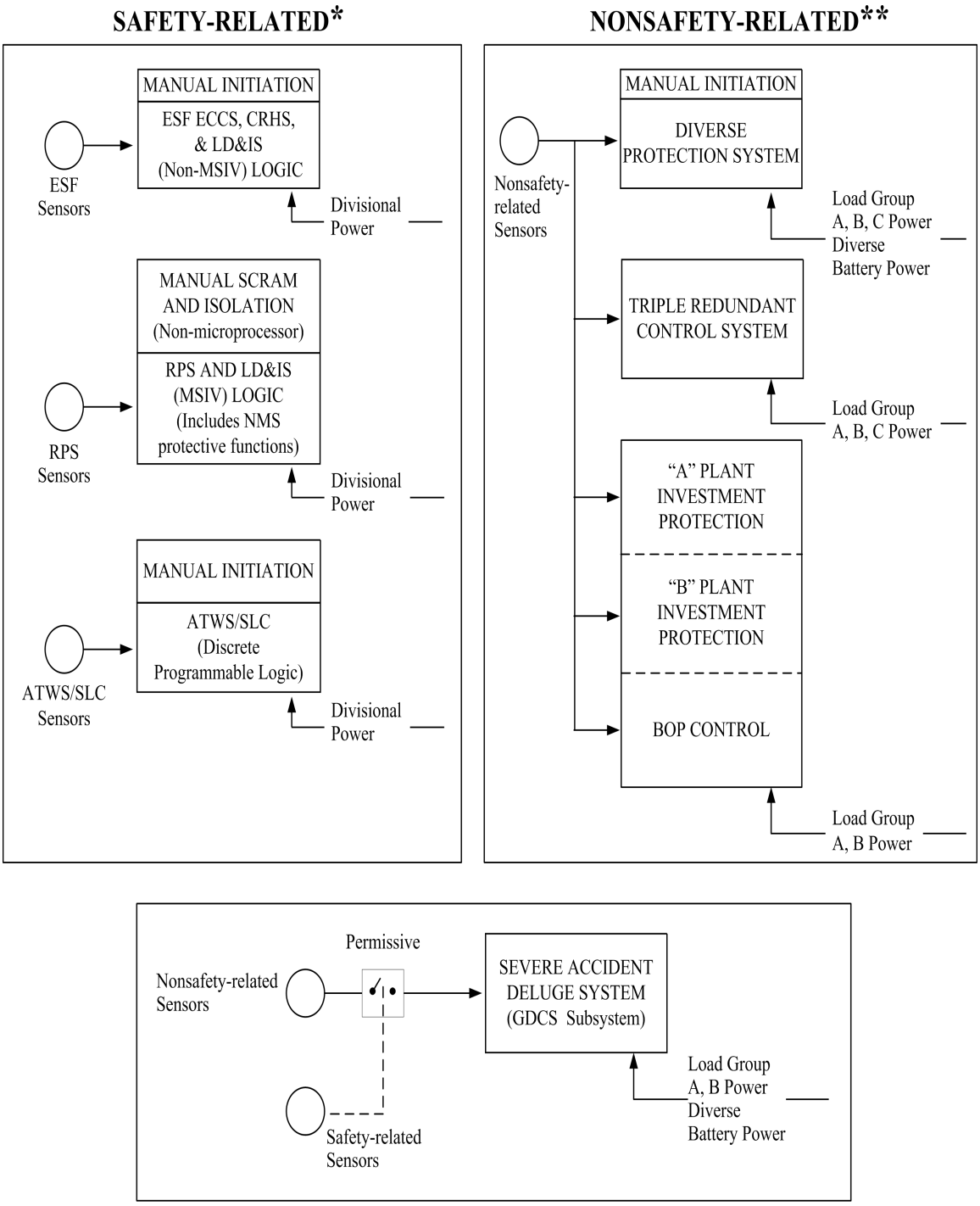


Figure 7.1-2. ESBWR Distributed Control and Information System (DCIS) Functional Network Diagram



* For safety-related systems, each enclosed box represents a different platform.

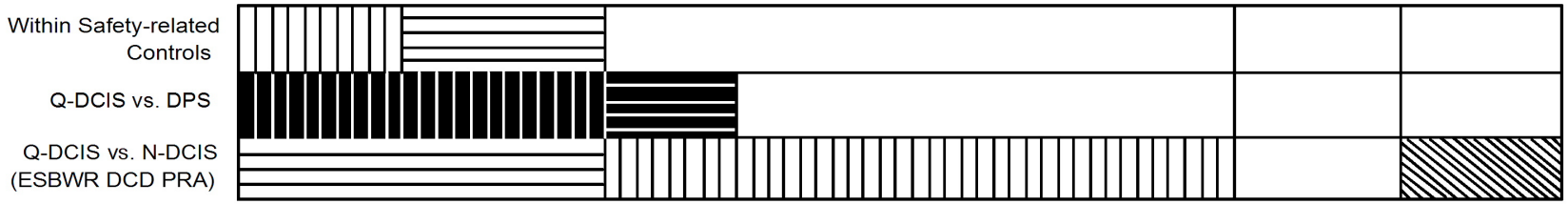
** For nonsafety-related systems, segmented systems are networked but can work independently.

Figure 7.1-3. ESBWR Distributed Power-Sensor Diversity Diagram

Safety Category	Safety-Related		Nonsafety-Related				
	Q-DCIS		N-DCIS				
System Families	RPS	ESF	DPS	CORE SYSTEMS	Balance of any N-DCIS Systems	PCF	Severe Accident
Architecture	Divisional	Divisional	Triple Redundant	Triple Redundant	Dual Redundant	Workstations **	PLCs
Systems/ Subsystems	RPS LD&IS (MSIV) NMS ATWS/SLC* CMS+	ICS ADS (SRV/DPV) GDCS SLC LD&IS (Non-MSIV) CRHS CMS+	RPS ECCS Backup	FWCS, PAS (Automation) SB&PC, TGCS	PIP A, PIP B Balance Of Plant (Power Generation)	HMI, Alarms, SPDF, Historian, 3D Monicore	Deluge System (GDCS Subsystem)

* Diverse (Discrete Programmable Logic)
\+ Diverse Sensor Inputs
** Dual redundant as necessary

Diversity Strategy



Note: Crosshatching denotes different hardware/software platforms.
Shading is for readability only.

Figure 7.1-4. ESBWR Hardware/Software (Architecture) Diversity Diagram

7.2 REACTOR TRIP SYSTEM

The Reactor Trip System includes the Reactor Protection System (RPS), the Neutron Monitoring System (NMS), and the Suppression Pool Temperature Monitoring System (SPTM) functions. These systems are discussed below in Subsection 7.2.1, 7.2.2 and 7.2.3, respectively.

7.2.1 Reactor Protection System

7.2.1.1 System Design Bases

The Reactor Protection System (RPS) safety-related design bases (IEEE Std. 603, Sections 4.1, 4.2, and 4.3) are:

- To initiate an automatic safe shutdown of the reactor (also known as reactor trip) by means of rapid hydraulic insertion of all control rods (scram):
  - When anticipated operational occurrences (transient) anomalous states occur, which may impair reactor safety.
  - When errors in operation take place resulting in transients which may impair reactor safety.
- To initiate reactor power reduction and safe shutdown of the reactor by means of rapid hydraulic insertion of a predefined group of the control rods when necessary for rapid reactor power reduction. (Several groups can be defined and scrammed in sequence.) This feature is called Select Rod Insert (SRI) and is initiated by reliable signals from the Diverse Protection System (DPS).
- To provide timely protection against the onset and effects of conditions threatening the integrity of the reactor fuel barriers, the reactor coolant pressure boundary (RCPB), or the primary containment vessel pressure boundary. This limits the uncontrolled release of radioactive materials from the fuel assembly or the RCPB. Also to provide such protection against conditions that threaten important plant equipment integrity.
- To initiate an automatic reactor trip whenever monitored process variables exceed or fall below their specified trip setpoints based on values determined by Anticipated Operational Occurrences (AOO), accident analyses, and instrument setpoint calculation methodology.
- To provide control switches for initiation of reactor scram by the plant operator when necessary.
- To provide mode selection for enabling the appropriate instrument channel trip functions required in a particular mode of plant operation. Mode selection also provides for bypassing instrument channel trip functions that are not required and for establishing other necessary interlocks associated with the major plant operating modes.

- To provide selective automatic and manual operational trip bypasses, as necessary, to permit proper plant operations. These bypasses allow for protection requirements depending upon specific existing or subsequent reactor operating conditions.
- To provide seal-in of specific trip logic paths after trip conditions have been satisfied and to inhibit the trip reset, as necessary, to ensure subsequent required protective action sequences are completed.
- To provide manual reset capability permitting restoration of the RPS and other affected systems to their normal operational status following seal-in of any trip logic path or after a full reactor scram.
- To provide isolated outputs to other systems sharing instrument channel signals with the RPS, using trip signals generated by the RPS, or requiring other indications of specific RPS status for their inputs.
- To provide isolated outputs to appropriate warning, trip, or bypass alarm annunciators to operator displays (for example, flat panel or Cathode Ray Tube [CRT] displays) and to the plant computer function of the Nonsafety-related Distributed Control and Information System (N-DCIS).
- To provide means for calibration and adjustment of trip function setpoints and to provide sufficient controls to permit surveillance and post-maintenance testing of RPS equipment.

The following bases ensure that the RPS is designed with sufficient reliability (IEEE Std. 603, Section 5.1, 5.2, 5.6, 5.9, 5.12 and 6.2).:

- Single failures, bypasses, repairs, calibration, or adjustments do not impair the normal protective functions of the RPS and do not result in inadvertent reactor scram or insertion of control rods. The RPS is capable of accomplishing its protection functions in the presence of any single failure within the RPS (with any three of the four divisions of safety-related power available), any failures caused by a single failure, and any failure caused by any design basis event requiring RPS protective action.
- The RPS is designed to cause reactor scram even during system shutdown and loss of electrical power sources.
- The RPS fails into a safe state if conditions such as disconnection of the system (or portions of the system), loss of electrical power, or adverse environment are experienced.
- Loss of a single power source directly associated with RPS equipment and protection functions does not cause instrument channel trips, division trips, or scram solenoid de-energization resulting in full reactor scram or insertion of any control rod.
- Once initiated, RPS protective actions continue in their intended sequence until completion of hydraulic control rod insertion. The RPS trip is sealed-in and can only be reset manually. All manual resets are automatically inhibited for 10 seconds to allow sufficient time for scram completion.

- The RPS has built-in redundancy in its design that fulfills the reliability and availability requirements of the system.
- The RPS has bypass capability for failed portions of each division's equipment without degrading operability.
- A separate and diverse manual trip function is provided through the use of two manual-trip switches. Actuation of both manual-trip switches is required for a full reactor scram.
- Physical separation and electrical isolation between redundant divisions of the RPS are provided by separate process instrumentation, separate racks, and separate or independent panels and cabling. In the control building (CB) separate equipment rooms perform this function.

The following features reduce the probability that RPS operational reliability is degraded by operator error:

- Access to trip settings, calibration controls, test points, and other terminal points are under the control of Operations supervisory personnel.
- Manual bypass of components is under the control of the main control room (MCR) operator. Any bypass of essential parts of the system is continuously alarmed in the MCR. The design does not allow more than one channel to be bypassed at a time.
- Selective automatic and manual trip bypasses are provided to permit proper plant operation.
- Controls for initiation of reactor scram by the plant operator, are provided.
- A Mode selection switch is provided to select the plant operation mode. This switch sends bypass and interlock signals to the RPS, instruments, and hardware.

7.2.1.2 System Description

7.2.1.2.1 Reactor Protection System Identification

The RPS is the overall complex of instrument channels, trip logics, trip actuators, manual controls, and scram logic circuitry. This complex initiates rapid insertion of control rods (redundant) to shut down the reactor when situations and circumstances arise that could result in unsafe reactor operating conditions. The RPS also establishes appropriate interlocks for different reactor operating modes and provides status and control signals to other systems and alarms.

To accomplish its overall function, the RPS interfaces with the:

- Safety-Related Distributed Control & Information System (Q-DCIS),
- Safety System Logic and Control / Engineered Safety Features (SSLC/ESF),
- Neutron Monitoring System (NMS),

- Nuclear Boiler System (NBS),
- Control Rod Drive System (CRDS),
- Containment Monitoring System (CMS) (including Suppression Pool Temperature Monitoring [SPTM] function),
- Rod Control and Information System (RC&IS),
- Leak Detection and Isolation System (LD&IS),
- Isolation Condenser System (ICS),
- Steam Bypass and Pressure Control (SB&PC) System,
- Plant Automation System (PAS),
- MCR Panels,
- N-DCIS,
- DPS,
- Uninterruptible AC Power Supply,
- Direct Current (DC) Power Supply, and
- Raceway System.

The RPS sensors, hardware, and logic are diverse from both ECCS logic and the DPS.

A simplified RPS functional block diagram is provided in Figure 7.2-1. A simplified RPS interfaces and boundaries diagram is provided in Figure 7.2-2.

7.2.1.2.2 Reactor Protection System Classification

The RPS is classified as a safety-related system. The functions and components of the RPS are safety-related unless otherwise indicated. The RPS electrical equipment also is classified as Seismic Category I and as IEEE electrical category safety-related.

7.2.1.2.3 Power Sources

AC electric power required by the four divisions of RPS logic is supplied from four pairs of physically separate, electrically independent, uninterruptible, safety-related 120 Volts Alternating Current (VAC) buses. Each RPS division uses the two independent, uninterruptible power sources from the same division. Either division of the power source supports the RPS division. Two divisions of the safety-related 120 VAC also are used as the power sources for the solenoids of the scram pilot valves.

7.2.1.2.4 Reactor Protection System Equipment Design

The RPS is designed to provide reliable, single-failure proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams

resulting from single failures. The RPS satisfies the single-failure criterion even when one entire division of channel sensors is bypassed and/or when one of the four automatic RPS trip logic systems is out of service (with any three of the four divisions of safety-related power available). This is accomplished through the combination of fail-safe equipment design, redundant sensor channel trip decision logic, and redundant two-out-of-four trip systems output scram logic. This dual two-out-of-four arrangement used in the RPS design ensures that the single-failure criterion is fully incorporated into the design. The RPS design satisfies the single-failure criterion requirement of IEEE Std. 603, Section 5.1.

Equipment within the RPS is designed to fail into a trip-initiating state upon loss of power, loss or disconnection of any input signal, or loss of any internal or external device-to-device connection signal. The failure does not affect trip bypass logic signals or trip bypass permissive logic signals.

The design of RPS includes two operator-controlled bypasses: the "division of sensors" and the "division of logic (division-out-of-service)" bypasses. These are independently controlled by separate fiber optic "joystick" switches allowing the operator to insert the bypass into only one division at a time. There is no combination of operator bypasses that can reduce the redundancy of the RPS system below the requirements of IEEE Std. 603 Sections 6.7 and 7.5. The system always is able to scram the reactor if any two like and un-bypassed parameters exceed their trip values. The required scram capability is maintained even if RPS back panel chassis are keylock-disabled (not an operator function).

7.2.1.2.4.1 Arrangement

The RPS-related equipment is divided into four redundant divisions of sensor (instrument) channels, trip logics, and trip actuators as well as two divisions of manual scram controls and scram logic circuitry. The sensor channels, divisions of trip logic, divisions of trip actuators, and associated portions of the divisions of scram logic circuitry together constitute the RPS automatic scram and air header dump (backup scram) initiation logic.

The divisions of manual scram controls and associated portions of the divisions of scram logic circuitry together constitute the RPS manual scram and air header dump initiation logic. The automatic and manual scram initiation logics are independent of each other and use diverse methods and equipment to initiate a reactor scram. A functional equipment arrangement is shown in Figure 7.2-1.

Sensor Channels: Equipment within a sensor channel consists of sensors (transducers or switches), Digital Trip Module (DTM), and multiplexers. The sensors within each channel monitor for abnormal operating conditions and send analog (or discrete) output either directly to the RPS cabinets or to the Reactor Trip and Isolation Function (RTIF) Remote Multiplexer Units (RMUs) within the associated division of the Q-DCIS. The RMU within each division performs signal processing including analog to digital, then sends the digital or digitized analog output values of the monitored variables to the DTM for trip determinations within the associated RPS sensor channel in the same division. The DTM in each sensor channel compares individual monitored variable values with trip setpoint values. For each variable the DTM sends a separate trip/no trip output signal to the functional Trip Logic Units (TLU) in the four divisions of trip

logic. DTM signals sent from one division to other divisions are isolated optically using fiber-optic cables. The DTMs and TLUs are microprocessor-based modules of the RPS.

The software associated with RPS channel trip and trip system coincident logic decisions installed in these modules is RPS unique. The number of channels used in the functional performance of the RPS is shown in Table 7.2-1 (IEEE Std. 603, Section 4.4).

Q-DCIS equipment within a single division of sensor channels is powered from the safety-related power source of the same division. However, different pieces of equipment may be powered from separate low-voltage DC power supplies within the panels belonging to the same division. Within a sensor channel the sensors themselves may belong to the RPS or may be components of another system. Signal conditioning and distribution performed by the RMUs are functions of the Q-DCIS.

Components within each of the four RPS sensor channels are fully separated physically and are independent from components of other sensor channels (fulfilling the independence requirement of IEEE Std. 603, Section 5.6). The RPS equipment is independent and physically separated from other safety-related or nonsafety-related systems fulfilling the requirements of IEEE Std. 603, Section 5.6.

Any necessary signal communication between the RPS and other systems is through optical isolation devices such as fiber optic cables, via the Communication Interface Module (CIM) of the RPS. There are no signal inputs from other systems affecting the safety function of the RPS. The application of this nonsafety-to-safety interface is described in detail in the GE Nuclear Measurement Analysis and Control (NUMAC) Licensing Topical Report (NEDO 33288) Reference 7.2-2). This topical report explains the CIM function, communication data link, and describes the buffer/gateway function for data transmitted from the nonsafety-related system to the safety-related system. The transfer of data between the safety-related system and nonsafety-related system is normally one-way which provides communication isolation. When passing data from nonsafety-related subsystems to safety-related systems, an operator action is required to place a switch in the Inoperative Mode.

Divisions of Trip Logic: Equipment within an RPS division of trip logic consists of TLUs, manual switches, Bypass Units (BPUs), and Output Logic Units (OLUs).

The TLUs perform the automatic scram initiation logic checking for two-out-of-four coincidence of trip conditions in any set of instrument channel signals coming from the four divisions of DTMs, or when a NMS-isolated digital trip signal (voted two-out-of-four in the NMS TLU) is received. The automatic scram initiation logic for any trip is based on the reactor operating mode switch status, channel trip conditions, NMS trip input, and bypass conditions. Each TLU, in addition to receiving the signals described above, also receives digital input signals from the BPU and other control interfaces in the same division. Signals from one RPS division to another RPS division are isolated electronically using fiber optic cables.

The various manual switches provide the operator with the means to enforce interlocks within RPS trip logic for special operation, maintenance, testing, and system reset. The BPUs perform bypass and interlock logic for the division of channel sensors bypass and the division TLU bypass. Each BPU sends a separate bypass signal for the four channels to the TLU in the same

division for channel sensors bypass. Each RPS BPU also sends the TLU bypass signal to the OLU in the same division.

The OLUs perform division trip, seal-in, reset, and trip test functions. Each OLU receives bypass inputs from the RPS BPU, trip inputs from the TLU of the same division, and manual inputs from switches within the same division. Each OLU provides trip outputs to the trip actuators.

Equipment within a division of trip logic is powered from the same division of safety-related power source. However, different pieces of equipment may be powered from separate low-voltage DC power supplies in the same division.

Divisions of Trip Actuators: Equipment within a division of trip actuators includes load drivers and controllers for automatic scram and air header dump initiation. The RPS includes two physically separate and electrically independent divisions of trip actuators receiving inputs from the four divisions of TLU. The load drivers are isolated, solid-state, current-interrupting devices with fast response times and are used for primary scram actuators. They are powered by 120 VAC and can tolerate the high current levels associated with Hydraulic Control Unit (HCU) scram solenoid operation.

The operation of the load drivers is such that a trip signal on the input side creates a high impedance current-interrupting condition on the output side. The output side of each load driver is isolated electrically from its input signal. The load driver outputs are arranged in the scram logic circuitry between the scram solenoids and scram solenoid 120 VAC power source. When in a tripped state, the load drivers cause the scram solenoids (scram initiation) to de-energize. The load drivers within a division interconnect with the OLU of all other divisions to form a special arrangement (connected in series and in parallel in two separate groups) that results in two-out-of-four scram logic. Reactor scram occurs if load drivers associated with any two or more divisions receive trip signals from the OLUs (Refer to Figure 7.2-1).

The controllers are used for back-up scram actuators, scram–follow initiation, and scram reset permissive actuators. When in a tripped state, the controllers cause the air header dump valve solenoids (air header dump) to energize. The controllers of the backup scram are arranged in a two-out-of four configuration similar to that described above for the primary scram load drivers. Backup scram is diverse in power source and function from primary scram.

Divisions of Manual Scram Controls: Equipment within a division of manual scram controls includes manual switches, contactors, and relays providing an alternate, diverse, manual means to initiate a scram and air header dump. Each division's manual scram function controls the power sources to the same division of scram logic circuitry for scram initiation and division of scram logic circuitry for air header dump initiation.

Divisions of Scram Logic Circuitry: The two divisions of primary scram logic circuitry are powered from independent and separate power sources. One of the two divisions of scram logic circuitry distributes Division 1 safety-related 120 VAC power to the A solenoids of the HCUs. The other division of scram logic circuitry distributes Division 2 safety-related 120 VAC power to the B solenoids of the HCUs. The HCUs (including the scram pilot valves and the scram valves) are components of the CRDS. A full scram of control rods associated with a particular

HCU occurs when both A and B solenoids of the HCU are de-energized. The arrangement of equipment groups within the RPS from sensors to actuator loads is shown in Figure 7.2-1. The RPS functional block diagram showing the RPS interfaces and boundaries diagram with other systems is shown in Figure 7.2-2.

7.2.1.2.4.2 Initiating Circuits

The RPS logic initiates a reactor scram in the individual sensor channels when any one or more of the conditions listed below exist (IEEE Std. 603, Section 4.1, 4.2 and 4.4). The system monitoring the process condition is indicated in parenthesis.

- High Drywell Pressure (CMS),
- Turbine Stop Valve (TSV) Closure (RPS),
- Turbine Control Valve (TCV) Fast Closure (RPS),
- NMS-monitored SRNM and APRM conditions exceed acceptable limits (NMS),
- High Reactor Pressure (NBS),
- Low Reactor Water Level (Level 3) decreasing (NBS),
- High Reactor Water Level (Level 8) increasing (NBS),
- Main Steam Line Isolation Valve (MSIV) Closure (Run mode only) (NBS),
- Low Control Rod Drive HCU Accumulator Charging Header Pressure (CRDS),
- High Suppression Pool Temperature (CMS),
- High Condenser Pressure (RPS),
- Power Generation Bus Loss (Loss of Feedwater Flow)(Run mode only) (RPS),
- Operator-initiated manual scram (RPS), and
- Reactor Mode Switch in “Shutdown” position (RPS).

With the exception of the NMS outputs, the MSIV closure, TSV closure and TCV fast-closure, loss of feedwater flow due to loss of power generation bus, main condenser pressure high, and manual scram outputs, the other systems provide sensor outputs through the RPS RMU.

The MSIV Closure, TSV closure and TCV fast-closure, loss of power generation bus, manual scram output, and main condenser pressure high signals are provided to the RPS through hardwired connections. The NMS trip signal is provided to the RPS through fiber optic cable. The systems and equipment providing trip and scram initiating inputs to the RPS for these conditions are discussed in the following subsections.

Neutron Monitoring System

The separate and isolated NMS digital Startup Range Neutron Monitor (SRNM) trip signals, and Average Power Range Monitor (APRM) trip signals from each of the four divisions of the NMS equipment are provided to their divisions of RPS trip logic as shown on Figure 7.2-1.

SRNM Trip Signals: The SRNM subsystem provides trip signals to the RPS to cover the range of plant operation from source range through startup range (more than 10% of reactor-rated power). Three SRNM conditions, monitored as a function of the NMS, comprise the SRNM trip logic output to the RPS. These conditions are:

- SRNM upscale (high count rate or high thermal neutron flux level),
- Short (fast) period, and
- SRNM inoperative.

The three trip conditions from every SRNM associated in NMS division are combined into a single SRNM trip signal for that division. The specific condition causing the SRNM trip output state is identified by the NMS, and is not detectable within the RPS. The SRNM trip functions are summarized in Table 7.2-2.

APRM Trip Signals: The APRMs provide trip signals to the RPS to cover the range of plant operation from a few percent of reactor-rated power to greater-than-rated power. Three APRM conditions, monitored as a function of the NMS, comprise the APRM trip logic output to the RPS. These conditions are:

- APRM high thermal neutron flux,
- High simulated reactor thermal power, and
- APRM inoperative.

The APRM trip functions are summarized in Table 7.2-4.

Within the APRM subsystem there is the Oscillation Power Range Monitor (OPRM) function, which is capable of generating a trip signal in response to core thermal neutron flux oscillation conditions, and thermal-hydraulic instability fast enough to prevent cladding thermal limit violation and fuel damage. This OPRM trip signal is combined with the other three APRM trip signals to form the final APRM trip signal to RPS. The NMS also provides the RPS with a simulated reactor thermal power signal to support the load rejection bypass algorithm.

Nuclear Boiler System

Reactor Pressure: Reactor pressure is measured by four physically separate pressure transmitters mounted on separate divisional local racks in the safety envelope within the Reactor Building (RB). Each transmitter is on a separate instrument line and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the RPS RMU, which digitizes and conditions the signal before sending it to the appropriate RPS DTM in one of the four RPS divisional sensor channels. The four pressure transmitters and associated instrument lines are components of the NBS.

Reactor Pressure Vessel (RPV) Water Level: RPV water level is measured by four physically separate level (differential pressure) transmitters mounted on separate divisional local racks in the safety envelope within the RB. Each transmitter is on a separate pair of instrument lines and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the RPS RMU, which digitizes and conditions the signal before sending it to the appropriate DTM in one of the four RPS divisional sensor channels. The four separate level transmitters and associated instrument lines are components of the NBS.

Main Steamline Isolation Valve Closure: Each of the four Main Steam Lines (MSLs) can be isolated by closing either its inboard or outboard isolation valve. Position (limit) switches are mounted on both isolation valves of each MSL. These switches provide output to the appropriate DTM in one of the four RPS divisional trip channels using hard wired connections. On each MSL, two position switches are mounted on each inboard isolation valve and each outboard isolation valve. Each of the two position switches on any one MSL isolation valve is associated with a different RPS divisional sensor channel. A reactor scram is initiated by either the inboard or outboard valve closure on two or more of the MSLs. The eight MSIVs and the 16 position switches supplied with these valves (for RPS use) are components of the NBS.

Control Rod Drive System

Locally mounted pressure transmitters measure the CRDS accumulator charging header pressure at four physically separate locations. Each transmitter is associated with a separate RPS division and is on a separate instrument line. Each transmitter provides an analog output signal to the RMU, which digitizes and conditions the signal before sending it to the appropriate DTM (in one of the four RPS divisional trip channels). The four pressure transmitters and associated instrument lines are components of the CRDS. This is an anticipatory scram because it initiates a scram before the HCUs have time to depressurize.

Reactor Protection System

Turbine Stop Valve Closure: TSV closure is detected by separate valve stem position switches on each of the four valves. Each position switch provides an open/close contact output signal through hard wired connections to the DTM in one of the four RPS divisional trip channels. The TSV closure trip occurs in each division of trip logic when any two or more position switches detect the TSV closure. The TSVs are components of the main turbine. The position switches are components of the RPS.

Turbine Control Valve Fast Closure: Low oil pressure in the hydraulic trip system, which is indicative of TCV fast-closure, is detected by separate pressure transmitters on each of the four TCV hydraulic mechanisms. Each pressure transmitter provides a 4-20 mA signal through hardwired connections to the DTM in each of the four RPS divisional trip channels. The TCV closure trip occurs in each division of trip logic when any two or more sensor channels detect low oil pressure in the hydraulic trip system. The TCV hydraulic mechanisms are components of the main turbine. The pressure transmitters are components of the RPS.

Turbine Bypass Valve Position: The Turbine Bypass Valves (TBV) provide position limit switch inputs to RPS as a permissive to inhibit reactor trip on TSV closure or TCV fast closure if the bypass valves open to their 10% position within a defined period of time. One switch with

four sets of contacts is mounted on each valve. Each contact is associated with one of the four RPS divisions to permit two-out-of-four logic. The position switches are components of the RPS.

High Condenser Pressure: High condenser pressure is detected by separate pressure transmitters mounted on the main condenser. Each pressure transmitter provides an analog output signal through hardwired connections to the DTM in each of the four RPS divisional trip channels. The pressure transmitters are components of the RPS. The reactor scram at high condenser pressure shuts off steam flow to the main condenser and protects the main turbine. This is an anticipatory scram in that high condenser pressure also trips the main turbine and prevents bypass valve operation.

Loss of Power Generation Bus (Loss of Feedwater Flow): The plant electrical system has four power generation buses operating at 13.8 kV. Although all four buses typically are energized, the loads on these buses are arranged such that any three buses' Feedwater (FW) pump can support power generation. Specifically, these buses supply power for the FW pumps and circulating water pumps. In the Run mode at least three of the four buses must be powered.

If the sensor (one per division) on each bus detects a low voltage, indicating that less than three buses are operating, a two-out-of-four logic initiates a scram after a preset delay time. This delay time (less than one second) is to allow the auto transfer from the Unit Auxiliary Transformer (UAT) feed to the Reserve Auxiliary Transformer (RAT) feed to restore normal bus voltages. Loss of more than one power generation buses is indicative of loss of the FW pumps and flow. It is also indicative of loss of condenser vacuum from the loss of the circulating water pumps.

The purpose of a scram on loss of the power generation buses is to mitigate the RPV water level drop to Level 1 following the loss of FW pump function. This scram terminates additional steam production within the RPV before Level 3 is reached.

Manual Scram: Two manual scram switches and the Reactor Mode Switch provide diverse means to initiate manually a reactor scram independent of conditions within the sensor channels, divisions of trip logic, and trip actuators. When the Reactor Mode Switch is placed in the shutdown position, power to the circuits affected by each manual scram pushbutton are interrupted resulting in a full scram. Each of the manual scram switches is associated with one of the two divisions of actuator load power. Both manual scram switches have to be actuated simultaneously to result in a full manual scram. Since the non-software-based manual scram capability of the RPS system operates directly on the scram solenoid power, only Divisions 1 and 2 are involved. If either of those two divisions is out of service (including maintenance), a half-scram results; depressing the other division manual scram pushbutton then results in a full scram. If either of the two divisions is out of service for non-power issues the manual scram capability remains unaffected. The operability of Divisions 3 and 4 has no effect on the RPS manual scram capability.

Manual scram switches also are provided in the remote shutdown (RSS) panel to achieve hot shutdown for the reactor from outside the MCR. There is a separate manual switch in each of the four divisions providing a means to manually trip all actuators in that division. An alternative manual scram can be accomplished by activating any two (or more) of the four manual divisional trip switches.

Reset Logic: A reset switch is provided to reset the manual scram in both (1 and 2) divisions of manual scram controls. A separate manual switch associated with each division of trip actuators provides the means to reset the seal-in at the input of all trip actuators in the same division. The reset does not have any effect if the conditions that caused the division trip have not cleared when a reset is attempted. All manual resets are automatically inhibited for 10 seconds to allow sufficient time for scram completion. The switch used to reset the manual scram circuitry permits resetting of the several scram groups in sequence, so re-energization of only one-half of the scram solenoids is performed at one time.

After a full scram the CRD charging header pressure will drop below the trip setpoint, resulting in a trip initiating input to all four divisions of trip logic. While this condition exists, the four divisions of trip logic cannot be reset until the CRD charging pressure trip is manually bypassed in all four divisions, and all other trip-initiating conditions have been cleared.

Containment Monitoring System

Drywell Pressure: Primary containment (drywell) pressure is measured at four physically separate locations by pressure transmitters located on separate divisional local racks in the safety envelope within the RB. Each transmitter is on a separate instrument line and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the RMU, which digitizes and conditions the signal before sending it to the appropriate DTM in the four RPS divisional trip channels. The four pressure transmitters and associated instrument lines are components of the Containment Monitoring System (CMS).

Suppression Pool Temperature: Four channels of safety-related divisional suppression pool temperature signals, each formed by the average value of a group of 16 thermocouples installed uniformly (both vertically and azimuthally) inside the suppression pool, provide the suppression pool temperature data for automatic scram initiation. For the suppression pool temperature high to be enabled, 12 of the 16 assigned thermocouples are required to be operable. When the established limits of high temperature are exceeded in two of the four divisions, scram initiation is generated.

Each temperature sensor provides an analog output signal to the RMU, which digitizes and conditions the signal before sending it to the appropriate DTM. The temperature sensors and associated instrument lines are components of the CMS. The suppression pool water level signals also are provided. When water level drops below selected temperature sensors, the exposed sensors are logically bypassed, so only sensors below water level are used to determine the averaged temperature signal to the RPS.

7.2.1.2.4.3 Reactor Protection System Outputs to Interfacing Systems

Scram Signals to the CRD System: Reactor trip conditions existing in any two or more of the four RPS automatic trip channels and/or in both RPS manual trip channels cause the output circuits of the RPS (normally supplying power to the solenoids of the scram pilot valves of the CRD system) to be disconnected from power, resulting in insertion of all control rods and reactor shutdown.

When the scram pilot valve solenoids are disconnected from power by the RPS trip signals, the two scram air header dump valves of the CRD system (backup scram valves) are actuated by the RPS trip signals to exhaust the air from the scram air header, resulting in backup scram action.

RPS Status Outputs to the NMS: Two types of RPS status condition signals (four combined signals each, one per division) are provided to the NMS by the RPS. Isolated output signals, indicating that the Reactor Mode Switch is in the Run position, are provided to the four divisions of the NMS whenever the mode switch is in that position. These signals are used by the NMS to bypass the NMS SRNM alarm and trip function, whenever the mode switch is in the Run position.

Scram Follow Signals to the RC&IS: Upon the occurrence of any full reactor scram condition the RPS provides isolated output signals to the RC&IS. This enables automatic rod run-in (scram-follow) logic in the RCIS to cause full insertion (or "run-in") of the fine motion control rod drives subsequent to scram. The RPS also provides the RC&IS with both scram test switch status, indicating the start of a rod pair scram test and the position of the Reactor Mode Switch.

Rod Block Signals to the RC&IS: Rod withdrawal inhibit signals (one for each channel) are provided by the RPS via isolated output signals sent to the RC&IS whenever there is a "Low CRD Charging Water Header Pressure" trip signal or when any CRD charging pressure trip bypass switch is in the Bypass position.

Outputs to the LD&IS: The drywell pressure output signals are sent to the LD&IS for RCPB and primary containment leakage alarm and isolation functions. The drywell pressure output signals are obtained from the RPS sensors (one for each division) and provided to the LD&IS via the Q-DCIS. Also, Reactor Mode Switch status signals from each division are provided. The RPS also provides an interlock to the LD&IS for bypassing the MSIV isolation (when not in the Run mode) that otherwise would result from high main condenser vacuum-pressure and/or low inlet-pressure to the turbine during startup and shutdown.

Outputs to Main Control Room Panels:

Safety-related status and alarm signals are sent from the RPS to the main control console.

Displays: Instrument channel sensor checks are capable of being performed at the main control console. Displays exist for readout and comparison of the current values of the variables or separate processes being monitored for each set of four (one per division). Displays related to RPS scram variables include the following minimum set of signals:

- Reactor vessel pressure,
- RPV water levels,
- Containment drywell pressures,
- CRD HCU accumulator charging header pressures,
- Suppression pool (local or bulk) temperatures,
- Power generation bus voltages,

- TSV position,
- Hydraulic Trip System oil pressure
- MSIV position,
- Main condenser pressure, and
- NMS outputs.

The values of all scram parameters are continuously sent through isolated gateways to the N-DCIS where displays of the scram parameters from all divisions are integrated to allow easy comparison between divisions. Additionally, the plant computers and alarm systems will alarm if any divisional parameter differs from the other divisions by more than a predetermined amount. The intent is that channel sensor checks be performed continuously.

Alarms: Alarms are provided at the main control console by the trip condition of any of the four sensor trip channels, by the trip condition of each automatic or manual trip system, and when bypassing a scram function. The alarm function is provided through isolated gateways to the plant computer functions (PCF).

The following alarms / indications related to RPS status are provided:

- RPS NMS trip (generated in NMS),
- Reactor vessel pressure high,
- RPV water level low (≤ Level 3),
- RPV water level high (≥ Level 8),
- Containment (drywell) pressure high,
- MSIV closure trip,
- TSV closure,
- TCV fast closure,
- Main condenser pressure high,
- Power generation bus loss (Loss of feedwater flow),
- CRD HCU accumulator-charging-header-pressure low,
- Suppression pool temperature high,
- RPS divisional automatic trip (auto-scram) (each of the four: Div. 1, 2, 3, 4 automatic trip),
- RPS divisional manual trip (each of the four: Div. 1, 2, 3, 4 manual trip),
- Manual scram trip (two: both Manual A and Manual B),

- Reactor Mode Switch in Shutdown position,
- Shutdown mode trip bypassed,
- Non-coincident NMS trip mode in effect (in NMS),
- NMS trip mode selection switch still in Non-coincident position, with Reactor Mode Switch in Run position (in NMS),
- Division in which channel A (B, C, or D) sensors are bypassed (four),
- Trip conditions in Channel A (B, C, or D) and Channel A (B, C, or D) sensors bypassed (four),
- Division 1 (2, 3, or 4) TLU out-of-service bypass (four),
- CRD accumulator-charging-header-pressure low trip bypass,
- Any CRD accumulator-charging-header trip with bypass switch still in Bypass position and the Reactor Mode Switch in Startup or Run mode,
- Auto-scram test switch in Test mode (manual trip of automatic logic) (four),
- TSV closure trip bypassed,
- TCV fast closure trip bypassed,
- MSIV closure trip bypassed,
- NMS SRNM trip bypassed in Run mode,
- Non-coincident NMS trip bypassed in Run mode,
- RPV water level high trip bypassed,
- Condenser pressure high trip bypassed,
- Special MSIV operational bypassed, and
- Power generation bus loss trip bypassed.

The above RPS displays and alarms meet the information display requirements of IEEE Std. 603, Section 5.8.

Outputs to Nonsafety-Related DCIS (N-DCIS) (Plant Computer Function): The PCF maintains loss of the tripped, bypassed, and reset conditions of the RPS instrument channels, divisions of logic, divisions of trip actuators, and scram logic circuitry as well as tripped and reset conditions of RPS automatic and manual trip systems through isolated gateway connections from the RPS to the N-DCIS. For conditions causing reactor trip the N-DCIS identifies the specific trip variable, the divisional channel identity, and the specific automatic or manual trip system. These signals also are provided to the sequence of events (SOE) function of the PCF.

Outputs to the Isolation Condenser System (ICS): Reactor Mode Switch status (that is, Run/NOT-Run indications) from the four divisions is provided by the RPS to the ICS to be used as automatic operation signal permissives or inhibits. Automatic operation signal permissives are generated whenever the Reactor Mode Switch is placed in the Run position, and automatic operation signal inhibits are generated whenever the Reactor Mode Switch is placed in any of its remaining three positions. The RPS also provides the loss of power generation bus voltage signal (Loss of Feed Water Flow) for automatic initiation of the ICS.

Outputs to the Plant Automation System (PAS): The RPS provides the Plant Automation System (PAS) with separate signals to indicate the position of the Reactor Mode Switch. The RPS also provides the auto scram signal from the OLU to the PAS.

Uninterruptible AC Power Supply: The AC electric power required by the four divisions of RPS logic is delivered from four pairs of physically separate and electrically independent uninterruptible safety-related 120 VAC buses. The power circuits of the "A" and "B" solenoids of the scram pilot valves are powered from two of the four divisional vital AC power supplies.

7.2.1.2.4.4 System Logic Architecture and Redundancy

The basic system architecture of the RPS ensures reliable processing of sensed plant variables by employing four independent trip logic systems in four separate divisions of safety protection equipment. Figure 7.2-1 illustrates the basic RPS functional arrangement.

Each divisional trip system processes the trip decisions of plant sensor inputs from the four divisions using two-out-of-four coincidence to confirm the final trip state for each variable in each division. Automatic reactor trip outputs from each system to the final actuators are also confirmed by two-out-of-four coincidence of division trip outputs. A separate and diverse manual trip method is provided in the form of two independent manual trip channels. Actuation of both manual trip systems is required for a full reactor scram. Availability is enhanced because any one division can be bypassed at one time to allow online repair without degrading operability. This satisfies the repair requirement of IEEE Std. 603, Section 5.10 while maintaining plant availability.

The RPS has built-in redundancy in its design. The RPS consists of four redundant divisions identical in design and independent in operation. Although each division constitutes a separate trip system, normally each division can make two-out-of-four trip decisions with or without a division of sensors being bypassed. There are four instrument channels provided for each process variable being monitored, one for each RPS division. Four sensors, one per division, are provided for each variable. When more than four sensors are required to monitor a variable the outputs of the sensors are combined into only four instrument channels. The logic in each division does not depend on absolute time of day and is asynchronous with respect to the other divisions. No division depends on the correct operation of another division. There is no combination of MCR-initiated bypasses that can unacceptably degrade the RPS.

7.2.1.3 Safety Evaluation

Table 7.1-1 identifies the RPS and the associated codes and standards applied, in accordance with the Standard Review Plan NUREG-0800. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.2.1.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The RPS conforms with these standards.

10 CFR 50.55a(h), Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: Safety-related systems are designed in conformance with Regulatory Guide (RG) 1.153 and IEEE Std. 603. Separation and isolation are preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6 and RG 1.75. The RPS is divisionalized and is designed with redundancy so that failure of any instrument does not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

10 CFR 50.34(f)(2)(v) [I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The RPS design of bypass and inoperable status indication conforms with these requirements and is consistent with the conformance of the RPS design with RG 1.47. It also conforms with the requirements of control and protection system interaction, as described in IEEE Std. 603, Sections 5.8 and 6.3.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for Instrumentation and Control (I&C) systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the RPS within the DCD documents conforms with this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.2.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 25, and 29:

- Conformance: The RPS is in conformance with the GDC identified above.

7.2.1.3.3 Staff Requirements Memorandum

Item II.Q of SECY-93-087, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The Reactor Trip (Protection) System design conforms with Item II.Q of SECY-93-087 NRC Branch Technical Position (BTP HICB-19) by the implementation of an additional Diverse Instrumentation and Control System as described in Section 7.8.

7.2.1.3.4 Regulatory Guides

RG 1.22 - Periodic Testing of Protection System Actuation Functions - This includes conformance with BTP HICB-8:

- Conformance: The system is capable of being tested, from sensor device to final actuator device, during plant operation. The tests must be performed in overlapping stages so an actual reactor scram would not occur as a result of the testing. Note that IEEE Std. 279 is withdrawn. Thus, the portions of the protection systems subject to periodic testing are designed in accordance with IEEE Std. 603, Sections 5.7 and 6.5.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems**:**

- Conformance: Automatic indication that a system is out of service is provided in the MCR (IEEE Std. 603, Section 5.8). Indicators show which part of a system is not operable and which division is bypassed.

  Annunciator test switches are provided in the MCR.

  Individual indicators are arranged together in the MCR to indicate which function of the system is out of service, bypassed, or otherwise inoperable. These automatic indicators remain available, and cannot be cleared until the function is operable (IEEE Std. 603, Sections 5.2 and 5.8).

  A manual switch or push button is provided for manual bypass actuation, which annunciates out-of-service conditions (IEEE Std. 603, Section 5.8).

  These display provisions serve to supplement administrative controls and aid the operator in assessing the availability of component and system-level protective actions (IEEE Std. 603, Section 5.8). These displays do not perform a safety-related function (IEEE Std. 603, Section 5.7).

  System out-of-service alarm circuits are electrically isolated from the plant safety-related systems to prevent adverse effects (IEEE Std. 603, Section 5.7).

Testing is included on a periodic basis when equipment associated with the display is tested.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems:

- Conformance: Compliance with Nuclear Regulatory Commission (NRC) RG 1.53 is satisfied by specifying, designing, and constructing the RPS to meet the single-failure criterion of IEEE Std. 603, Section 5.1, and IEEE Std. 379. Redundant sensors are used and the logic is arranged to ensure that a failure in a sensing element, decision logic, or an actuator does not prevent protective action. Separated channels are employed so a fault affecting one channel does not prevent the other channels from operating properly.

RG 1.62 - Manual Initiation of Protective Actions:

- Conformance: Means are provided for manual initiation of reactor scram through the use of two control switches and the Reactor Mode Switch (IEEE Std. 603, Section 6.2). Reactor scram is accomplished by operation of both pushbutton switches, or by placing the Reactor Mode Switch in the Shutdown position. These controls are located on the main control console.

  The common equipment required for initiation of both manual scram and automatic scram is limited to actuator load power sources, actuator loads, and cabling between the two. There is no shared trip or scram logic equipment for manual scram and automatic scram (IEEE Std. 603, Sections 5.6 and 6.2). No single failure in the manual, automatic, or common portions of the protection system would prevent initiation of reactor scram by manual or automatic means.

  Manual initiation of reactor scram, once initiated, goes to completion as required by IEEE Std. 603, Section 5.2.

RG 1.75 - Physical Independence of Electric Systems:

- Conformance: The RPS complies with the criteria set forth in IEEE Std. 603, Section 5.6, and RG 1.75, which endorses IEEE Std. 384. Safety-related circuits and safety-related associated circuits are identified and separated from redundant and nonsafety-related circuits. Isolation devices are provided where an interface exists between redundant safety-related divisions and between safety-related or safety-related associated circuits and nonsafety-related circuits. See chapter 8.0 Subsection 8.3.1.4.1 for RPS separation requirements.

RG 1.105 - Setpoints for Safety-Related Instrumentation:

- Conformance: The RPS initiation setpoints are consistent with this guide. A licensing topical report "General Electric Instrument Setpoint Methodology" (Reference 7.2-1) provides a detailed description of this methodology.

RG 1.118 - Periodic Testing of Electric Power and Protection System:

- Conformance: The RPS complies with RG 1.118 as amplified in IEEE Std. 338. The RPS is designed so its individual elements can periodically and independently be tested to demonstrate system reliability is being maintained. Safety-related RPS equipment allows for inspection and testing during periodic shutdowns and refueling.

RG 1.152 - Criteria for Digital Computers in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS complies with this RG. The hardware and software for the RPS function and other safety-related systems are developed in compliance with this RG, which endorses IEEE Std. 7-4.3.2. The structured development plan for the RPS includes conformance with all software standards referenced in IEEE Std. 7-4.3.2. Hardware and software are integrated into a final assembly validated by testing against input requirements.

RG 1.153 - Criteria for Safety Systems:

- Conformance: The configuration of RPS and other safety-related systems regarding independence, separation, and the single-failure criterion conforms with the requirements of this RG, which endorses IEEE Std. 603.

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

- Conformance: The RPS design conforms with the RG identified.

RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms with the RG identified.

RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms with the RG identified.

RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms with the RG identified.

RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms with the RG identified.

RG 1.173 - Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms with the RG identified.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The RPS design conforms with the RG identified.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The RPS design conforms with the RG identified.

7.2.1.3.5 Branch Technical Positions

BTP HICB-3: Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service:

- Conformance: There is no reactor coolant pump, so this BTP does not apply. .

BTP HICB-8: Guidance on Application of RG 1.22:

- Conformance: The RPS design conforms with this BTP.

BTP HICB-9: Guidance on Requirements for RPS Anticipatory Trips:

- Conformance: Hardware used to provide trip signals in the RPS is designed in accordance with IEEE Std. 603, Section 5.4 and is considered safety-related and meets the design requirements of this BTP.

BTP HICB-11: Guidance on Application and Qualification of Isolation Devices:

- Conformance: The RPS design conforms with this position. The RPS logic controllers use optical CIM and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

  Certain diverse and hardwired portions of RPS may use coil-to-contact isolation of relays or contactors. This is acceptable according to the BTP when the application is analyzed or tested per the guidelines of RG 1.75 and RG 1.153.

BTP HICB-12: Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The RPS design conforms with this position. The nominal setpoints are calculated based on the GEH instrument setpoint methodology (Reference 7.2-1). The setpoints are established based on instrument accuracy, calibration capability, and estimated design drift allowance data, and are within the instrument best accuracy range.

  The digital RPS trip setpoints do not drift and are reported to the N-DCIS as alarmed for any change. The analog-to-digital converters are self-calibrating, and the RPS uses self-diagnostics, all of which are reported to the N-DCIS through isolated gateways. It is expected that all of the variability in the parameter channel will be attributable to the field sensor. The established setpoints provide margin to fulfill both safety requirements and plant availability objectives.

BTP HICB-13: Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors:

- Conformance: The RPS uses sensor input for suppression pool temperature monitoring, which is based on thermocouple-type temperature sensors so this BTP does not apply.

BTP HICB-14: Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Safety Systems:

- Conformance: Development of software for the safety system functions within RPS conforms with the guidance of this BTP. Discussion of software development is included in the LTRs "ESBWR I&C Software Management Plan," NEDO-33226, NEDE-33226P, and "ESBWR I&C Software Quality Assurance Plan," NEDO-33245, NEDE-33245P. (References 7.2-3 and 7.2-4.) Safety-related software (to be embedded in the memory of the RPS controllers) is developed according to a structured plan as described in References 7.2-3 and 7.2-4. These plans follow the software life cycle process described in the BTP.

BTP HICB-16: Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: This BTP is applicable to all sections of the DCD. The RPS Section content conforms with this BTP.

BTP HICB-17: Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The RPS controllers conform with this BTP. Discussions on self-test and surveillance tests of RPS are provided in Subsection 7.2.1.4.

BTP HICB-18: Guidance on Use of Programmable Logic Controllers in Digital Computer-based Instrumentation and Control Systems:

- Conformance: Any portions of RPS design using commercial grade programmable logic controllers (PLCs) for safety-related functions conform with this BTP (and with BTPs 14, 17, and 21). Such PLCs are qualified to a level commensurate with safety-related system requirements.

BTP HICB-19: Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (Item II.Q of SECY-93-087):

- Conformance: The Reactor Trip (Protection) System designs conform with this BTP by implementation of an additional diverse instrumentation and control system described in Section 7.8 as the DPS.

BTP HICB-21: Guidance on Evaluation of Digital System Architecture and Real-Time Performance:

- Conformance: The real-time performance of RPS in meeting the requirements for safety-related system trip and initiation response conforms with this BTP. The real-time performance of the safety-related control system is deterministic based on the Q-DCIS

internal and external communication system design and the RPS controller design. Timing signals are neither exchanged between divisions of independent equipment nor between controllers within a division.

7.2.1.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for Chapter 7 and with Table 7.1-1, 10CFR50.34(f)(2)(v)(I.D.3) applies to the RPS and is addressed in section 7.2.1.3.1. TMI action plan requirements are generally addressed in Table 1A-1 of Tier 2, Chapter 1, Appendix 1A.

7.2.1.4 Testing and Inspection Requirements

7.2.1.4.1 System Testing: Operational Verifiability

The RPS is designed so its individual operating elements are tested periodically and independently to demonstrate that RPS reliability is maintained (IEEE Std. 603, Section 5.7 and 6.5).

The RPS design and the design of other systems providing the RPS with instrument channel inputs permit verifying the operational availability of each input sensor used by the RPS with a high degree of confidence even during reactor operation. Channel checks are continuously performed by the PCF.

The instrument channels are calibrated periodically and adjusted to verify that necessary precision and accuracy is being maintained. Such periodic checking and testing during plant operation is possible without loss of scram capability and without causing an inadvertent scram.

Safety-related RPS equipment is designed to allow inspection and testing during periodic shutdowns of the nuclear reactor and during refueling shutdowns.

7.2.1.4.2 Surveillance Testing and In-Service Inspection

The RPS equipment testing includes the following:

- Preoperational, startup and refueling/outage inspection testing; and
- In-service and operational surveillance testing.

7.2.1.4.3 Surveillance Testing

The RPS is designed to permit testing of an emergency reactor shutdown by methods simulating actual plant operation and duplicating, as closely as possible, the performance of protective actions even during reactor operation. These test methods support in-service verification of scram capability with high reliability. To the extent practical, the RPS components and testing strategies are designed so identifiable failures are detectable. Test methods are designed to facilitate recognition and location of malfunctioning component so they may be replaced, adjusted, or repaired.

In-service testing of the RPS is performed periodically to verify operability during normal plant operation and to ensure that each tested channel can perform its intended design function. The surveillance tests include: (a) instrument channel checks, (b) functional tests, (c)verification of proper sensor and channel calibration,(d) verification of applicable functions in the division of trip logic and division of actuators, and (e) response time tests.

7.2.1.5 Instrumentation and Control Requirements

7.2.1.5.1 Automatic Scram Variables

Refer to Subsection 7.2.1.2.4.2 for discussions of the automatic scram initiating circuits and the systems applying to them.

7.2.1.5.2 Automatic and Manual Bypass of Selected Scram Functions

7.2.1.5.2.1 Operational Bypasses

Manual or automatic bypass (take out of service) of certain scram functions permits the selection of suitable plant protection conditions during different conditions of reactor operation (IEEE Std. 603, Sections 6.6 and 7.4). These RPS operational bypasses inhibit actuation of those scram functions not required for a specific state of reactor operation.

The conditions of plant operation requiring automatic or manual bypass of certain reactor trip functions are described below:

- Main steam TSV closure and steam governing TCV fast closure trip bypasses**:** These permit continued reactor operation at low-power levels when the TSVs or TCVs are closed. The main steam TSV closure and the steam governing TCV fast closure scram trip functions are automatically bypassed when the APRM simulated thermal power of the NMS is below 40% of the rated thermal power output.

  The TSV closure and TCV fast closure trips are automatically bypassed if a sufficient number of the bypass valves are opened as indicated by their 10% position sensors with a preset time delay after the initiation of the reactor trip signal caused by the TCV fast closure or TSV closure to inhibit reactor trip. The NMS system provides the RPS with an analog simulated thermal power signal used to determine both the low-power bypass and the required number of bypass valves needed to open for a post turbine trip or for full load rejection conditions. The low-power bypass is automatically removed and both scram trip functions are enabled at a reactor power level above the bypass setpoint. The bypass permits the RPS to remain in its normal energized state under the specified conditions. This bypass condition is alarmed in the MCR.

- CRD HCU accumulator charging header low-pressure bypass**:** This bypass is allowed only when the Reactor Mode Switch is in either the Shutdown or Refuel position. If a bypass of a scram trip is required for CRD accumulator charging header low-pressure after a scram has occurred (indicated operational bypass), four administratively-controlled trip bypass switches in the MCR permit scram reset.

When the reactor is in the shutdown or refuel mode the low CRD HCU accumulator charging header pressure trip can be bypassed manually in each division of trip logic by separate, manual CRD HCU accumulator charging header pressure trip bypass switches. Control of this bypass is achieved through administrative means using bypass switches. This bypass allows RPS reset after a scram, while CRD charging header pressure is below the trip setpoint. The low charging water pressure condition would persist until the scram valves are re-closed. Each division of trip logic sends a separate rod withdrawal block signal to the RCIS when this bypass exists in the division. This operational bypass condition is alarmed in the MCR.

The bypass is automatically removed whenever the Reactor Mode Switch is put in either the Startup or Run mode, regardless of whether the CRD charging pressure bypass switches are in the bypass position. However, a separate alarm would result in the MCR if any of the bypass switches were left in the bypass position when the Reactor Mode Switch is in either the Startup or Run mode.

- MSIV closure for main steam isolation valve bypass (indicated operational bypass)**:** The scram trip for MSIV closure is automatically bypassed in each division whenever the Reactor Mode Switch is in the Shutdown, Refuel, or Startup position - with reactor pressure in the associated sensor channel less than a predetermined setpoint. This bypass condition is alarmed in the MCR and permits plant operation when the MSIVs are closed during low-power operation. The bypass is automatically removed if the Reactor Mode Switch is moved to the Run position. This bypass permits the RPS to be placed in its normal energized state for operation at low-power levels with the MSIVs either closed or not fully open.

- Special MSIV operational bypass (indicated operational bypass): Four manually-operated bypass switches are made available in the MCR to permit the bypass of trip signals from closed MSIVs on any one of the four main steam lines. This bypass permits continued reactor operation at reduced reactor power and steam flow when one steam line must be isolated for a prolonged period of time. This operational bypass is alarmed in the MCR.

- Loss of power generation bus bypass (indicated operational bypass): The Loss of Power Generation Bus (Loss of Feedwater Flow) scram trip function is automatically bypassed whenever the Reactor Mode Switch is in the Shutdown, Refuel, or Startup position. This bypass condition is alarmed in the MCR and is automatically removed if the Reactor Mode Switch is moved to the Run position.

- Reactor Mode Switch in Shutdown position bypass (indicated operational bypass): The RPS scram trip caused by the Reactor Mode Switch being placed in the Shutdown position is automatically bypassed after a time delay of approximately 10 seconds. This operational bypass condition permits resetting of the trip actuators and re-energization of the scram pilot valve solenoids and is alarmed in the MCR.

- NMS SRNM scram trip functions in Run mode bypass: Whenever the Reactor Mode Switch is in the Run mode, SRNM reactor scram trip functions are automatically bypassed. However, this bypass is not alarmed because it is the normal condition in the

Run mode. This bypass condition is indicated in the MCR. The SRNM rod block functions also are disabled when the Reactor Mode Switch is in the Run position.

- Non-coincident NMS scram trips in Run mode bypass: Whenever the Reactor Mode Switch is in the Run position, and the coincident/non-coincident NMS trip remains in the Non-coincident position, the non-coincident NMS scram trip functions are automatically disabled (bypassed). This logic is an NMS function.

  The non-coincident NMS trip function is required during initial fuel loading and subsequent refueling operations. During such operations the Reactor Mode Switch is in the Refuel position (or for certain testing conditions, in the Shutdown or Startup positions). A non-coincident NMS trip will occur in each division of trip logic (when any single SRNM trip signal is present in the NMS) if the coincident/non-coincident manual switch in the division is in the non-coincident position. This logic is an NMS function.

  The non-coincident NMS trip function is automatically removed when the Reactor Mode Switch is in the Run position. If the coincident/non-coincident NMS trip selection switch is in the Non-coincident position when the Reactor Mode Switch is in the Run position, there is an alarm in the MCR. When the reactor is in Shutdown, Refuel, or Startup mode, the non-coincident NMS trip can be bypassed manually by a separate "non-coincident trip disable" switch. These logics are NMS functions.

- RPV water level high trip bypass (indicated operational bypass): The RPV water level high trip function is automatically bypassed whenever the Reactor Mode Switch is the Shutdown, Refuel, or Startup position. This bypass condition is alarmed in the MCR and is automatically removed if the Reactor Mode Switch is moved to the Run position.

- Condenser pressure high trip bypass (indicated operational bypass): The condenser pressure high trip function is automatically bypassed whenever the Reactor Mode Switch is in the Shutdown, Refuel, or Startup position. This bypass condition is alarmed in the MCR and is automatically removed if the Reactor Mode Switch is moved to the Run position.

- APRM, OPRM, and SRNM scram trips bypasses: These have manual bypass capabilities within the NMS, not the RPS.

7.2.1.5.2.2 Maintenance Bypasses

Manual bypass capability is provided to allow certain portions of RPS-related equipment to be taken out of service for maintenance, repair, or replacement (IEEE Std. 603, Sections 6.7 and 7.5). Maintenance bypasses may reduce the degree of redundancy of RPS channels but do not affect or eliminate any scram function. Protective functions are available while any RPS equipment is in maintenance bypass. Except where indicated otherwise, any maintenance bypass generates a status alarm at the MCR operator's console.

The following maintenance bypasses are provided**:**

- Detector inputs (division of channel sensors scram trip) bypass (alarmed maintenance bypass): A manually operated bypass switch with interlock capability (for example, a

joystick-type switch) is installed in the MCR to bypass (take out of service) the division of channel sensors trip of one RPS division at a time. Once a bypass of one sensor channel has been established, bypasses of any of the remaining three sensor channels are inhibited. Whenever a division of channel sensors bypass switch is placed in the bypass position, there is an alarm in the MCR indicating the bypassed channel sensor division. The effect of the channel of sensors bypass is to convert the two-out-of-four trip to two-out-of-three trip logic. A channel of sensors bypass in any channel bypasses all trip-initiating input signals from the bypass division at the DTM trip input to the TLU. Bypassing a division of sensors allows each of the four divisions to determine the two-out-of-three trip. Loss of communication with a bypass switch is interpreted as a "no bypass" signal.

This bypass permits any one of the safety-related RPS components of the input sensor channels of one division to be repaired, replaced, or maintained off-line.

- TLU output (division-out-of-service scram trip) bypass (alarmed maintenance bypass): A manually-operated bypass switch with interlock capability (for example, a joystick-type switch) is installed in the MCR to bypass (redundant) the RPS trip output logic of one RPS electrical division at a time. This bypass is effective at the TLU trip input to the OLU and permits the RPS TLU of the associated division to be repaired, replaced, or maintained off-line. Loss of communication with the bypass switch is interpreted as a "no bypass" signal.

  The interlock ensures that the output signals of only one TLU (of one division) can be bypassed at any one time. Once a bypass of one division of trip logic has been established, bypasses of any of the remaining three division trip logics are inhibited. When a division-out-of-service bypass switch is placed in the bypass position, there is an alarm in the MCR indicating which division is out of service. With a division-out-of-service bypass in effect, the operator still is able manually to trip that division.

- The division-of-channel-sensors maintenance bypass function and the division-out-of-service maintenance bypass function are independent. Thus, one division of channel sensors may be bypassed (taken out of service at the sensor channels level) and, simultaneously, the same division or any other division may be taken out of service at the RPS trip system level. In all cases, the RPS system remains able to trip the reactor if any two (or more) un-bypassed parameters exceed their trip values.

7.2.1.5.3 Requirements for Manual Controls

Operator action by means of manual controls is limited to:

- Initiation of scram by manual scram switches,
- Reactor Mode Switch operation (results in scram if placed in the Shutdown position),
- Reset of automatic trip systems after trip input signals clear,
- Reset of manual trip systems (preferably after reset of the automatic trip systems),

- Manual bypasses for conditions that are specifically permitted, and
- Manual initiation of selected trip systems or trip actuators using trip logic test switches.

7.2.1.5.4 Reactor Mode Switch

A multi-function, multi-bank, control switch placed on the main control console provides mode selection for the necessary interlocks associated with the various plant modes: Shutdown, Refuel, Startup, and Run. This Reactor Mode Switch provides both electrical and physical separation between the components associated with each of the four separate divisions. The mode switch positions and their related bypass and trip/reset functions are as follows:

- Shutdown Position:
  - Initiates a reactor scram,
  - Enables NMS non-coincident trips,
  - Enables a manual CRD charging pressure trip bypass,
  - Enables automatic bypass of the TCV fast-closure trip,
  - Enables automatic bypass of the TSV closure trip,
  - Enables automatic bypass of the MSIV closure trip, and
  - Enables automatic bypass of the loss-of-power generation bus trip.
- Refuel Position:
  - Enables NMS non-coincident trips,
  - Enables the manual CRD charging pressure trip bypass,
  - Enables automatic bypass of the TCV fast-closure trip,
  - Enables automatic bypass of the TSV closure trip,
  - Enables automatic bypass of the MSIV closure trip, and
  - Enables automatic bypass of the Power Generation Bus Loss (Loss of Feedwater Flow) trip.
- Startup Position:
  - Enables NMS non-coincident trips,
  - Disables the manual CRD charging pressure trip bypass,
  - Enables the automatic bypass of the MSIV closure trip,
  - Enables automatic bypass of the TCV fast-closure trip,

  - Enables automatic bypass of the TSV closure trip, and
  - Enables automatic bypass of the loss-of-power generation bus trip.

- Run Position:
  - Disables all trip bypasses enabled by any of the other three modes, and
  - Enables automatic bypass of the NMS SRNM trip.

7.2.1.5.5 Manual Scram Switches

Two manual scram switches permit initiation of a scram, independent of conditions within other RPS equipment (sensor channels, divisions of trip logic, or divisions of trip actuators). Each manual scram switch is associated with one of the two divisions of actuator load power. Both manual scram switches are located on the main control console and do not require any microprocessor functionality; duplicate switches are included in the RSS panels.

7.2.1.5.6 Manual Divisional Trip Switches

Each of the four RPS automatic trip systems has manual trip capability provided by four divisional trip switches located in positions easily accessible for optional use by the plant operator. Each switch, when momentarily put into its trip position, trips the actuators that normally would be tripped by a scram condition for that division. Note that momentarily operating any two of the four manual divisional trip switches results in a full reactor scram.

7.2.1.5.7 Trip Reset Switches

Up to five trip-reset switches will reset any of the four automatic and two manual-scram trip systems that may have been tripped and sealed-in, as follows:

One trip reset switch resets both manual trip systems. The switch circuitry staggers the re-energization of the four groups of scram pilot valve solenoids so only two groups of “A” and “B” solenoids are re-energized simultaneously.

Four separate switches comprise the trip-reset function for resetting the sealed-in, automatic trip logic outputs in the four divisions. Thus, physical separation of the four electrical divisions is maintained.

7.2.1.5.8 Operational Bypass Switches

Requirements for operational bypass switches for RPS safety-related functions are addressed in Subsection 7.2.1.5.2.1. Operational bypass switches are under administrative control.

7.2.1.5.9 Reactor Mode Switch-In Shutdown Scram Bypass Switches

Two manual control switches are used to bypass the scram signal when moving the Reactor Mode Switch to its shutdown position. This bypass only would be permitted during an outage condition when the reactor already is shutdown.

7.2.1.5.10 Maintenance Bypass Switches

Requirements for RPS-related maintenance bypass switches are addressed in Subsection 7.2.1.5.2.2. The following maintenance bypasses are provided:

- Four division-of-channel-sensor maintenance bypass switches; and
- Four division-out-of-service maintenance bypass switches.

7.2.1.5.11 Test Switches

Test switches to aid in surveillance testing during reactor operations are provided in the RPS design.

7.2.2 Neutron Monitoring System

The NMS monitors reactor core thermal neutron flux from the startup source range to beyond rated power and provides trip signals initiating reactor scrams under excessive neutron flux or excessive rates of change in neutron flux (short period) conditions.

7.2.2.1 System Design Bases

The NMS comprises the following subsystems:

- Startup Range Neutron Monitor (SRNM),
- Power Range Neutron Monitor (PRNM),
- Automatic Fixed In-Core Probe (AFIP), and
- Multi-Channel Rod Block Monitor (MRBM)

The PRNM subsystem includes the Local Power Range Monitor (LPRM), APRM functions, and the OPRM.

The SRNM and PRNM subsystems are safety-related and are discussed below. The nonsafety-related AFIP Subsystem and the MRBM are addressed in Subsection 7.7.6. The application of this non-safety to safety interface is described in detail in Reference 7.2-2. This Topical Report addresses the CIM function, communication data link, data flow, and isolation requirements of IEEE Std. 603. The CIM has a two-way fiber optic communication data link and provides electrical isolation when passing data from non-safety related subsystems to safety-related systems.

7.2.2.1.1 Startup Range Neutron Monitor Subsystem

7.2.2.1.1.1 Trip Functions

The SRNM scram trip functions are discussed in Subsection 7.2.1.2.4.2, and rod block trip functions are discussed in Subsection 7.7.2.2. The SRNM channels also provide trip bypass.

The trip setpoints are adjustable. The SRNM trip functions are shown in Table 7.2-2 (IEEE Std. 603, Section 6.8). A short period signal (the period withdrawal permissive) inhibits continuous control rod withdrawal, thereby avoiding a reactor scram (due to the short reactor period caused by excessive rod withdrawal).

- The trip signals provided in the SRNM design are shown in Table 7.2-3.
- SRNM trips are active only when the Reactor Mode Switch is not in the Run position. When the NMS Coincidence/Non-Coincidence switch is in the Non-Coincidence position any one of the SRNM can generate trips. When the Reactor Mode Switch is in the Run position, the NMS trip is in the coincidence mode. For each division, the three SRNM scram trip signals are combined to form a divisional SRNM trip signal and then combined with the divisional APRM trip signal before being sent to the RPS.
- Trips dependent upon signal magnitude have setpoints adjustable in the instrument range.
- The period trip circuit compares the amplified and delayed neutron flux signal with its original signal and provides trips and/or alarms if the original signal exceeds the delayed one. The period alarm and scram setpoints are built-in through the period trip circuit or software algorithm.
- A short-period warning signal (Period Withdrawal Permissive) is provided to inhibit rod withdrawal to avoid an inadvertent scram due to excessive rod withdrawal.
- An SRNM interlock signal “ATWS Permissive” is established and sent to the Anticipated Transients Without Scram and Standby Liquid Control (ATWS/SLC) logic as a permissive signal to allow the initiation of liquid boron injection by the SLC system.
- The period trip is active except below a fixed power-level of approximately (1E-4%) of rated power. This approximately corresponds with the upper limit of the SRNM counting range.
- An instrument inoperative alarm is provided to signal that an SRNM channel is out of service.
- An SRNM channel is considered inoperative if any of the following conditions occur. Its Calibrate-Operate switch is not in the Operate mode, and
  - Any interlock in the channel is open,
  - The unit self-test function detects failures, or
  - The detector polarizing voltage falls below a preset level.

7.2.2.1.1.2 Safety-Related Design Bases

The general safety-related functional requirements follow:

- The SRNM is designed as a safety-related system. The SRNM generates a high neutron flux trip signal or a short-period trip signal used to initiate a reactor scram in time to prevent fuel damage resulting from AOOs or infrequent events.
- The SRNM and its preamplifier are qualified to operate under design basis accident and abnormal environmental conditions.
- The independence and redundancy incorporated in the SRNM functional design are consistent with the safety-related design basis of the RPS.
- The system is designed to produce a safety-related permissive signal to the ATWS/SLC system logic.

The SRNM is designed as a safety-related subsystem generating trip signals to prevent fuel damage in the event of any abnormal reactivity insertion transients (while operating in the startup power range). The trip signal results either from an excessively high neutron flux level or an excessive rate of neutron flux increase (a short reactor period).

The setpoints of these trips are such that under the worst reactivity insertion transients fuel integrity is always protected. Under the worst bypass condition, where one SRNM from each division is bypassed, the monitoring and protection functions still are adequately provided. The independence and redundancy requirements are incorporated into the design of the SRNM and are consistent with the safety-related design bases of the RPS.

7.2.2.1.1.3 Nonsafety-Related Design Bases

Neutron sources and neutron detectors together will provide a signal count rate of at least 3cps with the control rods fully inserted in a cold non-irradiated core.

The SRNM is designed to perform the following nonsafety-related functions:

- Indicate measurable increases in output signals, with the maximum permitted number of SRNM channels out of service during normal reactor startup operations.
- Provide continuous thermal neutron flux monitoring over a range of 10 decades (approximately 1×10^3 neutrons/cm^2/sec (nv) to 1.5×10^{13} nv).
- Provide continuous measurement of time rate-of-change of neutron flux (reactor period) over the range from approximately -100 seconds to (-) infinity and (+) infinity to approximately +10 seconds.
- Generate interlock signals to block control rod withdrawal if the neutron flux is greater-or-less-than a preset value, or if defined electronic failures occur.
- Generate rod block (inhibit control rod withdrawal) whenever the reactor period decreases below a preset value.
- The monitoring and alarming functions of the available monitors are not disabled upon the loss of single power bus.

7.2.2.1.2 Local Power Range Monitor

7.2.2.1.2.1 Safety-Related Design Bases

The general safety-related functional requirements are:

- A sufficient overall number of LPRM signals are provided to fulfill the APRM safety-related design bases.
- The LPRM is designed as a safety-related system to fulfill the APRM safety-related design bases.
- The LPRM is qualified to operate under design basis accidents and abnormal environmental conditions.

The LPRM is designed to monitor the local power level and to provide a sufficient number of LPRM signals to the APRM system to fulfill the safety-related design basis for the APRM. The LPRM itself has no safety-related design basis. However, it is qualified to safety-related standards.

7.2.2.1.2.2 Nonsafety-Related Design Bases

The LPRM performs the following nonsafety-related functions:

- Provides signals to the APRM that are proportional to the local neutron flux at various locations within the reactor core.
- Provides signals to alarm high or low local thermal neutron flux.
- Provides signals proportional to the local neutron flux to drive indicators and displays, and for the PCF used for operator evaluation of power distribution, etc.
- Provides signals proportional to the local neutron flux for use by other interface systems such as the RC&IS for the rod block monitoring function.

7.2.2.1.3 Average Power Range Monitor

7.2.2.1.3.1 Safety-Related Design Bases

The general safety-related functional requirements are:

- The APRM is designed to safety-related standards. The general functional requirements specify that, under the worst permitted input LPRM bypass conditions, the APRM is capable of generating a timely trip signal in response to excessive average neutron flux increases to prevent fuel damage. The independence and redundancy incorporated into the design of the APRM is consistent with the safety-related design bases of the RPS.
- The system is designed to produce a safety-related simulated thermal power signal to RPS to allow that system to support reactor power scram bypass requirements.

- The APRM provides information for monitoring the average power level of the reactor core in the power range. The APRM is capable of generating a timely trip signal to scram the reactor in response to excessive and unacceptable neutron flux increase to prevent fuel damage. Such a trip signal includes a trip from the simulated thermal power signal, representing the APRM flux signal through a time constant representing the actual fuel time constant. The resulting simulated thermal power signal accurately represents core thermal (as opposed to neutron flux) power and the heat flux through the fuel.

- Scram functions are assured when the minimum LPRM input requirement to the APRM is fulfilled. If this requirement cannot be met an inoperative channel trip signal is generated. Independence and redundancy requirements are incorporated into the design and are consistent with the safety-related design basis of the RPS.

7.2.2.1.3.2 Nonsafety-Related Design Bases

The APRM performs the following nonsafety-related functions:

- Provides continuous indication of average reactor power (neutron flux) from 1% to 125% of rated reactor power, which overlaps with the SRNM range. Such signals are made available as core power information to other interfacing systems.

- Provides interlock signals for blocking further rod withdrawal to avoid an unnecessary scram actuation.

- Provides a simulated thermal power signal derived from each APRM channel, which approximates the heat dynamic effects of the fuel.

- Provides a continuously available LPRM/APRM display for detection of any neutron flux oscillation in the reactor core.

7.2.2.1.4 Oscillation Power Range Monitor

7.2.2.1.4.1 Safety-Related Design Bases

The general safety-related functional requirements are:

- The OPRM is designed to safety-related standards. The general functional requirements specify that, under the worst permitted input LPRM bypass conditions, the OPRM is capable of generating a timely trip signal in response to core neutron flux oscillation conditions and thermal-hydraulic instability to prevent violation of the thermal safety limit. The independence and redundancy incorporated into the design of the OPRM is consistent with the safety-related design bases of the RPS.

- The OPRM provides monitoring and protection function for core-regional and core-wide neutron flux oscillation monitoring using the LPRM signals sent to the associated APRM channel in which the OPRM channel resides. The OPRM is capable of generating a timely trip signal to scram the reactor in response to excessive and unacceptable neutron flux oscillation to prevent fuel damage. Scram functions are ensured when the minimum

LPRM input requirement to the OPRM is fulfilled. Independence and redundancy requirements are incorporated into the design and are consistent with the safety-related design basis of the RPS.

7.2.2.1.4.2 Nonsafety-Related Design Bases

The OPRM provides core flux oscillation information for the plant computer and MCR display, and alarms when the OPRM is inoperative or has an insufficient number of LPRM inputs.

7.2.2.2 System Description

The safety-related functions of the NMS consist of the SRNM and PRNM Subsystems. (The LPRM, APRM, and OPRM collectively are called the PRNM Subsystem.) The nonsafety-related Automated Fixed In-Core Probe (AFIP) Subsystem of the NMS and the Multi-channel Rod Block Monitor (MRBM) are discussed in Subsection 7.7.6.

7.2.2.2.1 System Identification

The purpose of the NMS is to monitor reactor power generation and, for the safety-related aspects of the NMS, to provide trip signals to the RPS initiating a reactor scram whenever there is an excessive neutron flux (and thermal power) level, excessive neutron flux oscillation, or excessive rate of change in neutron flux (short period). In addition, it provides power information to the plant computer and the Automated Thermal Limit Monitor (ATLM) in the RC&IS, for control of the rod block function. The operating range of the various detectors is shown in Figure 7.2-3. A functional block diagram (Figure 7.2-4) shows a typical SRNM division. A functional block diagram (Figure 7.2-5) shows a typical PRNM division.

7.2.2.2.2 Neutron Flux Monitoring Ranges System Safety Classification

The SRNM, LPRM, APRM, and OPRM perform safety-related functions and are designed to meet the applicable design criteria. The system classification is shown in Section 3.2. The safety-related subsystems are qualified in accordance with Sections 3.10 and 3.11.

The AFIP Subsystem of the NMS and the MRBM are nonsafety-related and are discussed within Subsection 7.7.6.

7.2.2.2.3 Power Sources

The safety-related NMS equipment is powered by redundant 120 VAC divisional safety-related Uninterruptible Power Sources (UPS). The power sources for each system are discussed in the individual subsystem descriptions.

7.2.2.2.4 Startup Range Neutron Monitor Subsystem

7.2.2.2.4.1 General Description

The SRNM monitors neutron flux from the source range (approximately 1×10^3 nv) to approximately 1.5×10^{13} nv. The SRNM subsystem has 12 SRNM channels, each having one fixed in-core regenerative fission chamber sensor.

7.2.2.2.4.2 Power Sources

SRNM channels are powered as listed below:

- A, E, J: 120 VAC Div. 1 UPS
- B, F, K: 120 VAC Div. 2 UPS
- C, G, L: 120 VAC Div. 3 UPS
- D, H, M: 120 VAC Div. 4 UPS

Each SRNM cabinet is redundantly powered by two uninterruptible divisional 120 VAC power sources in the appropriate division; either source of power can support system operation.

7.2.2.2.4.3 Physical Arrangement

The 12 SRNM detectors are located at a fixed elevation about the mid-plane of the fuel region and are uniformly distributed throughout the core. The SRNM locations in the core, together with the neutron source locations, are shown in Figure 7.2-6. Each detector is contained within a pressure barrier dry tube inside the core with signal output exiting the bottom of the dry tube under-vessel. Detector cables are routed separately to the appropriate containment penetration according to divisional assignment. They are connected to their designated preamplifiers located in the respective divisional quadrants of the RB.

The SRNM preamplifier signals are transmitted to the SRNM digital processing equipment units, which provide algorithms for signal processing and calculations to provide neutron flux, power, period trip margin, and period. Additionally, they provide outputs for local and control console displays and recorders and to the PCF. The individual SRNM channel trips are combined to form a SRNM divisional trip in the NMS TLU function (as shown in Figure 7.2-4). This SRNM divisional trip is sent to the RPS through a safety-related network interface. (This is the logic in the Coincidence Mode. Further discussion of SRNM trip logic is included in Subsection 7.2.2.5.)

Alarm and trip outputs also are provided for both high flux and short period trip or alarm conditions. Such outputs include the instrument inoperative trip. The electronics for the SRNM and their designated bypass units are located in four separate cabinets, one in each of the four divisional RB quadrants, and in each of the CB divisional equipment room locations. The SRNM satisfies the IEEE Std. 603, Section 5.1 single-failure criterion stating the failure of any individual SRNM channel does not affect the protection function of the SRNM through channel bypasses discussed in Subsection 7.2.2.2.4.6 (with any three of the four divisions of safety-

related power available). It also satisfies the IEEE Std. 603, Section 5.6 independence requirement.

7.2.2.2.4.4 Signal Processing

Over the 10-decade power monitoring range two monitoring methods are used: (1) the counting method for the lower counting range (approximately 1×10^3 nv) to approximately 1×10^9 nv, and (2) the Campbelling technique Mean Square Voltage (MSV) for the higher range, from 1×10^8 nv to 1×10^{13} nv of neutron flux.

In the counting range, after pre-amplification, the discrete pulses produced by the sensors are applied to a discriminator. The discriminator, together with other digital noise-limiter features, separates the neutron pulses from gamma radiation and other noise pulses. The neutron pulses are counted. The reactor power is proportional to the count rate.

In the MSV range, where it is difficult to distinguish among the individual pulses, a DC voltage signal proportional to the mean square value of the input signal is produced. The reactor power is proportional to this mean square voltage. In the mid-range overlapping region, where both methods apply, the SRNM calculates a neutron flux value based on a weighted interpolation of the two flux values as calculated by each method. A continuous and smooth flux reading transfer is achieved in this manner. In addition, there is the calculation algorithm for the period-based trip circuitry generating a trip margin setpoint for the period trip protection function.

7.2.2.2.4.5 Trip Functions

The SRNM scram trip functions are discussed in Subsection 7.2.2.1.1, and rod block trip functions are discussed in Subsection 7.7.2.2. The SRNM channels also provide trip bypass. The trip setpoints are adjustable. The SRNM trips are shown in Table 7.2-2 (IEEE Std. 603, Section 6.8). A short period signal (the period withdrawal permissive) inhibits continuous control rod withdrawal to avoid a reactor scram (due to a shorter reactor period caused by excessive rod withdrawal).

7.2.2.2.4.6 Bypasses and Interlocks

The 12 SRNM channels are divided into four bypass groups. A controller allows only one SRNM at a time to be bypassed in each bypass group, allowing up to four SRNM channels to be bypassed at any one time. There is no additional SRNM bypass capability at the divisional level. However, it is possible to bypass all three SRNMs belonging to the same division. When this is required, a divisional bypass allows that division's NMS DTM to be bypassed. For SRNM calibration or repair, the bypass can be done for each individual channel separately through these SRNM bypasses without putting the whole division out of service. The SRNM subsystem satisfies the repair requirement of IEEE Std. 603, Section 5.10. Note that bypassing any of the SRNM sensors within a division does not affect the ability of the NMS to perform two-out-of-four trip determination using the trip decisions from the SRNM divisions (with any three of the four divisions of safety-related power available). The SRNM subsystem satisfies the IEEE Std. 603, Section 5.1 single-failure criterion.

The SRNM bypass switches are mounted on the MCR panel. Bypass functions for the SRNM and the APRM in the NMS are separate. There is no single NMS divisional bypass affecting both the SRNM and the APRM. No APRM bypass forces a SRNM bypass. The individual SRNM power signals are combined and averaged to form a divisional SRNM power signal. Also, all NMS bypass logic control functions are located within the NMS, not in the RPS.

The SRNM has several major interlock logics. The SRNM trip functions are in effect when the Reactor Mode Switch is not in the Run position. The SRNM upscale trip setpoint is lowered (IEEE Std. 603, Section 6.8) in the NMS Non-Coincidence mode (Table 7.2-2). The SRNM ATWS permissive signals are sent to the ATWS/SLC system to control initiation of SLC system boron injection and associated functions (such as feedwater runback).

7.2.2.2.4.7 Redundancy and Diversity

The signal outputs from the 12 SRNM channels are arranged so each of the four divisions includes a different set of designated SRNM channels covering different regions of the core. The SRNM monitoring and protection function is provided by an individual channel. Failure of an un-bypassed single SRNM channel causes an inoperative trip to only one of the four divisions, whereas a full scram requires divisional trips in two-out-of-four divisions within the NMS. Bypassing a single SRNM channel does not cause a trip output to the related SRNM division and does not prevent the remaining SRNM channels from performing their safety-related functions.

7.2.2.2.4.8 Environmental Considerations

The wiring, cables, and connectors located within the drywell are designed for continuous duty in the conditions described in Appendix 3H.

The SRNM instruments are designed to operate under the expected environmental conditions. Environmental qualification is discussed in Section 3.11. Additional information on equipment qualification with respect to environmental considerations is provided in the GEH Environmental Qualification program (Reference 7.1-2).

7.2.2.2.5 Local Power Range Monitor

7.2.2.2.5.1 General Description

The LPRM monitors local neutron flux in the power range. The LPRM provides input signals to the APRM (Subsection 7.2.2.2.6), the RC&IS (Subsection 7.7.2), and the PCF of the N-DCIS (Subsection 7.1.5).

7.2.2.2.5.2 Uninterruptible Power Supply

Alternating current power for the LPRM circuitry is supplied by four pairs of redundant divisional 120 VAC UPS buses corresponding to the four safety-related divisions. The cabinets can perform their functions with either of their redundant power sources. Each division supplies power to one-fourth of the detectors. Each LPRM detector is provided with a DC power supply,

housed in the designated divisional APRM instrument furnishing the detector polarizing potential.

7.2.2.2.5.3 Physical Arrangement

A single division of LPRMs consists of a total of 64 detectors - one detector from each LPRM assembly (from a total of 64 assemblies in the core). There is a total of 256 LPRM detectors in the core. Each assembly consists of four LPRM fission chamber detectors uniformly spaced at four axial positions in the fuel bundle vertical direction. The 64 assemblies are distributed uniformly throughout the whole core. Within the core, for each square fuel region of four-by-four fuel bundles, LPRM assemblies are located at the four corners.

The LPRM detector locations in the core are illustrated in Figure 7.2-7. The LPRM detector axial positions in the fuel bundle vertical direction are illustrated in Figure 7.2-8. The LPRM detector at the lowest position is designated LPRM A. Detectors above A are designated B and C, with the uppermost detector designated D.

The LPRM detector is a fission chamber with a polarizing potential of approximately 100 volts Direct Current (VDC). The four detectors comprising a detector assembly are contained in a common tube also housing the AFIP sensors (Subsection 7.7.6). The enclosing housing tube is perforated to promote coolant flow for detector cooling.

In addition, the LPRM assembly contains a set of two thermocouples mounted inside the lower portion of the assembly (at an elevation below the core plate). The thermocouple sensors provide core inlet temperature data to be used by the PCF of the N-DCIS for core flow determination using the heat balance method. A pair of thermocouple sensors is mounted on all 64 LPRM assemblies (at the same elevations). Figure 7.2-8 shows the relative elevations of the fixed in-core probe sensors and the thermocouples.

The LPRM cables are grouped by associated APRM trip channel under the reactor vessel and routed to the RB in conduit to maintain separation. The LPRMs provide inputs to each of the four APRM channels. The four APRM channels are mounted in separate bays with complete physical separation. This arrangement and wiring practice provides the required electrical isolation and physical separation to fulfill the independence requirement of IEEE Std. 603, Section 5.6.

7.2.2.2.5.4 Signal Processing

At the under-vessel pedestal region the LPRM detector outputs from the assembly are connected to respective coaxial cables routed through the containment penetrations and to the signal conditioning units in the RB. In the signal conditioning units the signals are processed, amplified, converted to digital data, and transmitted by fiber optic cable to the CB NMS cabinets located in the safety-related equipment rooms.

The amplified signal is proportional to the local neutron flux level. The LPRM signals are averaged and normalized to reactor power by the APRM logic, to produce an APRM signal (Refer to Subsection 7.2.2.2.6). Individual LPRM signals also are transmitted (with proper

electrical isolation) through dedicated interface units in the APRM from other systems such as the RC&IS and the PCF to provide local power information.

7.2.2.2.5.5 Trip Functions

The LPRM channels provide trip and status signals indicating when an LPRM is upscale, downscale, or bypassed.

7.2.2.2.5.6 Bypasses and Interlocks

Each LPRM channel may individually be bypassed. When the maximum allowed number of bypassed LPRMs for each APRM has been exceeded an inoperative trip is generated by the affected APRM channel.

7.2.2.2.5.7 Redundancy

The LPRM detectors are arranged in four divisional APRM channels with 64 LPRM detector signals in each. The redundancy criteria are met, ensuring (in the event of a single failure under permissible APRM bypass conditions) the safety-related protection function is performed as required (with any three of the four divisions of safety-related power available).

7.2.2.2.5.8 Environmental Considerations

The LPRM detector and detector assembly are designed to operate up to a gauge pressure of approximately 8.62 MPa (1250 psig) and at an ambient temperature of approximately 315°C (511°F). The wiring, cables, and connector located within the drywell are designed for continuous duty at drywell ambient conditions. The LPRMs are capable of functioning during and after design basis events, including earthquakes and anticipated operational occurrences (Refer to Sections 3.10 and 3.11). Additional information on equipment qualification with respect to environmental considerations is provided in the GEH Environmental Qualification program (Reference 7.1-2).

7.2.2.2.6 Average Power Range Monitor

7.2.2.2.6.1 General Description

The APRM performs a safety-related function. There are four APRM channels, one per division. Each APRM channel receives 64 LPRM signals as primary inputs (from the RB) through fiber optic cables. Each APRM channel then averages the inputs and normalizes the result to provide an APRM value corresponding to the average core thermal power signal. One APRM channel is associated with each division of the RPS.

7.2.2.2.6.2 Power Sources

APRM channels are powered as listed below:

- A: Redundant 120 VAC Div. 1 UPS,

- B: Redundant 120 VAC Div. 2 UPS,
- C: Redundant 120 VAC Div. 3 UPS, and
- D: Redundant 120 VAC Div. 4 UPS.

Either of the two redundant divisional power sources supports APRM operation. The bypass units and LPRM detectors associated with each APRM channel receive power from the same power sources as the APRM channel.

7.2.2.2.6.3 Physical Arrangement

The APRM subsystem consists of four independent and separate instrument channels. Each APRM channel receives 64 LPRM signal inputs. The assignment of individual LPRM sensors to each of the four APRM channels is performed ensuring an even and uniform selection of LPRM sensors from the whole core is allocated to each APRM channel. In this manner, the average value of the 64 LPRM signals from the entire core represents the average core power value. The LPRM signals within the APRM channel are averaged and normalized to form an average core power APRM signal. The LPRM assignment to APRM channels is shown in Figure 7.2-9.

7.2.2.2.6.4 Signal Conditioning

The APRM channel electronic equipment averages the output signals from 64 LPRM detectors to form an APRM signal for this channel. The averaging circuit automatically corrects for the number of un-bypassed LPRM input signals. The APRM channel electronics unit includes the capabilities for LPRM and APRM calibrations and diagnostics. The APRM has signal output interface units to send signals to other systems. A simplified PRNM block diagram is shown in Figure 7.2-5. Individual APRM channel trips are routed to the RPS directly. The APRM satisfies the IEEE Std. 603, Section 5.1 single-failure criterion, because the failure of any individual APRM channel does not affect the protection function of the APRM through channel bypasses, as discussed in Subsection 7.2.2.6.6 (with any three of the four divisions of safety-related power available). It also satisfies the IEEE Std. 603, Section 5.6, independence requirement, because the redundant portions of the NMS equipment are independent of (and physically separated from) each other, and the NMS equipment is separated from other systems.

7.2.2.2.6.5 Trip Function

The APRM scram trip function is discussed in Subsection 7.2.1.2.4.2. The APRM rod block trip function is discussed in Subsection 7.7.2.2. The APRM channels also provide trip and status signals indicating when an APRM channel is upscale, downscale, bypassed, or inoperative. The trip setpoints are adjustable. APRM system trips are summarized in Table 7.2-4.

7.2.2.2.6.6 Bypasses and Interlocks

One APRM channel out of four channels may be bypassed at any one time for repair during plant operation while maintaining the required APRM functions. This satisfies the repair requirement of IEEE Std. 603, Section 5.10. When one APRM channel is bypassed, the trip logic in the NMS

becomes two-out-of-three instead of two-out-of-four (with any three of the four divisions of safety-related power available).

The bypass of APRM channels is accomplished with a joystick-type switch having mutually exclusive positions. The APRM bypass switch is located on an MCR panel. Access to the panel and the switch is under administrative control. When a bypass is active, the input from the bypassed APRM/OPRM channel (APRM or OPRM trip function) will be bypassed by removing it from the vote. The remaining signals are voted with a two-out-of-three logic, thus retaining the ability to withstand a single-channel failure.

The final separate check of the signals, performed independently by each voter channel, ensures that no single-failure causes an inadvertent bypass. The bypass function uses physical means and independent logic to ensure that no more than one channel is bypassed at a given time.

There are no automatic bypasses for the APRM trip function. The APRM trip setpoint is automatically changed to a lower value (setdown) when the manually operated Reactor Mode Switch is not in the Run position. When any APRM (or OPRM) channel output is bypassed, the bypass is indicated on the plant operator's panel. The same channel bypass bypasses both the OPRM and APRM channels.

The APRM ATWS permissive signals are sent to the ATWS/SLC system as permissive signals for the ADS initiation inhibit function. The ATWS permissive value for ADS initiation is provided in Table 7.2-4.

7.2.2.2.6.7 Redundancy

Four independent channels of the APRM monitor neutron flux. Each channel is associated with one NMS division, with its optically isolated trip signal sent to the other three NMS divisions. The redundancy criteria are met ensuring (in the event of a single failure under permissible APRM bypass conditions) the safety-related protection function is performed as required (with any three of the four divisions of safety-related power available).

7.2.2.2.6.8 Environmental Considerations

Chapter 3 describes the APRM operating environments. The APRM is capable of functioning during and after the design basis events in which continued APRM operation is required (Sections 3.10 and 3.11). Additional information on equipment qualification with respect to environmental considerations is provided in the GEH Environmental Qualification program (Reference 7.1-2).

7.2.2.2.7 Oscillation Power Range Monitor

7.2.2.2.7.1 General Description

The OPRM consists of four independent safety-related channels. The OPRM channel uses the same set of LPRM signals used by the associated APRM channel in which the OPRM channel resides. Each OPRM receives identical LPRM signals from the corresponding APRM channel as

inputs and forms OPRM cells to monitor the neutron flux behavior in all regions of the core. Assignment of LPRMs to the four OPRM channels is shown in Figure 7.2-10.

The OPRM channel consists of OPRM cells formed by grouping LPRM inputs (maximum of four). The OPRM cell signal is the average of all grouped LPRM input signals and is used for detecting thermal hydraulic instability of the reactor core. The LPRM signals assigned to each cell are summed and averaged to provide an OPRM signal for that cell. The OPRM trip protection algorithm detects thermal hydraulic instability (flux oscillation with unacceptable amplitude and frequency) and provides a trip output if the trip setpoint is exceeded.

7.2.2.2.7.2 Power Sources

The OPRM function resides in the APRM equipment and is supplied with the same redundant APRM power.

7.2.2.2.7.3 Signal Conditioning

The OPRM function resides in its associated APRM channel equipment. The assignment of LPRMs to the four OPRM channels is shown in Figure 7.2-10. The OPRM channel consists of OPRM cells formed by grouping LPRM inputs. Each OPRM cell signal is the average of all grouped LPRM input signals for this cell and is used for detecting thermal hydraulic instability of the reactor core.

7.2.2.2.7.4 Trip Function

The OPRM trips are combined with the APRM trips of the same APRM channel and sent to the RPS. When there is an insufficient number of operating OPRM cells the OPRM function generates an alarm signifying an inoperative OPRM channel. If the number of operating LPRM inputs to an OPRM cell is less than the minimum required, the cell is considered to be inoperative. Similarly, the channel is inoperative if it does not have enough operating cells. Any cell can cause an OPRM channel alarm or trip condition.

The OPRM channel monitors OPRM cell signal responses and provides alarm and trip signals based on the oscillation detection algorithm to be defined in a detailed hardware and software design specification document. Any cell can cause an OPRM channel alarm or trip condition.

The OPRM channel trips are sent to the RPS. The OPRM function does not generate an inoperative trip but does generate an alarm signifying an inoperative OPRM channel when there is an insufficient number of operating OPRM cells. (An inoperative OPRM cell is a cell having an insufficient number of operating LPRM inputs).

A summary of OPRM trip functions is provided in Table 7.2-6.

7.2.2.2.7.5 Bypasses and Interlocks

The OPRM alarms and trips are bypassed in all reactor operation modes except Run and when operating below a preset power level. The OPRM bypass is controlled by the APRM channel in

which it resides. Bypass of the APRM channel also bypasses the OPRM trip function within this APRM channel.

7.2.2.2.7.6 Redundancy

The OPRM has the same redundancy design as the APRM. The redundancy criteria are met such that, in the event of a single failure under permissible APRM/OPRM bypass conditions, the safety-related protection function is performed as required (with any three of the four divisions of safety-related power available).

7.2.2.2.7.7 Environmental Considerations

The OPRM is subject to the same environmental considerations as the APRM.

7.2.2.3 Safety Evaluation

This evaluation covers the safety-related SRNM, LPRM, APRM, and OPRM functions of the NMS.

The evaluation of the trip inputs from the NMS to the RPS is discussed in Subsection 7.2.1.

The AFIP Subsystem and the MRBM are nonsafety-related subsystems of the NMS, and are evaluated in Subsection 7.7.6.

Table 7.1-1 identifies the NMS and the associated codes and standards applied, in accordance with the Standard Review Plan NUREG-0800. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.2.2.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The NMS conforms with these standards.

10 CFR 50.55a(h), "Protection and Safety Systems," compliance with ANS/IEEE Std. 603:

- Conformance: Safety-related systems are designed in conformance with RG 1.153 and IEEE Std. 603. Separation and isolation are preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6 and RG 1.75. The NMS is divisionalized and designed with redundancy so that failure of any instrument does not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

  There are 64 LPRM assemblies uniformly distributed in the core. There are four LPRM detectors within each LPRM assembly, equally spaced from near the bottom of the active fuel region to near the top of the active fuel region (Figure 7.2-8). The 256 detectors are assigned to four divisions comprising the four APRM channels. Any single LPRM detector is assigned to one APRM division. Each set of 64 LPRM detector signals is assigned to one APRM channel with these signals averaged and normalized to form an

APRM signal representing the average core power. Electrical and physical separation of the division is maintained and optimized to fulfill the safety-related system requirement.

With the four divisions redundancy requirements are met, because a scram signal still can be initiated with a postulated single failure of one APRM channel under allowable APRM bypass conditions.

Components used for the safety-related functions are qualified for the environments in which they are located. Additional information on NMS equipment qualification is included in Reference 7.2-2.

10 CFR 50.34(f)(2)(v) [I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The NMS design of bypass and inoperable status indication conforms with this requirement, consistent with conformance of the NMS design with RG 1.47. In addition, the design conforms with the requirements of control and protection system interaction as described in IEEE Std. 603, Sections 5.8 and 6.3.

  The 12 SRNM channels are divided into four divisions and are independently assigned to four bypass groups such that up to four SRNM channels may be bypassed at any one time while still providing the required monitoring and protection capability (with any three of the four divisions of safety-related power available).

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAAC are provided for I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the NMS within the DCD documents conforms with this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.:

7.2.2.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 25, and 29:

- Conformance: The NMS complies with these GDC.

7.2.2.3.3 Staff Requirements Memorandum

Item II.Q of SECY-93-087 (Defense Against Common-Mode Failures in Digital Instrument and Control Systems):

- Conformance: The NMS design, as part of the safety-related system, minimizes the likelihood of common mode failures, and conforms with this requirements by the implementation of additional Diverse Instrumentation and Control System capabilities, described in Section 7.8.

7.2.2.3.4 Regulatory Guides

RG 1.22 - Periodic Testing of Protection System Actuation Functions:

- Conformance: The NMS design conforms with the RG identified.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The NMS design conforms with the RG identified.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The NMS design conforms with the RG identified.

RG 1.75 - Physical Independence of Electric Systems:

- Conformance: The NMS design conforms with the RG identified. See chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for a discussion of how the design meets the requirements of RG 1.75.

RG 1.97 - Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident:

- Conformance: The NMS design conforms with the RG identified.

RG 1.105 - Instrument Setpoints for Safety-Related Systems:

- Conformance: The NMS design conforms with the RG identified.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems:

- Conformance: The NMS design conforms with the RG identified.

RG 1.152 - Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms with the RG identified.

RG 1.153 - Criteria for Power, Instrumentation and Control Portions of Safety Systems:

- Conformance: The NMS design conforms with the RG identified.

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

- Conformance: The NMS design conforms with the RG identified.

RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms with the RG identified.

RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms with the RG identified.

RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms with the RG identified.

RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms with the RG identified.

RG 1.173 - Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms with the RG identified.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The NMS design conforms with the RG identified.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The NMS design conforms with the RG identified.

7.2.2.3.5 Branch Technical Positions

BTP HICB-3 - Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service:

- Conformance: There is no reactor coolant pump, so this BTP does not apply.

BTP HICB-8 - Guidance for Application of RG 1.22:

- Conformance: The NMS design conforms with this BTP.

BTP HICB-10 - Guidance on Application of RG 1.97:

- Conformance: There are four divisional safety-related subsystems of the NMS. Each division is entirely redundant and identical in design. The divisions are independent of each other, and each is capable of providing indication of neutron flux for the required range. The NMS equipment is qualified to the requirements of IEEE Std. 323. Therefore, the NMS meets this BTP.

BTP HICP-11 - Guidance for Application and Qualification of Isolation Devices:

- Conformance: The NMS design conforms with this BTP position. The NMS equipment uses optical CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and non-safety related devices to meet the requirements of RG 1.75 and RG 1.153.

BTP HICB-12 - Guidance for Establishing and Maintaining Instrument Setpoints:

- Conformance: The analytical limits of the safety-related setpoints of the NMS are determined from safety analyses for each reactor fuel cycle to ensure the reactor core is protected from any rising neutron flux potentially exceeding these values. The nominal setpoints are calculated to be consistent with the GEH standard setpoint methodology (Reference 7.2-1), which conforms with RG 1.105. The setpoint margin calculated by this method also has considered additional uncertainties with the calibration interval. Therefore, the NMS meets this BTP.

  Most of the uncertainty associated with safety-related NMS trip setpoints is associated with the various neutron sensors because the digital electronics in the NMS do not drift, and the setpoints are monitored and alarmed by the PCF of N-DCIS.

BTP HICB-14 - Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Safety Systems:

- Conformance: Development of software for the safety-related system functions within NMS conforms with the guidance of this BTP as discussed in the LTRs "ESBWR I&C Software Management Plan," NEDO-33226, and "ESBWR I&C Software Quality Assurance Plan," NEDO-33245. (References 7.2-3 and 7.2-4.) Safety-related software to be embedded in the memory of the NMS controllers is developed according to a structured plan described in References 7.2-3 and 7.2-4. These plans follow the software life cycle process described in the BTP.

BTP HICB-16 - Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: This BTP is applicable to all sections of the DCD. The NMS section content conforms with this BTP.

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The safety-related subsystems of the NMS are designed to support the required periodic testing. (Refer to Subsection 7.2.2.4.) The NMS system equipment features a self-test design operating in all modes of plant operations. This self-test

function does not interfere with the safety-related functions of the system. The NMS design conforms with this BTP.

BTP HICB-18 - Guidance of Use of Programmable Logic Controllers in Digital Computer-based Instrumentation and Control Systems:

- Conformance: Any portions of the NMS design using commercial grade programmable logic controllers (PLCs) for safety-related functions conform with this BTP. The PLCs are qualified to a level commensurate with safety-related system requirements.

BTP HICB-19 - Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-based Instrumentation and Control Systems:

- Conformance: The NMS design conforms with this BTP by implementation of an additional diverse instrumentation and control system described in Section 7.8 as the DPS.

BTP HICB-21 - Guidance for Digital Computer Real-Time Performance:

- Conformance: The SRNM/APRM digital subsystems (and the OPRM digital subsystem) are designed to respond in real time to ensure the specified fuel limits are not exceeded, and core power oscillations are detected and suppressed. The NMS meets this BTP.

7.2.2.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for Chapter 7, and with Table 7.1-1, 10CFR50.34(f)(2)(v)(ID.3) applies to the NMS and is addressed in Section 7.2.2.3.1.

TMI action plan requirements are generally addressed in Table 1A-1 of Chapter 1, Appendix 1A.

7.2.2.4 Testing and Inspection Requirements

7.2.2.4.1 General Requirements

NMS instruments (not including sensors) outside the containment are designed so they can be tested, inspected, and calibrated as required during plant operation without causing plant shutdown or scram and with easy access for the service personnel.

NMS instrument modules, including SRNM and APRM, are designed with the capability of being tested for normal performance, trip performance, and calibration function through either an automated or manual process. Routine surveillance functions, including periodic tests and calibration, are automated with minimum operator involvement.

Detailed NMS instrument test function requirements, including periodic tests and calibration durations for each instrument, are included in the detailed NMS hardware and software system specification document.

For microprocessor-based instruments an instrument unit self-test function is provided.

7.2.2.4.2 Specific Requirements

7.2.2.4.2.1 Startup Range Neutron Monitor Testability and Calibration

Each SRNM channel is tested and calibrated using the procedures listed in the SRNM instruction manual. Each SRNM channel is checked to ensure that the SRNM high flux scram function and short period scram function are operable.

7.2.2.4.2.2 Local Power Range Monitor Testability and Calibration

LPRM channels are calibrated using data from the AFIP subsystem and based on PCF three-dimensional core power distribution calculations. The calibration follows procedures in the applicable instruction manual.

7.2.2.4.2.3 Average Power Range Monitor Testability and Calibration

APRM channels are calibrated using data from the PCF reactor heat balance calculation. The calibration follows procedures in the applicable instruction manual. Each APRM channel is checked individually (by introduction of test signals) for operability of the APRM high neutron flux scram and rod-blocking functions.

7.2.2.4.2.4 Oscillation Power Range Monitor Testability and Calibration

Each OPRM channel can be checked individually (by introduction of test signals) for operability of the OPRM trip protection algorithm.

7.2.2.5 Instrumentation and Control Requirements

7.2.2.5.1 Instrumentation Requirements

The design of NMS instruments primarily is based on digital instrument and control practices with digital electronics-based programmable and memory units. The NMS instruments follow a modular design concept so each modular unit or its subunit is easily replaceable. Each instrument has a flexible interface design to accommodate either metal wire or fiber optic communication links.

NMS instruments are provided with necessary operator-interface functions based on adequate NMS man-machine interface (MMI) requirements.

The NMS displays provided in the MCR include, as a minimum, the following:

- SRNM Reactor Period, Power Level, Count Rate (12),
- SRNM Upscale/Inop Trip, Reactor Period Trip Status,
- SRNM Upscale Rod Block, Reactor Period Rod Block, Downscale Rod Block Status,
- SRNM Channel Bypass Status,

- SRNM Period Based Permissive,
- SRNM ATWS Permissive Status,
- LPRM Bypass Status, LPRM Upscale Alarm, LPRM Downscale Alarm Status (256 each),
- Number of Bypassed LPRMs per APRM Channel,
- APRM Power Level (4),
- APRM Bypass Status (4),
- APRM Divisional Reactor Upscale/Inop Trip, Upscale Rod Block, Downscale Rod Block Status,
- APRM Simulated Thermal Power Level (4),
- APRM Simulated Thermal Power Upscale Trip Status,
- APRM ATWS Permissive Status (4),
- OPRM Divisional Trip Status,
- MRBM Main Channel Bypass Status,
- MRBM Main Channel Rod Block Status, and
- AFIP System Operability Status.

The alarms in the MCR include the following:

- SRNM Upscale Trip, Upscale Rod Block,
- SRNM Non-coincident Upscale Trip,
- SRNM Non-coincident Upscale Rod Block,
- SRNM Downscale Rod Block,
- SRNM Short Period Trip, Short Period Rod Block,
- SRNM Inoperative Trip,
- SRNM Period Withdrawal Permissive Alarm,
- LPRM Upscale, Downscale Alarm,
- APRM Upscale Trip,
- APRM Upscale Rod Block, Downscale Rod Block,
- APRM Simulated Thermal Power Upscale Trip,

- APRM Simulated Thermal Power Rod Block,
- APRM System Inoperative Trip,
- MRBM Upscale Rod Block, Downscale, Inoperative Rod Block,
- AFIP Inoperative, and
- OPRM Trip.

The above NMS displays and alarms fulfill the information display requirements of the IEEE Std. 603, Section 5.8.

7.2.2.5.2 Basic Control Logic Requirements

The control logic of the safety-related subsystems in the NMS is "fail-safe." That is, a trip signal is initiated if the control logic device fails due to critical hardware failure, power failure, or loss of communication failure.

The NMS controls located in the MCR panel include:

- SRNM Channel Bypass Controls (one for each bypass group) (hardware),
- APRM Channel Bypass Control (one for each division) (hardware), and
- Coincidence/Non-Coincidence switch. In the Non-Coincidence position (not in Run mode), any single SRNM channel trip condition sends a trip signal to RPS and causes a reactor scram.

Each SRNM, LPRM, OPRM, or APRM channel can be individually bypassed. Restrictions on the total number and distribution of bypassed channels (at one time) are followed to avoid a reactor trip due to inoperative NMS channels.

Each of the 12 SRNM channels belongs to one of the four bypass groups. Each group has one "multiple position" selector switch so only one SRNM channel in each group may be bypassed at a time. The SRNM channel bypassed status is displayed on the NMS user interface.

The APRM equipment allows the operator to bypass any one of the four APRM channels during normal plant operation. The APRM channel bypassed status is displayed on the NMS user interface. The trip logic at the NMS becomes two-out-of-three instead of two-out-of-four.

There are separate bypass functions for the SRNM and APRM in the NMS. (There is no single NMS divisional bypass affecting both the SRNM and the APRM.) An APRM bypass does not force an SRNM bypass. The SRNM and APRM bypasses are separate logics to NMS. All NMS bypass logic control functions are located within NMS but none are located in the RPS. Use of SRNM and APRM bypasses does not adversely affect the ATWS permissive and ADS inhibit output functions.

Individual LPRM channels are bypassed by first confirming, for a given APRM channel, that the minimum LPRM input requirement is still met after the bypasses are completed. The operator has to input the LPRM designator to be bypassed, then switch it into bypass. The LPRM channel

bypassed status is displayed on the NMS user interface. If the maximum allowed number of bypassed LPRMs associated with any APRM channel is exceeded an inoperative trip is automatically generated by that APRM channel.

A failure that causes a channel to become inoperative causes a channel trip output to the NMS.

When the Reactor Mode Switch is in Run position, the NMS is in a "Coincident" mode. When the Reactor Mode Switch is NOT in Run mode, this equates to a Non-Coincident mode for the NMS. SRNM trips are active only when the Reactor Mode Switch is not in the Run position. If the manual Coincident/Non-Coincident switch is in the "Non-Coincident" position when the Reactor Mode Switch is placed in the RUN position then an alarm is generated in the MCR. When the NMS is in Non-Coincident Mode, any one of the SRNMs channel trips can cause a reactor scram; in the coincident mode, at least two-out-of-four divisions must be tripped in order to activate the reactor scram.

7.2.2.5.3 Basic Instrument Arrangement Requirements

NMS instruments and equipment are located in appropriate areas in the CB and RB with appropriate divisional physical and electrical separation.

7.2.3 Suppression Pool Temperature Monitoring

The Suppression Pool Temperature Monitoring (SPTM) function (a subsystem of the Containment Monitoring System [CMS]) is classified as safety-related.

7.2.3.1 System Design Bases

7.2.3.1.1 Safety-Related Design Bases

The safety-related functional requirement of the SPTM is to prevent the suppression pool temperature from exceeding established limits. It does this by providing the inputs necessary for automatic reactor scram initiation, which limits heat addition to the suppression pool.

The SPTM is a safety-related four-divisional subsystem, designed for Seismic Category I requirements.

SPTM also provides the following:

(1) Safety-related inputs to the MCR for indication,

(2) Input for nonsafety-related suppression pool automatic cooling mode initiation, and

(3) Information for display, alarm, and recording inputs to the DPS.

7.2.3.1.2 Nonsafety-Related Design Bases

The nonsafety-related functional requirements are:

- To provide input for automatic suppression pool cooling mode initiation, and

- To provide input for data display, alarm, and recording on the MCR panels.

7.2.3.2 System Description

7.2.3.2.1 General

The SPTM provides suppression pool temperature data for automatic scram and automatic suppression pool cooling initiation when established high temperature limits are exceeded. In addition, the SPTM subsystem provides suppression pool temperature data for operator information and recording, and for post-accident conditions of the suppression pool. The SPTM subsystem outputs to other systems are shown in Table 7.2-5.

7.2.3.2.2 Power Sources

The SPTM hardware is redundantly powered by the appropriate dual divisional uninterruptible 120 VAC power sources - either of which can support the SPTM function.

7.2.3.2.3 Equipment Design

The SPTM system comprises four independent safety-related instrumentation divisions, each containing 16 thermocouples spatially distributed around the suppression pool. The sensor locations are established based upon the following considerations:

- To provide four-divisional, redundant measurements of suppression pool local and bulk-mean temperatures under normal plant operating conditions and under postulated accident and post-accident conditions,
- To provide 16 temperature sensors for use by the DPS,
- To implement the divisional separation of sensors in the azimuthal directions, with redundancy and separation of sensors realized in four divisions and with sensors appropriately covering the different elevations of the pool, and
- To locate sensors away from jet paths of SRV quenchers, horizontal vent discharges, and Passive Containment Cooling System (PCCS) vent line discharges. This limits the temperature differences between local and bulk-mean values.

The sensor electrical wiring, encapsulated in pliable, grounded sheathing, is terminated in Wetwell-sealed, moisture-proof junction boxes for easy sensor replacement or maintenance during a plant outage. The temperature sensor wiring from the Wetwell junction boxes is directed through the suppression pool divisional instrument penetrations to the four-divisional Q-DCIS RMUs and the DPS RMUs.

7.2.3.2.4 Signal Processing

Suppression pool temperature monitoring supports measurement and calculation of bulk average suppression pool temperatures for both normal operation and accident conditions. A minimum number of thermocouples per division is required to be operational. The SPTM logic

automatically compensates for inoperable thermocouples. If less than the required number of thermocouples is available a trip signal is generated in that division. These signals are transmitted through the divisional Q-DCIS to the RPS. Safety-related protective actions are generated by the RPS. Abnormal status alarms, data display, and recording are provided.

7.2.3.3 Safety Evaluation

Table 7.1-1 identifies the SPTM and the associated codes and standards applied, in accordance with the Standard Review Plan NUREG-0800. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.2.3.3.1.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: SPTM complies with these standards

10 CFR 50.55a(h), Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: Safety-related systems are designed in conformance with RG 1.153 and IEEE Std. 603. Separation and isolation are preserved - both mechanically and electrically - in accordance with IEEE Std. 603, Section 5.6 and RG 1.75. The SPTM portion of CMS consists of four redundant divisions so failure of any single temperature element does not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

10 CFR 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication:

- Conformance: SPTM demonstrates compliance by providing automatic indication of bypassed and inoperable status.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this section..

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the SPTM subsystem within the DCD documents conforms with this requirements.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.2.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 25, and 29:

- Conformance: The SPTM subsystem complies with the GDC identified above.

7.2.3.3.3 Staff Requirements Memorandum

Item II.Q, (Defense Against Common-Mode Failures in Digital Instrument and Control Systems):

- Conformance: The SPTM subsystem designs conform with item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of diverse instrumentation and control, described in Section 7.8.

7.2.3.3.4 Regulatory Guides

RG 1.22 - Periodic Testing of Protection System Actuation Function:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.62 - Manual Initiation of Protective Actions:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.75 - Physical Independence of Electric Systems:

- Conformance: The SPTM design conforms with the RG identified. See chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for a discussion of how the design meets the requirements of RG 1.75.

RG 1.97 - Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.105 - Setpoints for safety-related Instrumentation:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.118 - Periodic Testing of Electric Power and Protection System:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.152 - Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.153 - Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The SPTM design conforms with the RG identified.

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

- Conformance: The SPTM design conforms with the RG identified.

RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.173 - Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The SPTM design conforms with the RG identified.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The SPTM design conforms with the RG identified.

7.2.3.3.5 Branch Technical Positions

BTP HICB-3 - Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service:

- Conformance: There is no reactor coolant pump, so this BTP does not apply.

BTP HICB-8 - Guidance for Application of RG 1.22:

- Conformance: The SPTM design conforms with the BTP identified.

BTP HICB-10 - Guidance on Application of RG 1.97:

- Conformance: The SPTM design conforms with the BTP identified.

BTP HICB-11 - Guidance on Application and Qualification of Isolation Devices:

- Conformance: The SPTM design conforms with the BTP identified.

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The SPTM design conforms with the BTP identified.

BTP HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors:

- Conformance: The SPTM uses thermocouple-type temperature sensors so this BTP does not apply.

BTP HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The SPTM design conforms with the BTP identified.

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The SPTM design conforms with the BTP identified.

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The SPTM design conforms with the BTP identified.

BTP HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The SPTM design conforms with the BTP identified.

BTP HICB-19 - Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The SPTM design conforms with the BTP identified.

BTP HICB-21 - Guidance on Digital Computer Real-Time Performance:

- Conformance: The SPTM design conforms with the BTP identified.

7.2.3.3.6 TMI Action Plan Requirements

In accordance with the SRP for 7.2 and with Table 7.1-1, only I.D.3 applies to the SPTM subsystem. This is addressed in Subsection 7.2.3.3.1 for 10 CFR 50.34(f)(2)(v). However, TMI action plan requirements are generically addressed in Table 1A-1 of Chapter 1, Appendix 1A.

7.2.3.4 Testing and Inspection Requirements

Proper functioning of analog temperature sensors is verified by channel cross-comparison during the plant normal operation mode. The bulk pool temperatures are continuously compared between divisions and alarmed (for inconsistency) by the PCF.

Each of four SPTM safety-related divisions is testable during plant normal operation to determine the operational availability of the system. Each safety-related SPTM division has the capability for testing, adjustment, and inspection during a plant outage.

7.2.3.5 Instrumentation and Controls Requirements

The instrumentation and control requirements related to SPTM are addressed in Subsections 7.2.3.1 and 7.2.3.2.

7.2.4 COL Information

None

7.2.5 References

7.2-1 GE Nuclear Energy, "General Electric Instrument Setpoint Methodology," Licensing Topical Report NEDC-31336P-A, Class III (GE Proprietary), September 1996.

7.2-2 GE Nuclear Energy, NUMAC LTR, NEDO-33288, "Application of Nuclear Measurement Analysis and Control (NUMAC) for the ESBWR Reactor Trip System, March 2007".

7.2-3 GE Nuclear Energy, "ESBWR I&C Software Management Plan," NEDO-33226, Class I (Non-proprietary); and "ESBWR I&C Software Management Plan," NEDE-33226P, Class III (Proprietary), Revision 2, July 2007.

7.2-4 GE Nuclear Energy, "ESBWR I&C Software Quality Assurance Plan," NEDO-33245, Class I (Non-proprietary); and "ESBWR I&C Software Quality Assurance Plan," NEDE-33245P, Class III (Proprietary), Revision 2, July 2007.

Table 7.2-1

Channels Used in Functional Performance of RPS

Channel Description	Number of Channels of Sensors
NMS (APRM)	4
NMS (SRNM) [1]	4
NBS reactor vessel pressure	4
Drywell pressure	4
RPV narrow range water level	4
Low charging pressure to control rod hydraulic unit accumulator	4
MSIV position switches	16
TSV closure	4
TCV fast closure	4
Loss of Power Generation Bus (Loss of FW Flow)	4
High Condenser Pressure	4
SPTM	4

1. In modes other than Run

Table 7.2-2

SRNM Trip Function Summary

Trip function	Analytical Limit For Trip Setpoint [1]	Action
SRNM Upscale Flux Trip	45% power [2]	Scram (bypassed in Run)
SRNM Upscale Flux Alarm	35% power [3]	Rod Block (bypassed in Run)
SRNM Short Period Trip	10 seconds	Scram [4] (bypassed in Run & Refuel) (no scram function in counting range)
SRNM Short Period Alarm	20 seconds	Rod Block (bypassed in Run)
SRNM Period Control Rod Withdrawal Permissive	55 seconds	Rod Block (bypassed in Run) [5]
SRNM Inoperable	Module interlock disconnect; HV voltage low	Scram (bypassed in Run)
SRNM Downscale	3 cps	Rod Block
SRNM Intermediate Upscale Flux Trip	5E+5 cps	Scram [6]
SRNM Intermediate Upscale Flux Alarm	1E+5 cps	Rod Block [6]
SRNM ATWS Permissive	6% power	Permissive signal to ATWS/SLC system (all modes)

1. Instrument setpoint accuracy is determined by safety analyses using GEH instrument setpoint methodology (Reference 7.2-1).
2. This scram setpoint is equivalent to the upscale scram on the last range of BWR/5 IRM, at the 120/125 level.
3. This rod block setpoint is equivalent to the upscale rod block on the last range of BWR/5 IRM, at the 108/125 level.
4. Scram action only active in mean square voltage range, defined as above $1x10^{-4}$% power.
5. With the rod block at this setpoint, the reactor period never reaches 10 seconds because of rod withdrawal. Consequently, no reactor scram would result.
6. In NMS NON-COINCIDENCE mode. Conditions for activation are defined in the plant operating procedures.

Table 7.2-3

SRNM Trip Signals

			Indicator Type [6]		
Condition [1]	**Rod Block**	**N-DCIS**	**Alarm**	**Indication**	**Reactor Trip [5]**
Upscale Trip [2]		X	X	X	X
Upscale Alarm	X	X	X	X	
Period Trip [3]		X	X	X	X
Period Alarm	X	X	X	X	
Inoperative [4]	X	X	X	X	X
Downscale Alarm	X	X	X	X	
Channel Bypass		X		X	

1. No trips are active in Run mode or for a bypassed channel; however, they are active in other operating modes.
2. This includes both normal (% power) and set down level (counts per second) in non-coincident mode.
3. For trip conditions, see Section 7.2.2.1.1.1.
4. This covers the SRNM upscale and period trips with APRM downscale
5. This refers to channel/division trip signal provided to RPS (same definition in subsequent tables)
6. This is a system requirement.

Table 7.2-4

APRM Trip Function Summary

Trip Function	Analytical Limit For Trip Setpoint [1]	Action
APRM Upscale Flux Trip	120% power 15% power	Scram (only in Run) Scram (not in Run)
APRM Upscale Flux Alarm	108% power 12% power	Rod Block (only in Run) Rod Block (not in Run)
APRM Upscale Simulated Thermal Power Trip	115% power	Scram
APRM Inoperative	1. LPRM inputs too few; 2. Module interlocks disconnect	Scram & Rod Block Scram & Rod Block
APRM ATWS Permissive	6% power	ADS Permissive signal to SSLC system (all modes)
APRM Downscale	5% power	Rod Block (only in Run)

1. Instrument setpoint accuracy is determined by safety analyses using GEH instrument setpoint methodology of Reference 7.2-1.

Table 7.2-5

Outputs from SPTMs to Other Systems

Signal	Utilization
Sixteen divisional suppression pool local temperature signals to each safety-related DCIS RMU (in each of 4 divisions).	Input for divisional scram initiation and temperature status display within SSLC/ESF and RPS. Input for non-divisional suppression pool cooling mode initiation (FAPCS). Input for non-divisional suppression pool temperature data display, alarm and recording (within N-DCIS & MCR).

Table 7.2-6

OPRM Trip Function Summary

Trip Function	Analytical Limit For Trip Setpoint [1]	Action
OPRM Inoperative	LPRM inputs too few	OPRM Cell/Channel Alarm
OPRM Oscillation Detection	Per TRACG developed setpoint tables and ESBWR core stability curves	Channel Trip
OPRM Oscillation Detection	Per TRACG developed setpoint tables and ESBWR core stability curves	Channel Alarm
OPRM Bypass	N/A	Controlled by APRM bypass

1. Instrument setpoint accuracy is determined by safety analyses using GEH instrument setpoint methodology of Reference 7.2-1.

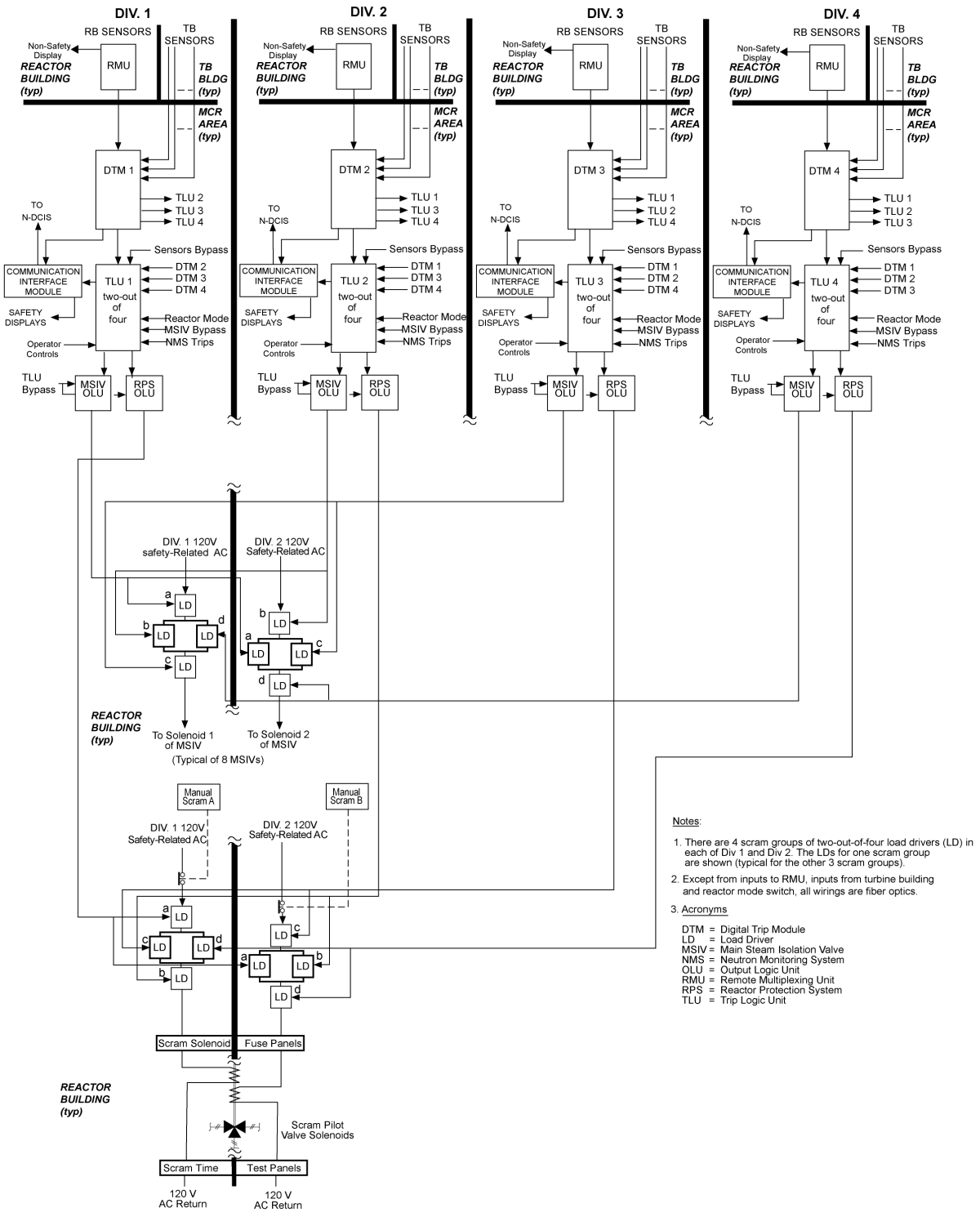


Figure 7.2-1. RPS Functional Block

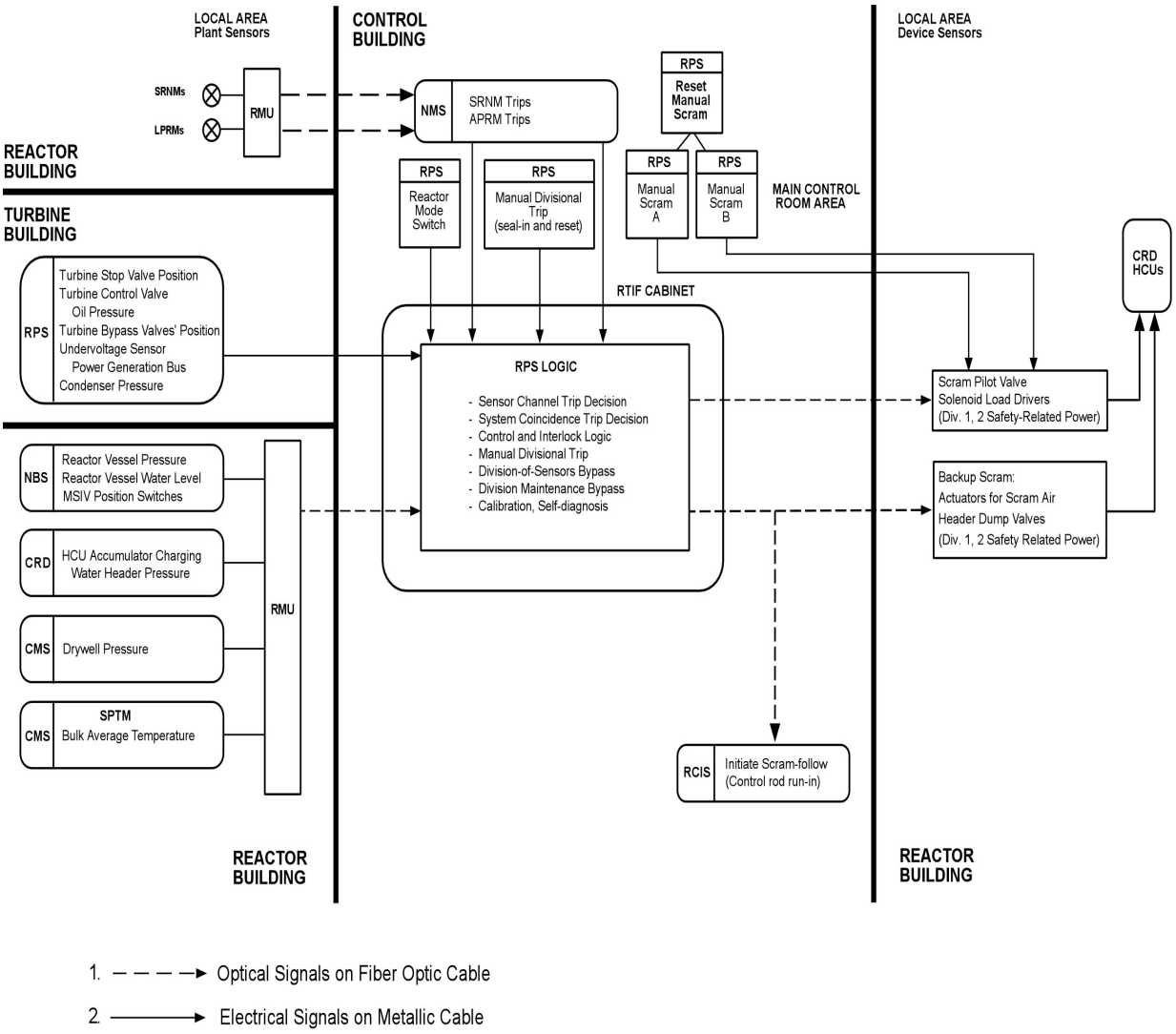


Figure 7.2-2. RPS Interfaces and Boundaries Diagram

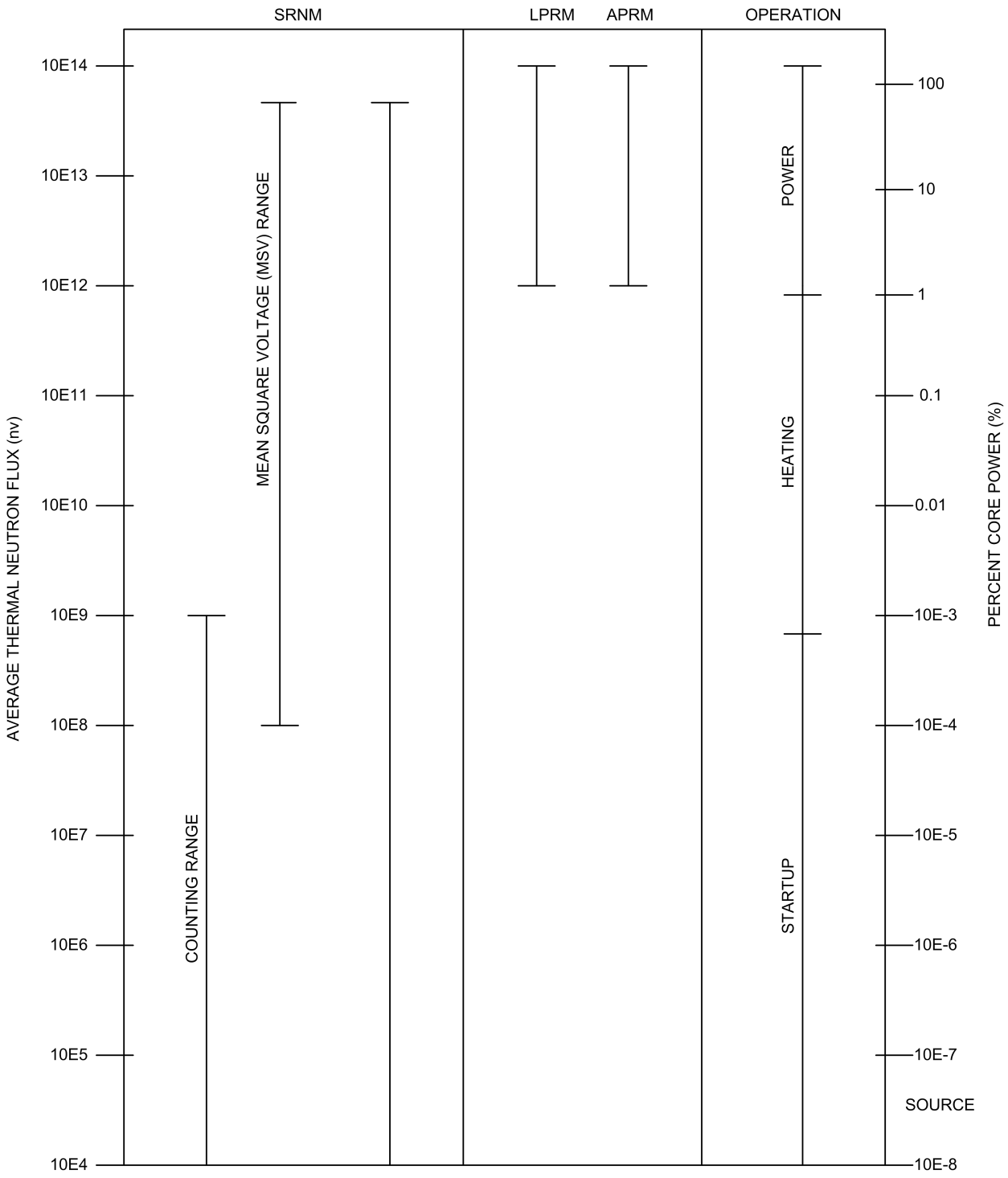


Figure 7.2-3. Neutron Flux Monitoring Ranges

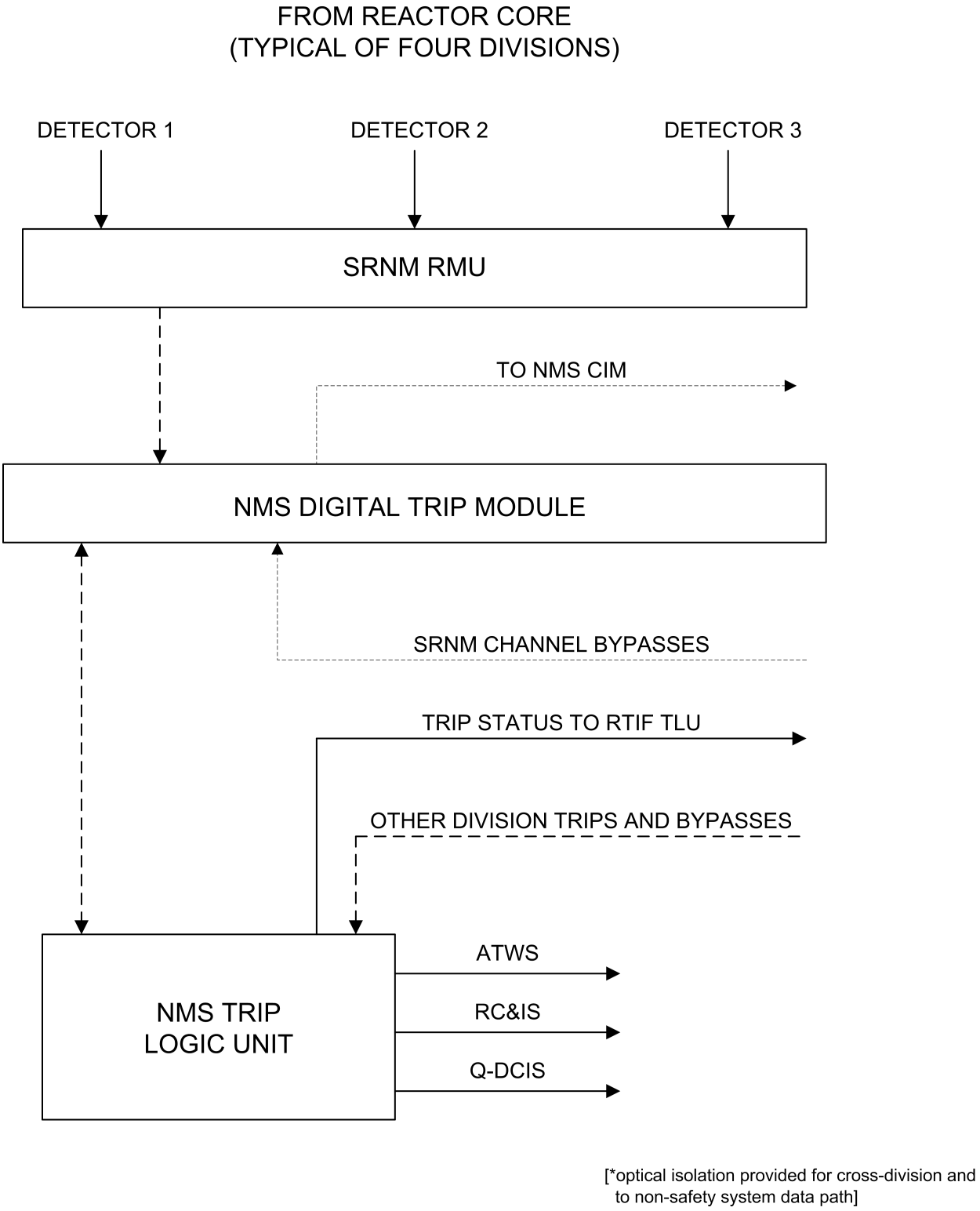


Figure 7.2-4. Basic Configuration of a Typical SRNM Subsystem

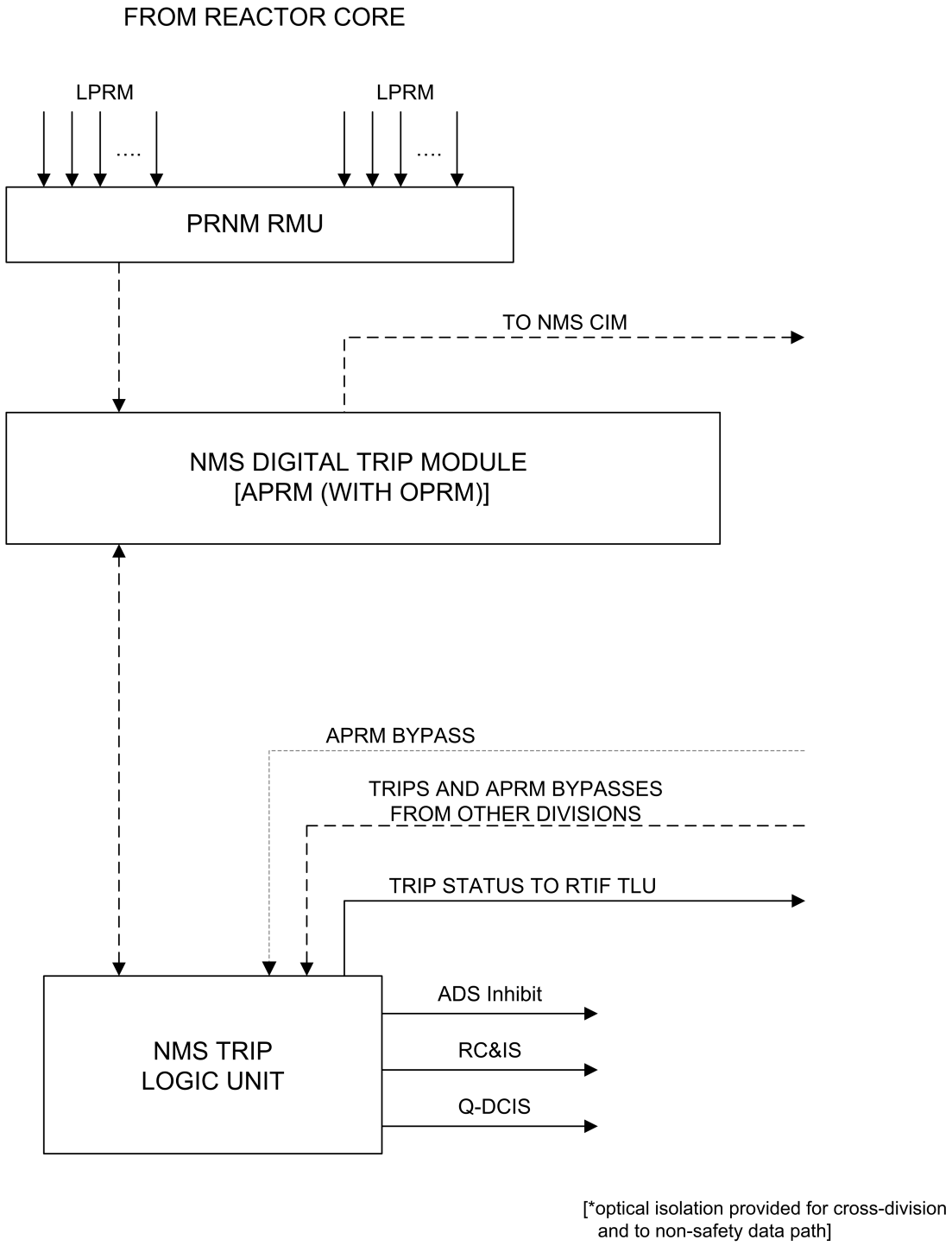


Figure 7.2-5. Basic Configuration of a Typical PRNM Subsystem

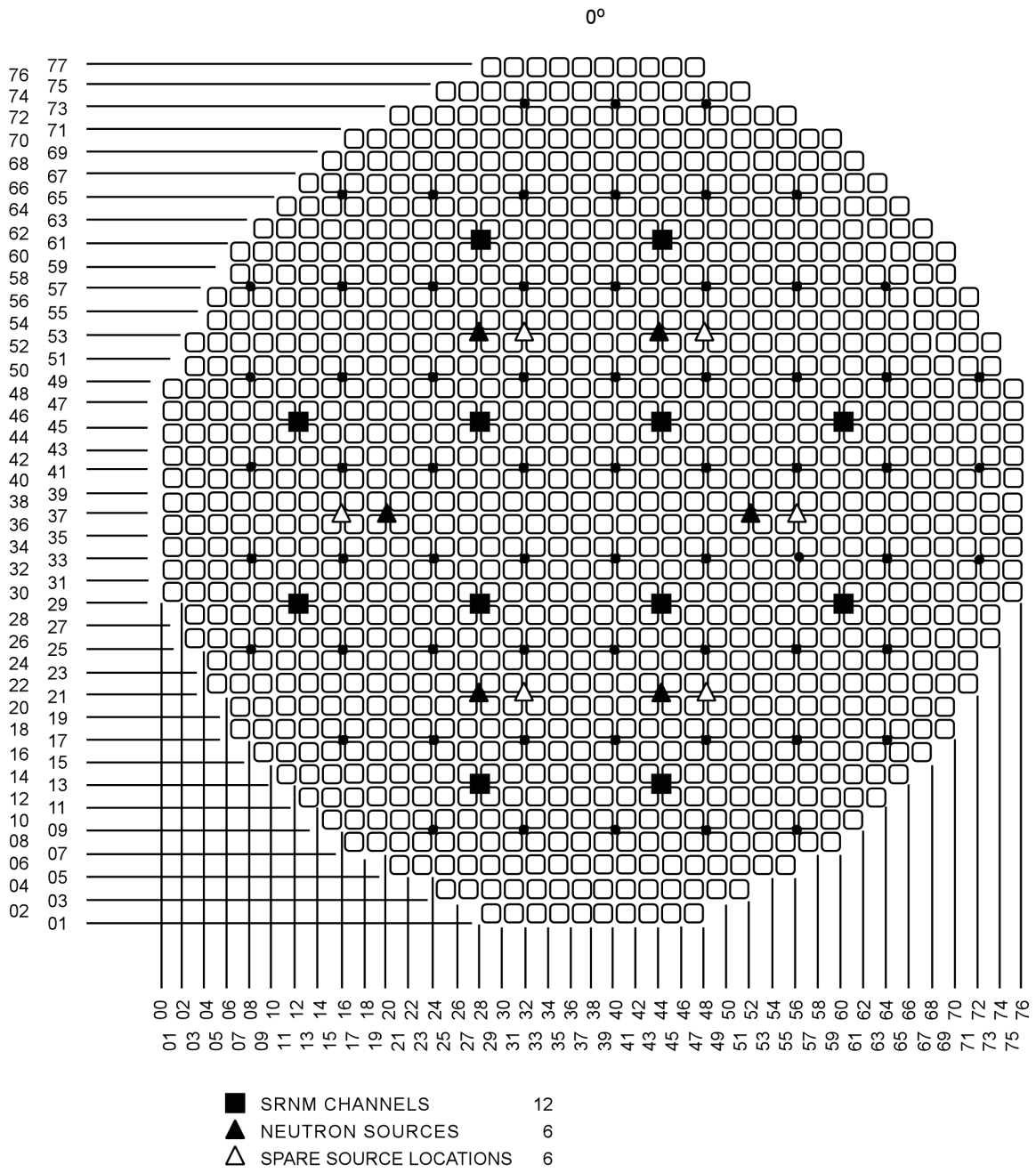
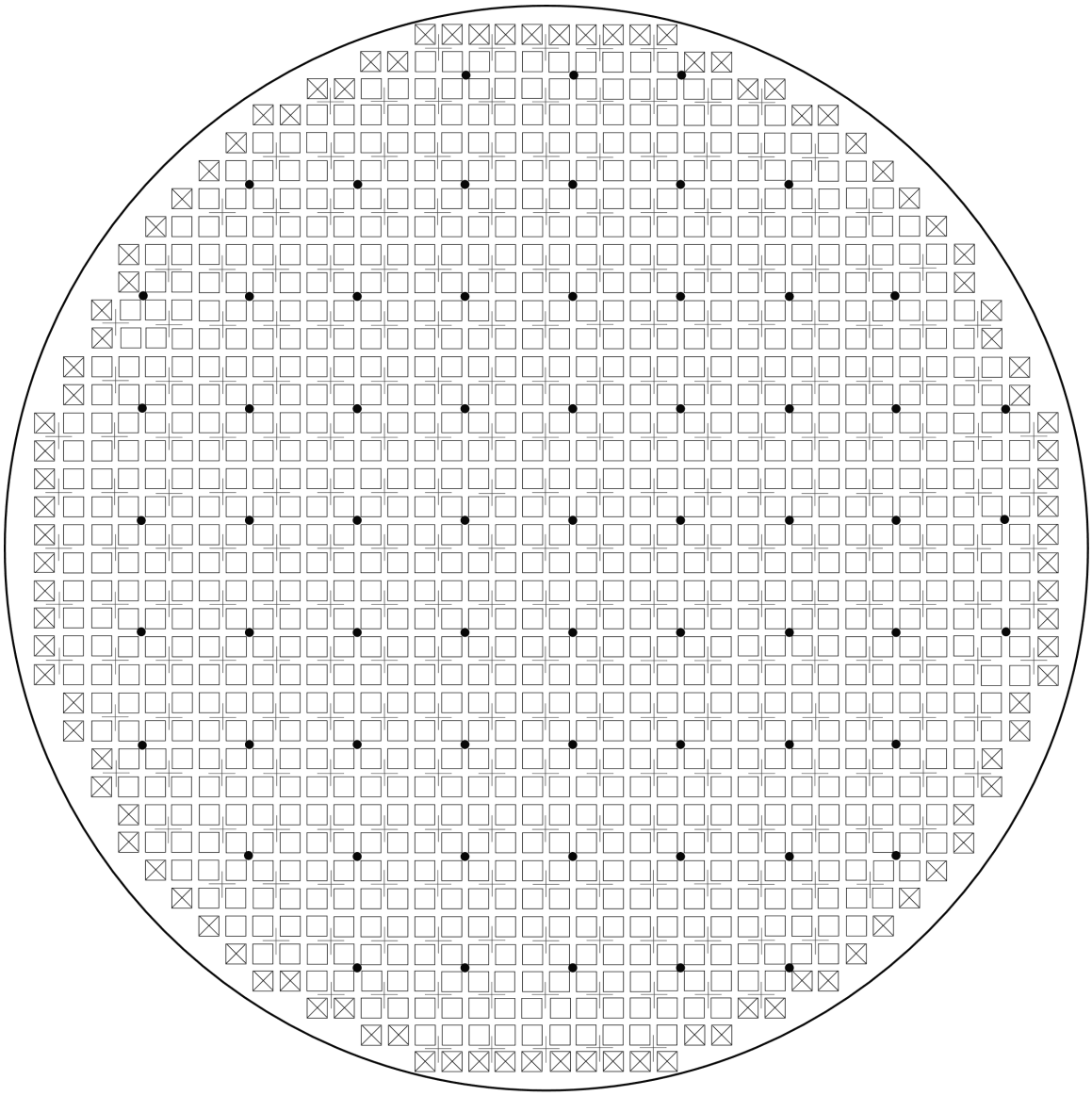


Figure 7.2-6. SRNM Detector Locations



Central Region Bundle	1028	Control Rod	269
Peripheral Region Bundle	104	LPRM	64
Total	1132		

ESBWR Core Map

Figure 7.2-7. LPRM Locations in the Core

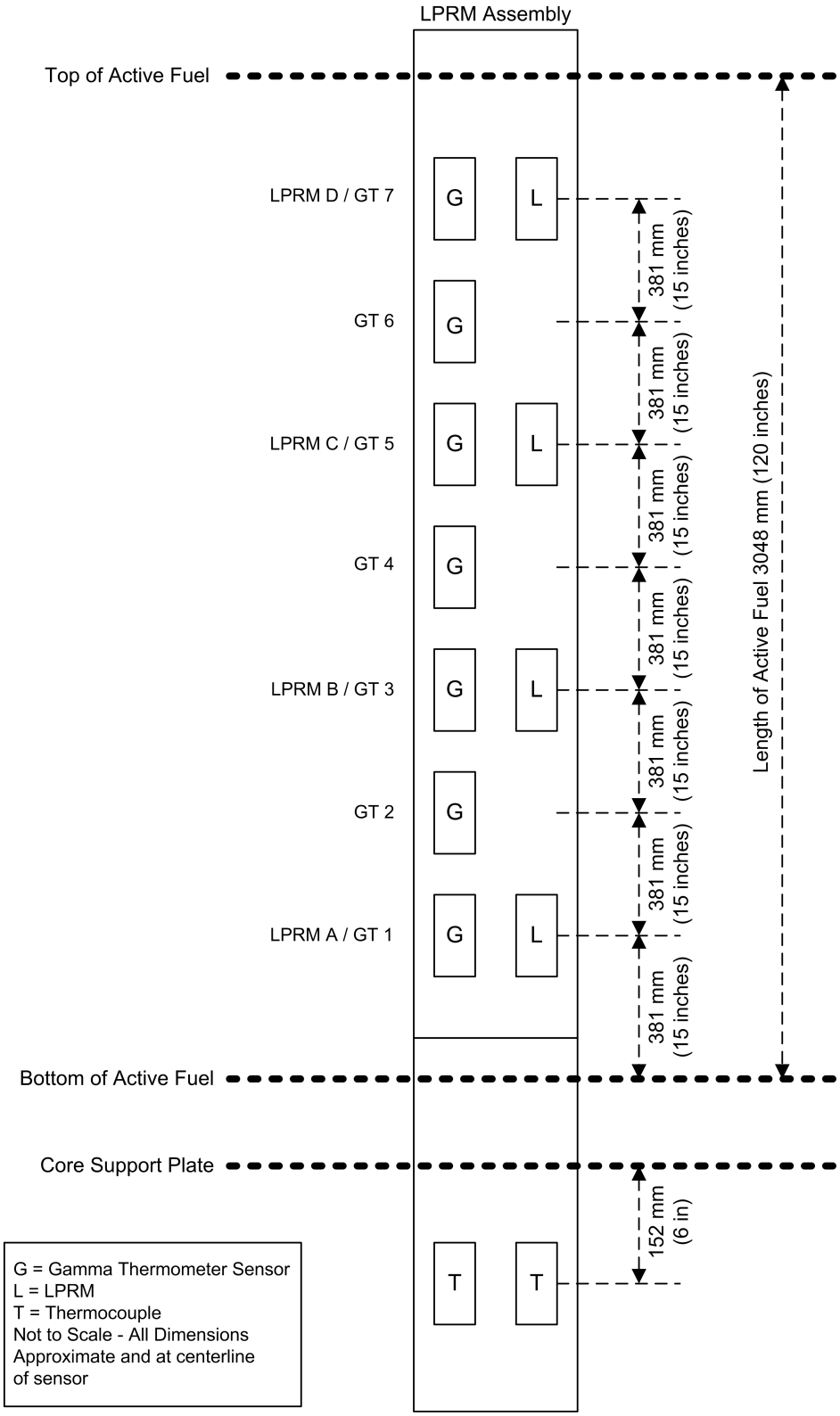


Figure 7.2-8. Axial Distribution of LPRM Detectors

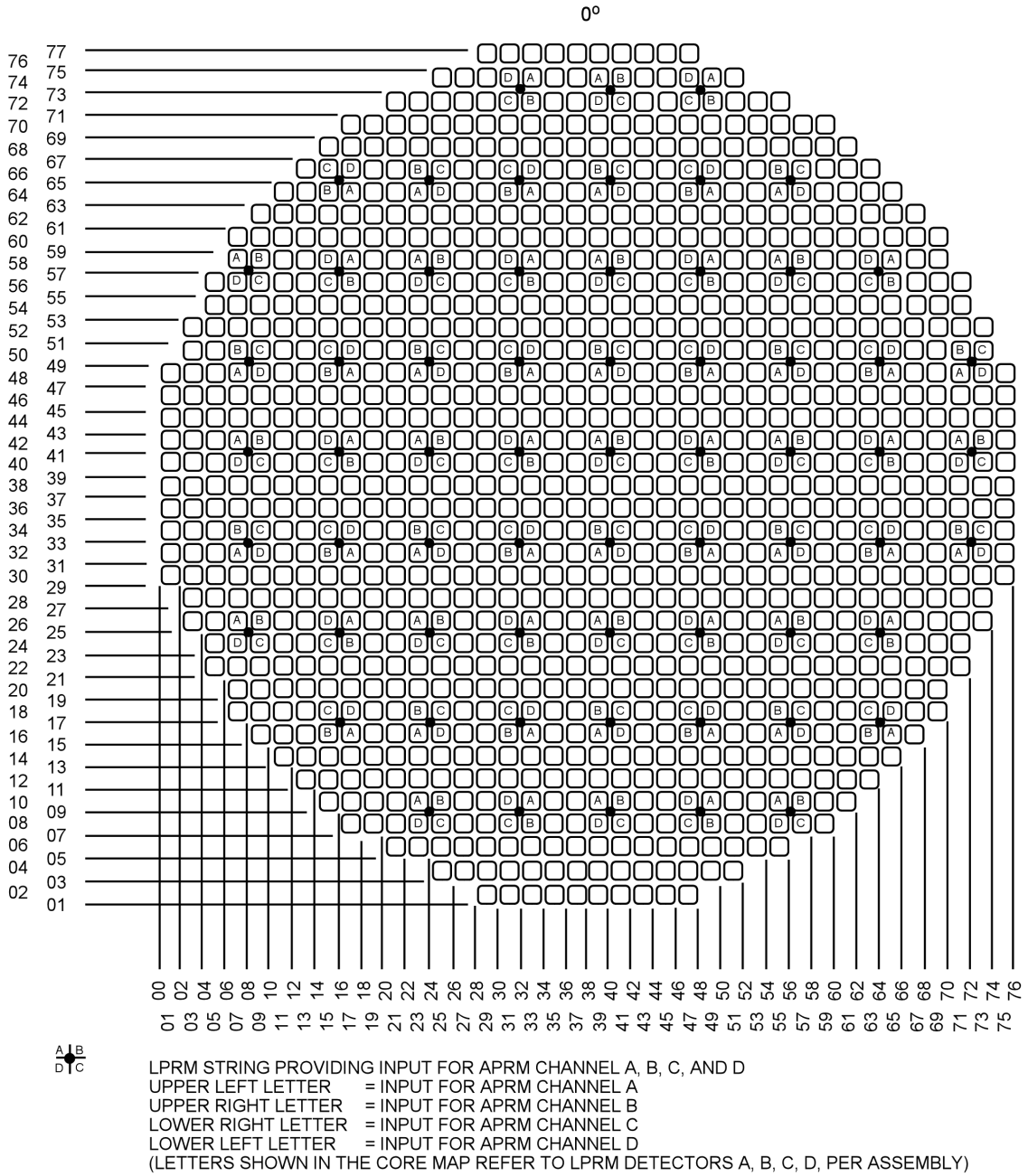
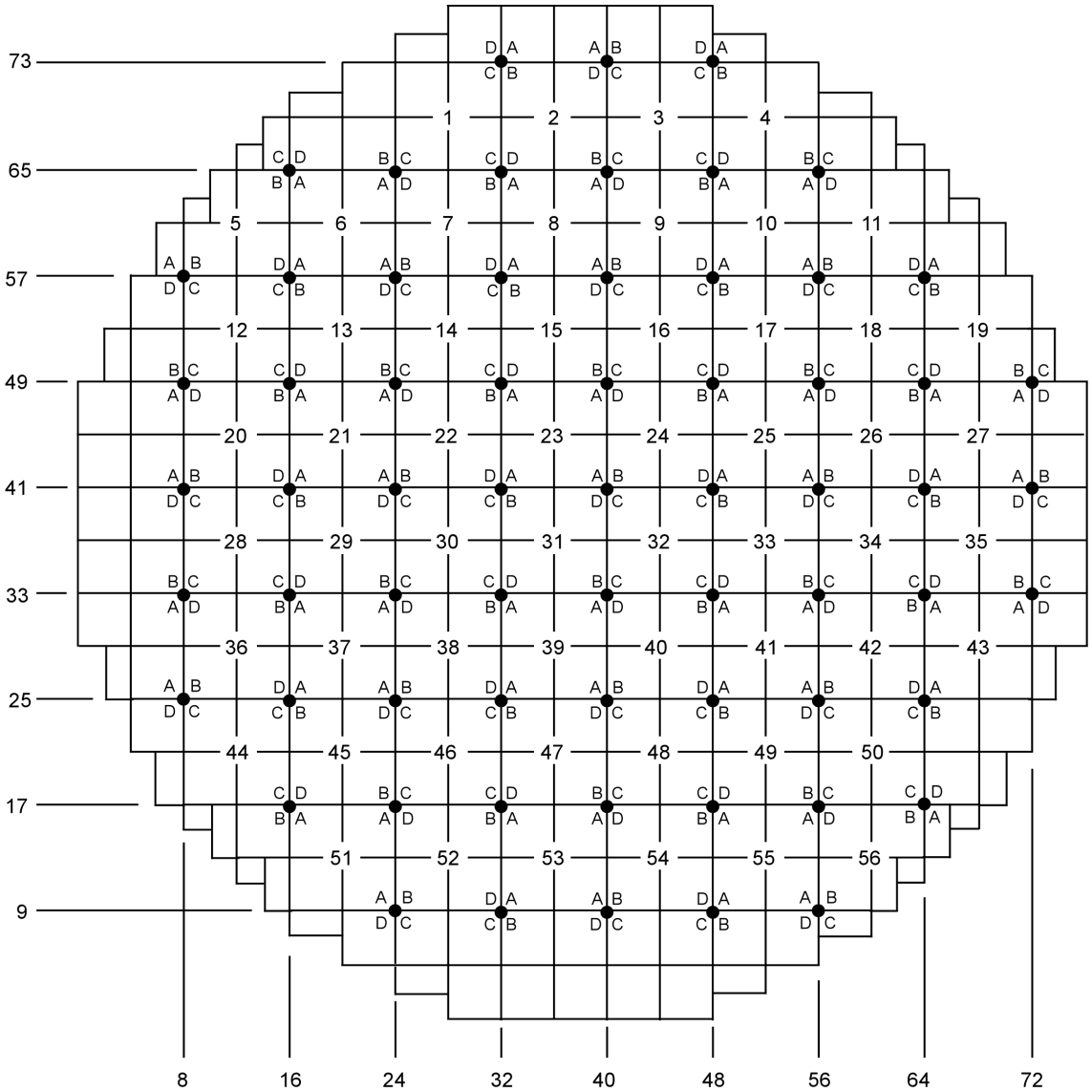


Figure 7.2-9. LPRM Assignments to APRM Channels



LPRMs PROVIDING INPUT TO OPRM CHANNELS A, B, C, AND D

UPPER LEFT LETTER = INPUT FOR OPRM CHANNEL A
UPPER RIGHT LETTER = INPUT FOR OPRM CHANNEL B
LOWER RIGHT LETTER = INPUT FOR OPRM CHANNEL C
LOWER LEFT LETTER = INPUT FOR OPRM CHANNEL D
(LETTERS IN THE MAP REFER TO LPRM DETECTORS A, B, C, D PER ASSEMBLY)

Figure 7.2-10. LPRM Assignment to OPRM Channels

7.3 ENGINEERED SAFETY FEATURES SYSTEMS

The Engineered Safety Features (ESF) systems are part of a group of systems collectively called the Safety-Related Distributed Control and Information System (Q-DCIS). A simplified functional block diagram of the Q-DCIS is included as part of Figure 7.1-1 and a functional network diagram appears as Figure 7.1-2. These diagrams indicate the relationships of the ESF systems with their safety-related peers and with nonsafety-related plant data systems collectively called the Nonsafety-Related Distributed Control and Information Systems (N-DCIS). Section 7.1 contains a description of these relationships.

7.3.1 Emergency Core Cooling System

The Emergency Core Cooling System (ECCS) comprises the Automatic Depressurization System (ADS), the Gravity-Driven Cooling System (GDCS), the Isolation Condenser System (ICS) (Subsection 7.4.4), and the Standby Liquid Control (SLC) system (Subsection 7.4.1).

7.3.1.1 Automatic Depressurization System

The ADS resides within the Nuclear Boiler System (NBS). It depressurizes the reactor so that the low-pressure GDCS can provide make up coolant to the Reactor Pressure Vessel (RPV).

7.3.1.1.1 System Design Bases

The ADS instrumentation and controls (I&C) meet the following safety-related requirements:

- Detect reactor low water level, Level 1 (see subsection 7.7.1.2.2 and Figure 7.7-1 for more information on definition of water levels);
- Automatically actuate the Safety Relief Valves (SRVs) and Depressurization Valves (DPVs) after Level 1 is reached;
- Actuate the SRVs and DPVs sequentially and in groups to achieve the required depressurization characteristics;
- Render no more than one valve inoperative for any single failure;
- Ensure physical and electrical separation and isolation between safety-related divisions and from nonsafety-related circuits and equipment; and
- Indicate the status of SRV and DPV in the Main Control Room (MCR).

The ADS controls and instrumentation meet the following nonsafety-related requirements:

- No single control or instrumentation failure inadvertently opens an SRV or a DPV, and
- ADS-parameter alarms are provided in the MCR.

7.3.1.1.2 System Description

The ADS is a subsystem of the Nuclear Boiler System (NBS) and comprises 10 SRVs, eight DPVs, and the associated Instrumentation and Controls (I&Cs). The SRVs are nitrogen operated solenoid actuated relief valves. The DPVs are electrically operated squib valves. The SRVs and DPVs are described in detail in Subsection 5.2.2 and Subsection 6.3.2, respectively. These valves are divided into groups, and lift in sequence when required.

The NBS functional components (including the ADS) are shown on Figure 5.1-2. The mechanical aspects of the ADS functions within the ECCS are discussed in Subsection 6.3.3. Typical SRV and DPV logic and control are shown on Figures 7.3-1a and 7.3-1b, respectively.

Automatic Operation

Actuation of ADS equipment is controlled automatically (IEEE Std. 603, Sections 6.1 and 7.1), without need for operator action. Capability for manual actuation also is provided (IEEE Std. 603, Sections 6.2 and 7.2).

Automatic actuation of the ADS occurs when the RPV water reaches Level 1. Four wide range RPV water level transmitters are used to detect Level 1. These transmitters are separate from those used for Reactor Protection System (RPS) functions and different from those used for the Diverse Protection System (DPS) wide range level transmitters.

When attainment of level 1 is detected five SRVs (group 1) are opened to start RPV pressure reduction, followed by the other five SRVs (group 2) after a time delay. See Table 7.3-2 for the time delay parameters. The sequence continues with groups of DPVs, each opening after further successive time delays. See Table 7.3-3 for the DPV groups and time delay parameters. This sequential operation minimizes the water loss as a result of liquid swell in the RPV when its pressure is rapidly reduced. See Table 5.2-2 for the SRV and DPV settings and/or capacities.

Additionally, as discussed in Subsection 7.8.1.2, the DPS has the ability to open independently the same SRVs and DPVs using the same logic, but using diverse hardware/software equipment and reactor-level sensors separate from those used in the primary ECCS functions. For the ADS, the DPS can actuate a fourth, nonsafety-related solenoid on each of the SRVs, and a fourth squib initiator on each of the DPVs.

Manual Operation

The safety-related Video Display Units (VDUs) in the MCR provide a display format allowing the operator to manually open each SRV and each DPV independently, using the primary SSLC/ESF logic function (IEEE Std. 603, Sections 5.8, 6.2 and 7.2). Each nonsafety-related VDU in the MCR provides a display format allowing the operator to manually open each SRV independently, using the DPS logic function. Each display uses an “arm/fire” configuration requiring at least two deliberate operator actions. Operator use of the “arm” portion of the display triggers a plant alarm. The two manual opening schemes from SSLC/ESF and from DPS are diverse.

Each safety-related VDU provides a display with an “arm/fire” switch (one per division) to manually initiate ADS as a system, rather than initiating each valve individually (IEEE Std. 603,

Sections 5.8, 6.2 and 7.2). If the operator uses any two of the four "arm/fire" switches, the ADS sequence seals in and starts the ADS valve opening sequence (IEEE Std. 603, Section 5.2). This requires at least four (two arm and two fire) deliberate operator actions.

Actuation Logic

See Figure 7.3-1a for typical SRV actuation logic, and Figure 7.3-1b for typical DPV actuation logic.

The ADS actuation logic is implemented in four (SSLC/ESF) divisions, each of which can make a Level 1 trip vote. Each of the divisional trip votes is shared with the other divisions. Normally, each of the four divisions makes a two-out-of-four trip decision from the four divisional votes; however, the entire SSLC/ESF system has a bypass control such that any single division of sensors can be removed from the two-out-of-four decision process, so that the remaining three divisions operate with a two-out-of-three trip decision.

The design allows only one division at a time to be bypassed, and can be used to facilitate either maintenance or calibration activities. Divisional bypasses are alarmed in the MCR. The four divisional water levels and their trip setpoints are continuously monitored for consistency by the N-DCIS plant computer functions (CPF). An inconsistency results in an alarm.

Each division of the SSLC/ESF has two trains of two-out-of-four trip logic (except the DPV logic, which has three trains) to support the requirement that single divisional failures cannot result in inadvertently opening any ADS valve (SRV or DPV). (See Figures 7.3-1a, 7.3-1b). Each initiating logic has access to one channel of wide-range level sensing for the Level 1 trip decision. The separate logic of each train issues the ECCS trip signal, if the RPV water drops below Level 1. The ECCS trip signal actuates a timer (see Table 7.3-2). If the trip signal resets (as, for example, from an instrument column transient), the timer resets and restarts when the next ECCS trip signal is received. If the ECCS trip signal persists for 10 seconds, the logic seals in and issues an "initial start" signal (IEEE Std. 603, Section 5.2). The initial start signal also is transmitted to the SSLC (Subsection 7.3.5) , ICS, (Subsection 7.3.5) and GDCS (Subsection 7.3.1.2). The initial start signal specifically actuates five timers in each of the two two-out-of-four trip logic trains (per division) of ADS logic.

Divisional separation is maintained by using optical isolators and separate raceway, conduit, and penetration wiring to each SRV or DPV. Any two divisions can open all of the ADS valves.

The actual firing circuit for the various squib initiators and SRV solenoids consists of the two load driver/discrete output circuits, followed by a continuity monitor and a keylock switch all arranged in series, and located in the appropriate divisional Remote Multiplexing Units (RMUs) and DPS RMUs in the Reactor Building (RB). Because there is the division of sensors bypass, and there are multiple trains of two-out-of-four logic, no additional division of trip logic bypass is implemented in the SSLC/ESF logic. It is undesirable to perform this level of bypass activity with the RMU electrically connected to the valve. The keylock switch described below provides the bypass function required. In addition to the usual RMU self-diagnostics, means are provided to indicate that each of the series load driver/discrete output circuits can be "closed" (the circuits can be exercised one at a time from the MCR) and to indicate that both have closed.

The keylock switch (Figure 7.3-1b) that disables the firing circuit affects one valve and does not interact with the other valves allocated to that RMU. Operation of any keylock switch triggers an MCR alarm indicating that the firing circuit is out of service. Although the load driver/discrete output checks can be done online (one at a time) without causing valve operation, opening the firing circuit with the keylock switch allows the continuity monitor to be tested, and allows online surveillance and maintenance activities to be done, with the assurance that a valve is not opened inadvertently. The operation of a keylock switch in any one division does not disable the SRV or DPV, since it may still be opened by its other divisional solenoid/squib initiator. Additionally it is not possible to lose single failure inadvertent actuation protection by any operator or keylock switch action.

The ADS design parameters shown in Table 7.3-1 ensure that no single failure of an ADS division logic, SRV actuation pilot, or DPV igniter circuit can prevent successful system operation as long as any three of the four divisions of safety-related power are available. This satisfies the single failure criterion (IEEE Std. 603, Section 5.1).

Supporting systems for the ADS include the instrumentation, logic, control, and motive power sources. The instrumentation and logic power is supplied by the corresponding divisional safety-related power sources. The actual SRV solenoid and DPV squib initiator power also is supplied by the corresponding divisional safety-related power sources (See Subsection 8.3.1.1.3). The motive power for the electrically-operated pneumatic pilot solenoid valves on the SRVs is from accumulators located near the SRVs, and supplied with nitrogen by the High Pressure Nitrogen Supply System (HPNSS).

7.3.1.1.3 Safety Evaluation

Chapter 15 and Section 6.3 evaluate the individual and combined capabilities of the ECCS systems, including the ADS. For the entire range of reactor coolant system break sizes, the ECCS systems ensure that the reactor core always is submerged.

SSLC/ESF initiating instrumentation, including the ADS, responds to the potential inadequacy of core cooling regardless of the location of the breach in the reactor coolant pressure boundary. Reactor pressure vessel (RPV) low water level, which is completely independent of breach location is used to initiate the ADS.

The redundancy of the control and monitoring equipment for the ADS is consistent with the redundancy of the four divisions of ADS.

No single failure in the ADS initiation circuitry can prevent the ADS from depressurizing the RPV, or cause an inadvertent actuation of ADS. This satisfies the single failure criterion of IEEE Std. 603, Section 5.1.

The ADS has no equipment protective interlocks that could interrupt automatic system operation.

The ADS instrumentation and logic, and the SRV and DPV initiation circuitry is powered by divisionally separated safety-related power sources.

Table 7.1-1 identifies the ADS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.3.1.1.3.1 Code of Federal Regulations

10 CFR 50.55a(1), Quality Standards for Systems Important to Safety:

- Conformance: The ADS complies with 10 CFR 50.55a(1).

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: The ADS complies with IEEE Std. 603.

10 CFR 50.34 (f) (2) (v) (l.D.3), Bypass and Inoperable Status Indication:

- Conformance: The ADS complies with 10 CFR 50.34 (f) (2) (v) (I.D.3).

10 CFR 50.34 (f) (2) (xiv) (lI.E.4.2), Containment Isolation Systems:

- Conformance: The ADS complies with 10 CFR 50.34 (f) (2) (xiv) (II.E.4.2).

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for Instrumentation and Control (I&C) systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this Section.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the ADS within the DCD conforms with this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.1.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23 and 24:

- Conformance: The ADS complies with the GDCs identified above.

7.3.1.1.3.3 Staff Requirements Memorandum

SRM to SECY 93-087, Item II.Q Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: Implementation of a Diverse I&C System, the DPS is described in Section 7.8.

7.3.1.1.3.4 Regulatory Guides

RG 1.22 - Periodic Testing of Protection System Actuation Functions:

- Conformance: Components are tested periodically during refueling outages every two years. The ADS conforms with this RG with the clarification that for the DPVs, periodic testing is interpreted to mean testing of the squib initiators in a laboratory after removal from the squib valves. Refer also to Subsection 7.3.1.1.4.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The ADS meets the guidance of RG 1.47. Automatic indication is provided in the MCR to inform the operator the system is inoperable or a division is bypassed.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The ADS meets the guidance of RG 1.53 and (IEEE Std. 603, Section 5.1) and (IEEE Std. 379).

RG 1.62 - Manual Initiation of Protective Actions:

- Conformance: The ADS conforms with this RG. Manual actuation of ADS requires the operator to actuate at least two dual action switches. This ensures that manual initiation of ADS is a premeditated act.

RG 1.75 - Physical Independence of Electric Systems:

- Conformance: The ADS design conforms with RG 1.75. See chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for a discussion of how the design meets the requirements of RG 1.75.

RG 1.105 - Instrument Setpoints for Safety Related Systems:

- Conformance: The setpoints used to initiate ADS are consistent with this guide. Because the discrete setpoints in the ADS logic do not drift, most of the variation is expected to be in the process transmitters. Setpoints are continuously monitored and alarmed by the plant computer functions (PCF). The GE design document, “General Electric Instrument Setpoints Methodology”, Reference 7.3-2, provides a detailed description of this methodology.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems:

- Conformance: The ADS conforms with the guidance of RG 1.118. A full functional test of the ADS is not practical, because a LOCA results if the non-reclosable DPVs are opened. Acceptable reliability of equipment operation is demonstrated by alternate test methods. System logic is periodically self-tested, and initiating circuits are continuously monitored as described in Subsection 7.3.1.1.2. DPV valve initiators periodically are removed and test-fired in a laboratory. RPV level transmitters are located outside containment. Calibration verification can be performed during plant operation.

RG 1.152 - Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms with RG 1.152.

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The ADS design conforms with RG 1.153.

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

- Conformance: The ADS design conforms with RG 1.168.

RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The ADS design conforms with RG 1.169.

RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms with RG 1.170.

RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms with RG 1.171.

RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms with RG 1.172.

RG 1.173 – Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms with RG 1.173.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The ADS design conforms with RG 1.180.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The ADS design conforms with RG 1.204.

7.3.1.1.3.5 Branch Technical Positions

BTP HICB-3 - Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service:

- This BTP is not applicable to the design because there is no reactor coolant pump.

BTP HICB-4 -Guidance on Design Criteria for Auxiliary Feedwater Systems:

- This BTP is not applicable to the ADS.

BTP HICB-6 - Guidance on Design of I&C Provided to Accomplish Changeover from Injection to Recirculation Mode:

- There is no recirculation pump and no active ECCS pumps. Therefore, this BTP is not applicable.

BTP HICB-8 - Guidance on Application of RG 1.22:

- This BTP calls for the identification of the actuated equipment not tested during reactor operation, and for a discussion of how each conforms with the justification criteria of Paragraph D.4 of RG 1.22.

  Because the DPVs are squib-actuated and cannot be closed once they are opened, there is no practicable system design to allow testing during reactor operation without creating an unacceptable breach of the Reactor Coolant Pressure Boundary (RCPB). The SRVs may be tested with the reactor at low power and at, or near, rated pressure. Both the squib wires and the SRV solenoids are continuously monitored for electrical continuity, as indicated in Subsection 7.3.1.1.3.

  The SRVs and DPV initiators can be tested when the reactor is shut down.

BTP-HICB-11 - Guidance on Application and Qualification of Isolation Devices:

- The ADS conforms with this BTP. ADS logic is controlled by the SSLC/ESF system. SSLC/ESF logic controllers use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices. The Q-DCIS provides the communication functions for SSLC/ESF. See Subsections 7.1.2, 7.1.3.2 and 7.1.3.3 for a description of the Q-DCIS communication system design.

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints:

- The ADS conforms with BTP HICB-12. See Reference 7.3-2.

BTP HICB-13 – Guidance on Cross Calibration of Protection System Resistance Temperature detectors:

- This BTP does not apply to the ADS, since this system does not use RTD-type sensors.

BTP HICB-14 – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- The ADS conforms with BTP HICB-14.

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- This BTP is applicable to all Sections, including this ADS section on ADS, whose content conforms with BTP HICB-16.

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions:

- The ADS conforms with BTP HICB-17.

BTP HICB-18 - Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and control Systems:

- The ADS conforms with BTP HICB-18.

BTP HICB-19 - Guidance on Evaluation of Defense-in-Depth and Diversity in digital Computer-based Instrumentation and Control Systems:

- The ADS conforms with BTP HICB-19.

BTP HICB-21 – Guidance on Digital Computer Real-Time Performance:

- The ADS conforms with BTP HICB-21.

7.3.1.1.4 Testing and Inspection Requirements

The ADS trip logic units continuously self-test (IEEE Std. 603, Sections 4.12, 5.7 and 6.5), as shown in Table 7.3-1. A very low current is used to test the continuity of the SRV pilot solenoids and the bridge wires within the DPV squib valve actuating circuitry. The test current is continuously applied, and triggers an alarm if the circuit is interrupted. Testing of ADS equipment is conducted during refueling outages. Refer to Subsection 6.3.2.8.4 for a discussion of mechanical tests performed on the ADS. The same continuity test also is applied to the GDCS squib valves described in Subsection 7.3.1.2.

7.3.1.1.5 Instrumentation and Control Requirements

System status during normal plant operation and ADS performance monitoring (IEEE Std. 603, Section 5.8) in an accident relies on the following MCR indications (additional discussion on the ADS instrumentation is contained in subsection 7.3.1.1.2):

- Status indication of the SRVs and DPVs;
- SRV discharge line temperature alarm;

- RPV pressure indication;
- Suppression pool high/low level alarm;
- GDCS pool low level alarm;
- Water level indication for the GDCS pools, suppression pools, and RPV; and
- Alarms for the following ADS parameters in the MCR:
  - Manual arming of ADS,
  - Manual actuation of ADS,
  - Two-out-of-four ADS Level 1 signals,
  - Automatic ADS initiation,
  - Aborted ADS initiation,
  - SRV solenoid loss of continuity,
  - DPV squib firing circuit loss of continuity,
  - Inconsistent wide range divisional water level alarms,
  - Any inconsistency of divisional input information from the four SSLC/ESF divisions to each Voter Logic Unit (VLU), as compared at the VLU, and
  - Any single load driver/discrete output trip in the firing circuit of a DPV or SRV.

ADS instrumentation essential for system operation (located in the drywell) is designed to operate in the environment resulting from a Loss of Coolant Accident (LOCA). Safety-related instruments located outside the containment also are qualified for the environment in which they must perform their safety function.

7.3.1.2 Gravity-Driven Cooling System

The basic components of the GDCS are within the containment. The GDCS pools, piping and valves are in the drywell. The suppression pool is on the outer periphery of the drywell within the containment envelope.

7.3.1.2.1 System Design Bases

The GDCS I&C is designed to meet the following safety-related requirements (IEEE Std. 603, Sections 4.1, 4.2, 4.5, 5.1, 5.8, 6.2, 7.2, and 7.3) and 10 CFR 50.2 Design Bases:

- Automatically initiate the GDCS to prevent fuel-cladding temperatures from reaching the limits of 10 CFR 50.46.

- Respond to a need for emergency core cooling following reactor depressurization, regardless of the physical location of the malfunction or break causing the need.
- Be completely automatic in operation. Manual initiation of GDCS is possible at any time, providing protective interlocks have been satisfied.
- Prevent the inadvertent actuation of the deluge valves thus preventing inadvertent draining of the GDCS pools.
- No single control logic and instrumentation failure will inadvertently open a GDCS injection valve or equalizing valve.
- Instrumentation indicating GDCS valve positions and GDCS pool levels is displayed on a mimic of the system in the MCR.

7.3.1.2.2 System Description

The GDCS comprises four injection lines from the three GDCS pools to the RPV and four equalization lines from the suppression pool to the RPV. There are two valves on each injection line, with four squib initiators per valve (three divisional initiators and one from the DPS [see Section 7.8]), for a total of eight GDCS injection valves and 32 squib initiators. There is one squib valve on each of the four equalizing lines and four squib initiators per valve (three divisional initiators and one from the DPS [see Section 7.8]), for a total of four equalizing valves and 16 squib initiators. The equalizing valves are used after reactor core decay heat has boiled away sufficient vessel inventory added by the GDCS to again begin lowering the RPV water level. With three divisional initiators per valve, the system can lose two divisions of power and still perform its intended function.

The GDCS pools are located within the drywell at an elevation significantly above the top of active fuel (TAF). The suppression pool is located within the drywell, with a water level a few meters above the TAF.

Redundant safety-related level transmitters - two for each pool - continuously monitor the GDCS pool water level. These values are continuously shown on the safety-related and nonsafety-related displays. Both high and low pool levels result in alarms from the plant computer functions (part of N-DCIS).

The overall design of the system assures that, when needed, all eight injection valves and all four equalizing valves are fired - even with a complete failure of any two divisions. However, no squib is fired inadvertently as a result of any single failure.

Automatic Operation

Actuation of the GDCS injection sub-system is performed automatically, without need for operator action once the RPV water surface reaches level 1. It is also possible for the plant operator to manually initiate the GDCS injection sub-system, or to individually fire squib initiators independently by sending trip signals to the automatic logic. The manual initiation of the GDCS injection sub-system is interlocked with a low reactor pressure signal to ensure that the GDCS pools are capable of flooding the reactor.

Following the initial start signal (opening the ADS and GDCS valves), after a time delay (Table 7.3-4), and when the RPV water surface drops below RPV Level 0.5 (1m above TAF), the four equalizing squib valves mounted on the suppression pool equalizing lines are actuated. With three divisional initiators per valve, the system can tolerate the complete loss of two divisions of power and still perform its intended function. It is also possible for the operator manually to initiate the equalizing valves, or to individually fire squib initiators independently by sending trip signals to the automatic logic.

Manual Operation

The safety-related VDUs in the MCR provide a display format allowing the operator to manually open each GDCS injection valve independently, using the primary SSLC/ESF logic function (IEEE Std. 603, Sections 5.8, 6.2 and 7.2). Each nonsafety-related VDU in the MCR provides a display format allowing the operator to individually open each GDCS injection valve independently, using the DPS logic function. Each display uses an "arm/fire" configuration (interlocked with a low reactor pressure signal) requiring at least two deliberate operator actions. Operator use of the "arm" portion of the display triggers a plant alarm. The two manual opening schemes from the SSLC/ESF and from the DPS are diverse.

In addition the safety-related VDUs in the MCR provide a display format allowing the operator manually to open each GDCS equalizing valve independently, using the primary SSLC/ESF logic function (IEEE Std. 603, Sections 5.8, 6.2 and 7.2). Each nonsafety-related VDU in the MCR provides a display format allowing the operator to individually open each GDCS equalizing valve independently, using the DPS logic function. Each display uses an "arm/fire" configuration requiring at least two deliberate operator actions (interlocked with a low reactor pressure signal). Operator use of the "arm" portion of the display triggers a plant alarm. The two manual opening schemes from the primary SSLC/ESF and from the DPS are diverse.

Each safety-related VDU provides a display with an "arm/fire" switch (one per division, for a total of four) manually to initiate the GDCS sequence as a system, instead of initiating each valve individually (IEEE Std. 603, Sections 5.8, 6.2 and 7.2). If the operator uses any two of the four switches, the GDCS sequence seals in and starts the GDCS valve sequencing (IEEE Std. 603, Section 5.2). (This manual actuation also is interlocked with a low reactor pressure signal.) This requires four deliberate (two-arm and two-fire) operator actions. For all of the manual initiations, operator use of the "arm" portion of the display triggers a plant alarm.

Actuation Logic

The logic elements providing controls for the actuation of the GDCS injection and equalizing squib valves are contained in the ESF portion of the Q-DCIS, outside the drywell containment. RPV level transmitters used to initiate GDCS are part of the NBS, and are located on racks outside the drywell.

The SSLC/ESF logic sends an initial start signal to the GDCS logic that automatically initiates the GDCS following reactor depressurization under Loss-of-Coolant-Accident (LOCA) conditions.

Each of the two trains per division is presented with the initial start signal from the same SSLC/ESF logic initiating the ADS. The SSLC/ESF logic adds a time delay (Table 7.3-4) to the initial start signal, and then operates all of the GDCS injection valves. Once the initial start signal is given to both ADS and GDCS (starting the various timers), the sequence is sealed in and cannot be aborted by the plant operator.

The GDCS injection and equalizing valve logic includes the SSLC/ESF "division of sensors" bypass switch, two-out-of-four trip decisions, and single-failure proof actuation logic - with any three of the four divisions of safety-related power available. The valve logic also is single-failure proof against inadvertent actuation, meaning each division of logic has two trains - each of which must operate for the associated squib valves to fire.

The wide range level sensors that are used for the ADS logic and fuel zone range RPV water level are also used for the GDCS equalizing valve logic; these are diverse from the sensors used for RPS functions and from those used by the DPS. Both sets of transmitters belong to the NBS.

The generation of the initial start signal for the GDCS is described in Subsection 7.3.1.1.2. The logic for all squib initiators is similar. The signals are acquired per division by RMUs of the same division. The data is sent via fiber optic cables to the SSLC/ESF cabinets located in the corresponding divisional I&C equipment rooms in the Control Building (CB). Each division's logic compares the measured parameters to setpoints. If there is a discrepancy outputs a sensor trip signal is sent both to its own division and to each of the other divisions by appropriately isolated fiber optic cables.

Each division has access to all four divisional sensor trip signals, and performs a redundant two-out-of-four vote on the four sensor trip signals. (The vote is two-out-of-three if one division is bypassed, because no more than one division can be bypassed at any one time.)

Each division therefore has two separate trip logics that can independently perform a two-out-of-four vote on the sensor trips. The effect is that any two divisions sensing the appropriate trip conditions results in all divisions providing a trip signal.

The existence of the multiple logic trips per division is necessitated by the requirement that no injection or equalizing squib valve inadvertently be fired as the result of a single failure (IEEE Std. 603, Section 5.1).

For the eight GDCS injection squib valves logic, each of the two (per division) initial start signals actuates an adjustable timer with a preset time delay (as specified in Table 7.3-4). After the time delay, each of the two timers outputs a trip signal to the GDCS squib load drivers/discrete outputs. There are eight injection squib valves, with three divisional squib initiators, and one DPS squib initiator per valve.

Within the RMU, for each squib initiator, there is a series circuit of divisional power, two load drivers/discrete outputs in series, a current monitor, and a normally closed keylock switch. Each of the two timers must transmit a trip signal to the corresponding series load driver/discrete output. The effect is that both two-out-of-four trip voters, both timers, and both load drivers/discrete outputs must operate to fire the squib initiator, making the design single failure proof against inadvertent actuation. Because each GDCS injection squib valve always has three

squib initiators, powered by three different divisions, the design is also single-failure proof if required to operate all eight valves, and even will initiate with the loss of two divisions of power.

The current monitor continuously verifies squib electrical continuity, and the keylock switch is used when performing maintenance or surveillance testing, or testing the current monitor. If the keylock switch opens the circuit, an alarm signal is sent to the MCR, indicating that the squib initiator (not the valve) is inoperable.

For diversity, the DPS also is able to fire its squib electrical initiator on each of the eight GDCS injection squib valves, using single-failure proof logic (both to operate and to avoid inadvertent operation). This is accomplished using a completely separate squib initiator connected to the DPS system (see Figure 7.3-1b). The DPS system uses diverse (from the ECCS) sensors, hardware, and software to operate the GDCS injection valves.

Figure 7.3-2 shows the initiation logic of a typical equalizing squib valve.

Within the RMU, for each squib initiator, there is a series circuit of divisional power, two load drivers/discrete outputs in series, a current monitor, and a normally closed keylock switch. To fire the squib initiator, each of the two equalization valve timers and two Level 0.5 outputs must transmit a trip signal to the corresponding series load driver/discrete outputs. The effect is that both two-out-of-four trip Level 0.5 voters, both timers, and both load drivers/discrete outputs must all operate to fire the squib initiator, making the design single-failure proof against inadvertent actuation.

Because each equalizing valve always has three divisional squib initiators powered by three different divisions, the design is also single-failure proof whenever required to operate all four valves, with any three of the four divisions of safety-related power available. The equalizing valves are needed for the long term, so they are not automatically operated by the DPS system. However, they are included in the manually initiated GDCS valve logic, and also may be fired individually from safety-related VDU displays or nonsafety-related DPS VDU displays.

Deluge System

The Deluge system is designed to flood the containment floor in the event of a core breach that results in molten fuel on the containment floor. This system is made up of two individual and identical trains both of which contain an automatic actuation and manual actuation ability. There are 12 deluge valves each with two squib initiators (one for each train). Each of these valves feeds the Basemat-Internal Melt Arrest Coolability (BiMAC) system, which floods the containment floor following a severe accident. The BiMAC system is described in more detail in Section 6.2.1. A typical squib deluge valve is shown in Figure 6.3-2. The logic for the deluge valves is executed in a pair of dedicated nonsafety-related PLCs and a pair of dedicated safety-related temperature switches.

Automatic actuation of the deluge valves is accomplished in concert with lower drywell high temperature. The containment floor is divided into 30 equal-area cells, with two installed in each cell. One thermocouple from each cell is monitored in one PLC, while the other thermocouple from each cell is monitored in a second PLC. When temperatures exceed the setpoint (see Table 7.3-4) at one set of thermocouples coincident with setpoints being exceeded at a second set of thermocouples in adjacent cells, a trip signal is generated in each PLC.

The trip signal in each PLC starts an adjustable deluge squib valve non-bypassable timer. At the end of the deluge squib valve set time delay, each of the two timers outputs a trip signal to the respective deluge valve squib load driver/discrete output. The timer outputs are wired in series so each of the two timers must transmit a temperature trip signal to the corresponding series load driver/discrete output. Additionally, a pair of dedicated safety-related temperature switches monitor the drywell temperature below the RPV. Each temperature switch uses a capillary and bulb action to close a contact wired in series with the PLC timer outputs. The effect is that both PLC timer outputs and both temperature switch outputs must operate to fire the squib initiator. The temperature switches serve as permissives for the deluge logic. These temperature switches are safety-related to prevent inadvertent actuation of the deluge system, which could needlessly drain the GDCS pools.

The deluge logic is completely separate from and independent of the Q-DCIS and the N-DCIS, and is powered by dedicated batteries supported by battery chargers operating on nonsafety-related power. The deluge valves also are powered by a pair of dedicated batteries supported by battery chargers operating on nonsafety-related power. The batteries for the deluge valves are separate from and independent of the batteries for the deluge logic. Each of these batteries can fire all 12 deluge valve squibs. All of the deluge batteries are separate from and independent of the other plant batteries.

The logic elements providing the controls for the actuation of the deluge valves are contained within a separate pair of dedicated nonsafety-related PLCs and a pair of dedicated safety-related thermocouples and associated temperature switches. The only safety-related function of the deluge logic is prevention of inadvertent actuation. The deluge logic is independent from all the other plant controls, and also is located outside containment.

Temperature indications and alarms, as well as continuity alarms and valve open/close indications for each squib valve are available in the MCR. Each valve has a normally closed keylock switch available for maintenance purposes.

Two control switches are furnished in the MCR, to allow the operator manually to open the 12 deluge valves. These switches are of the “arm/fire” type, and are wired in series such that four deliberate operator actions (two for “arm” and two for “fire”) are required to operate the valves. These switches actuate the squib initiator on each deluge valve. Operator use of the “arm” portion of the switch triggers a plant alarm in the PCF.

7.3.1.2.3 Safety Evaluation

Section 6.3 evaluates the individual and combined capabilities of ADS and GDCS. For the entire range of nuclear process system break sizes, the ECCS (ADS and GDCS) ensures that the reactor core is always submerged.

Instrumentation initiating the ADS and GDCS injection and equalizing functions must respond to the potential inadequacy of core cooling regardless of the location of the breach in the RCPB. Such a breach inside or outside the containment is sensed by RPV low water level. This signal is completely independent of breach location, and is therefore used to initiate the GDCS injection and equalizing functions.

The two temperature switches and the related contacts, are part of the deluge system, are safety-related only to prevent the inadvertent actuation of the deluge valves. No single-failure within the deluge system control and monitoring equipment causes an inadvertent actuation of the deluge system (IEEE Std. 603, Section 5.1). This is to protect against inadvertently draining the GDCS pools, thereby preventing the injection and equalizing systems from performing their safety functions.

No operator action is required to initiate the correct response of the GDCS. If the system fails to initiate, the MCR operator manually accomplishes GDCS initiation through controls and displays in the MCR. Sufficient alarms and indications in the control room allow the operator to assess the performance of the GDCS. Specific instrumentation is addressed in Subsection 7.3.1.2.5.

The redundancy of the control and monitoring equipment for the GDCS injection and equalizing functions is consistent with the redundancy of the four divisions of the GDCS. Control and monitoring equipment is located in the MCR and is under the supervision of the control room operator.

The initiation scheme for the GDCS injection and equalizing functions is designed such that no single-failure in the initiation circuitry, with any three of the four divisions of safety-related power available, can prevent the GDCS from providing the core with adequate cooling. This is assured by the redundancy of the components in the four divisions of the GDCS.

The GDCS has no equipment protective interlocks that could interrupt automatic system operation. To initiate the GDCS injection and equalization systems manually, a RPV low-pressure signal must be present. This prevents system initiation while the reactor is at operating pressure. The GDCS injection and equalizing functions are designed to operate from safety-related power. The system instrumentation is powered by divisionally separated safety-related power. The injection squib valve, and the equalizing squib valve logic and initiation circuitry is powered by divisionally separated, safety-related power (Refer to Section 8.3). The mechanical aspects of the GDCS are discussed in Subsection 6.3.2.

Two temperature switches per train and the related contacts are part of the deluge system and are safety-related only to prevent the inadvertent actuation of the deluge valves. No single failure within the deluge system control and monitoring equipment causes an inadvertent actuation of the deluge system (IEEE Std. 603, Section 5.1). This is to ensure against inadvertently draining the GDCS pools, and thereby preventing the injection and equalizing functions from performing their safety functions.

Table 7.1-1 identifies the GDCS and the associated codes and standards applied in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards. Any exceptions or clarifications are so noted.

7.3.1.2.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: GDCS complies with these standards.

10 CFR 50.55a(h), Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: safety-related systems are in conformance with RG 1.153 and IEEE Std. 603 as discussed in Subsection 7.1.6.4. Separation and isolation is preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6 and RG 1.75. The GDCS is divisionalized and redundantly designed with redundancy so failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

10 CFR 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication:

- Conformance: GDCS demonstrates compliance by providing automatic indication of bypassed and in operable status (IEEE Std. 603, Section 5.8).

10 CFR 50.34(f)(2)(xiv)(II.E.4.2), Containment Isolation Systems:

- Conformance: GDCS complies with this requirement.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this Section.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the GDCS within the DCD conforms with this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.1.2.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, and 24:

- Conformance: The GDCS complies with these GDCs.

7.3.1.2.3.3 Staff Requirements Memorandum

SECY-93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: The GDCS conforms with these criteria by providing diverse I&C, as described in Section 7.8.

7.3.1.2.3.4 Regulatory Guides

RG 1.22 - Periodic Testing of Protection System Function:

- Conformance: System logic is tested continually as described in Subsection 7.3.1.2.4. Components are tested periodically during refueling outages. The GDCS complies with RG 1.22.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety:

- Conformance: The GDCS meets the requirements of RG 1.47. Automatic indication is provided in the MCR to inform the operator the system is inoperable or a division is bypassed.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The GDCS meets the requirements of RG 1.53, IEEE Std. 603, Section 5.1, and IEEE Std. 379.

RG 1.62 - Manual Initiation of Protective Actions:

- Conformance: The GDCS complies with RG 1.62. Each division of the GDCS has a manual actuation switch in the MCR. Initiation of the system requires actuation of two switches to ensure that manual initiation is a premeditated act. There is an interlock between the manual initiation switches and a low reactor-pressure signal. This interlock prevents manual initiation of the system if the RPV is not depressurized.

RG 1.75 - Physical Independence of Electric Systems:

- The GDCS design conforms with RG 1.75. See chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for a discussion of how the design meets the requirements of RG 1.75.

RG 1.105 - Instrument Setpoints for Safety-Related Systems:

- Conformance: The setpoints used to initiate GDCS are established consistent with this guide. Reference 7.3-2 provides a detailed description of the GEH methodology.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems:

- Conformance: The GDCS complies with the guidance of RG 1.118.

RG 1.152 - Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms with RG 1.152.

RG 1.153 - Criteria for Power, I&C Portions of Safety Systems:

- Conformance: The GDCS complies with RG 1.153.

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

- Conformance: The GDCS design conforms with RG 1.168.

RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The GDCS design conforms with RG 1.169.

RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms with RG 1.170.

RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms with RG 1.171.

RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms with RG 1.172.

RG 1.173 – Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms with RG 1.173.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The GDCS design conforms with RG 1.180.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The GDCS design conforms with RG 1.204.

7.3.1.2.3.5 Branch Technical Positions

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following BTPs are addressed for the GDCS:

BTP HICB-1 - Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System:

- Because the portion of the GDCS downstream of the squib valves connected to the RPV has a design pressure equivalent to the reactor operating pressure, and the low pressure portion of the GDCS upstream of the squib valves is open to the GDCS pools, there is no need for overpressure protection of the low pressure portion. A high pressure interlock is provided to prevent inadvertent manual initiation of the GDCS.

BTP HICB-3 - Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service:

- This BTP is not applicable because the design has no reactor coolant pumps.

BTP HICB-4 -Guidance on Design Criteria for Auxiliary Feedwater Systems:

- This BTP is not applicable to the GDCS.

BTP HICB-6 - Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode:

- There is no recirculation pump and no active ECCS pumps. Therefore, this BTP is not applicable.

BTP HICB-8 - Guidance on Application of RG 1.22:

- This BTP requires the identification of actuated equipment not tested during reactor operation and a discussion of how each conforms with the provision of Paragraph D.4 of RG 1.22. In the GDCS, the squib valves are not actuated during reactor operation, because their actuation would adversely affect the operation of the plant by resulting in a reactor shutdown.
  - Given the GDCS system requirements for zero RCPB leakage over the 60-year life of the plant, the only practical solution is for the system actuation valve to be non-reclosing with a metal diaphragm seal that is ruptured to initiate system flow.
  - The GDCS is designed to provide adequate inventory make-up to the core in the event of a LOCA. The system has sufficient redundancy and reliability that core-cooling requirements are met in the event of a LOCA.

BTP-HICB-11 - Guidance on Application and Qualification of Isolation Devices:

- SSLC/ESF logic controllers for GDCS use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints:

- GDCS logic resides within the SSLC/ESF conforming with BTP HICB-12.

BTP HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors:

- This BTP does not apply to GDCS or to SSLC/ESF neither of which uses the instruments.

BTP HICB-14 – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- The GDCS conforms with BTP HICB-14.

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR 52:

- The GDCS conforms with BTP HICB-16

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions:

- The GDCS conforms with BTP HICB-17.

BTP HICB-18 - Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and control Systems:

- The GDCS conforms with BTP HICB-18.

BTP HICB-19 - Guidance on Evaluation of Defense-in-Depth and Diversity in digital Computer-based Instrumentation and Control Systems:

- The GDCS conforms with BTP HICB-19.

BTP HICB-21 – Guidance on Digital Computer Real-Time Performance:

- The GDCS conforms with BTP HICB-21.

7.3.1.2.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for Section 7.3 and Table 7.1-1, only Three Mile Island (TMI) I.D.3 and II.E.4.2 (addressed above) are considered applicable to the GDCS. Listed below are the TMI requirements that applied to previous ECCS systems in operating Boiling Water Reactors, (BWRs) and to licensed applicants potentially could apply for the GDCS. Following each TMI requirement is a brief discussion on why it does not apply to the GDCS:

TMI II.K.3(13) - HPCI and RCIC Initiation Levels:

- GDCS initiates on low-low water level and drains by gravity to the RPV. There is no high-level isolation or low-level restart with this system. This TMI item does not apply.

TMI II.K.3(15) - Isolation of HPCI and RCIC:

- This TMI item applies to ECCS with steam-driven pumps using differential pressure sensors on elbow taps in the steam supply line to isolate the steam supply in the event of a pipe break. The GDCS uses gravity to produce system-driving head. The system has no steam-driven pumps. This TMI item does not apply to the GDCS.

TMI II.K.3(21) - Restart of Core Spray and Low Pressure Coolant Injection Systems:

- This TMI item applies to Core Spray and Low Pressure Coolant Injection Systems that can be stopped by the operator. Once GDCS is initiated, the operator does not have the ability to stop it from completing the initiation sequence. This TMI item does not apply to the GDCS.

TMI II.K.3(22) - Automatic Switchover of RCIC Suction:

- This TMI item applies to reactor cooling systems that can take suction from multiple water sources. The GDCS takes suction from the GDCS pools and does not have the capability to manually or automatically switch over to an alternate source. This TMI item does not apply to the GDCS.

7.3.1.2.4 Testing and Inspection Requirements

The GDCS trip logic units are self-tested continually at preset intervals. The trip logic units of each logic division, and the timers for the automatic logic, can be tested during plant operation (IEEE Std. 603, Sections 5.7 and 6.5). GDCS equipment inside containment is tested during refueling outages. Refer to Subsection 6.3.2.7.4 for a discussion of mechanical tests performed on the GDCS.

7.3.1.2.5 Instrumentation and Control Requirements

The performance and effectiveness of the GDCS in a postulated accident is verified by observing the following control room indications (IEEE Std. 603, Section 5.8) (additional Discussion on the GDCS instrumentation is contained in Subsection 7.3.1.2.2 and in Subsection 6.3.2.7.5):

- Status indication of locked-open maintenance valves;
- Status indication and alarm of the squib-actuated valves;
- Position indication of the GDCS check valves;
- Drywell and RPV pressure indication;
- Suppression pool high/low level alarm;
- GDCS pool high/low level alarm;
- Water level indication for the GDCS pools, suppression pools and RPV; and
- Squib valve open alarm.

The GDCS instrumentation that is essential for system operation is designed to operate in a drywell environment resulting from a LOCA. The thermocouples that initiate the deluge valves are qualified to operate in a severe accident environment. Safety-related instruments, located outside the drywell, are qualified for the environment in which they must perform their safety-related function.

7.3.2 Passive Containment Cooling System

The Passive Containment Cooling System (PCCS) consists of heat exchanger loops that are an extension of the containment pressure boundary. The PCCS heat exchanger tubes are located in a pool of water the Isolation Condenser/Passive Containment Cooling (IC/PCC pool) outside the containment. A rise in containment (drywell) pressure above the pressure suppression pool (wetwell) pressure, similar to what occurs during a loss of reactor coolant into the drywell, forces flow through the PCCS heat exchanger loops. Condensate from the PCCS drains to the GDCS

pools. As the flow passes through the PCCS heat exchangers, heat is rejected to the IC/PCC pool, thereby cooling the containment atmosphere. This action occurs automatically, without the need for actuation of components. The PCCS does not have instrumentation, control logic, or power-actuated valves, and does not need or use electrical power for its operation. Other information on the PCCS is given in Subsection 6.2.2 and leak rates are discussed in subsection 16B.3.3.

7.3.3 Leak Detection and Isolation System

The primary function of the Leak Detection and Isolation System (LD&IS) is to detect and monitor leakage from the RCPB and to initiate the appropriate safety action to isolate the source of the leak. The system is designed to automatically initiate the isolation of certain designated process lines penetrating the containment, to prevent release of radioactive material from the RCPB. The initiation of the isolation functions closes the appropriate containment isolation valves. The LD&IS functions are performed in two separate safety-related platforms. The Main Steam Isolation Valve (MSIV) isolation logic functions are performed in the Reactor Trip and Isolation Function (RTIF) platform, while all other containment isolation logic functions are performed in the SSLC/ESF platform.

7.3.3.1 System Design Bases

The following system design criteria are applicable to the design of the LD&IS (IEEE Std. 603, Sections 5.1, 5.2, 5.6, 5.7, 5.9, 6.1, and 6.8):

- The LD&IS is engineered as a safety-related system, Seismic Category 1, and conforms with the regulatory requirements, guidelines, and industry standards listed in Table 7.1-1 for this system.
- The LD&IS logic design is fail-safe, such that loss of electrical power to one LD&IS divisional logic channel initiates a channel trip.
- Isolation is initiated with precision and reliability once leakage has been detected from the RCPB.
- Once isolation is initiated, the action goes to completion. Deliberate operator action is required to reopen the isolation valves.
- The LD&IS design meets the single failure criterion because no single failure within the system, with any three of the four divisions of safety-related power available, initiates inadvertent isolation or prevents isolation when required.
- Automatic isolation is initiated by coincidence of any two-out-of-four channel trips, as appropriate for each monitored variable.
- Electrical communication and physical independence is maintained between safety-related divisions and between safety-related and nonsafety-related equipment.

- The LD&IS design incorporates provisions to permit bypass of a single division of sensors at any one time.
- LD&IS instrumentation uses a diversity of sensed parameters and redundant channels for initiation of containment isolation.
- Manual isolation capability is provided for diversity from the automatic logic.
- The containment leak detection methods described in RG 1.45 are adopted in the LD&IS system design.
- Identified and unidentified leakages within the containment are monitored separately to quantify the flow rates.
- The LD&IS provides different divisional isolation signals to the containment isolation valves.

7.3.3.2 System Description

The LD&IS is a four-divisional system designed to detect and monitor leakage from the RCPB, and, in certain cases, isolate the source of the leak by initiating closure of the appropriate containment isolation valves. The LD&IS control and isolation logic uses two-out-of-four coincidence voting channels for each plant variable monitored for containment isolation. Various plant variables are monitored, such as flow, temperature, pressure, RPV water level, and radiation level. These are used in the logic to initiate alarms and the required control signals for containment isolation. Two or more diverse leakage parameters are monitored for each specific isolation function. The LD&IS logic functions reside in the framework of the RTIF and the SSLC/ESF platforms, where trip signals are generated, initiating the isolation functions of the LD&IS.

The following control and isolation functions are implemented by the LD&IS:

- Containment isolation following a LOCA event,
- Main steam lines and drain lines,
- ICS process lines,
- Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC) System process and sampling lines,
- Fuel and Auxiliary Pools Cooling System (FAPCS) suction lines and discharge from the GDCS pools,
- Chilled water system lines to drywell coolers,
- Drywell sumps liquid drain lines,
- Containment purge and vent lines,
- RB area air supply and exhaust ducts,

- Feedwater process lines, and
- Fission products sampling lines.

The following sources of leakage are detected and monitored:

- Condensate flow from the upper and lower drywell air coolers,
- Leakage to the drywell from valves equipped with leak off lines between the two valve stem packings,
- Fission product leakages into the drywell detected by the Process Radiation Monitoring System (by PRMS), and
- RPV head flange seal pressure leakage.

Drywell sump levels and flow rates are used to quantify identified and unidentified leakages.

The LD&IS control functions initiating automatic isolation functions are classified safety-related, and these functions use redundant divisional channels satisfying both the mechanical and electrical separation criteria as well as the single failure criterion (IEEE Std. 603, Sections 5.1 and 5.6). This system operates continuously during normal reactor operation, and during abnormal and accident plant conditions.

The system design is configured as shown in Figure 7.3-3. The LD&IS interfacing sensor parameters are provided in Table 7.3-5. A detailed description of detection methods, monitored plant parameters, and the monitoring instrumentation is included in Subsection 5.2.5.

7.3.3.3 Safety Evaluation

The LD&IS control and isolation functions, including the sensors and channel instrumentation, are a safety-related system, and qualified environmentally and seismically for continuous operation during normal, abnormal, and accident plant conditions. The system design is in conformance with the design bases described in Subsection 7.3.3.1. The LD&IS system design uses measurements and redundant instrument channels to detect and monitor reactor coolant leakage in (and external to) the containment, and to detect and isolate the source of the leak, thereby preventing radioactive releases to the environs. The isolation logic uses four redundant divisional channels to monitor a leakage parameter and uses the two-out-of-four coincidence voting logic technique for initiation of the isolation function. This design technique improves system availability to perform safety-related functions, satisfies the single failure criterion, and permits channel bypass for maintenance and repair during normal plant operation. Loss of one channel due to failure or power loss does not cause inadvertent isolation.

The four redundant divisional channels of the LD&IS comprise a fail-safe design. The isolation logic is energized under normal conditions and de-energized to initiate the isolation function on indication of abnormal leakage.

The LD&IS logic is designed to seal-in the isolation signal once the trip has been initiated (IEEE Std. 603, Section 5.2). The isolation signal overrides any control action to trigger the closure of

isolation valves. Reset of the isolation logic is required before any isolation valve manually can be opened.

The system logic design incorporates provisions to permit bypass of a single division of sensors at one time for repair and maintenance without affecting system capability to perform its safety-related functions. While in the Bypass mode, no other division of sensors simultaneously can be bypassed.

Manual control switches and associated logic are provided in the design of the LD&IS to give the operator the capability to perform manual control functions for initiation of isolation, logic reset, channel bypass and test functions (IEEE Std. 603, Section 6.2 and 7.2).

The instrumentation for the drywell Low Conductivity Waste (LCW) and High Conductivity Waste (HCW) sump levels is designed to meet the leakage rate requirements for identified and unidentified sources. The LD&IS includes isolation logic using the radiation detected in the LCW & HCW for the isolation of the drain lines transferring waste from the sumps to the liquid radwaste system. Additional information on LD&IS operation is contained in subsection 5.2.5.

Table 7.1-1 identifies the LD&IS function and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.3.3.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The LD&IS complies with these standards.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6, and RG 1.75. The LD&IS consists of four redundantly designed divisions so failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

10 CFR 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication:

- Conformance: The LD&IS demonstrates compliance by providing automatic indication of bypassed and inoperable status. (IEEE Std. 603, Subsection 5.8).

10 CFR 50.34(f)(2)(xiv)(II.E.4.2), TMI Action Plan Item IIE.4.2 Containment Isolation Systems:

- Conformance: LD&IS complies with this requirement.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: The resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in the Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the LD&IS in the DCD conform to this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, and 24:

- Conformance: The LD&IS complies with the GDCs identified above.

7.3.3.3.3 Staff Requirements Memorandum

SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The LD&IS and ESF designs conform with item II.Q of SECY-93-087 (BTP HICB-19) by implementation of diverse I&C, described in Section 7.8.

7.3.3.3.4 Regulatory Guide

RG 1.22 – (Safety Guide 22) Periodic Testing of Protection System Actuation Function:

- Conformance: The LD&IS design conforms with RG 1.22.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System:

- Conformance: The LD&IS design conforms with RG 1.47.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The LD&IS design conforms with RG 1.53.

RG 1.62 - Manual Initiation of Protective Actions:

- Conformance: The LD&IS design conforms with RG 1.62.

RG 1.75 - Physical Independence of Electric Systems:

- Conformance: The LD&IS design conforms with RG 1.75. See Chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for a discussion of how the design meets the requirements of RG 1.75.

RG 1.105 - Setpoints for Safety-Related Instrumentation:

- Conformance: The LD&IS design conforms with RG 1.105.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems:

- Conformance: The LD&IS design conforms with RG 1.118.

RG 1.152 - Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS design conforms with RG 1.152.

RG 1.153 - Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The LD&IS design conforms with RG 1.153.

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

- Conformance: The LD&IS design conforms with RG 1.168.

RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The LD&IS design conforms with RG 1.169.

RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS design conforms with RG 1.170.

RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS design conforms with RG 1.171.

RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS design conforms with RG 1.172.

RG 1.173 – Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS design conforms with RG 1.173.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The LD&IS design conforms with RG 1.180.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The LD&IS design conforms with RG 1.204.

7.3.3.3.5 Branch Technical Positions

BTP HICB-3 - Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service:

- This BTP is not applicable to the design, which has no reactor coolant pump.

BTP HICB-4 -Guidance on Design Criteria for Auxiliary Feedwater Systems:

- This BTP is not applicable to the ADS.

BTP HICB-6 - Guidance on Design of I&C Provided to Accomplish Changeover from Injection to Recirculation Mode:

- There is no recirculation pump and no active ECCS pumps. Therefore, this BTP is not applicable.

BTP HICB-8 - Guidance for Application of RG 1.22:

- Conformance: The LD&IS complies with BTP-HICB-8.

BTP HICB-11 - Guidance on Application and Qualification of Isolation Devices:

- Conformance: The LD&IS complies with BTP-HICB-11.

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The LD&IS complies with BTP-HICB-12.

BTP HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors:

- Conformance: This BTP does not apply to the LD&IS, since this system does not use RTD-type sensors.

BTP HICB-14 - Guidance on Software Reviews for Digital Computer-Based I&C Systems:

- Conformance: The LD&IS complies with BTP-HICB-14.

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The LD&IS complies with BTP-HICB-16.

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The LD&IS complies with BTP-HICB-17.

BTP HICB-18 - Guidance on the Use of PLC in Digital Computer-Based I&C Systems:

- Conformance: The LD&IS complies with BTP-HICB-18.

BTP HICB-19 - Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems:

- Conformance: The LD&IS complies with BTP-HICB-19.

BTP HICB-21 - Guidance on Digital Computer Real-Time Performance:

- Conformance: The LD&IS complies with BTP-HICB-21.

7.3.3.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for 7.3 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) (I.D.3) and 10 CFR 50.34(f)(2)(xiv) (II.E.4.2) apply to the LD&IS. The LD&IS complies with the requirements as indicated above. TMI action plan requirements are addressed in Appendix 1A to DCD Tier 2 Chapter 1.

7.3.3.4 Testing and Inspection Requirements

7.3.3.4.1 In-service & Surveillance Tests

In-service testing of the leak detection and monitoring channels is performed periodically to verify operability during normal plant operation and to assure that each tested channel can perform its intended design function. The surveillance tests include instrument channel checks, functional tests, verification of proper sensor and channel calibration, and response time tests.

The LD&IS instrument channels use conventional sensors for leak detection and monitoring, and require no special or unique testing methods.

The setpoint verifications, trip logic tests, and channel integrity tests for the safety-related functions of LD&IS are processed and tested by the RTIF and SSLC/ESF systems.

7.3.3.4.2 Main Steam Isolation Valve Closure Tests

The LD&IS design provides manual capability and incorporates logic provisions to test closure of each of the MSIVs during normal reactor operation (IEEE Std. 603, Sections 5.7 and 6.5). To verify MSIV closure capability, each MSIV is tested periodically for partial closure while in service without causing a plant outage (IEEE Std. 603, Section 6.5).

7.3.3.4.3 Testing and Maintenance in the Bypass Mode

Testing, calibration, and maintenance are performed on the equipment in accordance with established procedures when the channel is either out of service or deliberately has been bypassed.

7.3.3.5 Instrumentation and Controls Requirements

The LD&IS is designed to detect and monitor leakage from the RCPB, using a diversity of parameters and redundant instrument channels. The monitored leakage parameters are provided

continuously to the SSLC/ESF system for processing and initiation of trips required for the isolation functions.

The LD&IS instrumentation requirements for each specific monitoring and isolation function are described in detail in Subsection 5.2.5. The plant parameters monitored for leakage detection, isolation, and alarms are summarized in Tables 5.2-8 and 5.2-9.

7.3.4 Control Room Habitability System

The Control Room Habitability System (CRHS) is an ESF system that provides a safe environment within the MCR, to allowing the operator(s) to:

- Control the nuclear reactor and its auxiliary systems during normal conditions,
- Safely shut down the reactor, and
- Maintain the reactor in a safe condition during abnormal events and accidents.

The CRHS includes:

- CB shielding and area radiation monitoring;
- Control Room Habitability Area HVAC Subsystem (CRHAVS);
- Provision for emergency food, and water storage;
- Emergency kitchen and sanitary facilities;
- Provision for protection from, and removal of airborne radioactive contaminants; and

Provision for removal of smoke.

The Control Room Habitability Area (CRHA) envelope, ventilation inlet/return isolation dampers, redundant Emergency Filtration Units (EFUs) in the emergency HVAC, and their associated controls are safety-related. Section 6.4 and Subsections 9.4.1 and 9.5.1 provide detailed information on the CRHS.

7.3.4.1 System Design Bases

The design bases of the CRHS are detailed in Subsections 6.4.1 and 9.4.1.1.

7.3.4.2 System Description

The CRHS safety-related instrumentation is designed to isolate the control room envelope on detection of the following signals and re-align to the emergency filtration mode:

- High radiation in the inlet air supply, and
- Smoke in the inlet air supply, or smoke in the CRHA general area (isolation mode).

The PRMS consists of four redundant channels to monitor the air intake to the CB. The monitoring systems warn of the presence of significant radioactive contamination in inlet air. Each redundant radiation channel consists of a gamma sensitive detector and an area radiation monitor located in the MCR. The PRMS is safety-related as described in Subsection 11.5.3.1.3.

Each PRMS sensor provides an input signal to the associated SSLC/ESF VLU, on detection of high radiation in the inlet ventilation air. Typically, each air ventilation duct has a pair of isolation dampers connected in series. Each damper is controlled by two independent solenoids from two separate divisions. During radioactive release events, the SSLC/ESF voting algorithm in each division uses two-out-of-four logic to produce an actuation signal to de-energize one of the four solenoids to close one of the redundant isolation dampers. Because the two dampers in each redundant pair are in series, any one of the two dampers can close the airflow path. Because each damper is controlled by two independent solenoids, either of the solenoids can be de-energized to close the damper. This arrangement satisfies the N-2 design basis.

The functions of the SSLC/ESF are depicted in Figure 7.3-5 and detailed information is presented in Section 7.3.5. The four redundant divisions provide a fault-tolerant architecture allowing single division of sensors bypass for on-line testing, maintenance, and repair without losing reliable trip capability. In such a bypass condition the system automatically defaults to 2-out-of-3 coincident voting. If one of the three remaining active divisions fails, the two remaining independent and redundant divisions are able to generate an actuation signal to close isolation damper(s). At least one of the redundant dampers always actuates in response to the detection of high inlet air radiation under all of the postulated design basis failures. This arrangement thus conforms with safety-related system requirements for single-failure proof capability, fault tolerance, independence, and separation, as required by IEEE Std. 603, Sections 5.1, 5.5, and 5.6.

On detection of high radiation in the inlet ventilation air, the primary EFU starts for emergency filtration mode providing air to the CRHA. The backup or secondary EFU starts automatically to continue the emergency filtration mode on a low-flow signal or failure of the primary EFU or radiation being detected downstream of the primary EFU. In such a scenario, the primary EFU fan stops and its associated duct dampers are closed for isolation. The CRHA isolation also may be actuated manually, as required by IEEE Std. 603, Sections 5.8, 6.2, and 7.2.

Smoke detectors are provided as required by NFPA 90A to detect smoke in the system ductwork and in the CRHA general areas. The detection subsystems consist of four redundant channels to monitor the air intake to the CB. Each smoke detection channel consists of redundant smoke detectors monitored in the MCR. Each detector provides input to each of the SSLC/ESF divisions. The signal processing and actuation logic are the same as described above for isolation on high radiation at the CRHA inlet. When the isolation dampers are closed, the CRHAVS Air Handling Unit (AHU) continues to operate normally providing temperature control in the MCR. Smoke removal is described in Subsections 9.4.1.2 and 9.5.1.11.

The redundant safety-related components include the I&C (i.e., monitoring channels) in the CRHA, CRHA isolation dampers, and EFUs, meet the single-failure criterion. Each pair of isolation dampers is physically separated. They are separated from the EFUs physically as well. The nonsafety-related AHUs and the safety-related isolation dampers and EFUs are mechanically and electrically separated. There is no intervention of the nonsafety-related components on the safety-related components. Isolation dampers are closed on the loss of power

or control signal failures. This conforms with the fail-safe principle, in which components or systems are designed to return automatically to their safe condition upon failure or loss of power.

The CRHS isolation and EFUs actuation as part of SSLC/ESF system logic is illustrated in Figure 7.3-5. The required instrumentation for CRHS is described in Subsection 9.4.1.5. Alarms for CRHA/CRHAVS conditions are discussed in Subsection 6.4.8.

7.3.4.3 Safety Evaluation

A safety evaluation of the CRHS is provided in Subsections 6.4.5 and 9.4.1.3.

Table 7.1-1 identifies the CRHS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.3.4.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety

- Conformance: The CRHS complies with these standards.

10 CRF 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (IEEE Std. 603)

- Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603 and RG 1.75. The CRHS consists of four redundantly designed divisions so failure of any instrument will not interfere with system operation. Electrical separation is maintained between the redundant divisions.

10 CFR 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication

- Conformance: The CRHS demonstrates compliance by providing automatic indication of bypassed and inoperable status.

10 CFR 50.34(f)(2)(xiv)(II.E.4.2), TMI Action Plan Item IIE.4.2 Containment Isolation Systems

- Conformance: The CRHS complies with this requirement.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements

- Conformance: There are no interface requirements for this Section.

10 CFR 52.47(a)(2), Level of Detail

- Conformance: The level of detail provided for the CRHS in the DCD conforms with this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.4.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, and 24:

- Conformance: The CRHS system complies with the GDCs identified above.

7.3.4.3.3 Staff Requirements Memorandum

SECY 93-087, Item II.Q - Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The CRHS system and ESF designs conform with these criteria, as described in Subsection 7.8.2.2.

7.3.4.3.4 Regulatory Guides

RG 1.22 - RG Periodic Testing of Protection System Actuation Function:

- Conformance: The CRHS design conforms with RG 1.22 as discussed in subsection 7.1.6.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System:

- Conformance: The CRHS design conforms with RG 1.47 as discussed in subsection 7.1.6.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The CRHS design conforms with RG 1.53 as discussed in subsection 7.1.6.

RG 1.62 - Manual Initiation of Protective Actions:

- Conformance: The CRHS design conforms with RG 1.62 as discussed in subsection 7.1.6.

RG 1.75 - Physical Independence of Electric Systems:

- Conformance: The CRHS design conforms with RG 1.75. See chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for a discussion of how the design meets the requirements of RG 1.75.

RG 1.105 - Setpoints for safety-related Instrumentation:

- Conformance: The CRHS design conforms with RG 1.105 as discussed in subsection 7.1.6.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems:

- Conformance: The CRHS design conforms with RG 1.118 as discussed in subsection 7.1.6.

RG 1.152 - Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms with RG 1.152 as discussed in subsection 7.1.6.

RG 1.153 - Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The CRHS system conforms with all RG 1.153 as discussed in subsection 7.1.6.

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

- Conformance: The CRHS design conforms with RG 1.168.

RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The CRHS design conforms with RG 1.169.

RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms with RG 1.170.

RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms with RG 1.171.

RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms with RG 1.172.

RG 1.173 – Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms with RG 1.173.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: CRHS conforms with RG 1.180.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: CRHS conforms with RG 1.204.

7.3.4.3.5 Branch Technical Positions

BTP HICB-3 - Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service:

- This BTP is not applicable to the design, which has no reactor coolant pump.

BTP HICB-4 -Guidance on Design Criteria for Auxiliary Feedwater Systems:

- This BTP is not applicable to the CRHS.

BTP HICB-6 - Guidance on Design of I&C Provided to Accomplish Changeover from Injection to Recirculation Mode:

- There is has no recirculation pump and no active ECCS pumps. Therefore, this BTP is not applicable.

BTP HICB-8 - Guidance for Application of RG 1.22:

- Conformance: The CRHS complies with BTP-HICB-8.

BTP HICB-11 - Guidance on Application and Qualification of Isolation Devices:

- Conformance: The CRHS complies with BTP-HICB-11.

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The CRHS complies with BTP-HICB-12.

BTP HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors:

- Conformance: This BTP does not apply to the CRHS, since this system does not use RTD-type sensors.

BTP HICB-14 - Guidance on Software Reviews for Digital Computer-Based I&C Systems:

- Conformance: The CRHS complies with BTP-HICB-14.

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The CRHS complies with BTP-HICB-16.

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The CRHS complies with BTP-HICB-17.

BTP HICB-18 - Guidance on the Use of PLCs in Digital Computer-Based I&C Systems:

- Conformance: The CRHS complies with BTP-HICB-18.

BTPHICB-19 - Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems:

- Conformance: The CRHS complies with BTP-HICB-19.

BTP HICB-21 - Guidance on Digital Computer Real-Time Performance:

- Conformance: The CRHS complies with BTP-HICB-21.

7.3.4.3.6 Three Mile Island Action Plan Requirements

In accordance with Table 7.1-1, 10 CFR 50.34(f)(2)(v) (I.D.3) and 10 CFR 50.34(f)(2)(xiv) (II.E.4.2) apply to the CRHS. The CRHS complies with the regulatory requirements indicated above. TMI action plan requirements are addressed in Appendix 1A to DCD Tier 2, Chapter 1.

7.3.4.4 Testing and Inspection Requirements

Testing and inspections requirements are identified in Subsections 6.4.7 and 9.4.1.4.

7.3.4.5 Instrumentation and Control Requirements

The required instrumentation for CRHS is described in Subsection 9.4.1.5 and alarms for following CRHA/CRHAVS conditions are addressed in Subsection 6.4.8.

7.3.5 Engineered Safety Features Safety System Logic and Control

7.3.5.1 System Design Bases

The Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) system performs the control logic processing of the plant sensor data and manual control switch signals activating the functions of the LD&IS, ECCS and CRHS. The SSLC/ESF also performs control logic processing for the safe shutdown function of the ICS, and other safety-related functions.

The SSLC/ESF provides the following functions:

- Monitors safety-related signals providing automatic control of the plant safety protection systems;
- Performs processing of plant sensor and equipment interlock signals according to the required trip and interlock logic, including time delays, of each safety-related interfacing plant system or system important to safe plant operation;
- Meets the performance requirements of each safety-related interfacing plant system or system important to safe plant operation, including transient response, delay time, and overall time to trip system actuators, or initiates necessary system operation;

- Monitors safety-related manual control switches used for system or component test, protection system manual initiation, and individual control of equipment actuators;
- Furnishes trip outputs signals to actuators driving safety system equipment (for example, solenoids and squib explosive-actuated valves);
- Furnishes trip or initiation outputs signals to the logic of interfacing functions;
- Provides diagnostic facilities for detecting imminent failure of system components and provides an operator interface facilitating quick repair;
- Provides alarm and status outputs to operator displays, annunciators, and the plant computer; and
- Satisfies regulatory requirements for implementation of:
  - The Single failure criterion,
  - Defense-in-depth protection,
  - Testability,
  - Separation and independence, and
  - Bypass of certain functions and indication thereof.

7.3.5.2 System Description

SSLC/ESF is the decision-making control logic segment for ESBWR ESF systems. SSLC/ESF processes automatic and manual demands for ESF system actuations, based upon sensed plant process parameters or at operator request. The SSLC/ESF includes the controls and instruments implementing the non-MSIV isolation functions of the LD&IS, the ADS functions of the NBS for SRV and DPV control, the ECCS functions of the GDCS and SLC system, and the ECCS and shutdown cooling functions of the ICS. The SSLC/ESF architecture is presented in Triconex Topical Report 7286-545-1-a, "Qualification Summary Report" (Reference 7.3-1).

7.3.5.2.1 General SSLC/ESF Arrangement

SSLC/ESF resides in four independent and separated instrumentation divisions. SSLC/ESF integrates the control logic of the safety-related systems in each division into firmware or microprocessor-based, software-controlled, processing modules located in divisional cabinets in the safety-related equipment room of the CB. The SSLC/ESF runs without interruption in all modes of plant operation to support required safety functions.

The SSLC/ESF consists of the non-MSIV isolation functions of the LD&IS, the ECCS functions, and the isolation function of the CRHS. The ESF/ECCS part includes the functions of SRV and DPV initiation, GDCS initiation, SLC initiation, and the core cooling and shutdown cooling logic functions of the ICS. There are separate multiplexing networks for RTIF and SSLC/ESF functions within each division. Figure 7.3-4 shows a functional block diagram of the SSLC/ESF

portion of the system. The RPS function is discussed in Subsection 7.2.1, with the RPS functional block diagram shown in Figure 7.2-1. The ATWS/SLC mitigation function is discussed in Subsection 7.8.1.1.

Most SSLC/ESF input data are process variables multiplexed by the Q-DCIS in four physically and electrically isolated redundant instrumentation divisions (Subsection 7.1.3). Each of the four independent and separated Q-DCIS channels feed separate and independent trains of SSLC/ESF equipment in the same division.

7.3.5.2.2 Signal Logic Processing

Signals that must meet time response constraints and signals from system logic that are proximal to the SSLC/ESF cabinets are directly connected to the divisional cabinets in the safety-related equipment room in the CB. These signals are derived from redundant sensors that are redundant in the four divisions (for each sensed variable).

All input data are processed within the RMU function of the Q-DCIS. The sensor data are transmitted through the DCIS network to the SSLC/ESF Digital Trip Module (DTM) function for setpoint comparison. A trip (or non-trip) signal is generated from this function. Processed trip signals from a division and trip signals from the other three divisions are transmitted through the communication interface and are processed in the VLU function for two-out-of-four voting. The final trip signal (from two or more divisions) is then transmitted to the RMU function via the Q-DCIS network to initiate mechanical actuation devices.

There are two independent and redundant VLU functional trains (three for the DPV actuation logic) in each division of the SSLC/ESF equipment. The vote logic trip signals from each VLU functional train are transmitted to the RMU, where a two-out-of-two (or three-out-of-three) confirmation is performed. The redundant trains within a division are necessary to prevent single failures within a division from causing a squib initiator to fire; as a result each VLU logic train is required to operate to get an output. Self-tests within the SSLC/ESF determine whether any one VLU function has failed, and such a failure is alarmed in the MCR.

To prevent single I&C failure causing inadvertent actuations, a failed VLU function cannot be bypassed for any of the ECCS logic for squib valves initiation. Trip signals are hardwired from the RMU to the equipment actuator. The same logic process is performed for all four divisions. The resulting logic provides single-failure proof actuation and single-failure proof inadvertent actuation. The four-division, two-out-of-four coincident signal voting occurs simultaneously for the equivalent signals in the four divisions. This arrangement provides multiple, independent trip channels, to accommodate random single failure. The four divisions are interconnected by fiber optic communication links via a communication interface module. The fiber optic links provide electrical isolation for data transmission. Sections 7.1.2, 7.1.3.2, and 7.1.3.3 provide discussions of electrical isolation between divisions.

In summary, at the division level, the four redundant divisions provide a fault-tolerant architecture allowing single division of sensors bypass for on-line maintenance, testing, and repair without losing reliable trip capability. In such a bypass condition, the system automatically defaults to two-out-of-three coincident voting. The fault-tolerant arrangement thus

conforms with safety system requirements for single-failure tolerance, independence, and separation, as required by IEEE Std. 603, Sections 5.1 and 5.6.

The SSLC/ESF does not require operator intervention during normal operation and allows manual bypass under abnormal conditions or required maintenance conditions such as failure of sensors. Safety-related automatic operations are provided with manual switches in each division for equipment initiation. Key safety-related RPS and ESF trip logics are duplicated in the DPS, which addresses the common-mode failure concern and provides diverse protection of digital computer systems performing safety-related function. The DPS system is described in Section 7.8.

Testing and maintenance activities are supported through use of manual control switches that can activate the trip logic signal of each safety-related system. In addition, on-line self-diagnostic tests checking the safety-related performance of the digital control instruments are performed continuously within SSLC/ESF. An illustration of SSLC/ESF and its relationship with the RPS and other interfacing systems is shown in Figure 7.3-5.

The RPS trip logic and MSIV isolation functions of RTIF use “de-energized-to-trip” and “fail-safe” logic. The SSLC/ESF trip logic uses “energized-to-trip” and “fail-as-is” logic. The SSLC/ESF trip signal is transmitted via isolators (if required) and load drivers/discrete outputs to the actuators for protective action. The load drivers/discrete outputs are solid-state power switches, directing appropriate currents to devices such as the scram pilot valve solenoids, air-operated valves, and explosive-actuated squib valves. The logic is designed so once it is initiated automatically or manually, the intended sequence of protective actions continues until completion, satisfying the requirement of IEEE Std. 603, Section 5.2.

More detailed descriptions of the SSLC/ESF trip logics for ADS and GDCS initiation are included in Subsection 7.3.1.1.2 and 7.3.1.2.2.

7.3.5.2.3 Division-of-Sensors Bypass

Bypassing any single division-of-sensors is accomplished from each divisional SSLC/ESF cabinet by manual switch control. This bypass disables the DTM outputs of a division at the associated VLU inputs in the four divisions. Interlocks are provided by a joystick-type switch so only one division of sensors at a time can be placed in bypass. When such a bypass is made, all four divisions of two-out-of-four logic become two-out-of-three logic while the bypass is maintained. Bypass permits calibration and repair of sensors or the DTM function. Although all sensors for all systems are bypassed in one division, the remaining three divisions furnish sufficient redundant sensor data for safe operation. The logic is such that all four divisions still can perform two-out-of-four (two-out-of-three) trip decisions - even if sensors are bypassed. Bypass status is indicated to the operator until the bypass condition is removed. An interlock rejects simultaneous attempts to bypass more than one SSLC/ESF division. Any loss of communication with a bypass switch is interpreted as a “no bypass” signal.

7.3.5.2.4 Division-Out-of-Service Bypass

For a fail-safe design, a division-out-of-service bypass inhibits the trip output in a division from affecting the output load drivers/discrete outputs by maintaining that division’s load

drivers/discrete outputs in an energized state. Bypass status is indicated to the operator until the bypass condition is removed. Only one division can be bypassed at any one time. For the SSLC/ESF logic, since the division-of-sensors bypass is implemented, and there are multiple trains of two-out-of-four VLU logic, no additional division trip logic bypass is implemented. Each of the VLU trip outputs is directly applied to one of the load drivers/discrete outputs in series. Each VLU trip is required to prevent inadvertent trip initiation of the squib valves. It is undesirable to perform the VLU logic bypass activities with the RMU electrically connected to the valve. The keylock switch that bypasses (disables) the load driver/discrete output actuation for the squib initiators provides the effective bypass function required at the actuator level. (Refer to Figure 7.3-1a and Figure 7.3-1b.)

7.3.5.3 Safety Evaluation

SSLC/ESF consists of a set of logic processing functions for the ESF systems and therefore is a safety-related system. The functions related to sensor signal processing and trip output are safety-related.

The four separated divisions of logic processing equipment provide the necessary degree of redundancy and independence to maintain safe operation despite the loss of portions of the processing capacity.

The SSLC/ESF system is designed so no single equipment failure causes inability to:

- Perform a reactor trip,
- Establish containment isolation, or
- Initiate the ESF.

Physically separate divisions are established by their relationship with the RPV, which is divided into four quadrants. The sensors, logic, and output actuators of the various systems are allocated to these divisions.

The digital devices in SSLC/ESF are, in general, microprocessor-based, software-controlled instruments.

Microprocessor-based logic in the SSLC/ESF activates the solenoid-controlled SRVs squib-actuated DPVs, GDCS injection and equalizing valves, ICS valves, and SLC squib valves.

A diverse I&C system is incorporated, featuring a totally independent set of selected reactor trip logic functions and ESF initiation logic functions addressing the requirements of the BTP HICB-19 position. This system is described in Subsection 7.8. The RPS logic is implemented using a diverse vendor furnished microprocessor-based platform. The RPS logic is implemented using a diverse vendor furnished microprocessor-based platform.

The SSLC/ESF system is designed to operate in a mild environment in clean areas within the CB and RB safety envelopes. Refer to Subsection 9.4.6 for specific environmental conditions.

Panel internal environments are maintained to ensure that reliability goals are achieved. Panel internal cooling is by natural convection. Fans may be used to improve long-term reliability, but

no credit is taken for forced-air cooling in the qualification of safety-related functions. Thermal design adequacy is considered during detail equipment design by analysis of heat loads (per circuit module, per bay, and per module).

Table 7.1-1 identifies the SSLC/ESF and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.3.5.3.1 Code of Federal Regulations

10 CFR 50.55a(1), Quality Standards for Systems Important to Safety:

- Conformance: The SSLC/ESF conforms with these standards.

10 CFR 50.55a(h), Protection and Safety Systems Compliance with IEEE Std. 603:

- Conformance: Safety-related systems are designed in conformance with RG 1.153 and IEEE Std. 603 as discussed in Subsections 7.1.6.4 and 7.2.1.3.4.

10 CFR 50.34 (f)(2)(v) [I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The SSLC/ESF demonstrates compliance by providing automatic indication of bypassed and inoperable status (IEEE Std. 603, Sections 5.8, 6.2, and 7.2).

10 CFR 50.34 (f)(2)(xiv) [II.E.4.2]:

- Conformance: The SSLC/ESF logic controlling containment isolation functions conforms with these criteria.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this Section.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the SSLC/ESF within the DCD conforms with this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.5.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, and 24:

- Conformance: The SSLC/ESF complies with these GDCs.

7.3.5.3.3 Staff Requirements Memorandum

SRM to SECY-93-087, Item II.Q Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The Reactor Trip (Protection) System and ESF designs conform with Item II.Q of SRM to SECY-93-087 (BTP HICB-19) in conjunction with the implementation of the DPS, described in Section 7.8.

7.3.5.3.4 Regulatory Guides

RG 1.22 - Safety Guide 22 Periodic Testing of Protection System Actuation Functions:

- Conformance: The SSLC/ESF complies with the guidance of RG 1.22.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: SSLC/ESF provides bypass capability and status.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The SSLC/ESF meets the guidance of RG 1.53, IEEE Std. 603, Section 5.1 and IEEE Std. 379.

RG 1.62 - Manual Initiation of Protective Actions:

- Conformance: The SSLC/ESF meets the guidance of RG 1.62. Signals for manual initiation of protective actions are hardwired to the SSLC/ESF equipment.

RG 1.75 - Physical Independence of Electric Systems:

- Conformance: The SSLC/ESF design conforms with RG 1.75. See chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for a discussion of how the design meets the requirements of RG 1.75.

RG 1.105 - Instrument Setpoints for safety-related Systems:

- Conformance: The SSLC/ESF complies with RG 1.105, as delineated in Subsection 7.1.6.4.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems:

- Conformance: The SSLC/ESF conforms with RG 1.118 as amplified in IEEE Std. 338. Testing of the SSLC/ESF is performed in conjunction with the Q-DCIS.

RG 1.152 - Criteria for Programmable Digital Computer System Software in safety-related Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF meets the guidelines of RG 1.152 and IEEE Std. 7-4.3.2. Additional discussion is provided in Subsection 7.2.1.3 describing RPS system compliance.

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The SSLC/ESF, in conjunction with the Q-DCIS, conforms with RG 1.153.

RG 1.168 - Verification, Validation, Reviews, and Audits for Digital Computer Software Used In Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF complies with RG 1.168, as delineated in Subsection 7.1.6.4.

RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF complies with RG 1.169, as delineated in Subsection 7.1.6.4.

RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF complies with RG 1.170, as delineated in Subsection 7.1.6.4.

RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF complies with RG 1.171, as delineated in Subsection 7.1.6.4.

RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF complies with RG 1.172, as delineated in Subsection 7.1.6.4.

RG 1.173 - Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF fully complies with RG 1.168 through 1.173, as delineated in Subsection 7.1.6.4

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: SSLC/ESF conforms to RG 1.180.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: SSLC/ESF conforms to RG 1.204.

7.3.5.3.5 Branch Technical Positions

BTP HICB-3 - Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service:

- Conformance: This BTP is not applicable because there is no reactor coolant pump.

BTP HICB-4 -Guidance on Design Criteria for Auxiliary Feedwater Systems:

- This BTP is not applicable to the SSLC/ESF.

BTP HICB-6 - Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode:

- Conformance: There is no recirculation pump and no active ECCS pumps. Therefore, this BTP is not applicable.

BTP HICB-8 - Guidance on Application of RG 1.22:

- Conformance: The SSLC/ESF is fully operational during reactor operation, and is tested in conjunction with the Q-DCIS. Therefore, the SSLC/ESF meets this BTP.

BTP-HICB-11 - Guidance on Application and Qualification of Isolation Devices:

- Conformance: SSLC/ESF logic controllers use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices. The Q-DCIS provides the communication functions for SSLC/ESF. See Subsection 7.1.2, 7.1.3.2 and 7.1.3.3 for descriptions of the Q-DCIS communication system design.

  Defined diverse and hardwired portions of RPS and SSLC/ESF may use coil-to-contact isolation of relays or contactors. This is acceptable according to the BTP when the application is analyzed or tested in accordance with the guidelines of RG 1.75 and RG 1.153.

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The SSLC/ESF conforms with this BTP. Additional discussion is provided in Subsection 7.2.3.3.5.

BTP HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors:

- Conformance: This BTP does not apply to the SSLC/ESF, since this system does not use RTD-type sensors.

BTP-HICB-14 - Guidance on Software Reviews for Digital Computer-based Instrumentation and Control:

- Conformance: Development of software for the safety-related system functions within SSLC/ESF conforms with the guidance of this BTP as discussed in the LTRs "ESBWR I&C Software Management Plan," NEDO-33226, NEDE-33226P and "ESBWR I&C Software Quality Assurance Plan," NEDO-33245, NEDE-33245P. (References 7.3-3 and 7.3-4.) Safety-related software to be embedded in the memory of the SSLC/ESF controllers is developed according to a structured plan outlined in References 7.3-2 and 7.3-4.

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: This BTP is applicable to all sections of the DCD. This subsection content conforms with this BTP.

BTP-HICB-17 - Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based Instrumentation and Control Systems:

- Conformance: The RPS and SSLC/ESF controllers conform with this BTP. Discussions on self-test and surveillance tests of RPS and ESF are provided in Subsections 7.2.1.3.5 and 7.3.5.4, respectively.

BTP-HICB-18 - Guidance on Use of in Digital Computer-based Instrumentation and Control Systems:

- Conformance: Portions of SSLC/ESF design using commercial grade PLCs for safety-related functions conform with this BTP (and to BTPs 14, 17, and 21) because the PLCs are qualified to a level commensurate with safety-related system requirements.

BTP-HICB-19 - Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems:

- Conformance: SSLC/ESF has a four-division, independent and separated equipment arrangement. Isolation of signal transmission between safety-related divisions and between safety-related and nonsafety-related equipment, is provided by non-conductive fiber optic cable. System functions are segmented among multiple controllers. Automatic functions are backed up by diverse automatic and manual functions. Control system functions are separate, independent, and diverse from the protection system functions. Additional diverse features are discussed in Section 7.8, which specifically addresses the requirements of this BTP.

BTP-HICB-21 - Guidance on Evaluation of Digital System Architecture and Real-Time Performance:

- Conformance: The real-time performance of SSLC/ESF in meeting the requirements for safety-related system trip and initiation response conforms with this BTP. Each SSLC/ESF controller operates independently and asynchronously with respect to other

controllers. The real-time performance of the safety-related control system is deterministic based on the Q-DCIS internal and external communication system design and the SSLC/ESF controller design. Timing signals are not exchanged – neither between divisions of independent equipment, nor between controllers within a division.

7.3.5.4 Testing and Inspection Requirements

A periodic, automatic self-test feature is included to verify proper operation of each SSLC/ESF logic processor. The self-test is an on-line, continuously operating self-diagnostics function (IEEE Std. 603, Sections 5.7 and 6.5). On-line self-test operates independently within each of the four SSLC/ESF divisions.

The major purpose of automatic self-testing is improving system availability by checking and confirming transmission path continuity for safety-related signals, verifying operation of each two-out-of-four coincidence trip logic function, and detecting, alarming, and recording the location of hardware or software faults. Tests verify the basic integrity of each card and the microprocessors. Discrete logic cards contain diagnostic circuitry monitoring critical points within the logic configuration and determining whether a discrepancy exists between an expected output and the existing present state. The self-test operations are part of normal data processing and do not affect system response to incoming trip or initiation signals. Automatic initiation signals from plant sensors override automatic test sequences and perform the required safety function. Process or logic signals are not changed as a result of self-test.

The self-testing includes continuous error checking of transmitted and received data on the serial data links of each SSLC/ESF controller; for example, error checking by parity check, checksum, or Cyclic Redundancy Checking (CRC) techniques. Self-test failures are alarmed to the operator at the MCR console and logged by the plant computer function of the N-DCIS.

In-service testing of the SSLC/ESF is performed periodically to verify operability during normal plant operation and to assure that each tested channel can perform its intended design function. The surveillance tests include, as required, instrument channel checks, functional tests, verification of proper sensor and channel calibration, verification of applicable logic functions in the VLU trains, and response time tests.

All test features adhere to the single failure criterion, as follows:

- No single failure in the test circuitry incapacitates an SSLC/ESF safety function, and
- No single failure in the test circuitry causes an inadvertent scram, MSIV closure, other PCV isolation, or actuation of any ESF system.

7.3.5.5 Instrumentation and Controls Requirements

The SSLC/ESF equipment uses microprocessor-based programmable logic and control instruments, with standardized interchangeable modules. Discrete solid-state logic also is used when applicable.

Control programs for each microprocessor-controlled instrument are in the form of software residing in non-volatile memory. The storage medium is in general Programmable Read-Only Memory (PROM). Programs are under the control of a real-time operating system residing in non-volatile memory. The equipment is qualified with a verification and validation program conforming with applicable codes and standards.

Logic and controls for SSLC/ESF are located on each divisional SSLC/ESF cabinet in the equipment room in the CB, with key controls and system operating status available on the operator interface section in the MCR. The SSLC/ESF controls are used infrequently. Such controls typically do not require operator action during plant operation or during accident or transient conditions, and mainly are used for test and maintenance purposes. However, conditions such as equipment failure, maintenance, or testing, may require the operator manually to bypass a division of sensors or a division of trip logic. Under the bypass status, SSLC/ESF continues to run in automatic mode using the unaffected logic in the remaining divisions.

The following minimum required SSLC/ESF displays are provided in the MCR (per division):

- Division-of-sensors in bypass;
- SSLC/ESF controller inoperative (DTM or VLU), and
- Communication Interface Module (CIM) inoperative.

7.3.6 COL Information

None

7.3.7 References

7.3-1 Triconex Topical Report 7286-545-1-a, "Qualification Summary Report", March 08, 2002.

7.3-2 GE Nuclear Energy, "General Electric Instrument Setpoint Methodology," NEDC 31336P-A, Class III (Proprietary), September 1996.

7.3-3 GE Energy Nuclear, "ESBWR I&C Software Management Plan," NEDO-33226, Class I (Non-proprietary), and "ESBWR I&C Software Management Plan," NEDE-33226P, Class III (Proprietary), Revision 2, July 2007.

7.3-4 GE Energy Nuclear, "ESBWR I&C Software Quality Assurance Plan," NEDO-33245, Class I (Non-proprietary), and "ESBWR I&C Software Quality Assurance Plan," NEDE-33245P, Class III (Proprietary), Revision 2, July 2007.

Table 7.3-1

Automatic Depressurization System Parameters

Parameter	Value
Number of ADS divisions	4
Number of separate logics (trains) per division	2
Number of logic (trains) within a division used to actuate the separate solenoid-operated gas pilots on each SRV	2
Number of logic (trains) within a division used to actuate the separate igniter circuits on each squib-actuated DPV	2
Minimum number of ADS logic divisions to actuate any SRV pilot and open the SRV	2
Minimum number of ADS logic divisions to actuate (energize) one of the igniter circuits and open the DPV	2
Trip logic units self-test time interval	8 sec

Table 7.3-2

Safety Relief Valve Initiation Parameters

Parameter	Value*
Number of SRV groups	2
Number of SRVs in the first group (Group 1-initial ADS start signal)	5
Number of SRVs in the second group (Group 2 – second ADS start signal)	5
Time delay to confirm ECCS-LOCA signal	10 sec
Time after ECCS-LOCA confirmed initiating signal before signaling Group 1 SRVs to open	0 sec
Time after ECCS-LOCA confirmed initiating signal before signaling Group 2 SRVs to open	10 sec

*The time delay values represent design or analytical limits.

Table 7.3-3

Automatic Depressurization Valve Parameters

Parameter	Value*
Number of DPVs groups	4
Number of DPVs in Group 1 (third ADS start signal)	3
Number of DPVs in Group 2 (fourth ADS start signal)	2
Number of DPVs in Group 3 (fifth ADS start signal)	2
Number of DPVs in Group 4 (sixth ADS start signal)	1
Initial ADS time delay, after ECCS-LOCA confirmed initiating signal, before Group 1 DPVs are signaled to open,	50 sec
Additional ADS time delay, after Group 1 initiation, before Group 2 DPVs are signaled to open	50 sec
Additional ADS time delay, after Group 2 initiation, before Group 3 DPVs are signaled to open	50 sec
Additional ADS time delay, after Group 3 initiation, before Group 4 DPVs are signaled to open	50 sec

*The time delay values represent design or analytical limits

Table 7.3-4

Gravity Driven Cooling System Parameters

Parameter	Value*
Deluge squib valves initiated by lower drywell high temperature	>538°C (1000°F)
Injection squib valve time logic delay from initial start signal	150 sec
Equalization line squib valve initiation logic time delay	30 min
Manual equalization squib valve initiation logic time delay	30 min

*These values represent design or analytical limits.

Table 7.3-5

LD&IS Interfacing Sensor Parameters

Temperatures:

- Main Steam Line (MSL) Tunnel Area
- Drywell
- MSL in Turbine Building (or alternate method)

Pressures:

- MSL Turbine Inlet Pressure
- Main Condenser Pressure
- RPV Head Flange Seal Leakage
- Drywell
- Feedwater Line Differential

Radiation Levels:

- RCCWS Intersystem Leakage
- Drywell Fission Product
- RB HVAC Air Exhaust
- Refueling Handling Area Air Exhaust
- Drywell Sump LCW Drain Line to Radwaste
- Drywell Sump HCW Drain Line to Radwaste
- Isolation Condensers Pool Vent Exhaust

Flow Rates:

- MSL
- RWCU/SDC Differential Mass (Temperature Compensated)
- Drywell Air Cooler Condensate Discharge
- Isolation Condenser Steam Line
- Isolation Condenser Condensate Return Line

Levels:

- RPV Water Level 1 and Level 2
- Drywell and Containment Sump

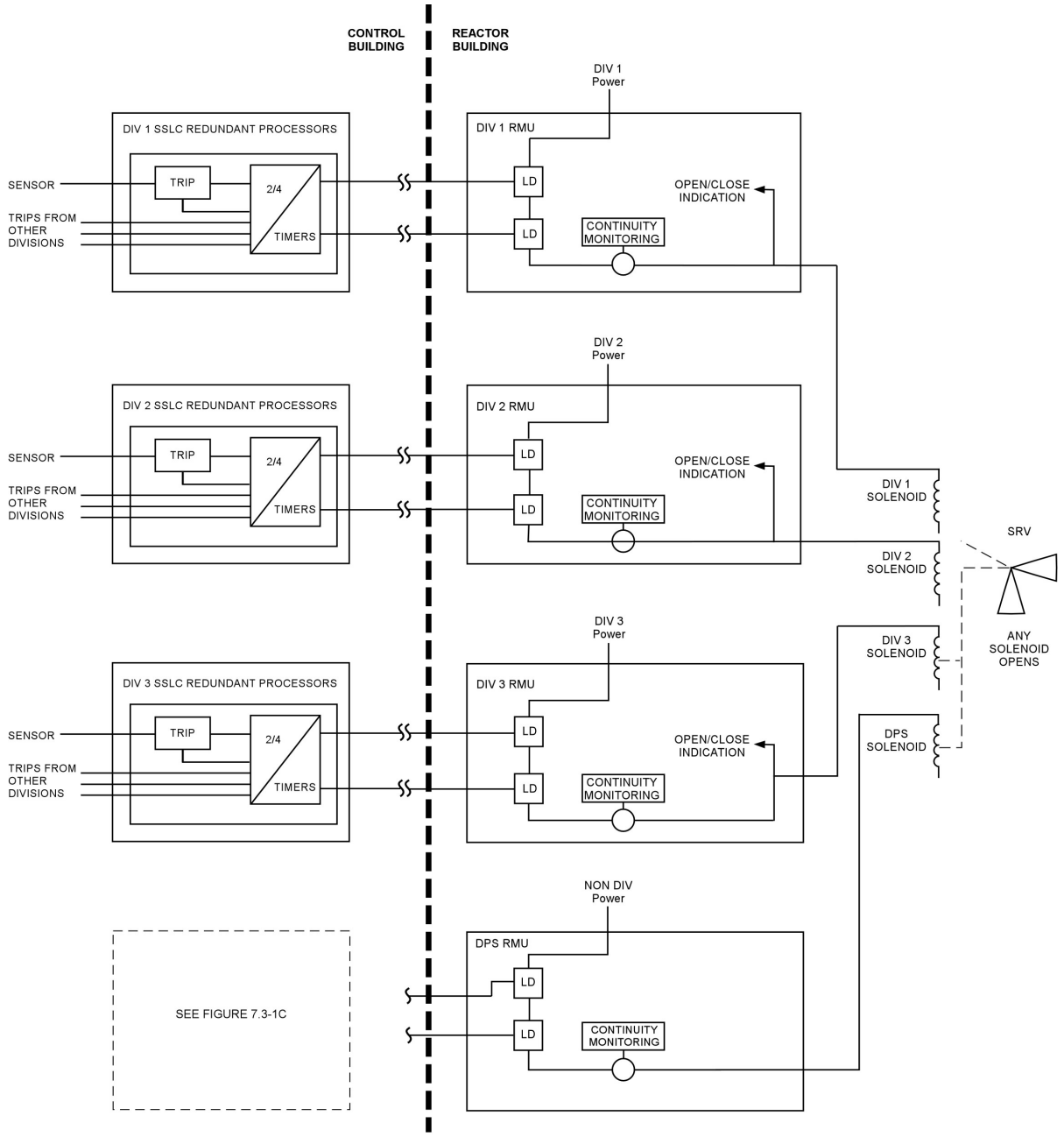
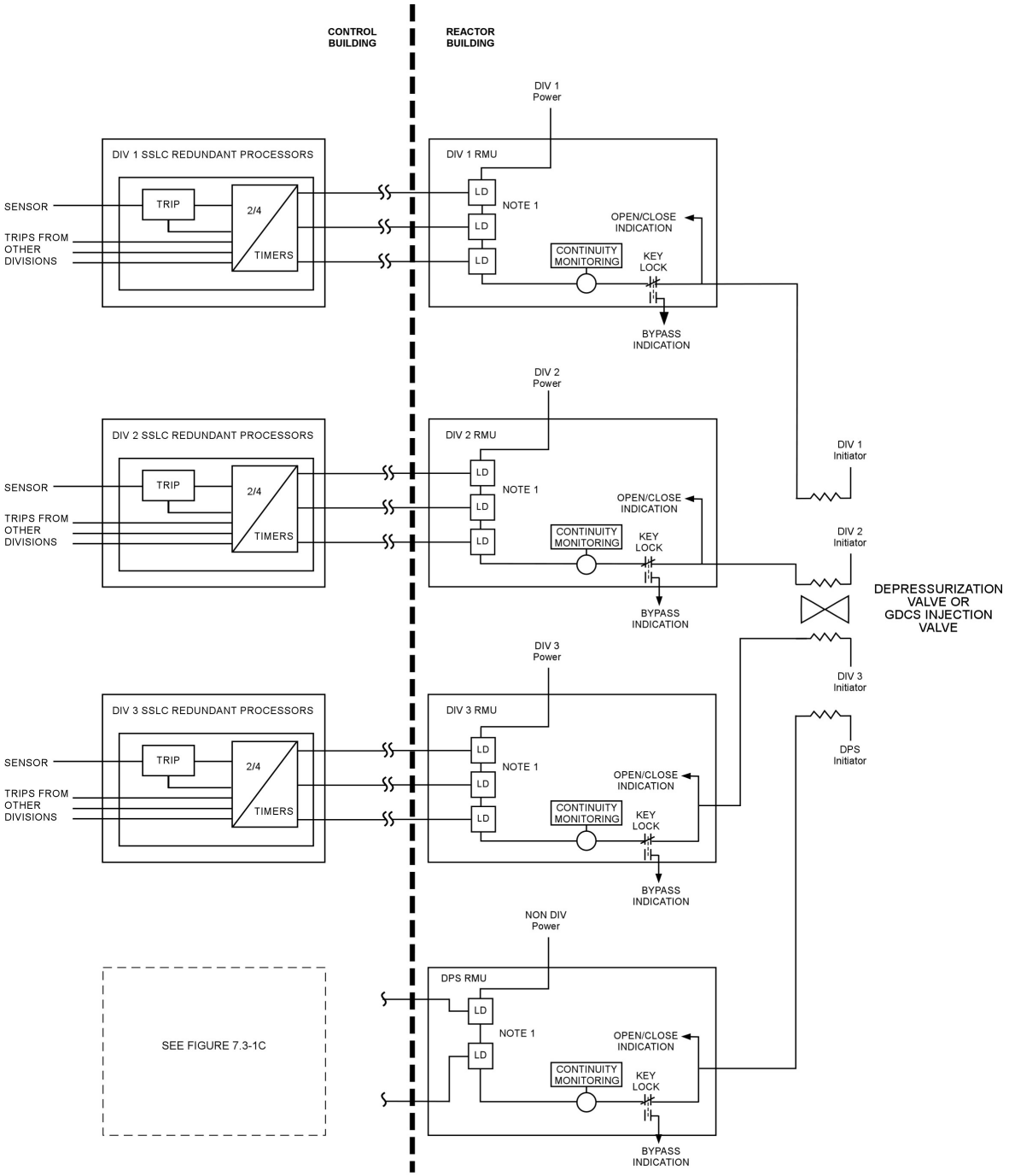


Figure 7.3-1a. SRV Initiation Logics



NOTE 1: THE THIRD SET OF 2/4 AND TIMER LOGIC AND THIRD LOAD DRIVER IS ONLY APPLICABLE TO THE DPV'S.

Figure 7.3-1b. GDCS and DPV Initiation Logics

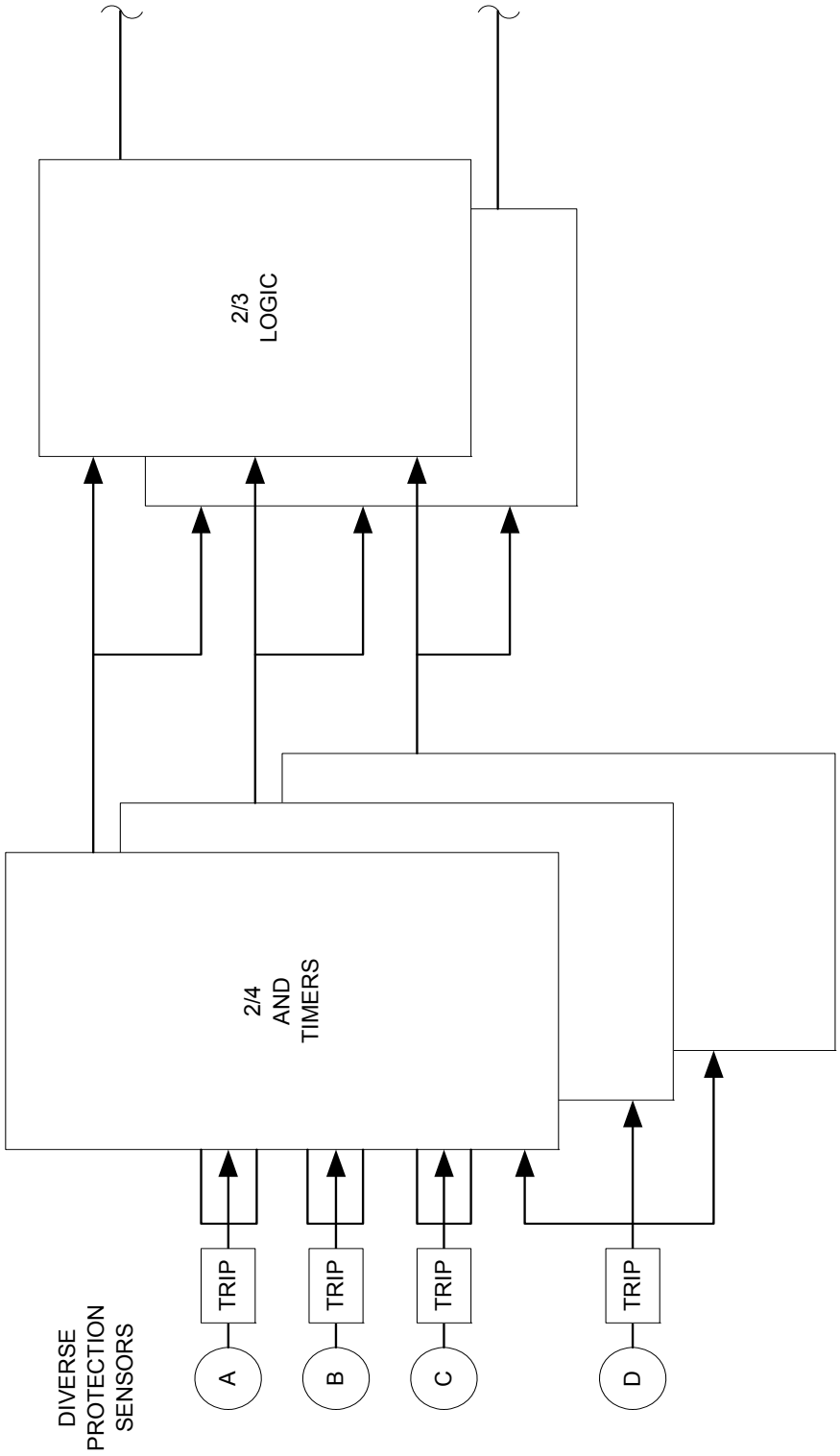


Figure 7.3-1c. DPS Initiation Logic

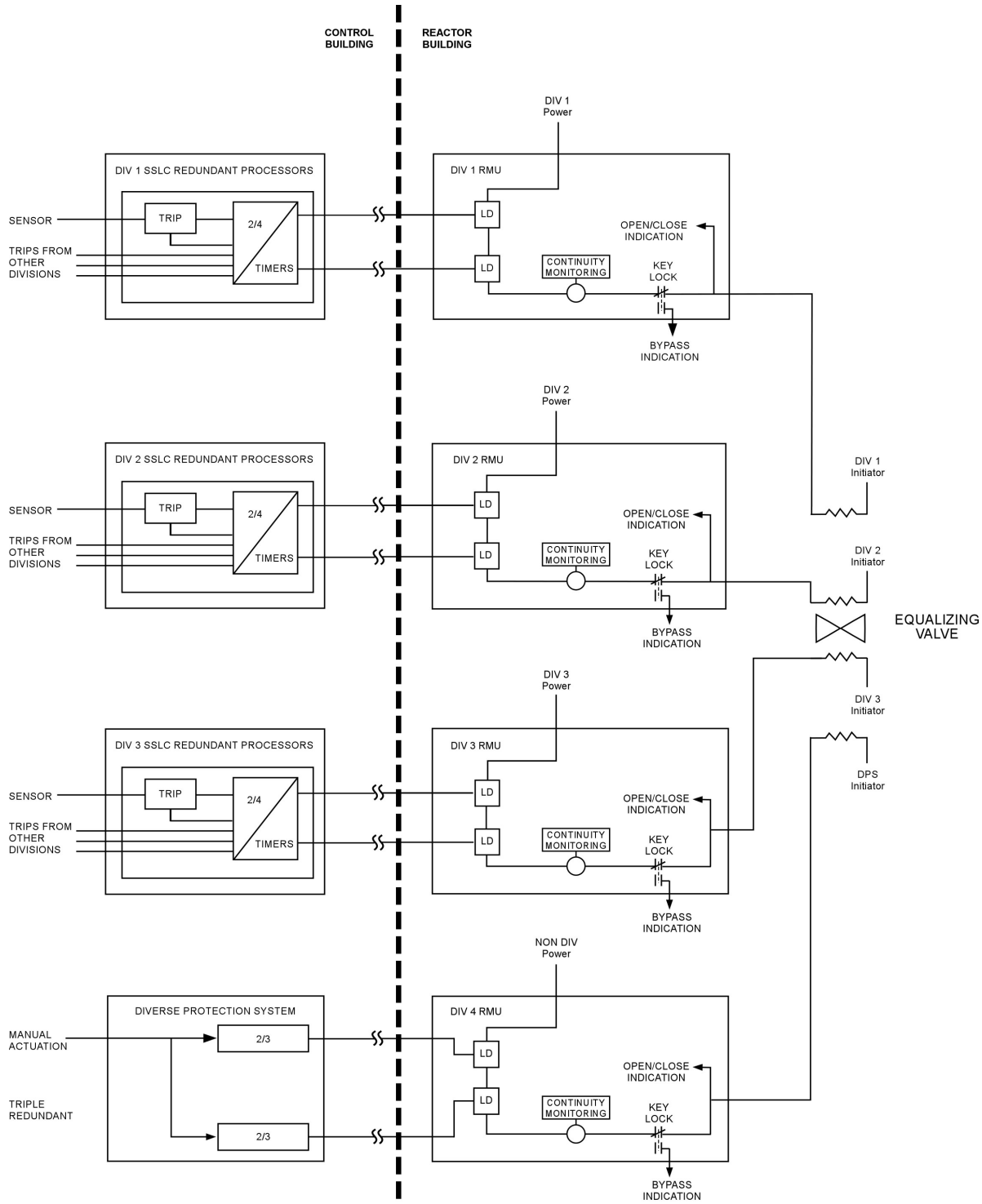


Figure 7.3-2. GDCS Equalizing Valve Initiation Logics

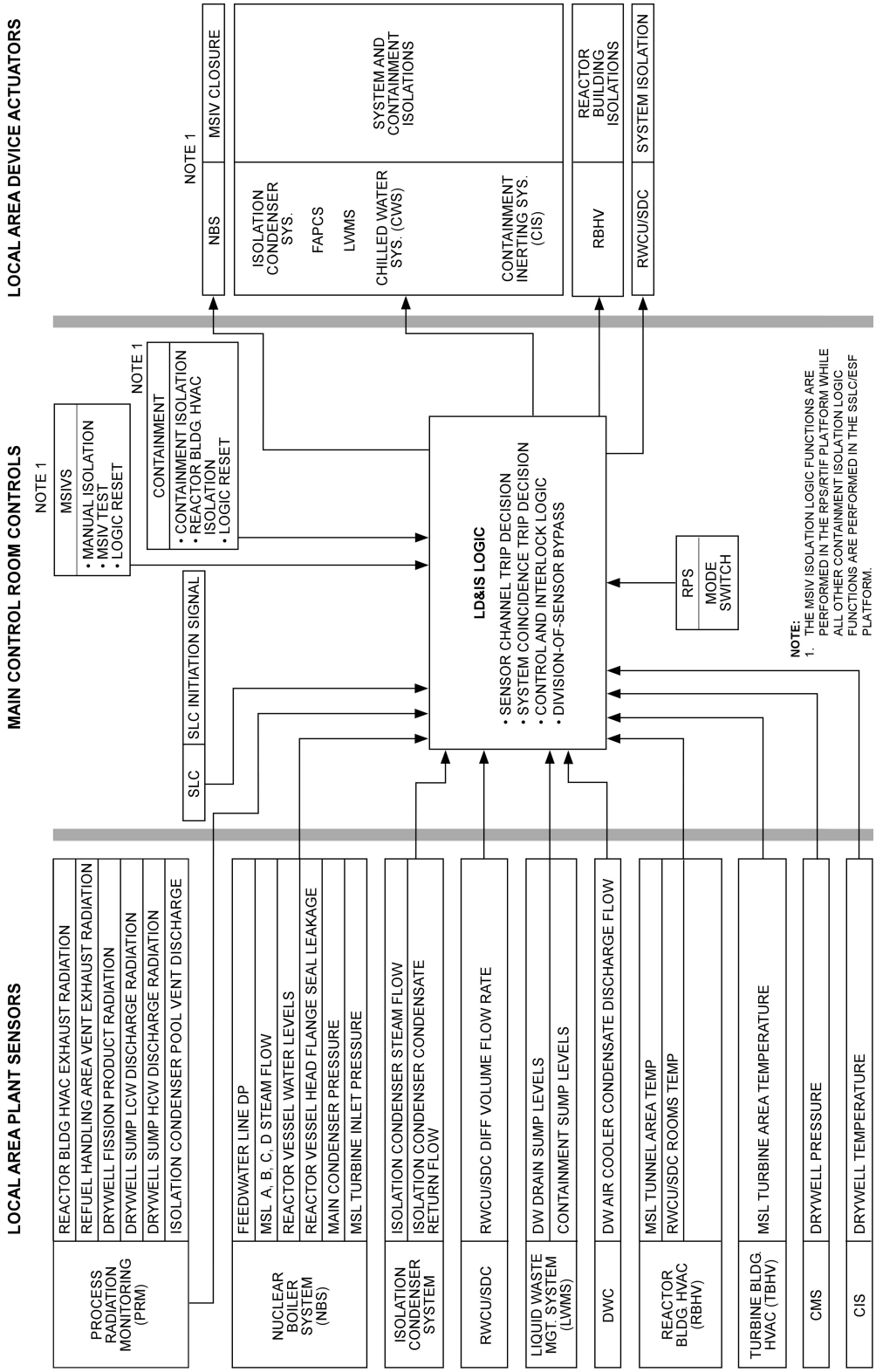
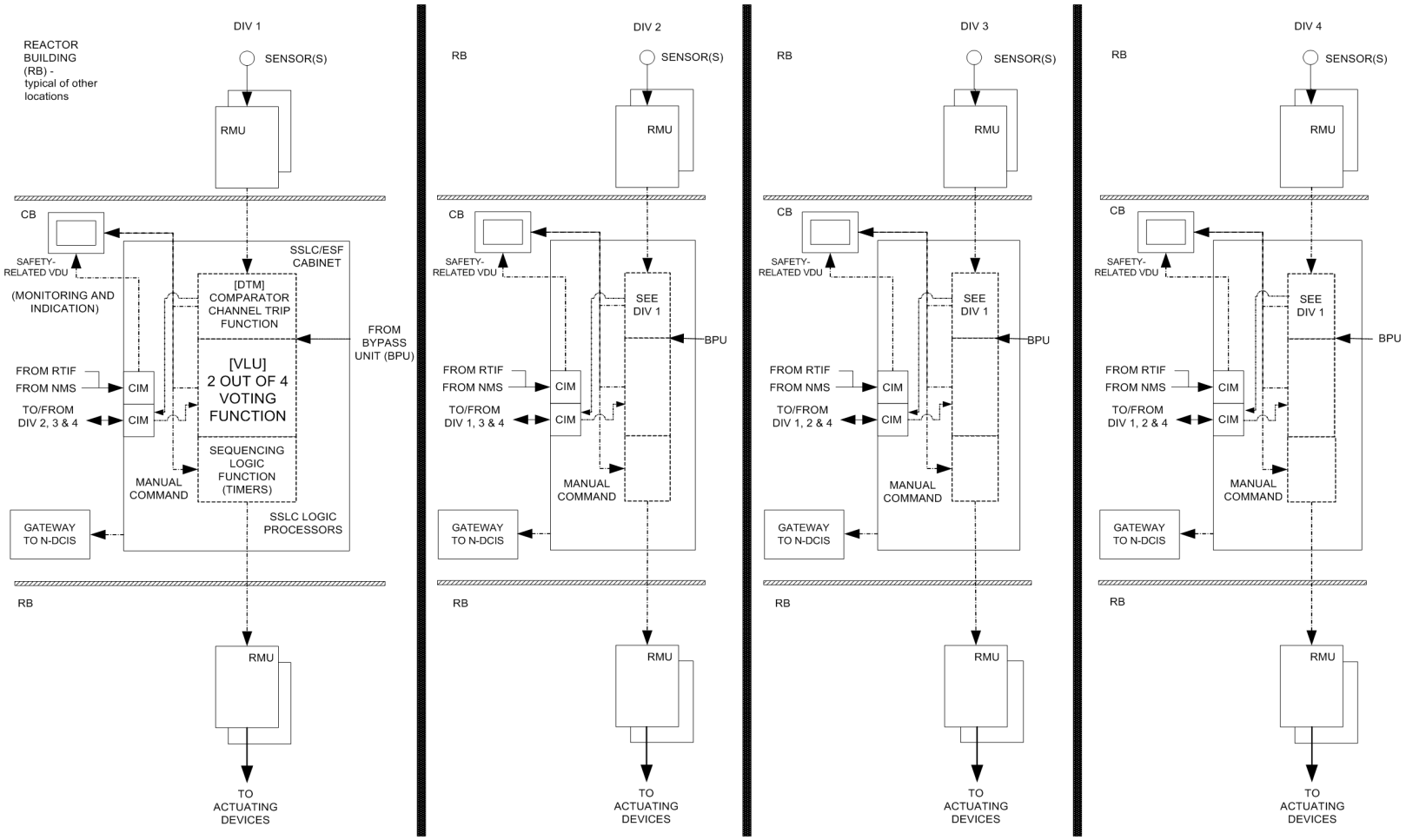


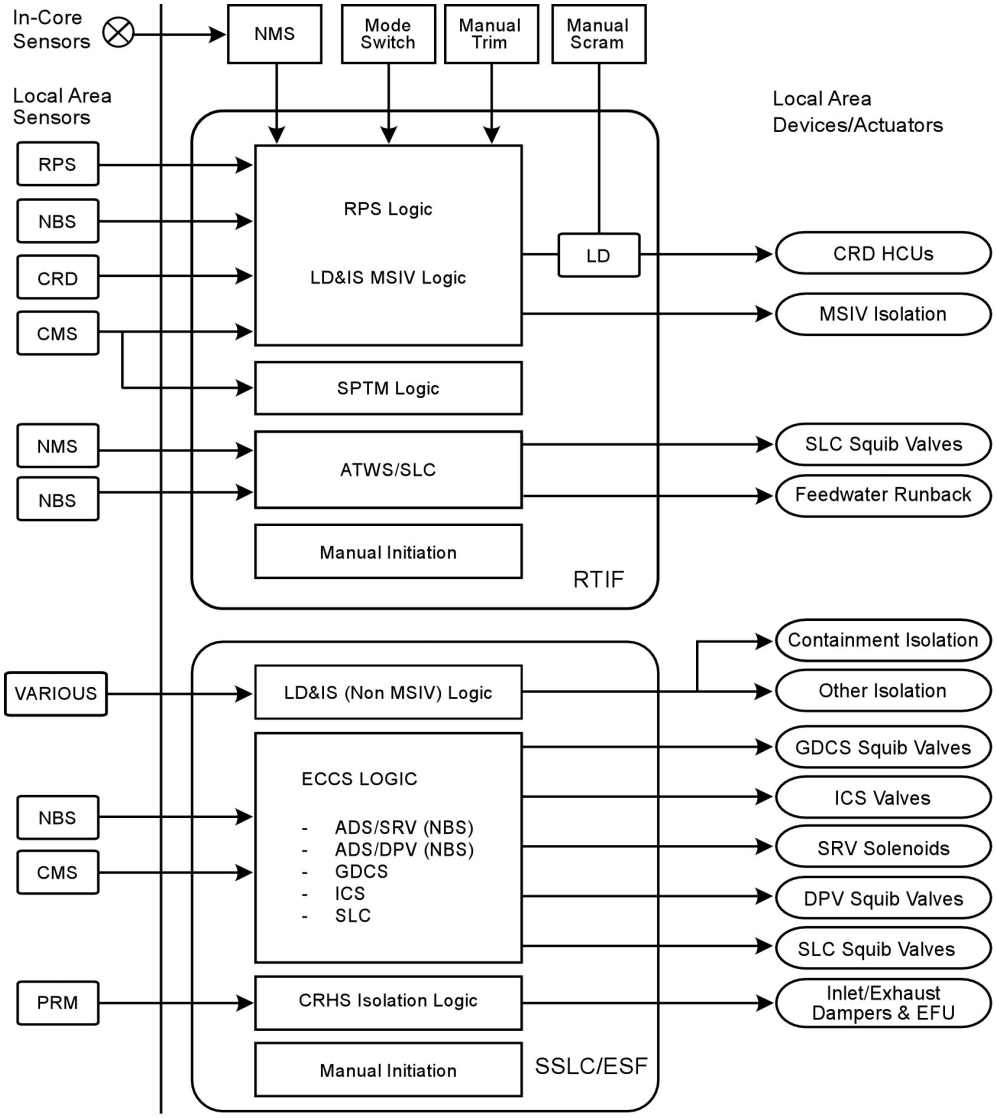
Figure 7.3-3. LD&IS System Design Configuration



NOTES:
FOR ECCS FUNCTION, THE VLU CONTAINS DUAL REDUNDANT 2-out-of-4 LOGIC WITH TWO INDEPENDENT TRIP OUTPUTS
Redundant DIV 1 and 2 VDUs are located at the Remote Shutdown Panels
CIM=COMMUNICATION INTERFACE MODULE-ISOLATOR

(Note: the VLU contains dual redundant 2/4 logics with two independent trip outputs.)

Figure 7.3-4. SSLC/ESF Functional Block Diagram



Note: 1) Local area sensors include:
RPS: Turbine stop valve position, turbine CV oil pressure, turbine bypass valve position, *
PRM: Process Radiation Monitoring
NBS: MSIV position (for RTIF only), RPV pressure, water level
CRD: HCU accumulator charging water header pressure
CMS: Drywell pressure, suppression pool temperature
2) Manual Scram interrupts power to the LD circuit
3) LD&IS shares sensor inputs with RTIF (for MSIV isolation) and SSLC/ESF (for Non-MSIV).
4) The various LD&IS sensors are depicted on Figure 7.3-3.

* Main condenser pressure, loss of power generation bus

Figure 7.3-5. SSLC/ESF System Interface Diagram

7.4 SAFETY-RELATED SAFE-SHUTDOWN AND NONSAFETY-RELATED COLD SHUTDOWN SYSTEMS

In accordance with the Standard Review Plan (SRP) (Reference 7.4-1), this section describes "...those instrumentation and control (I&C) systems used to achieve and maintain a safe shutdown condition of the plant." However, some I&C systems performing cold shutdown functions are not safety-related. This is justified by the existence of the safety-related systems (Isolation Condenser System [ICS], Gravity-Driven Cooling System [GDCS], Standby Liquid Control [SLC] system, and Passive Containment Cooling System [PCCS]) that use natural circulation in the performance of their shutdown functions. Additionally, some safety-related criteria, such as provision of redundant trains and single protection against failure, are implemented in the design of the nonsafety-related systems. Consequently, safety-related and nonsafety-related systems performing safe shutdown or cold shutdown functions, respectively, are addressed in this section.

7.4.1 Standby Liquid Control System

7.4.1.1 System Design Bases

The SLC system design bases are presented within Subsection 9.3.5 (IEEE Std. 603, Sections 4.1, 4.2, 4.5, 4.8, and 4.10).

The I&Cs for the SLC support the passive system capability requirements to perform the following:

- Provide a diverse, backup means to shut down the reactor from full power to a subcritical condition, using soluble boron injection, and maintain the reactor subcritical while it is brought to a cold shutdown condition. SLC system logic provides manual initiation capability in the Main Control Room (MCR), to satisfy the diverse shutdown requirements, and is independent of normal reactivity control provisions.

- Provide system actuation upon receipt of manual and automatic initiation signals in response to either Anticipated Transients Without Scram (ATWS) events, or design basis events requiring Emergency Core Cooling System (ECCS) operation.

Four divisions of safety-related sense and command logic are used for automatic SLC initiation and for automatic SLC accumulator isolation. Redundant SLC accumulator level and pressure instrumentation is provided to monitor system performance and to ensure reliable logic processing. Valve position indication and continuity monitoring of the SLC squib injection valves is provided to ensure availability.

Safety-related SLC system components are designed for the environmental conditions applicable to their location. Safety-related SLC system components are also designed to preclude adverse interaction from nonsafety-related portions of the system.

The SLC design bases are discussed further within Subsection 9.3.5, and Figure 9.3-1 shows the basic configuration. Design basis event mitigation crediting the SLC system is discussed in Chapter 15, "Safety Analyses" (IEEE Std. 603, Sections 4.1, 4.2, 4.5, 4.8, and 4.10).

The SLC system initiation function is part of a group of systems collectively called the Safety-Related Distributed Control and Information System (Q-DCIS). A functional block diagram of the Q-DCIS is included as part of Figure 7.1-1, and a functional network diagram appears as Figure 7.1-2. These diagrams indicate the relationships of the SLC system with its safety-related peers, and with nonsafety-related plant data systems collectively called the Nonsafety-Related distributed Control and Information System (N-DCIS). Section 7.1 contains a description of these relationships.

7.4.1.2 System Description

A detailed system description is given in Subsection 9.3.5.2. The controls and instrumentation of the SLC system are described below. The safety-related SLC system provides diverse backup capability for reactor shutdown, which is independent of the Reactor Protection System (RPS). For the reactor shutdown function, the SLC system is manually initiated from the MCR by using dual, key-locked control switches. Parameters such as neutron flux, reactor vessel pressure and level, and control rod position are available to the operator in the MCR to assess the need for manual SLC initiation. Additionally, accumulator pressure and solution level, as well as squib injection valve and shut-off valve status indication, is provided in the MCR to monitor the operating and performance status of the SLC system. (IEEE Std. 603, Section 4.5)

The SLC system is initiated automatically as part of the ECCS, to mitigate Loss-of-Coolant-Accident (LOCA) events. The SLC system receives an actuation command 50 seconds after a confirmed LOCA. The SLC actuation sequence corresponds to the first DPV actuation (as described in the Automatic Depressurization System [ADS] logic discussion in Subsection 7.3.1.1.2). The SLC system also receives a diverse ECCS initiation signal from the Diverse Protection System (DPS).

The SLC system also starts automatically on an ATWS mitigation signal persisting for 180 seconds. The ATWS mitigation (ATWS/SLC) logic performs the diverse emergency shutdown function (in compliance with requirements of 10 CFR 50.62). ATWS/SLC logic is described in Section 7.8, Diverse I&C Systems, and is depicted on Figure 7.8-3, ATWS Mitigation Logic (SLC System Initiation, Feedwater Runback).

The ATWS/SLC logic uses sensors, hardware, and software platforms diverse from the Safety System Logic and Control Engineered Safety Feature (SSLC/ESF), RPS, and DPS hardware/software platforms.

To avoid boron dilution during SLC operation, the SLC system logic transmits an isolation signal to the Reactor Water Clean-Up/Shutdown Cooling System (RWCU/SDC) via the Leak Detection and Isolation System (LD&IS).

To avoid the injection of nitrogen into the Reactor Pressure Vessel (RPV) System, four divisional, safety-related level sensors per SLC accumulator are used to provide automatic isolation of series accumulator shut-off valves on (a voted two-out-of-four) low accumulator

level. The SLC system processors of the ATWS/SLC mitigation logic platform perform the shut-off valve isolation logic.

Accumulator temperature, solution level, and accumulator pressure are indicated locally inside the accumulator room.

Boron injection and shut-off valve position status are provided in the MCR.

7.4.1.2.1 Power Sources

Power for the safety functions of the SLC system is derived from the safety-related 120 Volts Alternating Current (VAC) electrical systems (see Subsection 8.3.1.1.3). Divisional assignments are made to ensure the availability of each SLC system loop, assuming one safety-related division of power is not in service in addition to a single active failure. Additionally, a squib initiator in each loop is activated by the DPS as part of the diversity and defense-in-depth strategy (described in Subsection 7.8.1.2.2). To avoid adverse interaction, electrical isolation is maintained between the safety-related divisions, and between the safety-related divisions and the DPS (IEEE Std. 603, Sections 5.12, 8.1, and 8.2).

7.4.1.2.2 Control Functions

There are four control functions for the SLC system:

- The firing signals to the squib initiators originate from SSLC/ESF for the ECCS injection function, from ATWS/SLC for the ATWS mitigation function, and from manual control switches in the MCR. Successful firing of either or both squib valves in each SLC system loop assures completion of the SLC system operation. (IEEE Std. 603, Section 5.2).
- Control logic also is provided for automatic closure of the shut-off valves. Shut-off valve isolation occurs automatically on a two-out-of-four low-level logic, using the safety-related accumulator level instrumentation. Closure signals to the redundant, fail-as-is shut-off valves ensure that at least one valve closes, to prevent nitrogen entry into the RPV.
- Control logic also is provided for manual venting of the accumulators. This function is not safety-related. Serial solenoid valves in each vent line may be actuated by respective manual switches in the MCR.
- Automatic nitrogen makeup to the accumulators is provided to accommodate slow long-term leakage from the system. This makeup function only is required to maintain accumulator pressure. It is not required to assure full solution injection and therefore, is not safety-related.

7.4.1.3 Safety Evaluation

The safety evaluation for the mechanical aspects of the SLC system is presented in Subsection 9.3.5.3. (IEEE Std. 603, Section 4.8). The SLC I&C are capable of performing their

intended safety functions based on the following design features. The safety-related SLC instrumentation and controls are designed to operate under the environmental conditions anticipated at their equipment locations. (IEEE Std. 603, Section 5.4). Inter-division communication (and communication with nonsafety-related interfaces) occurs through qualified isolation devices (IEEE Std. 603, Section 5.6). Isolated ECCS initiation signals, as well as isolated ATWS mitigation signals from the DPS, are transmitted to the SLC squib injection valves to provide defense against a common mode software failure of the SSLC/ESF logic platform (discussed in Section 7.8).

The only automatic actuation logic originating from within the SLC system logic processors are the low accumulator-level isolation signals for the accumulator shut-off valves, and the RWCU/SDC isolation signal via the LD&IS on SLC system injection. The SLC logic processors are separate components of the diverse ATWS/SLC mitigation logic platform.

Redundant divisions of voting logic enable the SLC system to perform its safety-related function with one division removed from service coincident with a single failure (IEEE Std. 603, Section 5.1). Division of sensors bypass capability allows a safety-related SLC sensor to be removed from service, while maintaining a high level of reliability (IEEE Std. 603, Section 5.7, 6.5, and 6.7). Alarmed indication of the bypass condition provides off-normal condition status monitoring (IEEE Std. 603, Section 5.8). With an SLC accumulator-level sensor removed from service, the shut-off valve voting logic changes from two-out-of-four to two-out-of-three. Redundant signals are used to confirm the demand for squib injection valve operation. Series load drivers are provided to avoid spurious operation of the squib valves. Alarmed, key-lock switches are provided to allow removal of a squib valve and associated control circuit from service, and to protect against spurious operation while performing maintenance. Continuity monitoring of the squib injection valve circuitry is provided to confirm availability automatically. Position indication for the SLC system valves also is provided to determine system configuration.

Manual SLC system initiation requires operation of dual control switches, with each switch requiring two distinct operator actions. The manual SLC system switches are protected by key-locks to minimize the likelihood of inadvertent operation.

In addition to squib injection valve continuity monitoring, status indication of squib injection and accumulator shut-off valves, accumulator level and pressure indication, and alarms are provided to allow monitoring of SLC accumulator standby status.

The SLC system also conforms with the applicable general requirements for safety-related systems presented in Chapter 3. Codes and Standards applicable to the SLC system are identified in Table 7.1-1 and discussed below.

Table 7.1-1 identifies the SLC system and associated codes and standards applied, in accordance with the SRP (Reference 7.4-1). This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.4.1.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The SLC system conforms with these standards.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: The SLC system conforms with IEEE Std. 603. Separation and isolation is maintained both mechanically and electrically in accordance with IEEE Std. 603 and Regulatory Guide (RG) 1.75. The SLC is designed so a single failure does not interfere with system operation. Electrical separation is maintained between safety-related divisions, and between safety-related and nonsafety-related portions.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The SLC system conforms with this requirement, since SLC is an Emergency Core Cooling System (ECCS).

10 CFR 50.62, Requirements for Reduction of Risk from ATWS Events for light-water Cooled Nuclear Power Plants:

- Conformance: The SLC is automatically initiated, and is designed to perform its mitigation function reliably.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: The SLC system along with the other I&C systems complies with this criterion. Resolution of unresolved and generic safety issues is discussed in Subsection 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for I&C Equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for the SLC system.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the SLC system within the DCD conforms with this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Function:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.4.1.3.2 General Design Criteria.

In accordance with Table 7.1-1, the following General Design Criteria (GDC) are addressed for the SLC system:

GDC 1, 2, 4, 13, 19 and 24:

- Conformance: The SLC system conforms with these GDC.

7.4.1.3.3 Regulatory Guides

RG 1.22 – Periodic Testing of Protection System Actuation Functions:

- Conformance: The SLC system conforms with RG 1.22.

RG 1.47 – Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The SLC system conforms with RG 1.47.

RG 1.53 – Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The SLC system is a redundant backup to the reactor control and scram systems, and performs an ECCS function. The SLC system has two redundant and parallel squib-type valves in each loop. Only one valve in each loop is required for the safety-related function of the SLC system. The SLC system instrumentation assuring operability of the system also is redundant.

RG 1.62 – Manual Initiation of Protective Actions:

- Conformance: The SLC system conforms with RG 1.62. Dual (key-locked) control switches are provided, to actuate the SLC system.

RG 1.75 – Physical Independence of Electric Systems:

- Conformance: The SLC system conforms with RG 1.75. See Chapter 8 for a general discussion of compliance with RG 1.75.

RG 1.105 – Setpoints for Safety-Related Instrumentation:

- Conformance: The SLC system conforms with RG 1.105, as described in GE Nuclear Energy, "General Electric Instrument Setpoint Methodology" LTR NEDC-31336P-A, Class III (GE Proprietary), September 1996.

RG 1.118 – Periodic Testing of Electric Power and Protection Systems:

- Conformance: The SLC system conforms with RG 1.118.

RG 1.151 – Instrument Sensing Lines:

- Conformance: The SLC system conforms with RG 1.151.

RG 1.153 – Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: Consistent with the discussion of other RGs and the General Design Criteria, the SLC system conforms with RG 1.153.

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The SLC system conforms with RG 1.180 - with the assumption that the interpretations and clarifications identified in Subsection 7.1.6.4 also apply to the system.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The SLC system conforms with RG 1.204 - with the assumption that the interpretations and clarifications identified in Subsection 7.1.6.4 also apply to the system.

7.4.1.3.4 Branch Technical Positions

BTP HICB-8 – Guidance on Application of Regulatory Guide 1.22:

- Conformance: The SLC system conforms with this guidance.

BTP HICB-11 – Guidance on Application and Qualification of Isolation Devices:

- Conformance: The SLC system conforms with this guidance.

BTP HICB-12 – Guidance on Establishing and Maintaining Setpoints:

- Conformance: The SLC system conforms with this guidance.

BTP HICB-13 – Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors:

- Conformance: This BTP does not apply to the SLC system, since this system does not use RTD-type sensors.

BTP HICB-16 – Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The SLC system conforms with this guidance.

7.4.1.4 Testing and Inspection Requirements

Testing and inspection requirements are described further in Subsection 9.3.5.3. An initial SLC system performance verification test is conducted as part of the startup test program. This test is intended to demonstrate that the SLC system performance is in accordance with design requirements.

A full test of this system is no longer possible after plant operation. However, other than the two squib valves in each loop, there are no active components in this system, that are required to actuate for injection to occur. Only one squib valve actuation in each loop is required for injection to occur. If one of the valves in each loop actuates with the system in its normal

operating configuration, and critical system parameters (accumulator level and pressure) are within their normal ranges, injection would occur. Testing of the shut-off valve isolation logic is performed periodically to verify operability.

Routine testing, monitoring of critical system parameters, and surveillances ensure operability with an acceptably low probability of demand failure (IEEE Std. 603, Section 5.7).

7.4.1.5 Instrumentation and Control Requirements

Status indications of full-open or full-closed valve positions are provided for the key valves in the SLC system, such as the squib injection valves and the accumulator shut-off valves. An open indication for these valves is required to ensure SLC system operation (IEEE Std. 603, Section 5.8).

Pressure-level and solution-level alarms and indications for each accumulator (IEEE Std. 603, Section 5.8) are provided in the MCR to:

- Ensure operability of the system;
- Warn the operator of an out-of-tolerance level or pressure condition, and
- Provide verification of proper system operation after initiation.

The measurements are redundant to minimize vulnerability to instrument or indicator failure. The level instrumentation for each accumulator is four redundant to support the two-out-of-four initiation logic for closure of the shut-off valve. The pressure indications and alarms are dual redundant and the signals from both channels are needed before adding nitrogen to an accumulator. These instruments also provide local level and pressure indication.

Local indication and MCR alarm are provided for the nitrogen gas and neutron poison solution makeup. The low-level alarms are set to provide adequate time for recharging the manually operated nitrogen and sodium pentaborate solution supply systems.

7.4.2 Remote Shutdown System

7.4.2.1 System Design Bases

The safety-related Remote Shutdown System (RSS) is used to provide operators with the means to safely shut down the reactor from a place outside the MCR if it becomes uninhabitable. The RSS provides remote control of the systems needed to bring the reactor to a hot shutdown after a scram. The RSS also provides the subsequent capability to bring the plant to (and maintain) a cold shutdown condition.

7.4.2.2 System Description

7.4.2.2.1 General

The RSS has two redundant and independent panels. All parameters displayed and/or controlled from Division 1 and Division 2 in the MCR also are displayed and/or can be controlled from any of the two RSS panels (IEEE Std. 603, Section 5.8). Each panel contains the following:

- Division 1 Manual Scram Switch,
- Division 2 Manual Scram Switch,
- Division 1 Manual Main Steam Isolation Valve (MSIV) Isolation Switch,
- Division 2 Manual MSIV Isolation Switch,
- Division 1 Safety-Related Video Display Unit (VDU),
- Division 2 Safety-Related VDU,
- Nonsafety-Related VDU, and
- Nonsafety-Related Communications Equipment.

Because the VDUs on the RSS panels are connected to Q-DCIS or N-DCIS through the same networks serving corresponding VDUs at the MCR, all Division 1 and 2 safety-related and nonsafety-related display/control functions at the MCR also are available at the RSS panels. A simplified RSS panel schematic is provided in Figure 7.4-1. A functional block diagram of Q-DCIS and N-DCIS is included as part of Figure 7.1-1, and a functional network diagram appears as Figure 7.1-2. These diagrams indicate the relationships of safety-related or nonsafety-related systems with their peers, and with plant data acquisition systems. Section 7.1 contains a description of these relationships.

The two RSS panels are located in different rooms inside the Reactor Building (RB). Each RSS Panel room has a sliding fire door with a minimum fire rating of three hours. The RSS panel room environment typically is similar to the MCR environment. Access to and use of the RSS panels is administratively controlled. This satisfies the control access requirement of IEEE Std. 603, Section 5.9.

The RSS provides sufficient redundancy in its control and monitoring capability, to accommodate a single failure in the interfacing systems, a single failure in the RSS controls and the event that caused the MCR evacuation. The RSS is designed such that any failure within it does not degrade the capability of the interfacing systems. The RSS satisfies the single-failure criterion and independence requirements of IEEE Std. 603, Sections 5.1, 5.6, and 6.3.

7.4.2.2.2 Operating Conditions

The following conditions are assumed coincident with the event necessitating evacuation of the MCR and transfer of operation to the remote shutdown panel (IEEE Std. 603, Sections 4.1, 4.2, and 4.5):

- The plant is operating under normal conditions and at less than or equal to rated power. No Anticipated Operational Occurrence (AOO), seismic event, or other abnormal plant condition except for loss of off-site power is assumed.
- The remote shutdown panel is powered from buses supplied by uninterruptible safety-related and nonsafety-related 120 VAC systems.
- The reactor operator can either manually scram the reactor before leaving the MCR, or use the manual scram switches on the remote shutdown panel.
- Plant personnel have evacuated the MCR.
- The reactor operator can isolate the main steam lines by closing the manual MSIV isolation switches from the RSS.
- The reactor feedwater system, which is normally available, is conservatively assumed to be inoperable.
- The initiating event is assumed not to cause failure of the Alternating Current (AC) control power supplies to the remote shutdown panel, or failure of the power feeds to equipment functionally controlled from the remote shutdown panel. This assumption is justified because the power feeds to the RSS do not pass through the MCR.

7.4.2.2.3 System Operation

When evacuation of the MCR is necessary, the reactor is manually scrammed. If there has been no loss of off-site power, the turbine bypass valves automatically control reactor pressure, and the reactor feedwater system automatically maintains RPV water level. With these functions operable (and they should remain operable through the MCR evacuation), reactor cooldown is achieved through the normal heat sinks. This cooldown process can be supplemented from the remote shutdown panel using the RWCU/SDC system. The RWCU/SDC system provides the capability to bring the reactor from high-pressure conditions to cold shutdown. Control of both RWCU/SDC trains is provided on the remote shutdown panel. The Reactor Component Cooling Water System (RCCWS) is aligned to provide cooling water to the RWCU/SDC non-regenerative heat exchangers, and the PSW system is aligned to cool the RCCW heat exchangers. Control of two RCCW trains and two PSW trains is provided on the remote shutdown panel.

However, if the reactor feedwater system is not available due to loss of off-site power, as postulated in the first bullet of Subsection 7.4.2.2.2 Operating Conditions, control of the CRD system from the RSS may be utilized. Control of the high-pressure makeup injection capability of the CRD system ensures that the RPV water level remains above the ADS trip setpoint and above the elevation of the RWCU/SDC mid-vessel suction line nozzle. If main steam line isolation automatically occurs, or is manually initiated from the RSS, the ICS automatically controls reactor pressure. Because the logic processing equipment for the ICS (or any other safety or nonsafety-related system) is outside the MCR, ICS operation is not affected by an event necessitating MCR evacuation, and continued operation of the isolation condensers is assumed. If the event necessitating MCR evacuation results in a loss of the pressure regulator, but does not

cause main steam line isolation, the ICS initiates on high pressure. With the ICS in operation, the isolation condensers provide initial decay heat removal, and further reactor cooldown is achieved from the remote shutdown panels using the RWCU/SDC.

7.4.2.3 Safety Evaluation

The RSS is classified as a safety-related system that can control safety-related systems or equipment.

The RSS provides instrumentation and controls outside the MCR to allow prompt hot shutdown of the reactor after a scram and to maintain safe conditions during hot shutdown. It also provides capability for subsequent cold shutdown of the reactor through the use of suitable operating procedures.

Table 7.1-1 identifies the RSS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.4.2.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Design, fabrication, erection, construction, test, and inspection to quality standards commensurate with the importance of the safety function:

- Conformance: The RSS conforms with these requirements.

10 CFR 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (IEEE Std. 603):

- Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603, Section 5.6 and 6.3, and RG 1.75.

  With regard to IEEE 603, Section 5.1, an event is assumed to have occurred causing the evacuation of the MCR. The RSS is designed to accommodate a single failure in the interfacing systems or RSS controls for these scenarios (IEEE Std. 603, Section 5.1). The effects of such failures are analyzed below.

  The loss of one complete RWCU/SDC, RCCW or PSW loop could extend the time needed for the reactor to reach cold shutdown conditions. However, the ultimate ability of the RSS to facilitate such conditions is not impaired. Each RWCU/SDC loop provides 50% capacity for residual heat removal, and each RCCW and PSW train provides approximately 50% capacity for shutdown cooling. The RWCU/SDC, RCCW, and PSW systems, in conjunction with the ICS, can bring the plant to cold shutdown within 36 hours assuming the most restrictive single active failure.

  In the event that one CRD train fails or is out of service for maintenance, the remaining pump can provide sufficient makeup to maintain RPV water level during reactor cooldown.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: RSS conforms in that there are no unresolved issues for the RSS. Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC for the RSS are identified in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for RSS.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the RSS within the DCD conforms with this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.4.2.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, and 24:

- Conformance: The RSS conforms with the GDC identified.

7.4.2.3.3 Regulatory Guides

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The RSS conforms with IEEE Std. 603, Section 5.1. (Refer to subsection 7.4.2.3.1) and RG 1.53.

In addition, separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603, Sections 5.6 and 6.3, and RG 1.75.

RG 1.75 - Physical Independence of Electric Systems:

- Conformance: The RSS conforms with RG 1.75. See chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for a discussion of how the design meets the requirements of RG 1.75.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems:

- Conformance: The RSS conforms with RG 1.118.

RG 1.153 - Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The RSS conforms with RG 1.153.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems:

- Conformance: The RSS conforms with RG 1.180, based on the assumption that the interpretations and clarifications identified in Subsection 7.1.6.4 apply to the system.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The RSS conforms with RG 1.204, based on the assumption that the interpretations and clarifications identified in Subsection 7.1.6.4 apply to the system.

7.4.2.3.4 Branch Technical Positions

BTP HICB-11 - Guidance on Application and Qualification of Isolation Devices:

- Conformance: The RSS conforms with this guidance.

BTP HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The RSS conforms with this guidance.

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR, Part 52:

- Conformance: The RSS conforms with this guidance.

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The RSS conforms with this guidance.

BTP HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer Based Instrumentation and Control Systems:

- Conformance: The RSS conforms with this guidance.

BTP HICB-21 - Guidance on Digital Computer Real-Time Performance:

- Conformance: The RSS conforms with this guidance.

7.4.2.3.5 Three Mile Island Action Plan Requirements

In accordance with the SRP for 7.4 and with Table 7.1-1, there are no Three Mile Island (TMI) action plan requirements applicable for the RSS. However, TMI action plan requirements are generically addressed in Table 1A-1 in Chapter 1, Appendix 1A.

From the foregoing analyses, it is concluded that the RSS meets its design bases.

7.4.2.4 Testing and Inspection Requirements

The capability to safely shut down the reactor from outside the MCR is confirmed during the Initial Plant Test Program (Refer to Section 14.2). Testing to confirm the functionality of each RSS control circuit is performed during each refueling outage.

7.4.2.5 Instrumentation and Control Requirements

The parameters displayed and/or controlled from Division 1 and Division 2 in the MCR also are displayed and/or can be controlled from any of the two RSS panels.

7.4.3 Reactor Water Cleanup/Shutdown Cooling System

7.4.3.1 System Design Bases

7.4.3.1.1 Safety-Related Design Bases

The RWCU/SDC design bases are described further in Subsections 5.4.8.1 and 5.4.8.2, respectively. Figure 5.1-4 shows the basic configuration of the RWCU/SDC system.

RWCU/SDC is one of the dual redundant Plant Investment Protection (PIP) systems whose instrumentation belongs to the N-DCIS. A functional block diagram of N-DCIS is included as part of Figure 7.1-1, and a functional network diagram appears as Figure 7.1-2. These diagrams indicate the relationships of RWCU/SDC with its nonsafety-related peers, and with the safety-related plant data systems collectively referred to as Q-DCIS. Section 7.1 contains a description of these relationships.

7.4.3.1.2 Safety-Related Design Bases

RWCU/SDC system functions are not safety-related. Accordingly, the RWCU/SDC system has no safety-related design bases beyond a containment isolation function and providing instrumentation for detection of system breaks outside the containment (IEEE Std. 603, Sections 4.1 and 4.2). The containment is isolated by signals from the LD&IS (as described in Subsection 7.3.3). The RWCU/SDC system also is isolated by signals from LD&IS received from the SLC system.

7.4.3.1.3 Power Generation Design Bases

The RWCU/SDC system I&C is designed to provide suitable process indication, alarms, and manual and automatic devices for controlling the system as it:

- Removes reactor coolant impurities,
- Limits excess RPV water level during reactor heatup, startup, and shutdown cooling as well as hot standby modes of plant operation,
- Minimizes reactor coolant temperature gradients,

- Heats the RPV for hydrostatic tests, and
- Removes reactor core decay heat during typical plant shutdowns.

The RWCU/SDC shutdown cooling function modes are interlocked with reactor power operation to prevent increase in reactivity. During reactor power operation, the operator cannot start or select the RWCU/SDC shutdown cooling function modes. This interlock feature is designed to be single-failure proof. Interlocks are also provided to prevent inadvertent operation of pumps at higher speed and higher flow, and opening of regenerative heat exchanger (RHX) bypass valves during reactor power operation. An alarm is initiated if flow is higher than normal and the reactor is at power.

7.4.3.2 System Description

7.4.3.2.1 Summary Description

The RWCU/SDC system performs three basic plant functions. First, it provides a continuous purifying treatment of the reactor coolant during startup, normal operation, cooldown, hot standby, and shutdown modes of plant operation. Second, it removes core decay heat in conjunction with the main condenser or the isolation condensers during plant shutdown modes. Third, the RWCU/SDC system (with the feedwater system) provides reactor coolant heat-up during cold start-up. There are two redundant RWCU/SDC trains. The overall functional description of the RWCU/SDC system is provided in Subsection 5.4.8.

The I&C maintains the RWCU/SDC system process conditions within the limits necessary to control the system and satisfy its design bases. Protective features include isolating the RWCU/SDC system from the RPV in response to an LD&IS signal. The above isolation features protect the reactor core by minimizing the potential loss of RPV coolant inventory and by avoiding removal of boron from the reactor coolant if the SLC system is actuated.

7.4.3.2.2 Detailed System Description

The RWCU/SDC system measurements of flow, pressure, temperature, and conductivity are recorded or indicated with suitable alarms in the MCR. Valves behind shielding are furnished with on-off air operators that are individually controlled from local panels or from extension stems penetrating the shielding.

Indicating and control instruments and components are mounted on panels or local racks and are visible and accessible for repair, calibration, and testing.

The main process pumps are started automatically or from the MCR by VDU control with status indication. The pumps are driven by solid-state adjustable speed drives. Temperature elements located in the Nuclear Boiler System (NBS) and a reactor cooldown controller with temperature feedback control each pump to limit the rate of reactor water cooldown. A low pump suction flow interlock either prevents the pumps from starting or runs back or stops the pumps automatically. A reactor low water level (Level 3) pump speed runback interlock is provided to protect the pumps from cavitation during shutdown.

The pumps typically are supplied from separate and preferred power sources. The power supplies are automatically switched to dual on-site standby diesel-generators following the loss of preferred power (LOPP).

Motor-operated valves are operable automatically or manually by a VDU switch from the MCR. Each valve motor is stopped by limit switches or torque switches. The positions of air/nitrogen-operated containment isolation valves are indicated in the MCR to permit the plant operators to assess their status. An automatic signal overrides a manual signal to these valves. Containment isolation valve closing speeds are selected to protect the reactor core and limit radioactivity release in case of a RWCU/SDC system pipe break outside the containment.

The following signals prevent all containment isolation valves, with the exception of reactor bottom suction sampling line containment isolation valves, from opening (if closed) or closing the valves (if open):

- SLC system actuation is sent to the RWCU/SDC system via LD&IS, and
- LD&IS actuation occurs.

The isolation signal from LD&IS to the reactor bottom suction sampling line containment isolation valves can be overridden by a manual opening signal when a reactor bottom fluid sample is required for post-accident sampling purposes.

The plant LD&IS, including the portion related to the RWCU/SDC system, is further described in Subsection 7.3.3.

A flow control valve from the upper RPV nozzle controlling flow from the upper RPV region is located on the RWCU/SDC system suction line. The flow is set manually using a flow controller located in the MCR. Using thermocouples on the RPV bottom head drain line and the system suction line, the control valve from the RPV upper region is throttled during certain modes of plant operation (for example, startup, shutdown) to maintain the required temperature difference across the vessel. The valve actuator is air-operated.

The RWCU/SDC system also has a dump, or "overboarding," control valve to maintain RPV water level during certain modes of plant operation. This excess water typically is overboarded to the main condenser (Subsection 5.4.8). The valve is operated using instrument air and controlled both manually and automatically from the MCR using a controller and flow indicator. Pressure switches or transmitters located downstream of the overboarding control valve protect low pressure components by alarming in the MCR on high pressure and by closing the control valve with a high-high pressure signal. When the overboarding valve is used during reactor high-pressure conditions, a downstream orifice is used to assist in reducing system pressure; otherwise the orifice is bypassed using a motor-operated valve. The overboarding control valve fails closed upon loss of power or air pressure.

The demineralizer bypass piping has an air-operated modulating flow control valve that bypasses the excess flow above the demineralizer capacity. The demineralizer is protected from over-temperature by automatic controls that first open the demineralizer bypass valve and then close the demineralizer inlet valve.

Conductivity cells are located in the influent and effluent process sample streams of the demineralizers. These detectors are located in sample systems, which cool the sample stream to a constant temperature of 25°C (77°F), so conductivity elements are not required to be temperature compensated. Influent and effluent conductivity are continuously measured and transmitted to MCR recorders. Measured values in excess of water quality requirements are alarmed in the MCR.

The reactor coolant is sampled manually during cooldown, flood-up, or early periods of fuel off-loading when spiking of soluble and insoluble radioisotopic concentrations of corrosion products may occur.

Temperature elements are provided in the RPV bottom drain, the regenerative heat exchanger supply inlet and outlet, the non-regenerative heat exchanger outlet, the demineralizer influent (located at the pump suction), and the inlet and outlet of the regenerative heat exchanger return.

Temperature elements located in the NBS and a reactor cooldown controller with temperature feedback are used to provide the necessary signals to control pump speed during cooldown to maintain the required cooldown rate.

Density compensated system mass flow is measured in the process lines (by mid-vessel nozzles with venturi-type flow elements in each line) from the reactor bottom, located inside the containment. Flow elements also are provided in the Seismic Category I RWCU/SDC return lines to the feedwater lines and in the overboarding lines. The flow transmitters for all of these flow elements are arranged in a two-out-of-four logic configuration used to detect high RWCU/SDC differential mass flow due to a break outside the containment and to close the inboard and outboard containment isolation valves of the affected RWCU/SDC train. The containment isolation function on detection of RWCU/SDC high differential mass flow (due to a break outside the containment) is part of the LD&IS described in Subsection 7.3.3. See Figures 7.4-2A through 7.4-2E for the logic for detection of a RWCU/SDC pipe break outside containment.

Plate-type flow orifices are used for flow monitoring of demineralizer inlet flow and to open the demineralizer bypass control valve if the flow exceeds the demineralizer capacity.

7.4.3.3 Safety Evaluation

The RWCU/SDC system functions are nonsafety-related, with the exception of containment isolation functions and providing instruments to detect high differential mass flow following a RWCU/SDC break outside the containment. Refer to Subsection 6.2.4 for the containment isolation functions, and Subsection 7.3.3 for containment isolation and break detection function performed by LD&IS.

Table 7.1-1 identifies the RWCU/SDC and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.4.3.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Design, fabrication, erection, construction, test, and inspection to quality standards commensurate with the importance of the safety function:

- Conformance: The RWCU/SDC conforms with these requirements.

10 CFR 50.55a(h) (IEEE Std. 603):

Addressing RG 1.153 and IEEE Std. 603 below covers 10 CFR 50.55a(h) conformance.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues for I&C is discussed in Subsection 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for RWCU/SDC.

7.4.3.3.2 General Design Criteria

GDC 2, 4, 13, 19, and 24:

- Conformance: The RWCU/SDC system is nonsafety-related, but is designed in conformance with the listed GDC.

7.4.3.3.3 Regulatory Guides

In accordance with Table 7.1-1, RWCU/SDC conforms with the following RGs, based on the assumption that the interpretations and clarifications identified in Subsection 7.1.6.4 apply to the system:

- RG 1.180 Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems, and
- RG 1.204 Guidelines for Lightning Protection of Nuclear Power Plants

7.4.3.3.4 Branch Technical Positions

BTP HICB-16 - Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The RWCU/SDC system conforms with this guidance.

7.4.3.4 Testing and Inspection Requirements

The RWCU/SDC system instruments are calibrated and tested during the preoperational testing program to confirm the instrumentation is correctly installed and functions as designed. In addition, calibration and surveillance testing of the containment isolation devices is performed at regular intervals (IEEE Std. 603, Section 5.7 and 6.5). To the maximum extent possible, instrumentation requiring regular calibration, testing, and maintenance is mounted on accessible panels or racks located outside high radiation areas.

7.4.3.5 Instrumentation and Control Requirements

Operation of the RWCU/SDC system is from the MCR. The main instrumentation available to the MCR operator includes the following:

- Manual and automatic flow controllers for system, demineralizer, and overboarding flow,
- Flow indications for system, demineralizer, and overboarding flow,
- Position indications for containment isolation valves, flow control valves, and motor-operated valves,
- Temperature indication for demineralizer influent water,
- Conductivity recorders for demineralizer influent and effluent,
- Temperature of the system supply water (from the bottom RPV head),
- Temperature of the system return (to feedwater line) water,
- Temperatures of the non-regenerative and regenerative heat exchanger water (reactor water sides),
- Process alarms (for example, high water temperatures, high overboarding line pressure, low system flow, high system flow, high conductivity, etc.), and
- Pressure indication for the overboarding line.

7.4.4 Isolation Condenser System

7.4.4.1 System Design Bases

Refer to Subsection 5.4.6.1 for the design bases of the ICS (IEEE Std. 603, Sections 4.1 and 4.2). Figure 5.1-3 shows the basic configuration of the ICS.

The ICS is one of the Engineered Safety Feature (ESF) systems whose instrumentation belongs to a group of systems collectively called the Q-DCIS. A functional block diagram of Q-DCIS is included as part of Figure 7.1-1, and a functional network diagram appears as Figure 7.1-2. These diagrams indicate the relationships of the ICS with its safety-related peers, and with nonsafety-related plant data systems collectively called N-DCIS. Section 7.1 contains a description of these relationships.

7.4.4.2 System Description

Refer to Subsection 5.4.6.2 (IEEE Std. 603, Sections 4.12 and 5.4). Since the ICS is designed as a safety-related system, it fully complies with the equipment qualification requirements of IEEE Std. 603, Section 5.4.

7.4.4.3 Safety Evaluation

Conformance of ICS equipment with the requirements of IEEE Std. 603 (other than I&C) is addressed in Subsections 5.4.6.2 and 5.4.6.3. The paragraph on "Isolation Condenser Operation" in subsection 5.4.6.2 addresses the requirements of IEEE Std. 603, Section 4.10. Subsection 5.4.6.3 addresses the requirements of IEEE Std. 603, Section 4.8. Conformance of ICS I&C equipment with the requirements of IEEE Std. 603, Sections 5.1 and 8.1, is addressed in this subsection. The ICS is designed to operate from safety-related power sources. The system instrumentation is powered by four divisionally separated sources of safety-related power. The ICS uses two-out-of-four logic for automatic operation or isolation of each of the four separate isolation condenser (IC) trains as shown in Figure 7.4-3. The actuating logic and actuator power for the inner isolation valves for the four ICS trains are on two safety-related 120 VAC divisional power sources (Refer to Subsection 8.3.1.1.3) different from the two divisional power sources for the outer isolation valves.

Interdivisional fiber optic isolators are used to separate the four sensor inputs to the single divisional actuation logic circuits. An ICS train requires power from at least one of three safety-related divisional power sources to automatically start. Each of the four ICS trains has three of the four safety-related power sources. Consequently, the loss of two of the four safety-related power supplies does not result in the loss of any one ICS train. However, second and third sources of safety-related power are provided to operate the ICS automatic venting system during long-term ICS operation; otherwise the manually controlled backup venting system, which uses one of the divisional power sources starting the ICS, can be used for long-term operation.

If the three safety-related power supplies used to start an individual ICS train fail, then the IC would automatically start, because of the "fail open" actuation of the condensate return bypass valves upon loss of electrical power to the solenoids controlling its nitrogen-actuated valves.

The ICS is initiated automatically as part of the ECCS to provide mitigation for LOCA events. The ICS receives an actuation command following a confirmed LOCA signal after a time delay corresponding to the first depressurization valve actuation (as described in the ADS logic discussion in Subsection 7.3.1.1.2).

The ICS typically starts operating automatically upon high reactor pressure, low reactor water level (Level 2) with time delay, low reactor water level (Level 1), loss of power generation buses (from the same signal that initiates reactor scram), loss of feedwater (loss of power to two-out-of-four feedwater pumps) in reactor run mode, or MSIV position indication (indicating closure) whenever the Reactor Mode Switch is in the Run position.

Each ICS train also can be manually initiated, and so the operator is able to stop any individual ICS train whenever the RPV pressure is below a reset value override to the ICS automatic actuation signal following MSIV closure.

The residual heat removal function of the safety-related ICS is further backed up by the safety-related ESF combination of ADS, PCCS, and GDCS; by the nonsafety-related RWCU/SDC loops; or by the make-up function of the CRD system operating in conjunction with safety relief valves and the suppression pool cooling systems.

The DPS discussed in Section 7.8 provides diverse nonsafety-related signals for ICS actuation and other ICS functions.

Table 7.1-1 identifies the ICS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.4.4.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The ICS conforms with these standards.

10 CFR 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (IEEE Std. 603):

- Conformance: Separation and isolation is preserved both mechanically and electrically, in accordance with IEEE Std. 603, Section 5.6 and 6.3, and RG 1.75. The ICS is divisionalized and redundantly designed so failure of any instrument does not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The ICS conforms with this requirement, since it is an Emergency Core Cooling System (ECCS).

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- There are no interface requirements for ICS.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the ICS within the DCD conforms with this BTP.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.:

7.4.4.3.2 General Design Criteria

In accordance with the SRP for Section 7.4 and Table 7.1-1, the following GDC are addressed for the ICS:

GDC 1, 2, 4, 13, 19 and 24:

- Conformance: The ICS conforms with these GDC.

7.4.4.3.3 Regulatory Guides

RG 1.22 – Periodic Testing of Protection System Actuation Functions:

- Conformance: The ICS system conforms with RG 1.22.

RG 1.47 – Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The ICS conforms with RG 1.47.

RG 1.53 - Application of the Single-Failure to Nuclear Power Protection Systems:

- Conformance: The ICS meets the requirements of RG 1.53.

RG 1.62 – Manual Initiation of Protective Actions:

- Conformance: The ICS conforms with RG 1.62.

RG 1.75 - Physical Independence of Electric Systems:

- Conformance: Separation within the ICS is such that controls, equipment, and wiring are segregated into four separate safety-related logic groups. See chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for further discussion of how the design meets the requirements of RG 1.75.

RG 1.105 - Instrument Setpoints for Safety-Related Systems:

- Conformance: The setpoints used to initiate ICS automatic operation or isolation are established consistent with this guide. Reference 7.4-2 provides a detailed description of this methodology.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems:

- Conformance: The ICS conforms with RG 1.118.

RG 1.152 - Criteria for Digital Computers in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS conforms with RG 1.152.

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The ICS conforms with RG 1.153.

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

- Conformance: The ICS conforms with RG 1.168.

RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS conforms with RG 1.169.

RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS conforms with RG 1.170.

RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS conforms with RG 1.171.

RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS conforms with RG 1.172.

RG 1.173 - Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS conforms with RG 1.173.

RG 1.180-Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems:

- Conformance with above RG is based on the assumption that the interpretations and clarifications identified in Subsection 7.1.6.4 apply to the system.

RG 1.204-Guidelines for Lighting Protection of Nuclear Power Plants:

- Conformance: Conformance with the above RGs is based on the assumption that the interpretations and clarifications identified in Subsection 7.1.6.4 apply to the system.

7.4.4.3.4 Branch Technical Positions

BTP HICB-8 – Guidance for Application of RG 1.22:

- Conformance: The ICS conforms with this guidance.

BTP HICB-11 - Guidance on Application and Qualification of Isolation Devices:

- Conformance: The ICS conforms with this requirement. SSLC/ESF logic controllers for ICS use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The ICS logic resides within the SSLC/ESF that conforms with this BTP. Additional discussion is provided in Subsection 7.2.1.3.5.

BTP HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors:

- This BTP does not apply to ICS, since this system does not use RTD-type sensors.

BTP HICB-14 - Guidance on Software Reviews for Digital Computer-Based I&C Systems:

- Conformance: The ICS conforms with this guidance.

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The ICS description conforms with this guidance.

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The ICS conforms with this guidance.

BTP HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer Based I&C Systems:

- Conformance: The ICS conforms with this guidance.

BTP HICB-21 - Guidance on Digital Computer Real-Time Performance:

- Conformance: The ICS conforms with this guidance.

7.4.4.4 Testing and Inspection Requirements

Refer to Subsection 5.4.6.4. (IEEE Std. 603, Sections 5.7 and 6.5).

7.4.4.5 Instrumentation and Control Requirements

Refer to Subsection 5.4.6.5. (IEEE Std. 603, Sections 4.4, 4.5, 5.7, and 6.5).

The following ICS indications are reported in the MCR (IEEE Std. 603, Section 5.8):

- Radiation level in each IC pool compartment airspace,
- Mass flow rate in condensate return line,
- Mass flow rate in steam supply line,

- Temperatures of steam and condensate return lines,
- Temperatures of IC top and bottom vent lines, and
- Valve positions.

The following manual controls are provided by the ICS (IEEE Std. 603, Sections 6.2 and 7.2) to:

- Open/close condensate return valves,
- Close condensate return isolation valves,
- Close steam supply isolation valves,
- Open/close all bottom vent valves,
- Open/close all top vent valves, and
- Open/close purge line valve.

7.4.5 COL Information

None

7.4.6 References

7.4-1 USNRC, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plant" NUREG-0800, Section 7.4.

7.4-2 GE Nuclear Energy, "General Electric Instrument Setpoint Methodology," Licensing Topical Report NEDC-31336P-A, Class III (GE proprietary), September 1996.

.

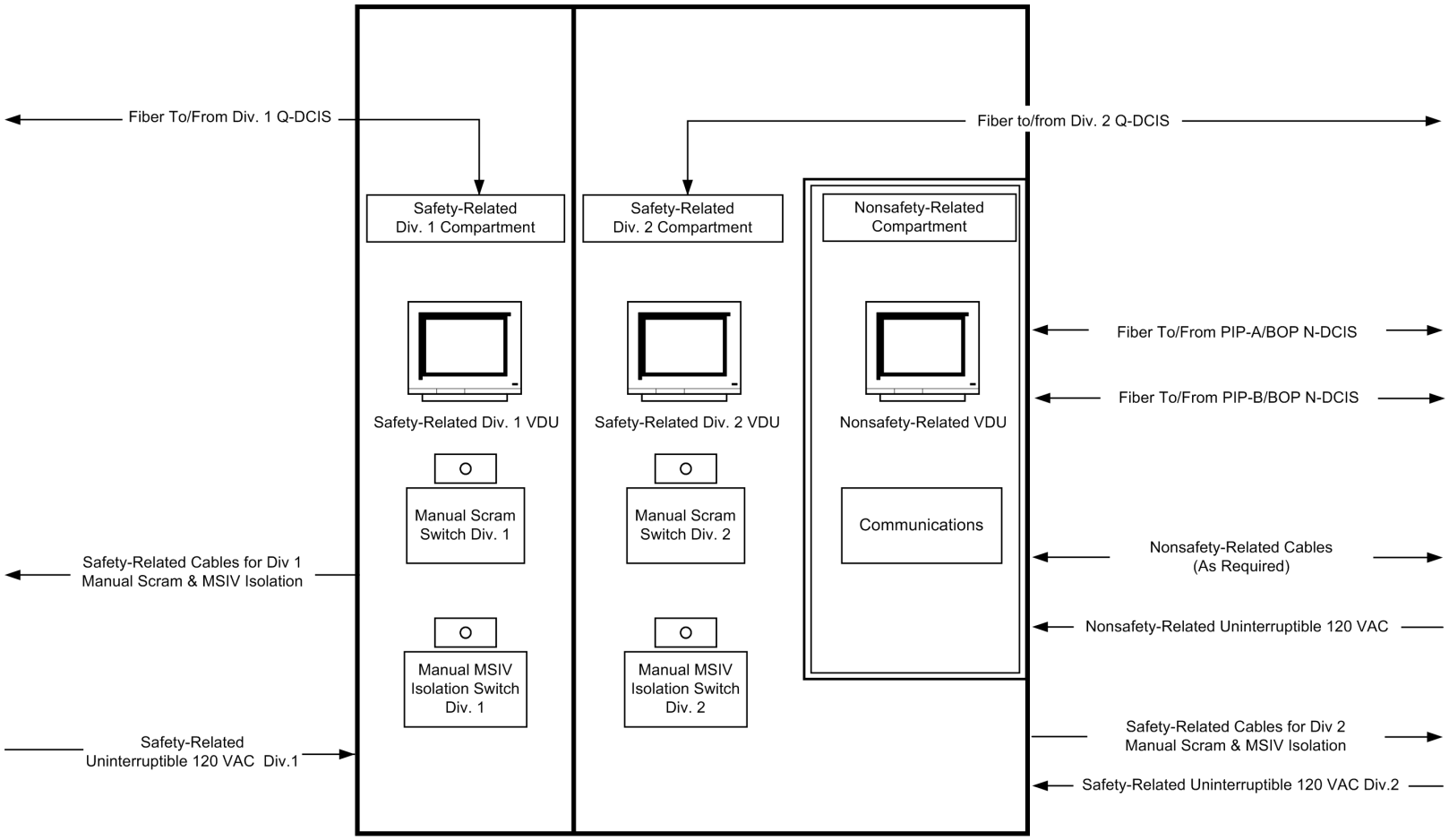


Figure 7.4-1. Remote Shutdown System Panel Schematic

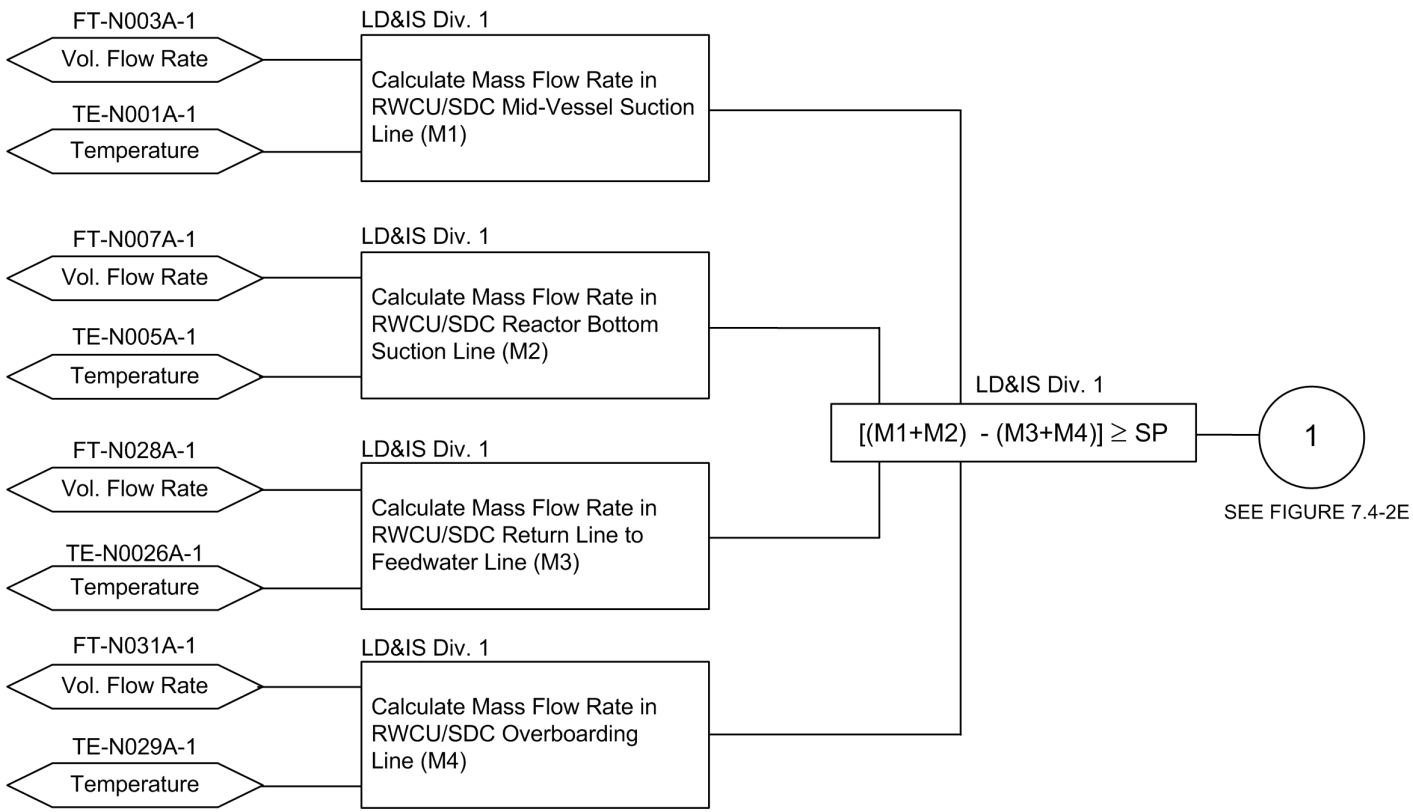


Figure 7.4-2a. RWCU/SDC System Train A Differential Mass Flow Logic- Division 1 (Typical For Train B)

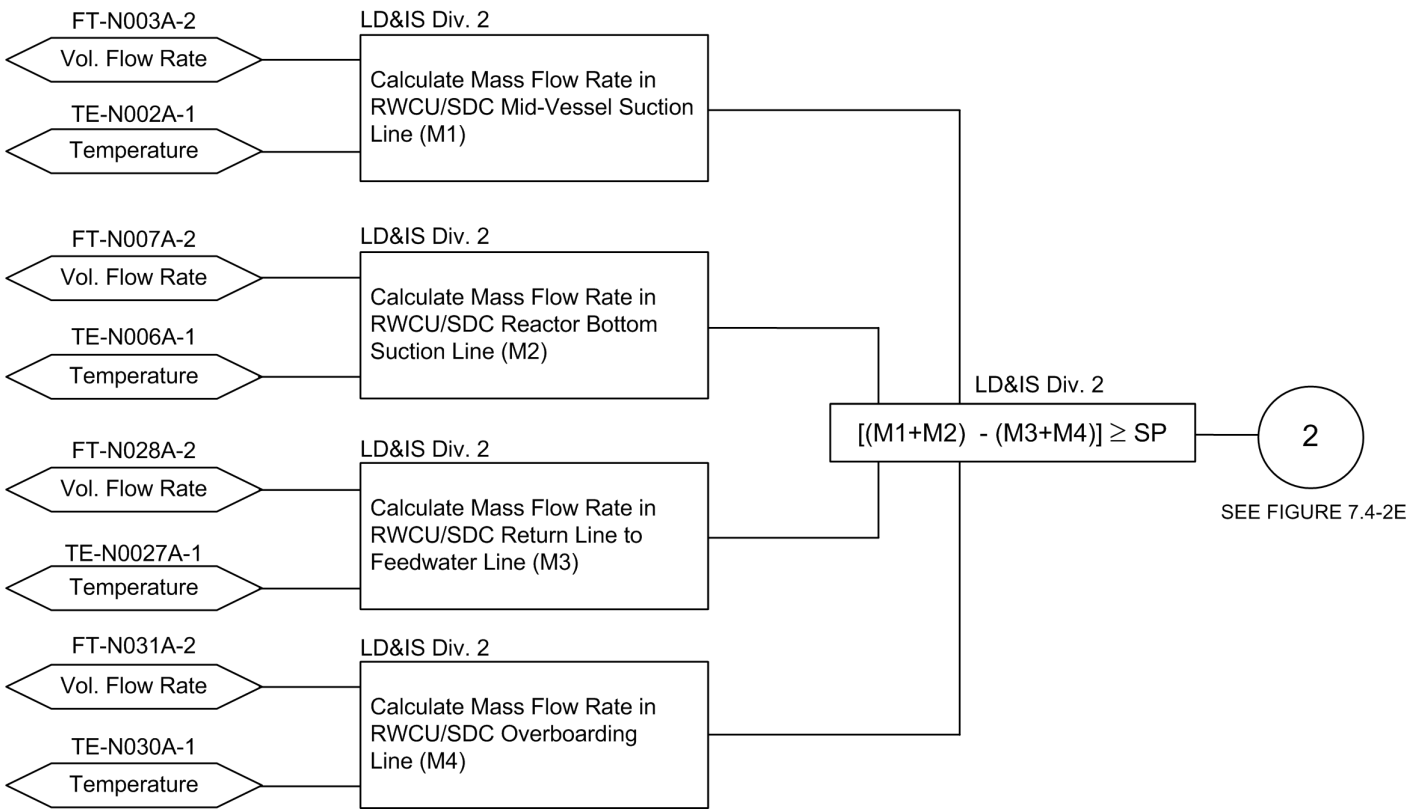


Figure 7.4-2b. RWCU/SDC System Train A Differential Mass Flow Logic- Division 2 (Typical For Train B)

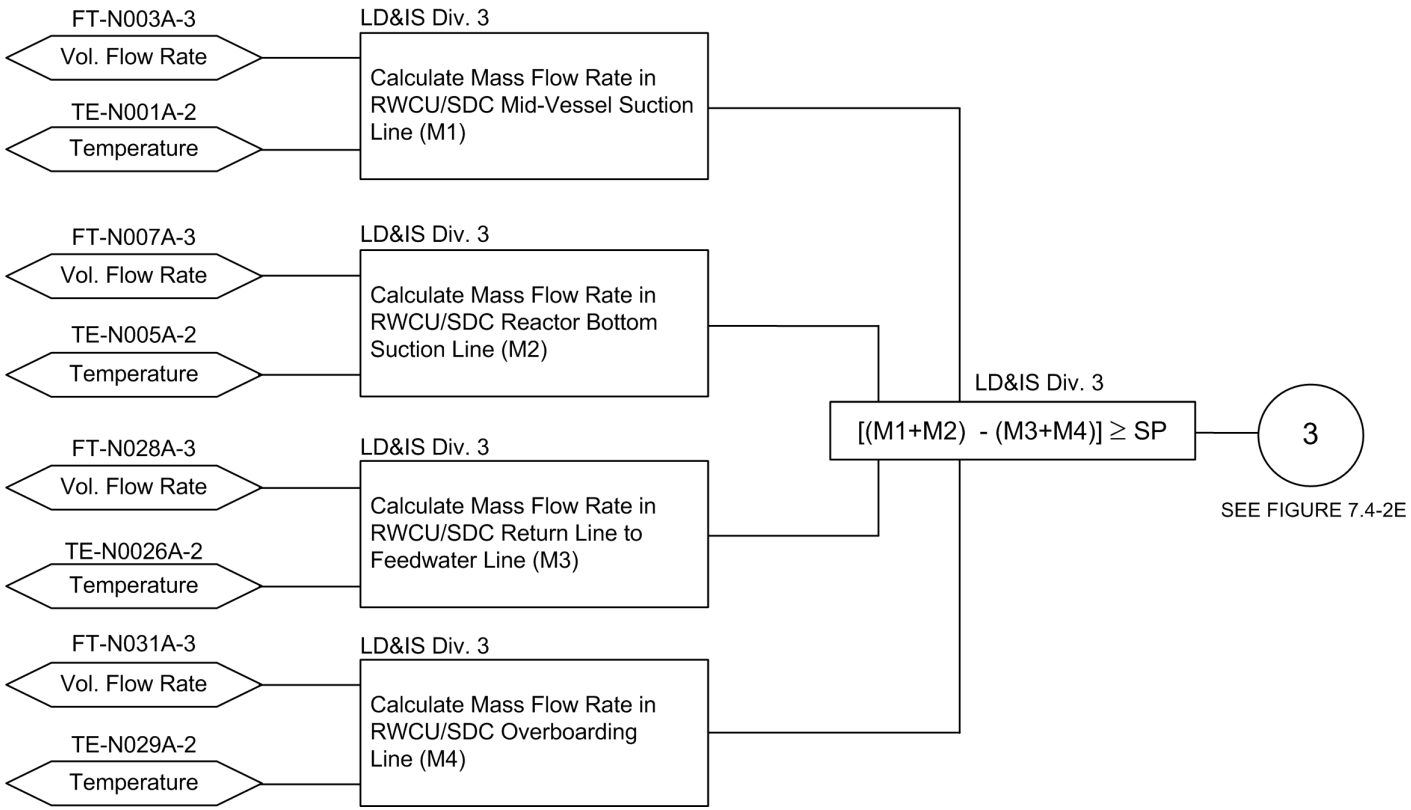


Figure 7.4-2c. RWCU/SDC System Train A Differential Mass Flow Logic- Division 3 (Typical For Train B)

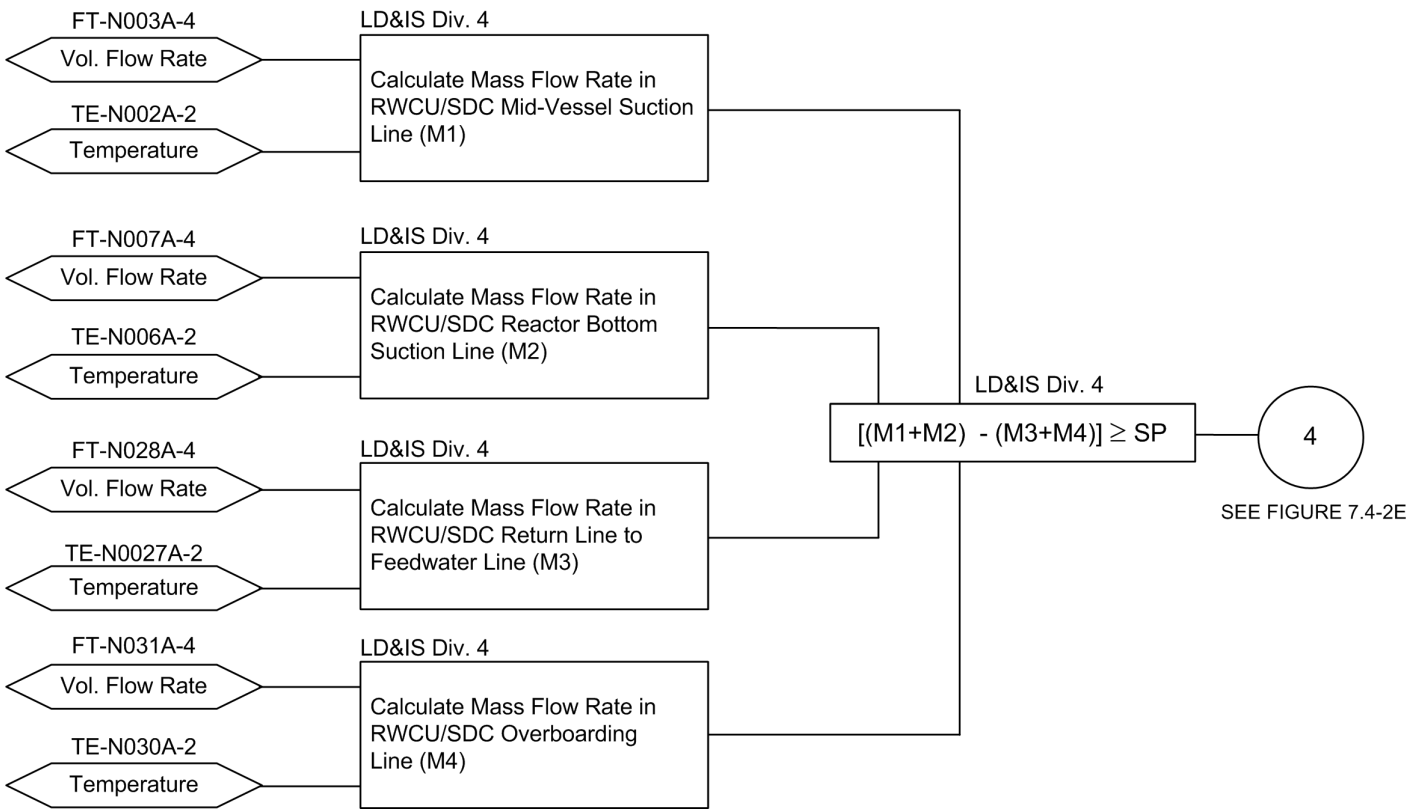


Figure 7.4-2d. RWCU/SDC System Train A Differential Mass Flow Logic- Division 4 (Typical For Train B)

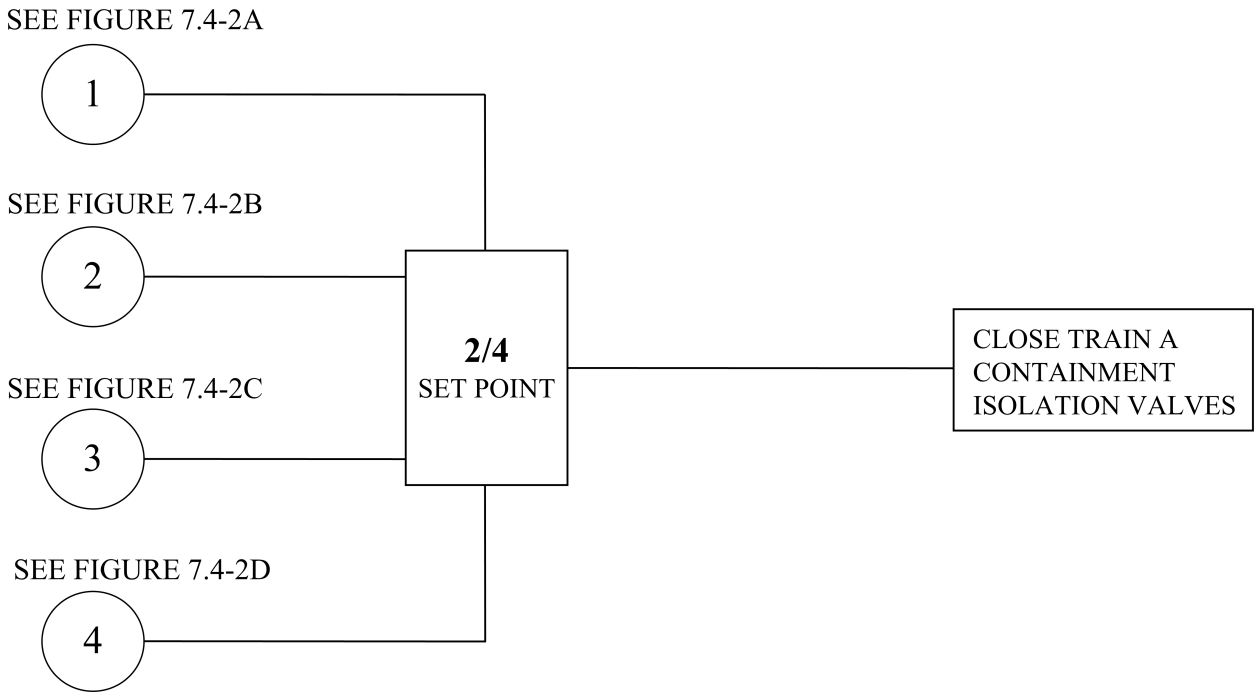


Figure 7.4-2e. RWCU/SDC Line Break Outside Containment Train A Isolation Logic (Typical For Train B)

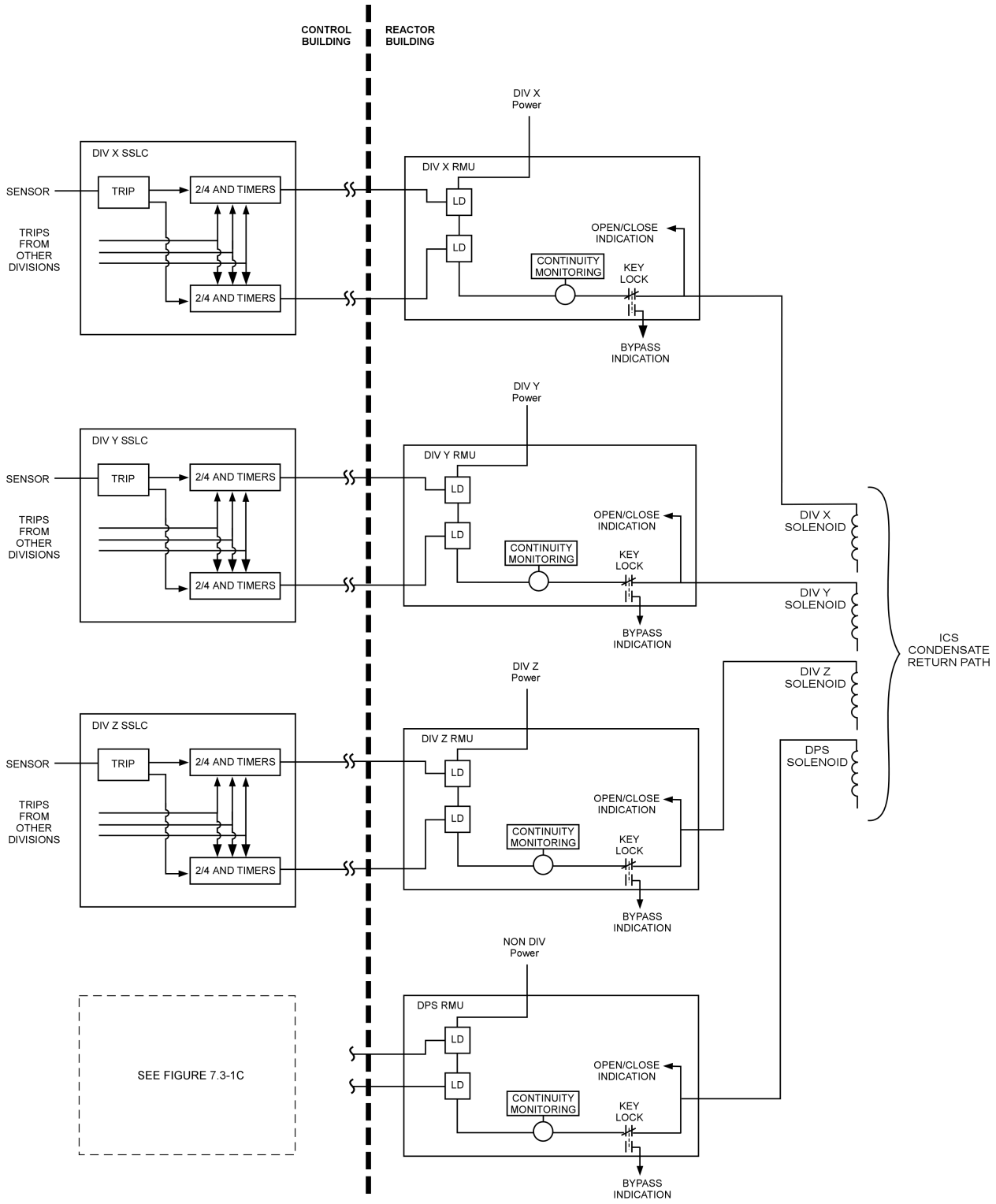


Figure 7.4-3. Isolation Condenser System Initiation and Actuation

7.5 SAFETY-RELATED AND NONSAFETY-RELATED INFORMATION SYSTEMS

This section discusses instrumentation associated with the following:

- Post Accident Monitoring (PAM),
- Containment Monitoring System (CMS),
- Process Radiation Monitoring System (PRMS),
- Area Radiation Monitoring System (ARMS), and
- Pool Monitoring Subsystems.

The safety-related portions of the PAM Instrumentation, CMS, PRMS, Pool Monitoring Subsystems and Wetwell to Drywell Vacuum Breakers are part of a group of systems collectively called the Safety-Related Distributed Control and Information System (Q-DCIS). A functional block diagram of the Q-DCIS is included as part of Figure 7.1-1 and a functional network diagram appears as Figure 7.1-2 (not all systems are shown on these figures.)

These diagrams generally indicate the relationships of a safety-related system with its safety-related peers and with nonsafety-related plant data systems called the Nonsafety-Related Distributed Control and Information System (N-DCIS). Section 7.1 contains a description of these relationships.

The nonsafety-related portions of the PAM Instrumentation, CMS, PRMS, and the ARMS are part of the N-DCIS.

7.5.1 Post Accident Monitoring Instrumentation

7.5.1.1 System Design Bases

The PAM instrumentation has the following safety design basis:

- Provide instrumentation to monitor variables and systems over their anticipated ranges for accident conditions as appropriate to ensure adequate safety.
- Provide the appropriate Main Control Room (MCR) instrumentation and displays to provide the information from which actions can be taken to maintain a safe plant condition under accident conditions, including Loss-of-Coolant Accidents (LOCAs).
- Provide equipment (including the necessary instrumentation) at appropriate locations outside the MCR with the capability for prompt hot shutdown of the reactor, and
- Provide the means for monitoring the reactor containment atmosphere, spaces containing components that recirculate LOCA fluids, effluent discharge paths, and plant environs for radioactivity that may be released as a result of accidents.

7.5.1.2 System Descriptions

The safety-related portion of the PAM systems are those systems that provide information for the safe operation of the plant during normal operation, Anticipated Operational Occurrences (AOOs) and accidents, to help ensure performance of manual safety-related functions. The safety-related information systems:

- Include those systems that provide information for manual initiation and control of safety-related systems,
- Indicate that safety-related plant functions are being accomplished, and
- Provide information, from which appropriate actions can be taken to mitigate the consequences of accidents.

The nonsafety-related portion of the PAM systems include the Safety Parameter Display System (SPDS), information systems associated with the emergency response facilities and the Emergency Response Data System (ERDS), none of which do not perform safety-related functions.

7.5.1.3 Safety Evaluation

Table 7.1-1 identifies the PAM instrumentation and the associated regulatory requirements, guidelines, codes and standards applied in accordance with NUREG-0800. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.5.1.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards Important to Safety

- Conformance: The PAM instrumentation complies with these standards.

10 CFR 50.55a(a)(h), Protection and Safety Systems compliance with IEEE Std. 603

- Conformance: The PAM Instrumentation complies with these requirements.

10 CFR 50.34a(f)(2)(v) [I.D.3], Bypass and Inoperable Status Indication

- Conformance: The PAM Instrumentation conforms with the Bypass and Inoperable Status Indication (BISI) requirements of 10 CFR 50.34(f)(2)(v)(I.D.3). The systems providing inputs to the PAM Instrumentation to which these requirements apply are defined in Table 7.1-1. General conformance is discussed in Subsection 7.1.6.1, and specific conformance is discussed in the system specific sections.

10 CFR 50.34(f)(2)(xvii) [II.F.1], Accident Monitoring Instrumentation

- Conformance: The PAM System complies with these requirements.

10 CFR 50.34(f)(2)(xviii) [II.F.2], Inadequate Core Cooling Instrumentation

- Conformance: The PAM instrumentation complies with this requirement. The direct water-level instrument system provides for the detection of conditions indicative of inadequate core cooling (Refer to Table 1.A-1, Three Mile Island [TMI] Action Plan Items).

10 CFR 50.34(f)(2)(xix) [II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage

- Conformance: The PAM instrumentation meets the intent of this requirement. The PAM instrumentation design meets the intent of RG 1.97. Additional information is provided in Subsection 7.5.1.3.1.4.

10 CFR 50.34(f)(2)(xxiv) [II.K.3.23], Recording of Reactor Vessel Water Level

- Conformance: The PAM instrumentation meets this requirement. (Refer to Table 1.A-1 TMI Action Plan Items).

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), Inspections, Tests Analyses, and Acceptance Criteria (ITAAC) in Design Certification Applications

- Conformance: ITAAC are provided for the Instrumentation and Control (I&C) systems and equipment in Tier 1.

10 CFR 52.47(a)(1) (vii), Interface Requirements

- Conformance: There are no interface requirements for this section.

10 CFR 52.47(a)(2), Level of Detail

- Conformance: The level of detail provided for the PAM instrumentation within the DCD conforms with this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.5.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 23, 24 and 64:

- Conformance: The PAM Instrumentation is in conformance with the GDC identified above.

7.5.1.3.3 Staff Requirements Memorandum

Item II.T of SECY 93-087 Control Room Annunciator (Alarm) Reliability:

- Conformance: The alarm management system meets the intent of the Control Room Annunciator (Alarm) Reliability requirements of SECY 93-087, Item II.T. The systems to which this requirement applies are defined in Table 7.1-1. General conformance is discussed in Subsection 7.1.6.3, and specific conformance is discussed in the system specific sections.

7.5.1.3.4 Regulatory Guides

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The PAM Instrumentation conforms with RG 1.180 as discussed in Subsection 7.1.6.4.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The PAM Instrumentation conforms with RG 1.204 as discussed in Subsection 7.1.6.4.

RG 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The design meets the intent of RG 1.97, which endorses (with certain exceptions specified in Section C of the RG) IEEE Std. 497. IEEE Std. 497 establishes flexible, performance-based criteria for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables. IEEE Std. 497 identifies five types of variables for accident monitoring and the criteria for the selection of each type of variable.

Variable Types and Selection Criteria

The five variable types (A, B, C, D, E) and their selection criteria are defined in Section 4 and Table 1 of IEEE Std. 497. Table 1 summarizes the selection criteria for each variable type and the source documents such as plant accident analysis licensing basis, Emergency Procedure Guidelines (EPGs) or plant specific Emergency Operation Procedures (EOPs) and Abnormal Operating Procedures (AOPs) related to the variable type.

The Functional Requirements Analysis (FRA), Allocation of Functions (AOF), (Section 18.4) and Task Analysis (TA) (Section 18.5) address Critical Safety Functions (CSF), and provide an independent list of the required RG 1.97 parameters via their respective Results Summary Reports (RSR). The FRA, AOF and TA are iteratively integrated into the design process to provide a final design that effectively balances human factors and system design.

The list of parameters, generated by the Human Factors Engineering (HFE) process, is compared with the information generated from the design process and the differences are entered into the Human Factors Engineering Issue Tracking System (HFEITS) for resolution. During the

detailed (second iteration) TA, the RG 1.97 parameters are categorized into the five variable types.

When the EPG/ Severe Accident Guidelines (SAG)/AOP guidelines are released, they are compared with the list of RG 1.97 parameters and the differences are entered into the HFEITS for resolution.

Performance Criteria

Performance criteria defined in IEEE Std. 497-2002, Section 5 include:

- Range,
- Accuracy,
- Response time,
- Required instrumentation duration,
- Reliability, and
- Performance assessment documentation.

RG 1.97 endorses IEEE Std. 497 Section 5, "Performance Criteria" with modification (the RG provides guidance on the application of these requirements).

Performance criteria (identified in IEEE Std. 497, Section 5) are developed during the design process using inputs from the HFE process together with other design and accident analysis inputs. The performance criteria (range, accuracy, response time, required instrument duration, and reliability) for each required variable are documented in the PAM Variable List.

Performance is verified to meet the as-designed performance criteria per Section 18.11, Human Factors Verification and Validation (HF V&V). Performance deviations are entered into the HFE ITS for resolution. The results of this assessment are documented in the HF V&V RSR.

Design Criteria

The Design Criteria defined in IEEE Std. 497, Section 6, include:

- Single failure;
- Common cause failure;
- Independence and separation;
- Isolation;
- Information ambiguity;
- Power supply;
- Calibration;

- Testability;
- Direct measurement;
- Control of access;
- Maintenance and repair;
- Minimizing measurements;
- Auxiliary supporting features;
- Portable instruments; and
- Documentation of design criteria.

RG 1.97 endorses IEEE Std. 497 Section 6, "Design Criteria" with modification.

The design meets the intent of the specific criteria identified in IEEE Std. 497, Section 6. Each specific criterion is addressed and documented during the detailed design process using appropriate inputs from the licensing basis, the design process and the HFE process, as identified in Chapter 18.

Qualification Criteria

The design meets the intent of the requirements to qualify the instrumentation associated with the identified variables within each type (A, B, C, D, E) in accordance with the qualification criteria of IEEE Std. 497-2002 Criteria, Section 7, "Qualification Criteria". Specific qualification requirements are developed during the design process for the following:

- Type A variables,
- Type B variables,
- Type C variables,
- Type D variables,
- Type E variables,
- Portable instruments,
- Post event operating time, and
- Documentation of qualification criteria.

Display Criteria

The display criteria defined in IEEE Std. 497 Section 8 include:

- Information characteristics,
- Human factors,

- Anomalous indications,
- Continuous vs. on –demand display,
- Trend or rate information,
- Display identification,
- Type of monitoring channel display,
- Display location,
- Information ambiguity,
- Recording,
- Digital display signal validation, and
- Display criteria documentation.

The design meets the intent of the specific display criteria identified in IEEE Std. 497, Section 8. Display Criteria defined in Chapter 18, Human Factors Engineering, include all the display criteria listed above. In addition Chapter 18 addresses:

- Results of an analysis of the system functions required to respond to an accident; and
- Analysis of the tasks required of the operator to implement those functions during design basis events.

Display characteristics consistent with inputs from Design, Safety Analysis, and Human Factors Engineering include:

- Range,
- Accuracy,
- Precision,
- Display format,
- Units, and
- Response time.

The Distributed Control and Information System (DCIS) provides the required signal paths to process the information. The DCIS is subdivided into the Q-DCIS and the N-DCIS. These DCIS systems are described in Section 7.1.

For accident monitoring instrumentation associated with CSF and powered from the safety-related sources, the Q-DCIS provides the required signal path to process this information. This information then is shown on Q-DCIS divisional safety-related displays.

The safety-related information also can be transmitted via isolated safety-related gateways to the N-DCIS for input to nonsafety-related displays, Plant Computer Functions (PCF) and the Alarm Management System (AMS). Type A, Type B, and Type C variables are powered from safety-related sources. For Type D and Type E variables that are powered from nonsafety-related sources the N-DCIS provides the required signal paths to process information.

The Q-DCIS has four separate divisions, each powered by a different safety-related uninterruptible power source. The safety-related power is discussed in Subsection 8.3.1.1.3. The design meets the intent of required instrument duration requirements of IEEE Std. 497, Section 5.4, as modified by RG 1.97.

The nonsafety-related AMS, Safety Parameter Displays, and Bypassed and Inoperable Status Indication (BISI) are discussed in Subsection 7.1.4 and 7.1.5. Subsection 7.1.5.3.3 discusses additional acceptance criteria applicable to Annunciator Systems (SECY-93-087, Item II.T). The PCF provides nonsafety-related navigational or top-level displays for Safety Parameter Displays, Alarms and Annunciators, and BISI. The N-DCIS also provides data support functions (for example, Technical Support Center [TSC] and Emergency Operations Facility [EOF], and Emergency Response Data Systems [ERDS]).

Quality Assurance

All equipment is provided in accordance with the GEH 10 CFR 50 Appendix B Quality Assurance Program, as accepted by the Nuclear Regulatory Commission (NRC). The NRC accepted GEH Quality Assurance Program, along with its implementing procedures constitute the Quality Assurance system that is applied to the safety-related I&C system design. It satisfies all applicable requirements of the following:

- 10 CFR 50 Appendix B,
- American National Standards Institute (ANSI) / American Society of Mechanical Engineers (ASME) NQA-1, and
- ISO 9001.

Post Accident Monitoring Variable List Documentation

The PAM variable list is prepared as a separate document, using inputs from the design process, licensing design basis, and HFE process, including the development of the EPGs and/or EOPs and AOPs.

The PAM variable list document provides summary information for each PAM variable as applicable. Typical information provided includes:

- PAM variable name,
- Type,
- Range,
- Extended range (TYPE C),

- Instrument channel accuracy,
- Required instrument duration,
- Power source,
- Required number of channels,
- Qualification criteria, and
- Type of monitoring channel display.

7.5.1.3.5 Branch Technical Positions

BTP HICB-10, Guidance on Application of RG 1.97:

- Compliance: RG 1.97, Revision 4, Section A, states that Branch Technical Position HICB 10 will require updates for consistency with Revision 4 of RG 1.97. Compliance with these requirements is addressed during the detailed design phase.

7.5.1.4 Testing and Inspection Requirements

Testing and inspection requirements for RG 1.97 instrumentation are defined in IEEE Std. 497, Criterion 6.8, "Testability" and Criterion 6.11, "Maintenance and Repair". Compliance with these requirements is addressed during the detailed design phase.

7.5.1.5 Instrumentation and Controls Requirements

Instrumentation requirements for RG 1.97 instrumentation are defined in IEEE Std. 497. Identification of specific instrument requirements and compliance with these requirements is addressed during the detailed design phase.

7.5.2 Containment Monitoring System

The CMS provides the instrumentation to monitor the:

- Atmosphere in the containment for high gross gamma radiation levels,
- Pressure of the drywell and wetwell,
- Drywell/wetwell differential pressure,
- Lower and upper drywell water level (post-LOCA),
- Temperature of the suppression pool water,
- Suppression pool water level,
- Drywell/wetwell hydrogen/oxygen concentration, and
- Containment area radiation.

These parameters are monitored during both normal reactor operations and post-accident conditions to evaluate the integrity and safe conditions of the containment. Abnormal measurements and indications initiate alarms in the MCR.

7.5.2.1 System Design Bases

The CMS design is in conformance with the following system design criteria:

CMS is classified as safety-related and Seismic Category 1 except as noted, and conforms with the relevant codes and standards specified in Table 7.1-1 for this system. IEEE Std. 603, Sections 4.5 and 5.8, apply to the safety-related portions of the CMS.

The safety-related Hydrogen/Oxygen (H_2/O_2) analyzers are active during normal operation. Additional sampling capacity is automatically initiated by a LOCA signal for post-accident monitoring of oxygen and hydrogen content in the containment.

Each CMS gas sampling subsystem monitors the atmospheric oxygen and hydrogen contents in the drywell and the wetwell, and provides measurements in the MCR in percent by volume for each of the sampled gases. Sampling of the drywell or the wetwell is initiated either manually (locally) or automatically.

Dual redundant divisions of gas sampling and radiation monitoring are provided.

Nonsafety-related radiation monitoring consists of two channels per division. Each radiation monitoring channel portion consists of a gamma sensitive Radiation Detection Assembly and a digital Signal Conditioning Unit. The Radiation Detection Assemblies are installed at widely separated locations to provide comprehensive coverage of the containment volume. The channels measure gross gamma radiation in the drywell and wetwell. The gross gamma radiation signals are provided to the MCR where they are continuously displayed. The channels are equipped with upscale alarms to indicate high radiation and an alarm to indicate channel malfunction.

MCR alarms are provided for indications of high radiation dose rates, inoperative radiation monitors, high oxygen levels, high hydrogen levels, and abnormal samples for each subsystem.

Each gas sampling rack is provided with its own gas calibration sources of known concentration levels to calibrate periodically the oxygen and hydrogen analyzers and the sensors.

The lower drywell water level is monitored to indicate any boiloff from the Isolation Condenser/Passive Containment Cooling System (IC/PCCS) that may accumulate in the lower drywell following a LOCA condition.

The upper drywell water level is also monitored and compared with the RPV nozzle elevations.

The drywell and wetwell pressure instrumentation is located throughout the containment and provides safety-related and nonsafety-related functions for both normal and post-accident monitoring. In addition, pressure signals are provided to the Diverse Protection System (DPS) for diverse scram protection monitoring.

The drywell and wetwell volumes are provided with two additional safety-related differential pressure transmitters, connected between these two volumes. These channels are used for vacuum breaker valve monitoring.

MCR alarms and indication are provided for suppression pool temperature (see Subsection 7.2.3).

7.5.2.2 System Description

The CMS is a divisionalized and segregated (safety/nonsafety-related) monitoring system (IEEE Std. 603, Section 5.6.3), and is configured as shown in Figure 7.5-1. The specific system features are as follows:

- Radiation monitoring and gas H_2/O_2 sampling are provided for the drywell and for the airspace above the suppression pool.
- Each radiation monitoring channel uses one gamma-sensitive ion chamber and one digital log radiation monitor. Four channels are provided, two for the drywell and two for the suppression pool (wetwell) airspace.
- During normal plant operation, both the radiation monitoring and gas sampling subsystems are operating. For post-accident monitoring, the gas sampling subsystem is automatically activated by the LOCA signal to alternate its sampling between the drywell and the wetwell. The area of sampling can be selected manually or sequentially controlled.
- Heat tracing is provided on the gas sampling lines for control of moisture and condensation.
- Two isolation valves are provided on each sample and return line that penetrates the containment. Each line has one manual inner valve and one remote-control outer valve.
- Each gas sampling analyzer has dual redundant pumps. One is used during normal operation; the other is used for added capacity or backup.
- Separate oxygen and hydrogen gas sources are provided in each CMS sampling rack with known compositions for monitor calibration.
- CMS piping connections are provided.
- The drywell pressure instrumentation consists of transmitters located throughout the containment.
- Four drywell pressure transmitters are provided for safety-related signals for use by the Reactor Protection System (RPS) for reactor scram. These drywell pressure signals also are transmitted to the Leak Detection and Isolation System (LD&IS), where they are used to initiate isolation of containment valves, transfer pump suction, and initiate suppression pool cooling. In addition, these pressure signals and alarms are hardwired to the MCR to provide diverse information for operator use.

- Two wide-range safety-related pressure transmitters are used for providing safety-related drywell pressure information meeting the requirements of post-accident monitoring.
- Four nonsafety-related drywell pressure transmitters are used by the DPS for diverse scram protection monitoring and by the Containment Inerting System (CIS) for controlling the position of the nitrogen makeup pressure control valve.
- The drywell and wetwell volumes also are provided with two additional safety-related differential pressure transmitters, connected between these two volumes. These channels also are used for vacuum breaker valve monitoring.
- The suppression pool water level is monitored during all plant operating conditions and post-accident conditions. Suppression pool water level monitoring consists of ten channels of water level detection sensors distributed into four safety-related narrow-range and four nonsafety-related wide-range instruments. The narrow range suppression pool water level signals are used to detect the uncovering of the first set of suppression pool temperature sensors below the pool surface. When the suppression pool water level drops below the elevation of a particular set of temperature sensors, those sensor signals are not used in computing the average pool temperature.
- Two of the wide range water level signals are used for displaying suppression pool water level on the Remote Shutdown System (RSS) Panels.
- Suppression pool temperatures are monitored (see Subsection 7.2.3).

7.5.2.3 Safety Evaluation

The CMS design, including the sensors and the instrumentation channels, is engineered into both safety-related and nonsafety-related subsystems. Safety-related systems are environmentally and seismically qualified for continuous monitoring during reactor operation, as well as abnormal and accident plant conditions. The system design conforms with the System Design Bases.

Table 7.1-1 identifies the CMS and the associated regulatory requirements, guidelines, and codes and standards applied, in accordance with NUREG 0800. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.5.2.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The CMS complies with this requirement.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6 and RG 1.75. The CMS safety-related subsystems are divisionalized and are designed with redundancy so that failure of any instrument does not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The CMS demonstrates compliance by being able to provide automatic indication of bypassed and inoperable status.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The CMS complies with this requirement.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The CMS complies with this requirement.

10 CFR 50.44(c)(4), Combustible Gas Control For Nuclear Power Reactors, Monitoring:

- Conformance: The CMS complies with this requirement.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the CMS within the DCD conforms with this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.5.2.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, and 24:

- Conformance: The CMS design complies with these GDC.

7.5.2.3.3 Staff Requirements Memorandum

SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability

- Conformance: The CMS AMS meets the requirements of SECY-93-087, Item II.T for redundancy, independence, and separation in that the "alarm system" is considered redundant as follows:
  - Alarm points are sent via dual networks to redundant message processors using dual power supplies. The processors are dedicated to alarm processing.
  - The alarms are displayed on multiple independent Video Display Units (VDUs) (dual power supplies on each).
  - The alarms are driven by redundant datalinks to the AMS (dual power). There are redundant alarm processors.
  - There is one horn and one voice speaker. Test buttons are available to test the horn and all the lights.
  - There are no alarms requiring manually controlled actions for safety systems to accomplish their safety-related functions.

7.5.2.3.4 Regulatory Guides

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

RG 1.53 - Application of the Single Failure Criterion to Nuclear Power Protection Systems

RG 1.75 - Physical Independence of Electrical Systems

RG 1.105 - Setpoints for Safety-Related Instrumentation

RG 1.118 - Periodic Testing of Electric Power and Protection Systems

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The CMS conforms with all of the RGs listed above, with the assumption that the interpretations and clarifications identified in Subsection 7.1.6.4 apply.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the SSLC/ESF system, as discussed in Subsection 7.1.6.4.

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The CMS conforms with RG 1.180 as discussed in Subsection 7.1.6.4.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The CMS conforms with RG 1.204 as discussed in Subsection 7.1.6.4.

7.5.2.3.5 Branch Technical Positions

BTP HICB-11 - Guidance on Application and Qualification of Isolation Devices

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints

BTP HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

BTP HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions

BTP HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems

BTP HICB-21 - Guidance on Digital Computer Real-Time Performance:

- Conformance: The CMS complies with all the above HICBs. Subsection 7.3.5.3.5 provides a discussion of BTP HICB-14, BTP HICB-17, BTP HICB-18, and BTP HICB-21 in conjunction with the SSLC/ESF system. BTP HICB-13 does not apply to the CMS, since this system does not use RTD-type sensors.

7.5.2.3.6 Three Mile Island Action Plan Requirements

In accordance with SRP 7.5, and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) [I.D.3], 10 CFR 50.34(f)(2)(xvii) [II.F.1] and 10 CFR 50.34 (f)(2)(xix)[II.F.3] apply to the CMS. The CMS complies with these requirements, as indicated above. TMI action plan requirements are addressed generically in Appendix 1A.

7.5.2.4 Testing and Inspection Requirements

In-service and Surveillance Testing – In-service testing is performed periodically on each CMS subsystem to verify operability and to ensure its readiness status for post accident monitoring (IEEE Std. 603, Section 6.5). Surveillance testing includes instrument channel checks of the radiation and gas monitors, functional tests to verify equipment operability, sensor calibration and response tests, and leakage tests of the gas sampling lines.

Validation Test of the Calibrated Gas Sources - Tests is conducted on the gas calibration sources to verify equipment operability and to certify that the required gas concentration levels are within acceptable limits.

Specific Channel Calibration Checks - Each radiation monitoring channel is checked and calibrated using a known gamma radiation source. Channel response shall be checked for proper measurement and display and for alarm initiation.

Each oxygen and hydrogen gas-sampling channel is checked for proper calibration and response using at least two input gas levels (Refer to Table 7.5-4).

Sample Gas Leakage Tests - The design leakage from the sampling lines and associated gas analyzer panel is specified in Table 7.5-4.

7.5.2.5 Instrumentation and Control Requirements

Radiation Level Monitoring - Each compartment in the primary containment is monitored by two-divisional channels for gross gamma radiation levels. Each channel consists of an ion chamber detector and a digital log radiation monitor, with trip circuits set for high radiation and low/INOP indications.

Oxygen/Hydrogen Concentration Monitoring - Two divisional racks for analysis and measurement sample the oxygen/hydrogen concentration levels in each compartment of the containment. The range of measurement of hydrogen and oxygen contents is displayed in percent (by volume) for the inerted containment. Separate gas indicators for measurement of oxygen and hydrogen content are provided in the MCR for each CMS subsystem. Trip circuits for alarm initiation are set for high oxygen and hydrogen concentration levels and for abnormal sampling flow indication.

7.5.3 Process Radiation Monitoring System

The Process Radiation Monitoring System (PRMS) provides the instrumentation for radiological monitoring, sampling and analysis of the following:

- Turbine Building,
- TSC,
- Radwaste Building,
- Control Building,
- Reactor Building,
- Fuel Building, and
- Plant Stack.

The PRMS alerts operators to radiation levels in excess of preset limits and initiates automatically the required protection action to isolate, contain or redirect radioactivity releases from the environs. See Subsection 11.5.1.1.2 for process and effluent paths and/or areas with excessive radiation levels.

The system is configured as shown in Figure 11.5-1 and Table 11.5-3.

7.5.3.1 Design Bases

The design bases are provided in Section 11.5.

7.5.3.2 System Description

The system description is provided in Section 11.5.

7.5.3.3 Safety Evaluation

The safety-related PRMS design, including the sensors and the instrumentation channels, is environmentally and seismically qualified for continuous monitoring during reactor operation as well as abnormal and accident plant conditions. The system design conforms with the System Design Bases.

Table 7.1-1 identifies the PRMS and the associated regulatory requirements, guidelines and codes and standards applied, in accordance with the NUREG-0800. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.5.3.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The PRMS complies with these standards.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6, and RG 1.75. The PRMS safety-related subsystems are divisionalized and are designed with redundancy so failure of any instrument does not interfere with system operation. Electrical separation is maintained between the redundant divisions.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The PRMS demonstrates compliance by being able to provide automatic indication of bypassed and inoperable status.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The PRMS complies with this requirement.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The PRMS complies with this requirement.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the PRMS within the DCD documents conforms with this requirement.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.5.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 24, and 64:

- Conformance: The PRMS complies with these GDC.

7.5.3.3.3 Staff Requirements Memorandum

SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability

- Conformance: The PRMS AMS meets the requirements of SECY-93-087, Item II.T for redundancy, independence, and separation in that the "alarm system" is considered redundant as follows:
  - Alarm points are sent via dual networks to redundant message processors using dual power supplies. The processors are dedicated to alarm processing.
  - The alarms are displayed, on multiple independent VDUs (dual power supplies on each).
  - The alarms are driven by redundant data links to the AMS (dual power). There are redundant alarm processors.
  - There is one horn and one voice speaker. Test buttons are available to test the horn(s) and all the lights.
  - There are no alarms requiring manually controlled actions for systems to accomplish their safety-related functions.

7.5.3.3.4 Regulatory Guides

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

RG 1.53 - Application of the Single Failure Criterion to Nuclear Power Protection Systems

RG 1.75 - Physical Independence of Electrical Systems

RG 1.105 - Setpoints for Safety-Related Instrumentation

RG 1.118 - Periodic Testing of Electric Power and Protection Systems

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The PRMS conforms with all of the RGs listed above, with the assumption that the interpretations and clarifications identified in Subsection 7.1.6.4 apply.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the SSLC/ESF system, Subsection 7.1.6.4.

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The PRMS conforms with RG 1.180 as discussed in Subsection 7.1.6.4.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The PRMS conforms with RG 1.204 as discussed in Subsection 7.1.6.4.

7.5.3.3.5 Branch Technical Positions

BTP HICB-11 - Guidance on Application and Qualification of Isolation Devices

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints

BTP HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

BTP HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions

BTP HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems

BTP HICB-21 - Guidance on Digital Computer Real-Time Performance:

- Conformance: The PRMS complies with the above BTPs. BTP HICB-14, BTP HICB-17, BTP HICB-18, and BTP HICB-21 are addressed in conjunction with the SSLC/ESF in Subsections 7.3.5.3.5 and 7.1.6.5. BTP HICB-13 does not apply to the PRMS, since this system does not use RTD-type sensors.

7.5.3.3.6 Three Mile Island Action Plan Requirements:

In accordance with SRP 7.5 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) [I.D.3], 10 CFR 50.34(f)(2)(xvii) [II.F.1] and 10 CFR 50.34 (f)(2)(xix)[II.F.3] apply to the PRMS. The

PRMS complies with these requirements, as indicated above. However, TMI action plan requirements are generically addressed in Appendix 1A.

7.5.3.4 Testing and Inspection Requirements

The capability for testing and calibration is discussed in Subsections 11.5.6.1, 11.5.6.2, and 11.5.6.3 and complies with the requirements of IEEE Std. 603, Sections 5.7 and 6.5.

7.5.3.5 Instrumentation and Control Requirements

See Subsections 11.5.2.1, 11.5.2.2, 11.5.3.1 and 11.5.3.2.

7.5.4 Area Radiation Monitoring System

The primary function of the nonsafety-related ARMS is to continuously monitor the gamma radiation levels within the various areas of the plant and to provide an early warning that predetermined radiation levels are exceeded. The ARMS consists of area radiation detectors located at accessible areas of the plant and utilizes local and MCR alarms for immediate warning. The gross gamma radiation levels are monitored on a continuous basis, because changes are caused by operational transients or maintenance activities. Any high radiation levels are indicated by audible area alarms and MCR alarms.

A functional block diagram of the ARMS is as shown in Figure 7.5-3.

7.5.4.1 Design Bases

The ARM system design conforms with the System Design Bases.

7.5.4.2 System Description

A design description of this system, together with detector locations, channel ranges, and alarm requirements, is covered in Subsection 12.3.4.

7.5.4.3 Safety Evaluation

The ARMS design, including the sensors and the instrumentation channels, is engineered as a nonsafety-related system designed for continuous monitoring during reactor operation, as well as during abnormal and accident plant conditions. The system design conforms with the System Design Bases.

Table 7.1-1 identifies the ARMS and the associated regulatory requirements, guidelines and codes and standards applied, in accordance with the NUREG-0800. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.5.4.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The ARMS complies with these standards.

10 CFR 50.55a(h), Protection and Safety Systems Compliance with IEEE Std. 603:

- Conformance: Since ARMS is a nonsafety-related system, this regulation is not applicable.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The ARMS complies with this requirement.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The ARMS complies with this requirement.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this section.

7.5.4.3.2 General Design Criteria

GDC 2, 4, 13, 19, 24, and 64:

- Conformance: The ARMS complies with these GDC.

7.5.4.3.3 Regulatory Guides

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The ARMS conforms with RG 1.180 as discussed in Subsection 7.1.6.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The RMS conforms with RG 1.204 as discussed in Subsection 7.1.6.

7.5.4.3.4 Branch Technical Positions

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The DCD Tier 2 level of detail for the ARMS complies with the above BTP.

7.5.4.3.5 Three Mile Island Action Plan Requirements

In accordance with SRP 7.5 and with Table 7.1-1, 10 CFR 50.34(f)(2)(xvii) [II.F.1] and 10 CFR 50.34(f)(2)(xix) [II.F.3] apply to the ARMS. The ARMS complies with these requirements, as indicated above. TMI action plan requirements are addressed generically in Appendix 1A.

7.5.4.4 Testing and Inspection Requirements

Surveillance Testing and In-Service Inspection (ISI) activities for the ARMS follow.

All ARM channels are tested and calibrated per the plant operating and maintenance procedures. Each Signal Conditioning Unit (SCU) is equipped with an internal self-diagnostic feature to detect and locate instrument failures. The SCU is also equipped with internal software to facilitate electronic calibration. Each SCU is provided with a means for adjustment of electronic calibration and trip setting. These adjustments do not require equipment removal from its associated panel. The SCU is also provided with a means for generating internal signals that can be used both to check the calibration of the electronic circuits that process the Radiation Detector Assembly's signal and to verify trip setpoints.

The SCU is provided with a means for administrative control of all adjustments and setpoints.

7.5.4.5 Instrumentation and Control Requirements

Every ARM channel consists of a gamma sensitive detector and a digital area radiation processor. All channels are provided with local visual and audible alarms and local readouts. Where appropriate, additional readouts and alarms are provided by local auxiliary units.

7.5.5 Pool Monitoring Subsystems

General Functional Requirements Conformance

Instrumentation is provided for automatic suppression pool cooling initiation. Visual indication of pool temperature is continuously provided for operator awareness under all operating and accident conditions. The system is automatically initiated and continuously monitors pool temperatures during reactor operation as discussed in Subsection 7.2.3. Refer to Subsection 9.1.3 for additional information on the Fuel and Auxiliary Pools Cooling System (FAPCS).

Suppression Pool

The CMS is provided with temperature and level instruments for monitoring suppression pool water temperature and water level, respectively. The temperature instrument generates a high water temperature signal when the suppression pool water temperature exceeds a high temperature limit. The suppression pool cooling mode of FAPCS is automatically initiated by a high pool-temperature signal provided that one of the FAPCS Train A or Train B is in standby

mode. The water level instrument generates a low water level signal when the suppression pool level decreases to a low level setpoint. The signal trips the FAPCS pump when it operates with suction from the suppression pool.

These instruments provide functions necessary to maintain suppression water temperature and level required for safety-related ECCS functions. For this reason, they are classified as safety-related.

Gravity-Driven Cooling System Pools

The Gravity-Driven Cooling System (GDCS) pools are provided with instruments that monitor water level. Each instrument generates high or low water level signals when its water level reading increases above or decreases below setpoint. Each high and low-level signal initiates an alarm in the MCR. Additionally, a low-level trips the FAPCS system pump operating in the GDCS pool cooling mode. The high-level setpoint is established to avoid overflow of GDCS pool water. The low water level setpoint is established to prevent inadvertent draining of the pool water below the minimum safe level.

The instruments provide necessary information to the operator for maintaining GDCS water level required for the safety-related ECCS function. For this reason, they are classified as safety-related.

IC/PCC Expansion Pools

The Isolation Condenser / Passive Containment Cooling System (IC/PCCS) expansion pools are provided with instruments that monitor water level. Each instrument generates high or low water-level signals when its water level reading increases above or decreases below its setpoints. Each high or low level signal initiates an alarm in the MCR. Additionally, a low level signal trips the IC/PCCS pool cooling and cleanup system . The high water-level setpoint is established to avoid overflow of IC/PCCS expansion pool water. The low water-level setpoint is established to prevent inadvertent draining of the IC/PCCS expansion pool water below the minimum safe level.

The instruments provide necessary information to the operator for refilling the IC/PCCS pools following an accident. For this reason, each is classified as a safety-related component.

Spent Fuel Pool

The Spent Fuel pool is provided with instruments that monitor water level. Each instrument generates a high and low water level signal when its water level reading increases above or decreases below its setpoint. Anti-siphoning holes are provided in all submerged portions of FAPCS discharge line at the elevation of normal water level to prevent significant draining of the pool in the event of a pipe break. These level instruments are safety-related to ensure proper level is maintained.

The skimmer surge tanks are used for receiving overflow water from the spent fuel pool, and as a pump suction source during the spent fuel pool cooling mode of operation. These tanks are provided with instruments that monitor their water level. The instruments generate high, low, and low-low water level signals when the water level reading exceeds its setpoints. The high and

low level signals are used for the opening and closing of Condensate Storage and Transfer System valve for make up water to skimmer surge tanks. The high high and low low signals initiate high and low water level alarms in the MCR. Additionally, the low level signal is used for tripping the FAPCS pump operating in the spent fuel pool cooling mode. The high level setpoint is established to avoid overflow of skimmer surge tank water. The low water level setpoint is established to prevent inadvertent draining of the tank water below the minimum safe level.

The level instruments for the spent fuel pool are classified as safety-related components because they provide necessary information to the operator for performing the safety-related function of refilling the spent fuel pool following an accident.

7.5.5.1 System Design Bases

See Subsection 9.1.3.1.

7.5.5.2 System Description

See subsection 9.1.3.2.

7.5.5.3 Safety Evaluation

See Subsection 9.1.3.3.

7.5.5.4 Testing and Inspection Requirements

See Subsection 9.1.3.4.

7.5.5.5 Instrumentation and Control Requirements

See Subsection 9.1.3.5.

7.5.6 Wetwell-to-Drywell Vacuum Breaker Monitoring

The wetwell-to-drywell vacuum breakers are provided with four safety-related proximity sensors in four safety-related instrument divisions that monitor their closed position. See Subsection 6.2.1 for further discussion.

7.5.7 COL Information

None

7.5.8 References

None

Table 7.5-1

Design and Qualification for Instrumentation - (Deleted)

Table 7.5-2

PAM Variable List – (Deleted)

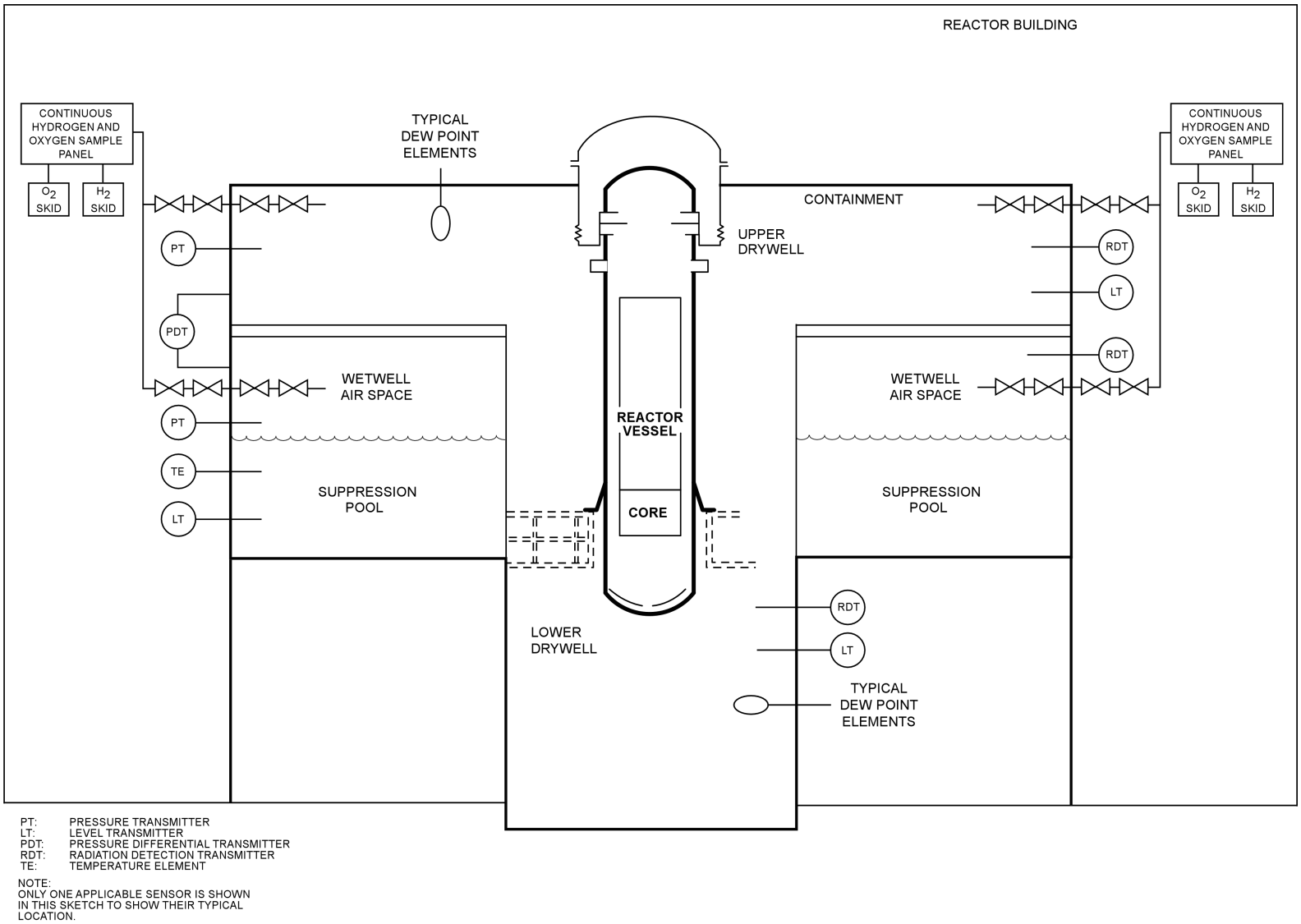
Table 7.5-3

Type A Variables – (Deleted)

Table 7.5-4

CMS Testing and Inspection Requirements

Specified Channel Calibration - Each oxygen and hydrogen gas sampling channel	[0%] gas concentration and nominal level from [2%] to [5%] from calibrated sources
Sample Gas Leakage Test - Sample lines and associated gas analyzer panel	Less than 0.01cc/sec at peak sample pressure



PT: PRESSURE TRANSMITTER
LT: LEVEL TRANSMITTER
PDT: PRESSURE DIFFERENTIAL TRANSMITTER
RDT: RADIATION DETECTION TRANSMITTER
TE: TEMPERATURE ELEMENT

NOTE:
ONLY ONE APPLICABLE SENSOR IS SHOWN IN THIS SKETCH TO SHOW THEIR TYPICAL LOCATION.

Figure 7.5-1. Containment Monitoring System Design

Figure 7.5-2. (Deleted)

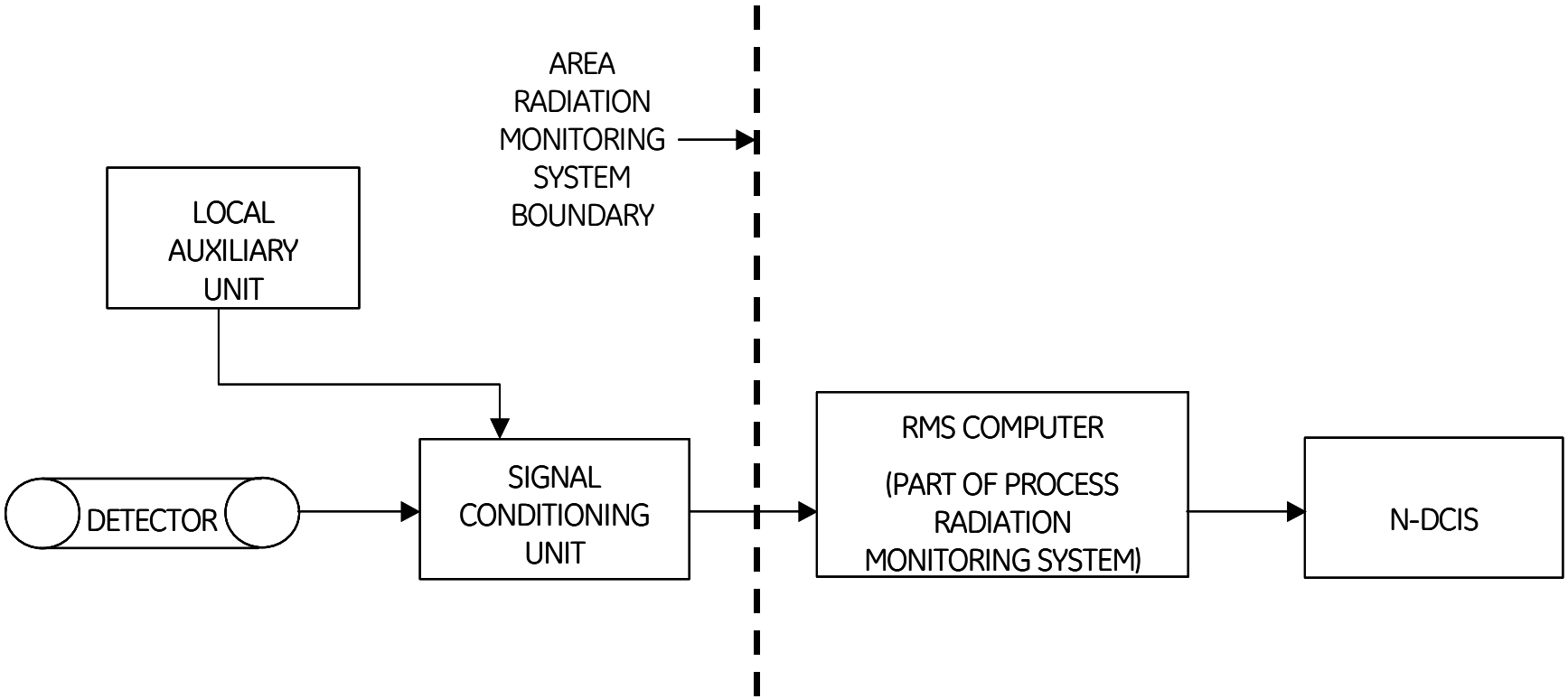


Figure 7.5-3. Area Radiation Monitoring System Functional Block Diagram

7.6 INTERLOCK SYSTEMS

In accordance with the Standard Review Plan (NUREG-0800), the systems addressed in this section are "those interlock systems important to safety which operate to reduce the probability of occurrence of specific events or to maintain safety systems in a state to assure their availability in an accident." This is further clarified to include two types of interlock systems: (1) High Pressure/Low Pressure (HP/LP) interlock systems to prevent over-pressurization of low-pressure systems (which are connected to high pressure systems), and (2) systems to isolate safety-related systems from nonsafety-related systems. Both types of systems are addressed in this section.

7.6.1 High Pressure/Low Pressure Interlock Systems

7.6.1.1 System Design Bases

The Fuel and Auxiliary Pools Cooling System (FAPCS) is a low pressure piping system. Its Low Pressure Coolant Injection (LPCI) line is connected to the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) system Loop B discharge line, which is connected to the Reactor Pressure Vessel (RPV) via the Feedwater Loop A discharge line.

During reactor power operation, the high pressure in the RWCU/SDC system piping exceeds the design pressure of the low pressure FAPCS piping. The following subsections describe the interlock system provided to prevent over-pressurization of the FAPCS piping. The FAPCS design is discussed in Subsection 9.1.3. The reactor pressure instruments of the Nuclear Boiler System (NBS) are discussed in Subsection 7.7.1.

The only other HP/LP interface exists in the Gravity-Driven Cooling System (GDCS). Because the GDCS piping down stream of squib valves connected to the RPV has a design pressure equivalent to the reactor operating pressure, and the low pressure GDCS piping upstream of squib valves end is open to the GDCS pools, there is no need for overpressure protection of the low pressure portion. A high pressure interlock is provided to prevent inadvertent manual initiation of the GDCS. The GDCS design basis is discussed in Subsection 7.3.1.2.1. The subsequent subsections of 7.6.1 describe the LPCI line HP/LP interlock system.

7.6.1.2 System Description

7.6.1.2.1 Function Identification

Isolation valves consist of two parallel air-operated, testable check valves and two-parallel, air-operated gate valves to protect the FAPCS low pressure piping from over-pressurization during reactor power operation. These valves are normally closed. Parallel valves are provided for redundancy and fire zone separation. Both sets of parallel valves have identical interlock logic for operation except that the power supplies to nonsafety-related solenoids are provided from different sources, Plant Investment Protection (PIP) PIP A and PIP B buses, for redundancy. The HP/LP interlock system prevents the isolation valves from opening, and closes them if opened, whenever there is a high pressure signal from the reactor vessel pressure transmitters of the NBS.

The high pressure signal also prevents testing of the air-operated testable check valves and closes them if they are open for testing. It also prevents the operation of the LPCI mode of FAPCS (IEEE Std. 603, Section 4.10). The FAPCS modes are described in Subsection 9.1.3.2.

7.6.1.2.2 Power Sources

The power supplies for the safety-related reactor pressure instruments and the safety-related valve control logic are provided from divisional safety-related power supplies, backed up by safety-related batteries (IEEE Std. 603, Sections 5.12 and 8.1). Nonsafety-related redundant logic is powered by a nonsafety-related power supply, backed up by nonsafety-related batteries. Redundant power supplies to nonsafety-related solenoids are provided from different sources (PIP A and PIP B buses). Refer to Chapter 8 Subsection 8.3.2 for DC power supplies and Subsection 8.3.1 for AC power supply.

7.6.1.2.3 Equipment Design

Divisionally separate safety-related reactor pressure instruments located on the RPV sensing lines provide a high pressure signal to the FAPCS HP/LP interlock system when the reactor pressure exceeds the setpoint based on the design pressure of the low pressure FAPCS piping. Upon receipt of a high reactor pressure signal, the HP/LP interlock system sends a signal to close the isolation valves and testable check valves and prevents them from opening or being tested.

7.6.1.2.4 Logic Description

The HP/LP interlock system logic is processed in the divisionally separate Safety-Related Distributed Control and Information System (Q-DCIS) and Nonsafety-Related Distributed Control and Information System (N-DCIS). See Subsections 7.1.3 and 7.1.5 for description of the Q-DCIS and N-DCIS, respectively. The divisional high reactor pressure signals from the NBS are sent to determine whether a high pressure condition exists in the RWCU/SDC discharge line to the RPV feedwater inlet line. If a high pressure condition exists, the safety-related and nonsafety-related interlock system sends a valve close signal to the divisionally separate safety-related solenoids and redundant nonsafety-related solenoids to close the isolation valves. This signal prevents testing of the check valves and also prevents the LPCI mode of operation of the FAPCS. (IEEE Std. 603, Sections 5.1, 6.1, 6.2, 6.3, and 7.1.)

7.6.1.2.5 Logic Sequencing

Deleted (provided above)

7.6.1.2.6 Bypasses and Interlocks

The HP/LP interlock system design has no bypass.

7.6.1.2.7 Redundancy and Diversity

The LPCI line uses redundant isolation valves (a parallel set of air operated valves in series with a parallel set of testable check valves) in series for over-pressure protection, when the reactor

pressure is above the FAPCS design pressure. Diversity is provided by a check valve equipped with a pneumatic-assist actuator having a fail-closed feature and an air-operated fail as-is normally closed valve. A relief valve down stream of the isolation valve serves to detect leakage through the check valves and the isolation valves.

7.6.1.2.8 Actuated Devices

The LPCI line air-operated, parallel isolation valves and air-operated, parallel check valves are the actuation devices affected by the HP/LP interlock system. Divisionally separated solenoids are used for controlling air to each of the actuators. Nonsafety-related solenoids powered by separate power buses are used for controlling air to each of the actuators. Valves are designed as fail as-is. Backup air supply is provided by an air bottle for each valve in the event that the normal air supply is not available to open or close the valve (IEEE Std. 603, Section 8.2).

7.6.1.2.9 Separation

Divisionally separate safety-related reactor pressure signals are from divisionally separate instruments as discussed in Subsection 7.7.1. Safety-related logic is implemented in the divisionally separate Q-DCIS and nonsafety-related logic is implemented in the N-DCIS. See Subsections 7.1.3 and Subsection 7.1.5 for details of the Q-DCIS and N-DCIS respectively. Solenoids provided for actuator action are safety-related for safety-related logic and are nonsafety-related for nonsafety-related logic and are physically separate (IEEE Std. 603, Section 5.6).

7.6.1.2.10 Testability

Testing of the reactor pressure instruments is discussed in Subsection 7.7.1.

Due to the high pressure interlock , the LPCI line isolation valves and check valves are stroke-tested only during low reactor pressure conditions. These valves are not subjected to the 10 CFR 50 Appendix J leak rate test, because they are neither containment isolation valves nor part of the reactor coolant pressure boundary. However, they are leak rate tested per American Society of Mechanical Engineers (ASME) Code Section XI. (IEEE Std. 603, Sections 4.12, 5.7, and 6.5).

7.6.1.2.11 Environmental Considerations

The instrumentation and controls (I&C) for the HP/LP interlock system classified as safety-related equipment are qualified according to the environmental conditions at the locations of the devices. (IEEE Std. 603, Sections 4.8 and 5.4.)

7.6.1.2.12 Operational Consideration

The HP/LP interlock system prevents manual initiation of the LPCI mode of FAPCS until the RPV has been depressurized below the reactor pressure instrument setpoint.

7.6.1.2.13 Reactor Operator Information

The status of each valve providing the HP/LP boundary is indicated in the Main Control Room (MCR). The state of the sensors also is indicated in the MCR.

7.6.1.2.14 Setpoints

The setpoint is based on the design pressure of the low pressure FAPCS piping.

7.6.1.3 Safety Evaluation

The design does not have a HP/LP interface involving a safety-related system. There is a nonsafety-related HP/LP interface involving the low pressure FAPCS LPCI line, which interfaces with the high pressure condition in the RWCU/SDC system piping. The RWCU/SDC system piping interfaces with the feedwater line, which maintains the reactor coolant pressure boundary.

The FAPCS HP/LP interlock system prevents opening of the isolation valves on the LPCI discharge line. The interlock system prohibits the LPCI line isolation valves from being opened whenever the reactor pressure is greater than the reactor pressure permissive setpoint for the interlock, thereby protecting the low pressure FAPCS piping from over-pressurization during reactor power operation. The interlock system is designed to permit LPCI mode initiation when the reactor pressure is below the reactor pressure permissive setpoint allowing the operator to manually open either isolation valve. The interlock system operates automatically, and its status is provided to the reactor operator in the MCR (IEEE Std. 603, Sections 4.1, 4.2, 4.3, 4.4 and 4.5).

Table 7.1-1 identifies the HP/LP interlock systems and the associated codes and standards applied, in accordance with NUREG-0800. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.6.1.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety

- Conformance: The HP/LP interlock system complies with these requirements.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603

- Conformance: Separation and isolation, both mechanically and electrically, are preserved in accordance with IEEE 603 and RG 1.75. Electrical separation is maintained between the redundant divisions.

10 CFR 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication

- Conformance: The HP/LP interlock system does not have a bypass feature.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), Inspections, Tests, Analyses and Acceptance Criteria (ITAAC) in Design Certification Applications

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements

- Conformance: There are no interface requirements for this section.

10 CFR 52.47(a)(2), Level of Detail

- Conformance: The level of detail provided for the interlock system within the DCD conforms to this criterion.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.6.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 24 and 25:

- Conformance: The HP/LP interlock system does not involve reactivity control, hence GDC 25 is not applicable. The interlock system is in compliance with the remaining GDC listed above.

7.6.1.3.3 Regulatory Guides

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The HP/LP interlock system does not have a bypass feature.

RG 1.53, Application of the Single Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The HP/LP interlock system complies with these requirements.

RG 1.75, Physical Independence of Electrical Systems:

- Conformance: The HP/LP interlock system design conforms with RG 1.75. See chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for a discussion of how the design meets the requirement of RG 1.75.

RG 1.105, Setpoints for safety-related Instrumentation:

- Conformance: The HP/LP interlock system complies with these requirements.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: The LPCI line isolation valves and check valves are stroke-tested only during low reactor pressure conditions due to the interlock.

RG 1.151 – Instrument Sensing Lines:

- Conformance: The HP/LP interlock system complies with these requirements.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The HP/LP interlock system conforms with the RG listed above.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 1.173, 1.180 and 1.204 are addressed in conjunction with the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) in Subsections 7.3.5.3.4 and 7.1.6.4.

7.6.1.3.4 Branch Technical Positions

BTP HICB-1 - Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System (IEEE Std. 603).

BTP HICB-11 - Guidance on Application and Qualification of Isolation Devices.

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints.

BTP HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems.

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52.

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions.

BTP HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems.

BTP HICB-21 - Guidance on Digital Computer Real-Time Performance:

- Conformance: The interlock system complies with the above BTPs. Discussion of BTPs HICB-14, 17, 18, and 21 is addressed in conjunction with the SSLC/ESF, in Subsections 7.3.5.3.5 and 7.1.6.5.

7.6.1.3.5 Three Mile Island Action Plan Requirements

In accordance with the NUREG-0800 for 7.6 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) (I.D.3) applies to the HP/LP interlock system and is addressed above. Three Mile Island (TMI) action plan requirements are generically addressed in Appendix 1A.

7.6.1.4 Testing and Inspection Requirements

HP/LP interlock system instruments and control functions are calibrated and tested during the preoperational testing program to confirm that the instrumentation is installed correctly and that the HP/LP interlock system functions as designed (IEEE Std. 603, Section 6.5).

Testing and inspection of the NBS system pressure instrument channels are described in Subsection 7.7.1.4.

The LPCI line isolation valves and check valves are stroke-tested during low reactor pressure conditions because of the interlock.

7.6.1.5 Instrumentation and Control Requirements

The following information is available to the reactor operator in reference to the instrumentation and interlock system described in this subsection:

- The reactor pressure is indicated in the Main Control Room (MCR) and at four local racks in the Reactor Building outside the containment.
- HP/LP interlock system status is indicated in the MCR and is alarmed when any LPCI valve is open and the interlock system is active (IEEE Std. 603, Section 5.8).
- The open and closed position of the isolation valves and check valves are indicated in the MCR.

7.6.2 Other Interlock Systems

7.6.2.1 Isolation – Between the Diverse Protection System and Safety-Related Systems

The separation and isolation of the nonsafety-related Diverse Protection System (DPS) operation and the safety-related Reactor Protection System (RPS) and Safety System Logic and Control Engineered Safety Feature (SSLC/ESF) systems are addressed in Subsection 7.8.2.3. The separation and isolation between nonsafety-related systems and safety-related systems complies with IEEE Stds. 603 and 384; therefore, no interlock system exists between nonsafety-related and safety-related systems.

7.6.3 COL Information

None

7.6.4 References

None

7.7 CONTROL SYSTEMS

This section describes the Instrumentation and Control (I&C) systems for normal plant operation that do not perform plant safety-related functions. However, these systems do control plant processes that have a significant impact on plant safety. These systems can affect the performance of safety-related functions either through normal operation or through inadvertent operation. The control systems described in this section include:

- The Nuclear Boiler System (NBS) – nonsafety-related subsystems,
- Rod Control and Information System (RC&IS),
- Feedwater Control System (FWCS),
- Plant Automation System (PAS),
- Steam Bypass and Pressure Control (SB&PC) System,
- Neutron Monitoring System (NMS) - nonsafety-related subsystems, and
- Containment Inerting System (CIS).

The safety-related monitoring and control portions of the NBS and NMS are part of a group of systems that are collectively referred to as the Safety-Related Distributed Control and Information System (Q-DCIS). A functional block diagram of the Q-DCIS is included as part of Figure 7.1-1, and a functional network diagram appears as Figure 7.1-2. These diagrams indicate the relationships of the NBS and NMS with their safety-related peers and with nonsafety-related plant data systems. Section 7.1 contains a description of these relationships.

The nonsafety-related monitoring and control for RC&IS, FWCS, PAS, SB&PC, and CIS system are part of a group of systems that are collectively referred to as the Nonsafety-Related Distributed Control and Information System (N-DCIS). A functional block diagram of the N-DCIS is included as part of Figure 7.1-1, and a functional network diagram appears as Figure 7.1-2. These diagrams indicate the relationships of RC&IS, FWCS, PAS, SB&PC, and CIS with their nonsafety-related peers and with safety-related plant data systems that are collectively referred to as the Q-DCIS. Section 7.1 contains a description of these relationships.

7.7.1 Nuclear Boiler System

The NBS instrumentation provides monitoring and control input for operational variables during normal plant operating modes and during the plant response to accidents. The NBS sensors used for safety-related system actuation and control functions are addressed in other subsections within this chapter. This subsection describes only the safety-related NBS instrumentation used for indication and only those instruments used for actuation and control of nonsafety-related systems.

7.7.1.1 System Design Bases

7.7.1.1.1 Safety Design Bases

The NBS I&C meets the following safety-related requirements (IEEE Std. 603, Sections 4.1, 4.2, 4.8, and 4.10):

- Provide reactor pressure vessel (RPV) water level and dome pressure measurements over the ranges and to the accuracies necessary for adequate operator monitoring of RPV water level during normal, transient, and accident conditions.
- Instrumentation provided for RPV water level and dome pressure measurement is qualified for the design basis loadings of the Safe Shutdown Earthquake (SSE), loadings associated with design basis accidents, and the environmental conditions associated with design basis accidents.
- Provide redundancy so that a single failure does not result in the loss of level and pressure indication.

7.7.1.1.2 Power Generation (Non-safety) Design Bases

The NBS instrumentation meets power generation requirements by providing indication of the following parameters in support of normal plant operations:

- Reactor coolant and RPV temperatures;
- RPV water level:
  - Shutdown range,
  - Narrow range,
  - Wide range, and
  - Fuel zone range.
- RPV pressure;
- Safety Relief valve discharge line temperature; and
- Main steam flow.

To the extent practical, the NBS instrumentation design provides for periodic calibration and testing of its instrumentation during plant operation.

7.7.1.2 System Description

7.7.1.2.1 Summary Description

The NBS instruments and systems are used to provide the operator with information during normal, transient, accident, and post-accident conditions. The instrumentation discussed in this subsection is also discussed in Section 5.1, and is shown in Figure 7.3-1a and 7.3-1b, NBS Automatic Depressurization System (ADS) Initiation Logic.

Safety-related instrumentation is powered from safety-related 120 Volts Alternating Current (VAC) Uninterruptible Power Supply (UPS). Nonsafety-related instruments are powered from the nonsafety-related instrument power supply buses.

For instruments that are located below the process tap, including the RPV water level measurements, the sensing line slopes downward from the process tap to the instrument to preclude air traps. Where it is impractical to locate the instruments below the process connection, the sensing lines descend below the process connection before sloping upward to a high point vent located at an accessible location with a fill connection. This permits filling and venting of noncondensible gases from the sensing line during calibration procedures.

Level and pressure sensing lines, up to the outboard excess flow check valve, are connected to the Reactor Coolant Pressure Boundary (RCPB) and are classified as Quality Group A, ASME Section III, safety-related, and Seismic Category 1. The typical arrangement for these sensing lines is a restricting orifice located inside the containment and a manual isolation valve located outside the containment which is followed by an excess flow check valve.

7.7.1.2.2 Detailed System Description

Reactor Coolant and Reactor Pressure System Vessel Temperature Monitoring

The reactor coolant temperatures are measured at the mid-vessel inlet to the Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC) system and at the bottom head drain. Coolant temperature can also be determined in the steam-filled parts of the RPV and steam-water mixture by measuring the reactor pressure. In the saturated system, reactor pressure connotes saturation temperature. Coolant temperatures (core inlet temperature) can normally be measured by the redundant core inlet temperature sensors located in each Local Power Range Monitor (LPRM) assembly below the core plate elevation.

The RPV outside surface temperature is measured at the head flange and at the bottom head locations. Temperatures needed for operation and for compliance with the Technical Specification operating limits are obtained from these measurements.

Reactor Pressure Vessel Water Level

Figure 7.7-1 shows the water level range and the vessel penetrations for each water level range. The instruments are differential pressure devices calibrated for the specific vessel pressure and liquid temperature conditions. The reactor water level measurement is temperature compensated through the thermocouples installed on the sensing line. As described in Subsection 4.6.1.2.4, the Control Rod Drive Hydraulic Subsystem (CRDHS) provides a purge flow which keeps the

RPV water level reference leg instrument lines full. These lines are filled to address the effects of noncondensible gases in the instrument lines and to prevent erroneous reference information after a rapid RPV depressurization event. The reactor water level instrumentation is referenced to level zero, which is at the Top of Active Fuel (TAF).

Reactor water level instrumentation that initiates safety-related systems and engineered safety features systems is discussed in Subsections 7.2.1 and 7.3.1. Reactor water level instrumentation that is used as part of the FWCS is discussed in Subsection 7.7.3. Reactor water level instrumentation used for Diverse Protection System (DPS) functions is discussed in Subsection 7.8.1.

The Shutdown Range Water Level range is used to monitor the RPV water level during shutdown conditions when the head is removed and the reactor system may be flooded for refueling or maintenance. The water level measurement design method is the condensing chamber reference leg type and uses differential pressure devices as its primary elements. The vessel temperature and pressure conditions that are used for the calibration are given in Section 5.1. The two vessel instrument nozzle elevations used for this water level measurement are located at the top of the RPV head and just below the bottom of the dryer skirt.

The Narrow Range Water Level range uses the RPV taps near the top of the steam outlet nozzle and the taps near the bottom of the dryer skirt. The instruments are calibrated to be accurate during normal reactor operating conditions. The method of water level measurement is the condensing chamber reference leg type and uses differential pressure devices as its primary elements. The FWCS uses this range for its water level control and indication inputs. Refer to Subsection 7.7.3 for more information on the FWCS.

The Wide Range Water Level range uses the RPV taps above the TAF. The upper taps are also used for the Narrow Range Water Level. The instruments are calibrated to be accurate at normal power operating conditions. The water level measurement method is the condensing chamber reference leg type and uses differential pressure devices as its primary elements. Information from the RPV Wide Range Water Level instrumentation is used for safety-related and nonsafety-related applications, for DPS, and is provided for the range of normal, transient, and accident conditions. Separate sensors and indicators are provided for Wide Range Water Level indication.

The Fuel Zone Range Water Level range uses the RPV taps near the top of the steam outlet nozzle and the taps below the bottom of the active fuel. The instruments are calibrated to be accurate at zero Pa gauge (0 psig) and saturated conditions. The water level measurement method is the condensing chamber reference type and uses differential pressure devices as its primary elements. The RPV Fuel Zone Water Level instrumentation is safety-related and is provided for post-accident monitoring situations in which the water level may be substantially below the normal range. Separate sensors and indicators are provided for Wide Range Water Level indication.

Reactor Pressure Vessel Pressure

Pressure transmitters detect RPV pressure from the instrument lines used for measuring RPV water level and provide indication in the Main Control Room (MCR).

Pressure transmitters and trip actuators for initiating scram, and pressure transmitters and trip actuators for bypassing the main steam line isolation valve (MSIV) closure scram are discussed in Subsection 7.2.1. High pressure and low pressure (HP/LP) interlocks are discussed in Subsection 7.6.1.1.

Pressure transmitters that are used for pressure recording are discussed in Subsection 7.2.1.2.4.2.

Safety Relief Valve Leak Detection

Thermocouples are located in the discharge pipes of ten Safety Relief Valves (SRVs) (Reference Section 5.2.5). The temperature signals are recorded, and temperatures indicative of a leaking SRV are alarmed in the MCR.

Main Steam Flow Rate

Differential pressure transmitters are used to infer steam flow rate. Pressure taps from the throat of the RPV steam outlet nozzles, in conjunction with the RPV dome pressure taps, measure differential pressure. Differential pressure is proportional to the main steam flow rate. Safety-related transmitters input to the Leak Detection and Isolation System (LD&IS) logic. Nonsafety-related transmitters are used for feedwater control.

7.7.1.3 Safety Evaluation

Table 7.1-1 identifies the NBS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

The safety-related reactor water level and dome pressure instruments are designed to withstand the loads and environmental conditions under which they must function. Sufficient separate sensors and indicators are provided so that a single failure cannot result in the loss of level indication. The combined range of the wide range and fuel zone water level instrumentation ensures that adequate level information is available over the entirety of postulated design basis accident conditions (IEEE Std. 603, Sections 4.8 and 5.1).

The nonsafety-related instruments discussed in this subsection are designed to operate under normal and peak operating conditions of system pressure and at ambient pressures and temperatures. Any mechanical interface between nonsafety-related instruments and safety-related instrument piping or the RCPB is classified as safety-related to avoid compromise of the safety-related sensing capability and/or the RCPB. If a line break occurs in a nonsafety-related portion of a sensing line, the excess flow check valve closes to stop the flow of reactor coolant. If there is a single failure of the excess flow check valve, a restriction orifice limits the flow of coolant to within acceptable bounds.

7.7.1.3.1 Code of Federal Regulations

10 CFR 50.55a(1), Quality Standards Important to Safety:

- Conformance: The NBS conforms with these criteria, as shown by the following commitments to applicable Regulatory Guides (RG) and standards.

10 CFR 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (IEEE Std. 603):

- Conformance: Safety-related systems are designed in conformance with RG 1.153 and IEEE Std. 603, as discussed in Subsections 7.1.6.4, and 7.2.1.3.4.

10 CFR 50.34(f)(2)(v) [I.D.3], Bypass and Inoperable Status Indication:

- The NBS design of bypass and inoperable status indication conforms with this requirement.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- ITAAC are provided for the I&C systems and equipment in DCD.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- There are no interface requirements for this section.

10 CFR 52.47(a)(2), Level of Detail:

- The level of detail provided for the NBS within the DCD conforms with this regulation.

10 CFR 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions:

- The I&C design does not use innovative means for accomplishing safety functions.

7.7.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19 and 24:

- Conformance: The NBS complies with these GDC.

7.7.1.3.3 Staff Requirements Memorandum

Staff Requirements Memorandum (SRM) to SECY 93-087 II.Q (Defense Against Common-Mode Failures in Digital Instrument and Control Systems):

- Conformance: In addition to the design features already incorporated in the design on defense-in-depth and against common mode failures that address this SRM, the NBS ADS function and other Engineered Safety Features (ESF) designs conform with Item II.Q of SECY-93-087 (NRC Branch Technical Position [BTP] HICB-19) through the implementation of an additional Diverse Instrumentation and Control System described in Section 7.8.

7.7.1.3.4 Regulatory Guides

RG 1.75 - Physical Independence of Electric Systems:

- Conformance: The NBS system design conforms with RG 1.75. See chapter 8.0 Subsections 8.3.1.3 and 8.3.1.4 for a discussion of how the design meets the requirements of RG 1.75.

RG 1.105 - Instrument Setpoints for safety-related Systems:

- Conformance: The NBS complies with RG 1.105 as discussed in Subsection 7.1.6.4.

RGs 1.151 - Instrument Sensing Lines:

- Conformance: The instrument sensing lines for the NBS instrumentation are in conformance with the guidelines of RG 1.151 and ISA-67.02. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02 and RG 1.151 are met as applicable for each installation.

RG 1.153 - Criteria for Safety Systems:

- Conformance: Consistent with the discussion of other RGs and the GDC, the NBS complies with this RG.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172, and 1.173 are discussed in Subsection 7.1.6.4.

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The NBS system conforms with RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.

7.7.1.3.5 Branch Technical Positions

BTP HICB-11 - The approach to compliance with RG 1.75 and RG 1.153 is discussed above.

BTP HICB-12 - The NBS design complies with BTP HICB-12.

BTP HICB-16 - The level of detail provided for this system complies with BTP HICB-16.

BTP HICB-14, 17, 18, 19, and 21 are discussed in association with the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) in Subsection 7.3.5.3 and in Subsection 7.1.6.5.

7.7.1.4 Testing and Inspection Requirements

Calibration and testing of the various instruments are performed during preoperational testing to confirm the instrumentation is installed correctly and performs as intended.

Pressure, differential pressure, water level, and flow instruments are located outside the drywell so that calibration and test signals can be applied during reactor operation. Temperature elements located inside the drywell can be tested and calibrated from junction boxes located outside the drywell (IEEE Std. 603, Section 5.7).

7.7.1.5 Instrumentation and Control Requirements

The following information is available to the reactor operator from the instrumentation discussed in this subsection (IEEE Std. 603, Section 5.8):

- RPV water level is indicated in the MCR on displays associated with the different water level ranges;
- The reactor pressure is indicated in the MCR and at four local instrument racks in the Reactor Building;
- The discharge line temperatures of the SRVs are viewed on safety-related VDUs in the MCR. Any temperature exceeding the trip setting is alarmed to indicate leakage of a SRV seat;
- RPV temperature is indicated and recorded in the MCR, and low temperature is alarmed in the MCR; and
- Main steam flow is indicated in the MCR.

7.7.2 Rod Control and Information System

7.7.2.1 System Design Bases

7.7.2.1.1 Safety Design Basis

The RC&IS has no functional safety-related design basis and is designed so that it does not adversely affect functional capabilities of safety-related systems.

7.7.2.1.2 Power Generation (Non-safety) Design Bases

The main objective of the RC&IS is to control the Fine Motion Control Rod Drive (FMCRD) motors of the Control Rod Drive (CRD) (explained in Subsections 4.6.1 and 4.6.2) to permit changes in core reactivity so that reactor power level and power distribution can be controlled. By controlling the FMCRD motors and the CRD brakes, the RC&IS acquires status and control rod position information from the CRD FMCRD instrumentation. It sends purge water valve control signals to and acquires status signals from the Hydraulic Control Units (HCUs) of the CRD. The RC&IS also sends and receives status and control signals to and from other plant systems and RC&IS modules. The RC&IS performs the following functions:

- Controls changes to the core reactivity, and thereby reactor power, by moving neutron absorbing control rods within the reactor core as initiated by the following:
  - The plant operator, when the RC&IS is placed in a manual or semiautomatic mode of operation.

  - The automatic rod movement mode of the PAS, when the RC&IS is placed in an automatic mode of operation.

- Displays summary information to the plant operator about positions of the control rods in the core and the status of the FMCRDs and RC&IS. This summary information is provided by a RC&IS Dedicated Operator Interface (DOI) in the MCR. There are dual redundant measurements of the absolute rod position during normal FMCRD conditions. If one position detector fails for an individual FMCRD, the failed position detector can be bypassed, and the unit can continue to operate without power restrictions.

- Provides RC&IS and FMCRD status data and control rod position data to other plant systems that require this data, such as the N-DCIS.

- Provides automatic, electric motor run-in of all operable control rods following detection of activation of the hydraulic insertion of the control rods, by a reactor scram. This is called the scram-follow function.

- Automatically enforces rod movement blocks to prevent potentially undesirable rod movements. These blocks do not affect a hydraulic scram insertion function, the scram-follow function, the Alternate Rod Insertion (ARI) function, or the Selected Control Rod Run-in (SCRRI) function.

- Manually and automatically inserts all control rods by an alternate and diverse method called the ARI motor run-in function. The associated ARI activation signals, which are activated if the automatic or manual ARI function is activated by the N-DCIS scope logic, are provided to the RC&IS from the N-DCIS. The RC&IS logic is designed so that a single failure in the single-channel FMCRD control logic and equipment associated with one FMCRD, cannot result in insertion failure of that rod when the ARI function is activated.

- Inserts selected control rods depending on the circumstances. Selected control rods are inserted to either mitigate a loss of feedwater heating event or provide needed power reduction after the occurrence of a load rejection event or a turbine trip event that does not result in a reactor scram. This SCRRI function is automatically activated based upon SCRRI command signals from the N-DCIS. Manual initiation capability is also available based on simultaneous actuation of two manual SCRRI pushbuttons located on the main control console in the MCR. The RC&IS also sends a SCRRI signal to the DPS to initiate a Select Rod Insertion (SRI).

- Ensures that the pattern of control rods in the reactor is consistent with specific control rod pattern restrictions. This function is performed by the Rod Worth Minimizer (RWM) subsystem of the RC&IS and is only effective when reactor power is below the Low Power Setpoint (LPSP).

- Enforces fuel operating thermal limits Minimum Critical Power Ratio (MCPR) and Maximum Linear Heat Generation Rate (MLHGR) when reactor power is above the LPSP. This function is performed by the Automated Thermal Limit Monitor (ATLM) subsystem of the RC&IS.

- Provides for FMCRD-related surveillance tests, including periodic individual HCU scram performance testing.
- Through the capabilities of the gang rod selection and verification logic of the Rod Action and Position Information (RAPI) subsystem, enforces adherence to a predetermined rod pull/insert sequence, the Reference Rod Pull Sequence (RRPS), during automatic and semi-automatic rod movements.

7.7.2.2 System Description

A simplified, typical RC&IS block diagram is shown in Figure 7.7-2 that depicts the major components of the RC&IS and their interconnections and interfaces with other plant systems.

7.7.2.2.1 System Configuration

The RC&IS uses a dual redundant architecture of two independent channels for normal monitoring of control rod positions and executing normal control rod movement commands. Under normal conditions, each channel receives separate input signals, and both channels perform the same functions. The outputs of the two channels are continuously compared. For normal functions of enforcing and monitoring control rod positions and emergency rod insertion, the outputs of the two channels must agree. Any sustained disagreement between the two channels results in a rod block. However, when the conditions for generating a rod block signal in a single channel are satisfied, that channel alone (independent of the other channel) issues a rod block signal.

For the FMCRD emergency insertion functions (Scram-Follow, ARI, SCRRI), 3-out-of-3 logic is used in the Induction Motor Controller (IMC) logic with the additional input signal coming from the associated emergency rod insertion panels. An automatic single channel bypass feature is activated when an emergency insertion function is activated. It ensures high availability for the emergency insertion functions when a single channel failure condition exists.

Failure or malfunction of the RC&IS has no effect on the hydraulic scram function of the CRD. The circuitry for normal insertion and withdrawal of control rods in the RC&IS is completely independent of the Reactor Protection System (RPS) circuitry controlling the scram valves. This separation of the RPS scram and the RC&IS normal rod control functions prevents any failure in the RC&IS circuitry from affecting the scram circuitry.

The RC&IS consists of multiple types of cabinets, or panels, that contain special electronic/electrical equipment modules for performing the RC&IS logic in the Reactor Building (RB) and Control Building (CB). It also includes a DOI on the main control panel in the MCR. The RC&IS DOI provides summary information to the plant operator with respect to control rod positions, FMCRD, RC&IS status, and HCU status. The RC&IS also provides controls for performing normal rod movement functions, bypassing major RC&IS subsystems, performing CRD surveillance tests (except the FMCRD holding brake testing performed during a refueling outage), resetting RC&IS trips and most abnormal status conditions. A few abnormal status conditions require reset actions at local control panel equipment. There are nine types of electronic/electrical cabinets/panels that perform the logic functions of the RC&IS:

Rods Action Control Subsystem Cabinets

There are two types of cabinets in the back-panel area referred to as the Rod Action Control System (RACS). The RACS consists of RAPI panels and an ATLM/RWM panel, which provides for a dual redundant architecture. The RAPI panels consist of a RAPI-A panel and a RAPI-B panel. The channel A logic is in the RAPI-A panel, and the channel B logic is in the RAPI-B panel. In addition, the RAPI-A panel includes the RAPI DOI that displays the same information that is available on the RC&IS DOI in the MCR. The RAPI DOI also serves as a backup for the RC&IS DOI control capabilities, should the RC&IS DOI become unavailable. A hard wired switch located in the RAPI-A panel changes the selection of DOI control operation capability between the RC&IS DOI and the RAPI DOI. In other words, only one of these DOIs can be selected for control capability at any given time. Normally, the RC&IS DOI rather than the RAPI DOI is selected for control functions.

The two ATLM/RWM panels each contain channel logic for the ATLM, the RWM and the RAPI Signal Interface Unit (SIU).

Remote Communication Cabinets

The Remote Communication Cabinets (RCCs) are located in sets with each set containing a dual channel File Control Module (FCM). The FCMs interface with the Rod Server Modules (RSMs) that are contained in the same set of cabinets, and interface with the RAPI subsystems in the MCR, through the RC&IS multiplexing network. Each RSM comprises logic for two Rod Server Processing Channels (RSPCs A and B) so that there is a dual redundant logic design for each RSM. There are also associated Resolver-to-Digital Converters (RDCs A and B) that convert the Resolver A and Resolver B analog signals of the CRD system into two independent digital representations of the absolute position of the corresponding FMCRD.

The logic for both RSPCs receives the digital representations from both RDCs for use in the RSPC control and monitoring logic. The logic for each channel of the RSPC can either be located in the associated FCM channel equipment or located in a separate, replaceable RSPC module located in the RCC. Figure 7.7-2 shows a typical representation with the logic of each RSPC channel implemented in a separate RSPC module. However, regardless of the final detailed RCC hardware configuration for RSPC logic implementation, channel A RSPC logic is implemented in equipment separate from the equipment in which the channel B RSPC logic is implemented, to maintain tolerance for single channel failures.

Induction Motor Controller Cabinets

The Induction Motor Controller Cabinets (IMCCs) consist of motor control equipment required for turning on and off the Alternating Current (AC) power required for energization of the FMCRD 3-Phase motor and its directly associated Motor Built-in Brake (MBB) to perform FMCRD movements. The control capability includes AC phase swapping, of the 3-phase AC power supplied to each motor, so that both insertion and withdrawal movements of each FMCRD can be accomplished. The MBB accurately positions each FMCRD. The de-energization of this brake, promptly after AC power is turned off by the motor control, prevents excessive movement after the desired stopping position has been reached. Each motor controller includes logic to process rod movement commands received from the logic of the associated

RSPCs in a RCC. Each motor control also provides status signals to the associated RSPCs. All motor controls also receive a separate discrete input signal from an Emergency Rod Insertion Control Panel (ERICP) used in the logic for providing the emergency rod insertion movement functions (that is scram-follow, ARI, or SCRRI).

Rod Brake Controller Cabinets

The Rod Brake Controller Cabinets (RBCCs) contain electrical and/or electronic logic and other associated electrical equipment for the proper operation of the FMCRD holding brakes. The Rod Brake Controllers (RBCs) receive signals for brake disengagement or engagement from the logic of the associated RSPCs. RBC logic provides two separate brake status signals (channel A and channel B) to the logic of the associated RSPCs.

Emergency Rod Insertion Control Panel

The ERICP is located in the back-panel area of the MCR. It serves as an additional logic panel that contains relay (or solid-state equivalent) hardware needed to transmit discrete output signals to the Emergency Rod Insertion Control Panels (ERICP) in the RB. The discrete output signals are activated by input signals received from the RPS portion of the SSLC panels (that indicate a scram-follow function is active or based upon input signals received from the N-DCIS) that indicate a ARI function or automatic SCRRI function is active or by input signals from the two manual SCRRI pushbuttons on the Main Control Room Panel (MCRP).

Emergency Rod Insertion Panels

The ERIP are located in the RB and provide discrete output signals to the IMCs in the IMCCs. The discrete output signals are activated by input signals received from the ERICP that indicate the scram-follow function, the ARI function or the SCRRI function is active.

Scram Time Recording Panels

The Scram Time Recording Panels (STRPs), located in the RB, monitor the FMCRD position reed switch status using Reed Switch Sensor Modules (RSSMs). They communicate this information to the RAPI through the RC&IS multiplexing network. Also, the STRPs automatically record and time tag FMCRD scram timing position reed switch status changes. It does this either after initiation of an individual HCU scram test at the RPS Scram Time Test Panel or after a full-core reactor scram has been initiated. The recorded scram timing data can be transmitted to the scram time recording and analysis panel in the MCR back-panel area.

Scram Time Recording and Analysis Panel

The Scram Time Recording and Analysis Panel (STRAP), located in the MCR back-panel area, receives scram timing position information from the STRPs and performs scram timing performance analysis. The recorded performance information can also be transmitted to the N-DCIS equipment for further data analysis and archiving.

RAPI Auxiliary Panels

RAPI Auxiliary Panels, located in the RB, provide output signals to open a purge water valve whenever either FMCRD associated with the corresponding HCU receives an insertion

command from the RAPI subsystem. These panels also monitor scram valve position status as well as whether the HCU accumulator water pressure and level status are normal or abnormal. Communication of this information to and from the RAPI subsystem is achieved through the N-DCIS equipment. Two or more of the nonsafety-related remote multiplexing unit cabinets of the N-DCIS equipment scope are used as the RAPI auxiliary panels that are physically not part of the RC&IS equipment scope, even though they provide the RC&IS related functions described above.

7.7.2.2.2 Multiplexing Network

The RC&IS multiplexing network consists of two separate channels that use fiber optic communication links. The first channel handles communication between the RACS and the RSPCs in the RCCs (through the FCMs), and communication between the STRPs and the RACS. The second channel handles communication between the STRPs and the STRAP. Communication between the RAPI auxiliary panels, for HCU purge water valve control and HCU status monitoring, and the RAPI channels is achieved by the N-DCIS equipment, not the RC&IS multiplexing network.

The plant Q-DCIS communication equipment interfaces with FMCRD dual redundant separation switches (A and B). It provides the appropriate status signals to the RACS cabinets used in the RC&IS logic for initiating rod block signals of the appropriate FMCRD if a separation occurs. The Q-DCIS communication equipment provides these signals to the RAPI SIUs of the RC&IS via communication with the N-DCIS through proper isolation. Refer to Subsection 7.1.3.3. The Q-DCIS and N-DCIS communication equipment is not part of the RC&IS equipment scope. Each RAPI SIU transmits status signals to the associated RAPI channel for use in the RAPI rod block logic.

7.7.2.2.3 Classification

The RC&IS is not classified as a safety-related system because it has a control design basis only and is not required for the safe and orderly shutdown of the plant. A failure of the RC&IS cannot result in gross fuel damage. The rod block function of the RC&IS, however, is important in limiting the potential consequences of a rod withdrawal error during normal plant operation. An abnormal operating transient that might result in local fuel damage is prevented by the rod block functions of the RC&IS.

7.7.2.2.4 Power Sources

Normal - The Low Voltage Distribution System normally provides the required incoming 3-phase AC power for the IMC equipment. This provides a 3-phase AC power source required for energization of the associated FMCRD induction motors and motor built-in brakes by the IMCCs. The Low Voltage Distribution System also provides the required AC power for the rod brake controller power supplies in the RBCCs, the ERIPs and the associated ERICP. The Medium Voltage Distribution System power bus and equipment design assures that the associated Low Voltage Distribution System equipment that provides required AC power to the IMCCs, RBCCs, and ERIPs is automatically powered from the standby AC diesel generators if the normal power source is lost. Excitation power required for logic in the ERICP is provided directly from the ERIPs.

The power distribution design provides three distinct electrical groups of power. The distribution of these three groups of electrical power to FMCRDs is such that approximately one third of the FMCRDs belong to each group. The distribution of FMCRDs in each electrical group is scattered throughout the reactor core so complete insertion of the FMCRDs (in any two of the three electrical groups to the full-in position) assures that the reactor reaches hot shutdown conditions. This approach provides increased reliability for the capability of the motor run-in ARI function, if activated, to ensure that the reactor achieves hot shutdown conditions.

The power for all RC&IS equipment, except as noted above, is derived from two separate, non-divisional AC power sources (See Chapter 8) with at least one of the redundant AC power sources being an Uninterruptible Power Supply (UPS). Redundant power supplies are also provided for this equipment so that failure of a single power source or of a single power supply, does not result in the complete loss of capability of the RC&IS to perform rod movements. For certain types of power sources or supply failures, the operator has to perform appropriate bypass of the affected RC&IS equipment in order to restore rod movement capability.

On the loss of the normal power source, the nonsafety-related standby diesel generators provide an alternate power source for the IMCCs, RBCCs, and emergency rod insertion panels.

7.7.2.2.5 Scope

The RC&IS scope includes the following equipment:

- All the electrical/electronic equipment contained in the RACS cabinet, the RCCs, the IMCCs, the RBCCs, the STRPs, the STRAP, the ERIPs, and the ERICP. (Note: RAPI auxiliary panels are designated as part of the N-DCIS);
- The RC&IS multiplexing network equipment;
- The cross-channel communication links between equipment located in the RACS cabinets; and
- The dedicated RC&IS DOI and the communication links from the RACS cabinets to this interface.

7.7.2.2.6 Cabinet Subsystems

The RACS cabinets each have four identical dual-channel subsystems: the RAPI, the RWM, the ATLM, and the RAPI SIU. This subsection describes the key functions performed by the RAPI and RWM subsystems.

The RAPI is the primary RC&IS equipment that performs the following functions:

- Accepts and responds appropriately to manual, semi-automatic, and automatic rod movement commands;
- Enforces rod blocks based upon signals, internal and external, to RC&IS. Internal RC&IS signals include those initiated from either of the two channels of rod blocks initiated by signals from the ATLM, RWM, RAPI SIU equipment, and those caused by

any RAPI two-channel disagreement. External input signals to each RAPI channel that are used for the rod block logic originate from:

- The safety-related four divisions of the RPS (required isolation provided by RPS related equipment);
- The safety-related four divisional Startup Range Neutron Monitor (SRNM) and Average Power Range Monitor (APRM) subsystems of the NMS (required isolation provided by the NMS);
- The safety-related FMCRD dual redundant separation switches (A & B) of each control rod through Divisions 1 and 2 of the Q-DCIS communication (required isolation is provided by fiber optic cable and one way communication links to the N-DCIS equipment);
- The nonsafety-related dual-channel Multi-Channel Rod Block Monitor (MRBM) of the NMS; and
- Refueling equipment.

- Enforces adherence to a predetermined rod pull sequence that is stored in RRPS memory. The RRPS memory defines the order in which gangs of control rods are selected and moved when either semi-automatic or automatic rod movements are performed (that is the equivalent to the pull sheet used by plant operators when performing manual rod movements for conventional Boiling Water Reactor (BWR) plants). Violation of the RRPS causes RAPI logic to issue the following:
  - A switch to manual mode when the RC&IS is in the automatic rod movement mode or the Semi-automatic rod movement mode.
  - An alarm signal when the RC&IS is in the manual rod movement mode. (Gangs of rods can still be moved while in manual mode, but are limited to the RRPS gangs and only one gang at a time can be moved.)
- Provides control rod position and FMCRD status information to the N-DCIS, the NMS, the RWM, and the ATLM. The RAPI transmits signals required by the NMS, ATLM, and RWM to the associated RAPI SIU. The RAPI SIU then transmits required status signals to both channels of the ATLM, RWM, and the MRBM channels of the NMS.
- Provides the scram-follow function that automatically activates motor run-in of the ballnuts of all operable FMCRDs to the normal full-in position after a reactor scram has occurred. If the rapid hydraulic insertion function for any FMCRD does not work properly, this function provides an electric motor driven backup means to achieve full insertion of all operable FMCRDs.
- Provides the SCRRI function that results in automatic insertion of predefined control rods to specified target insertion positions so that required reactor power reduction is achieved when this function is activated. The RC&IS also sends a SCRRI signal to the DPS to initiate the SRI function.

- Provides for ARI motor run-in of all ARI control rods based on the receipt of the ARI initiation signals from the N-DCIS.
- Sends/receives rod movement commands, rod position, FMCRD status information and RC&IS related status information from the logic of all of the RSPC (A & B) of each RSM in the RCCs, by means of FCMs and the RC&IS multiplexing network. The RAPI also receives FMCRD position reed switch status information from the STRPs by means of the RC&IS multiplexing network.
- Sends and receives information and control signals to and from the other RAPI channel.
- Sends HCU purge water valve control signals, to and receives HCU status signals from, the N-DCIS equipment.
- Provides for different CRD surveillance tests, including the following:
  - Scram Time Test,
  - Coupling Check Test, and
  - Double-Notch Test.
- Enforces the applicable RWM rod block by sending appropriate rod block signals to the logic of the RSPCs in the RCCs. Either channel of RWM can cause a rod block independently.

The RWM issues a rod withdrawal block signal and a rod insertion block signal that is used in the RAPI rod block logic. This rod block signal ensures that:

- Absolute rod pattern restrictions, called the Ganged Withdrawal Sequence Restrictions (GWSR) when reactor power is below the LPSP, are not violated. This is only applicable when the RPS Reactor Mode Switch is in either the Startup or Run position. The GWSR assure that control rod worths are maintained to within reasonable values by only allowing rod patterns that result in relatively low rod worths when control rods are withdrawn.
- Only the two control rods associated with the same HCU can be withdrawn for the 2-CRD scram time test when the RPS Reactor Mode Switch is in the Refuel position and the scram test mode has been activated. This function provides for performing individual HCU scram testing during planned refueling outages.

The RWM also includes logic for performing shutdown margin testing when the RPS Reactor Mode Switch is in the Startup position. This mode allows only a limited set of pre-specified control rods to be withdrawn to perform this special testing.

The ATLM issues internal rod withdrawal block signals within RC&IS. These signals, when RC&IS is in the Automatic rod movement mode, cause RC&IS to transfer to the manual rod movement mode. The ATLM-based rod block prevents violation of normal operating limit restrictions on fuel thermal limit values, (MCPR and MLHGR operating limits) if operations stay in the automatic mode. The ATLM algorithm is based upon input signals from the LPRMs and

APRMs of the NMS and control rod positions and status data and other plant data from the RAPI signals transmitted from RAPI channels via the RAPI SIUs. The ATLM operating limit setpoints can be updated based upon calculated inputs from the core monitoring function of the N-DCIS. Updates of the ATLM setpoints can occur automatically or they can occur manually when the operator uses the N-DCIS VDU capabilities to request a manual ATLM update. Either channel of the ATLM can cause transfer to the Manual mode from the Automatic mode and rod withdrawal block initiation independently.

7.7.2.2.7 Operation Description

7.7.2.2.7.1 Single Rod Movements

Though this mode of rod movement is not normally used, the capability exists for the plant operator to perform manual movements of individual control rods. To perform this type of rod movement, the operator must select the manual, single rod movement mode by controls provided at the RC&IS DOI, and designate the individual rod to be moved. After confirming that the correct rod has been designated, the operator then selects the desired rod movement mode, either step movement, notch movement, or continuous mode.

Step movement means movements of 36.5 mm (1.44”) nominal distance for each step movement activated except for the last withdrawal or for the first step movement from normal full-out position, which have a nominal step distance of 37.5 mm (1.48”). Notch movement means movement to the next rod position that is an integer multiple of 2 steps movement from being fully-inserted. In the Continuous mode, rod movement continues as long as the operator activates a movement command, and after the operator deactivates the movement command, the rod settles to the effective target position.

To accomplish the desired movement in the selected movement mode, the operator activates the “insert” or “withdraw” movement command. This is done by activating associated hard pushbutton switches located adjacent to the RC&IS DOI on the main control panel in the MCR. The desired rod movement occurs if no abnormal conditions, such as a rod block, are activated. If any of the higher priority automatic rod movement actions are activated (for example SCRRI, scram-follow, or ARI), these movements override the operator desired normal movement and is completed as required. This is true no matter what mode of normal rod movement is activated.

The RAPI of the RC&IS enforces rod blocks based upon signals internal or external to the system. These rod blocks can prevent desired rod movements or stop rod movements, if activated while normal rod movements are underway. This applies to both single rod movement and ganged rod movement modes.

The internal signals include those signals from ATLM and RWM. If there is any disagreement between the two-channel logic of the subsystems of the RC&IS, rod block signals are transmitted to the RSM unless one of the channels of logic has been manually bypassed.

Examples of external input signals which could cause rod withdrawal blocks include those from the SRNM and APRM subsystems and the multi-channel rod block monitor subsystems of the NMS or from FMCRD separation status signals received from the Q-DCIS through data transmission to the RC&IS. A rod withdrawal block condition is activated from the corresponding FMCRD if the status of either separation switch A or B indicates that FMCRD

separation has occurred, if the RPS Reactor Mode Switch is in either the Startup or Run position, and if that rod is currently selected for normal movement. A more complete list of rod block conditions is provided later in this subsection.

When normal rod movements are performed (no abnormal conditions exist), the RAPI of the RC&IS transmits the appropriate rod movement command signals to a dual channel FCM located in a RCC. These rod movement command signals are received at the dual channel FCM and routed to logic for the associated rod server processing channel RSPC A and RSPC B of the RSMs of the selected rod. They are then transmitted as channel A and channel B inputs for the corresponding induction motor controller. Channel A and channel B brake energization signals are transmitted to the associated RBC. The IMC performs two-out-two voting on the command signals received from the logic of both RSPCs. It then activates the proper power control signals to accomplish the FMCRD motor movement that provides the required 3-phase AC power output to the FMCRD motor and power to the associated motor built-in brake to perform the desired movement.

The rod brake controller similarly performs two-out-of-two voting and energizes (mechanically releases) the FMCRD holding brake just prior to the start of FMCRD motor movement. It then de-energizes (mechanically engages) the FMCRD holding brake just after the desired normal rod movement is completed.

The RDCs of the RSM interface with instrumentation of the FMCRD, a subsystem of the CRD. They collect absolute rod position for the corresponding FMCRD by converting the resolver A and resolver B analog signals into digital data representing the FMCRD rod position. The data is used in the associated RSPCs' logic and transmission (via the RC&IS multiplexing system) to the RAPI logic and for the RAPI to transmit rod position data to other systems and subsystems and to the RC&IS DOI.

7.7.2.2.7.2 Ganged Rod Movements

There are three means of controlling ganged rod motion. The RC&IS provides for automatic mode, semi-automatic mode, and manual mode. When in the automatic mode of operation, commands for insertion or withdrawal are received from the PAS.

The RC&IS DOI provides controls for activating the automatic, semi-automatic, or manual rod movement mode of operation. When the system is in the semi-automatic mode, all rod movements are controlled by the operator. However, the RC&IS, by using a database called the RRPS and keeping track of the current control rods' positions, provides for automatic selection of the next gang, as required, to perform the sequence of rod movements in accordance with the RRPS definition. With this approach, the operator only needs to decide when to either insert or withdraw control rods and does not have to decide which gang of control rods to select next. This ensures that the RRPS sequence is followed.

When the RC&IS is in manual mode, the ganged rod movement mode has been chosen, and the operator selects a specific rod in a gang, the logic automatically selects all associated rods in that gang. The operator does not have to follow the RRPS sequence when performing manual rod movements; however, in order to re-establish either semi-automatic or automatic rod movement

modes, the operator has to establish an initial rod pattern that is consistent with the RRPS allowed rod patterns.

When the automatic mode is active, the RC&IS responds to signals for a rod movement request from the PAS. In this mode, the PAS simply requests either desired control rod insertion or withdrawal movements. The RC&IS responds to this request by using the RRPS and the current rods' positions and automatically selects the appropriate gang and executes the next in sequence withdrawal/insert commands as required.

In order for the automatic rod movement feature of the RC&IS to be active, the soft switch on the RC&IS DOI for automatic rod movement mode must be activated with none of the abnormal conditions that could prevent the RC&IS automatic operation mode from being active. The operator has the option of discontinuing the automatic operation by changing the RC&IS mode switches to the manual or the semi-automatic position.

7.7.2.2.7.3 Establishment of RRPS

The RRPS is normally established before plant startup and stored in the memory of the N-DCIS equipment and the RC&IS. The N-DCIS and RC&IS allow modifications to be made to the RRPS through operator actions. The N-DCIS provides compliance verification of the proposed changes to the RRPS with the ganged withdrawal sequence requirements.

The RC&IS provides the capability for an operator to request a download of the RRPS from the N-DCIS. The new RRPS data is loaded into the RAPI. Download of the new RRPS data can only be completed when the RC&IS is in manual rod movement mode and when a permissive switch located at the RAPI-A panel is activated. The RC&IS provides feedback signals to the N-DCIS to confirm a successful download of the RRPS data.

Rod withdrawal block signals are generated whenever selected single or ganged rod movements differ from those allowed by the RRPS. The RC&IS can either be in the automatic or semi-automatic rod movement mode. The RC&IS provides for activation of an alarm at the operator's panel for an RRPS violation.

7.7.2.2.7.4 Rod Block Function

The rod block logic of the RC&IS, upon receipt of input signals from other systems and internal RC&IS subsystems, inhibits movement of control rods. In most cases, only a rod withdrawal block is activated. However, the RWM can also activate a rod insertion block for enforcement of the GWSR.

Rod block signals to the RC&IS from safety-related systems are appropriately isolated. This provides required isolation between safety-related and nonsafety-related systems while keeping electrical failures from propagating into the safety-related systems (IEEE Std. 603, Section 5.6.3).

The presence of any rod block signal, in either channel or both channels of the RC&IS logic, causes automatic changeover from automatic mode to manual mode. The automatic rod movement mode can be restored by taking the appropriate action to clear the rod block and by using the selector switch to restore the automatic rod movement mode.

If either channel or both channels of the RC&IS logic receives a signal from any of the following type of conditions, a rod block is initiated:

- Rod separation detection (rod withdrawal block only for those selected rod(s) for which the separation condition is detected and are not in the Inoperable Bypass condition, applicable when the RPS Reactor Mode Switch is in the Startup or Run position);
- Reactor Mode Switch in Shutdown position (rod withdrawal block for all control rods, applicable when the RPS Reactor Mode Switch is in the Shutdown position);
- SRNM withdrawal block (rod withdrawal block for all control rods, not applicable when the RPS Reactor Mode Switch is in the Run position);
- APRM withdrawal block (rod withdrawal block for all control rods);
- CRD charging water low pressure (rod withdrawal block for all control rods);
- CRD charging water low-pressure trip bypass (rod withdrawal block for all control rods);
- RWM withdrawal block (rod withdrawal block for all control rods, applicable below the Low Power Setpoint);
- RWM insert block (rod insertion block for all control rods, applicable below the Low Power Setpoint);
- ATLM withdrawal block (rod withdrawal block for all control rods, not applicable below the Low Power Setpoint);
- MRBM withdrawal block (rod withdrawal block for all control rods, not applicable below the Low Power Setpoint);
- Gang large deviation (for example, gang misalignment) withdrawal block (rod withdrawal block for all operable control rods of the selected gang, applicable when RC&IS Gang mode selection is active);
- Refuel mode withdrawal block (rod withdrawal block for all control rods, applicable when the RPS Reactor Mode Switch is in the Refuel position if a fuel bundle is being handled by the refueling platform while positioned over the RPV);
- Startup mode withdrawal block (rod withdrawal block for all control rods, applicable when the RPS Reactor Mode Switch is in the Startup position if the refueling platform is positioned over the reactor pressure vessel);
- RAPI trouble (rod withdrawal block and rod insertion block for all control rods);
- RAPI SIU trouble (rod withdrawal block for all control rods);
- Electrical group power abnormal (rod withdrawal block and rod insertion block for all control rods);

The RC&IS enforces all rod blocks until the rod block condition is cleared. The bypass capabilities of the RC&IS permit clearing certain rod block conditions that are caused by failures or problems that exist in only one channel of the logic.

7.7.2.2.7.5 RC&IS Reliability

The RC&IS has a high reliability and availability due to its dual channel configuration design. The design allows its continual operation, when practicable, in the presence of component hardware failures. This is achieved because the operator is able to reconfigure the operation of the RC&IS through bypass capabilities while the failures are being repaired.

The expected system availability during its 60-year life exceeds 0.99. The expected reliability is based upon the expected frequency of an inadvertent movement of more than one control rod, due to failure. The expected frequency is less than or equal to one inadvertent movement in 100 reactor operating years.

The RC&IS design ensures that no credible single failure or single operator error can cause or require a scram or require a plant shutdown. The RC&IS design preferentially fails in a manner that results in no further normal rod movement.

7.7.2.2.7.6 RC&IS Bypass Capabilities

The RC&IS provides the capability to bypass resolver A, or resolver B if it fails, and select resolver B, or resolver A, to provide rod position data to both channels of the RC&IS. The RC&IS logic prevents the simultaneous bypassing of both resolver signals for an individual FMCRD.

The RC&IS allows the operator to completely bypass up to eight control rods by declaring them "Inoperable" and placing them in this bypass condition. More control rods can be bypassed when the RPS Reactor Mode Switch is in the Refuel position, as described below. Through operator action, an update to the status of the control rods placed into the "inoperable" bypass can be performed at the RC&IS DOI.

Activating a new RC&IS "Inoperable Bypass Status" to the RAPI is only allowed when the RC&IS is in a manual rod movement mode and when a bypass permissive switch located near the RC&IS DOI on the main control panel in the MCR is activated.

The operator can substitute a position for the rod that has been placed in this bypass state in both channels of the RC&IS, if the substitute position feature is used. The substituted rod position value entered by the operator is used as the effective measured rod position that is stored in both RAPI channels and sent to other subsystems of the RC&IS and to other plant systems (such as the N-DCIS). The position substitution status of each FMCRD can also be displayed at the RC&IS DOI and the RAPI DOI.

To conduct periodic inspections on FMCRD components, RC&IS only allows up to 54 control rods to be placed in an "inoperable" bypass condition, when the RPS Reactor Mode Switch is in the Refuel position.

The RC&IS enforces effective rod movement blocks when the control rod has been placed in an inoperative bypass status. When the inoperative bypass status is active, the RC&IS logic does not send any rod movement or brake energization power to the associated FMCRD.

In response to activation of either normal rod movement or special insertion functions, such as ARI, control rods in this bypass condition do not respond to movement commands.

The RC&IS Single/Dual Rod Sequence Restriction Override (S/DRSRO) bypass feature allows the operator to perform special dual or single rod scram time surveillance testing at any power level of the reactor. In order to perform this test, it is often necessary to perform single or HCU pair rod movements that are not allowed normally by the sequence restrictions of the RC&IS. When a control rod or pair of control rods associated with an individual HCU is placed in a S/DRSRO bypass condition, the control rod(s) are no longer used to determine compliance with the RC&IS sequence restrictions (for example, the ganged withdrawal sequence and RRPS).

The operator can only perform manual rod movements of control rods in the S/DRSRO bypass condition. The logic of the RC&IS allows this manual single/dual rod withdrawal for special scram time surveillance testing. The operator can place up to two control rods associated with the same HCU in the S/DRSRO bypass condition. The dedicated RC&IS DOI display information contains status indication of control rods in the S/DRSRO bypass condition.

The RC&IS ensures that S/DRSRO bypass logic conditions have no effect on special insertion functions for an ARI, SCRRI, or SCRAM following condition. There is also no effect on other rod block functions, such as MRBM, APRM, or SRNM rod blocks.

The drive insertion following a single/dual rod scram test occurs automatically. The operator makes the necessary adjustment of control rods in the system prior to the start of the test for insertions, and restores the control rod to the desired positions after test completion.

In addition to the RC&IS bypass functions that affect both channels (the bypass capabilities are described above), there are additional RC&IS bypass functions provided for the operator to establish conditions that affect only one channel of the RC&IS. The interlock logic prevents the operator from placing both channels in bypass for these types of bypass conditions. Logic enforces bypass conditions to ensure that the capability to perform any special function (such as an ARI, scram following, and SCRRI) is not prevented by the bypass conditions.

The RC&IS logic ensures enforcement of associated special restrictions placed on plant operation during invoked bypass conditions that affect a single channel. The status and extent of the bypass functions can be determined at the RC&IS DOI.

Bypass conditions generally allow continuation of normal rod movement capability by bypassing failed equipment in one RC&IS channel. After repair or replacement of the failed equipment is completed, the operator can restore the system or subsystem to a full two-channel operability. The operator has the capability to establish single-channel bypass conditions within the following system or subsystems:

- RSPC channel A or B bypass,
- FCM channel A or B bypass,

- ATLM channel A or B bypass,
- RWM channel A or B bypass, or
- RAPI channel A or B bypass.

7.7.2.2.7.7 Automated Thermal Limit Monitor Algorithm Description

The ATLM is a microprocessor-based subsystem of the RC&IS that executes two different algorithms for enforcing fuel operating thermal limits when reactor power is above the low power setpoint. One algorithm enforces Operating Limit Minimum Critical Power Ratio (OLMCPR), and the other enforces the Operating Limit Minimum Linear Heat Generation Rate (OLMLHGR). For the OLMCPR algorithm, the core is divided into multiple regions, each region consisting of 16 fuel bundles. For the OLMLHGR algorithm, each region is further vertically divided into four segments. During a calculation cycle, ATLM Rod Block Setpoints (RBS) are calculated for OLMCPR monitoring and for OLMLHGR monitoring. The calculated setpoints are compared with the real time averaged LPRM readings for each region/segment. The ATLM issues a trip signal if any regionally averaged LPRM reading exceeds the calculated RBS. This trip signal causes a rod block within the RC&IS.

The ATLM algorithm is also based upon control rod positions and status data and other plant data from the RAPI. The ATLM operating limit setpoints may be updated based upon calculated inputs from the core monitoring function of the N-DCIS. Updates of the ATLM setpoints can occur either automatically or by operator request.

7.7.2.2.7.8 Operational Considerations

RC&IS DOI in the MCR, along with associated hard switches located close to the RC&IS DOI such as withdrawal and insertion pushbuttons, are the main interfaces for the operator to perform manual or semi-automatic control rod movements, activate and deactivate the RC&IS automatic rod movement mode, and activate and deactivate RC&IS bypass conditions. In addition, the operator can determine the details of the RC&IS status and related FMCRD status information at this interface. Dedicated hard switches are also provided on the main control panel for manual initiation of an ARI function and for manual initiation of an SCRRI function. The ARI manual initiation switches interface directly with the DPS equipment that provides associated signals to the N-DCIS. The N-DCIS sends associated ARI motor run-in initiation signals to the RC&IS. The DPS directly activates the ARI valves of the CRD system for accomplishing the hydraulic ARI function. The SCRRI manual initiation switches are within the scope of the RC&IS.

7.7.2.2.7.9 Reactor Operator Information

The RC&IS DOI provides the primary interface for the operator to access detailed RC&IS information, including details of the RC&IS status and related FMCRD status. RC&IS detection of abnormal conditions activates alarms so that the operator is notified of the change in RC&IS and/or FMCRD status. In addition, the RC&IS provides FMCRD position information and summary RC&IS and FMCRD status information to the N-DCIS equipment that provides for additional operator information to be displayed on other nonsafety-related VDUs in the MCR.

7.7.2.2.7.10 Setpoints

The RC&IS has no safety setpoints. The ATLM rod block setpoints are continuously calculated when the reactor power is above the low power setpoint. These setpoints also depend upon the last operating thermal limit information received from the N-DCIS during an ATLM thermal limit update process. All other setpoints are established prior to plant startup operations and only adjusted, if needed, as a result of plant startup testing results. It is anticipated that none or very few of the RC&IS setpoints (besides the continual ATLM rod block setpoint updates) require adjustment as a result of startup testing results.

7.7.2.2.7.11 Environmental Considerations

The RC&IS is not required for safety-related purposes, nor is it required to operate after a design basis accident. This system is required to operate in the normal plant environmental conditions for the location of the RC&IS equipment, in the back-panel area of the MCR and in applicable areas of the RB.

7.7.2.3 Safety Evaluation

Table 7.1-1 identifies the RC&IS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

The circuitry described for the RC&IS is completely independent of the circuitry controlling the scram valves. This separation of the scram and normal rod control functions prevents failures in the RC&IS circuitry from affecting the scram circuitry. The scram circuitry is discussed in Subsection 7.2.1. Because the RC&IS directly controls movement of each control rod as an individual unit, a failure that results in inadvertent movement of a control rod affects only one control rod. The malfunctioning of any single control rod does not impair the effectiveness of a reactor scram. Therefore, no single failure in the RC&IS prevents a reactor scram. Repair, adjustment, or maintenance of the RC&IS components does not affect the scram circuitry.

Chapter 15 examines the various failure mode considerations for this system. The expected and abnormal transients and accident events analyzed envelope the failure modes associated with this system's components.

7.7.2.3.1 Code of Federal Regulations

10 CFR 50.62, Requirements for reduction of risk from Anticipated Transients Without Scram (ATWS) events for light-water-cooled nuclear power plants:

- Conformance: The ATWS mitigation functions are designed in accordance with the requirements of 10 CFR 50.62.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Resolution of unresolved and generic safety issues for I&C is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- There are no interface requirements for this section.

7.7.2.3.2 General Design Criteria

GDC 13, 19, 24, 28 and 29:

- Conformance: The RC&IS complies with these GDC.

7.7.2.3.3 Regulatory Guides

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The RC&IS system conforms with RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.4.

7.7.2.3.4 Branch Technical Positions

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the RC&IS conforms with this BTP.

7.7.2.4 Testing and Inspection Requirements

The RC&IS equipment is designed with consideration for online testing capabilities. The system can be maintained on line while repairs or replacement of hardware take place without causing any abnormal upset condition. The single-channel bypass capabilities support having continued RC&IS operation while repair or maintenance work is being performed on the dual-channel scope of the RC&IS equipment.

7.7.2.5 Instrumentation and Control Requirements

The CRD system is the RC&IS main direct interface to gather control rod position information and FMCRD status information and execute control rod movement commands. The FMCRD-related instrumentation that provides direct input to the RC&IS is addressed as part of the CRD system in Subsection 4.6.1. The primary output of the RC&IS to accomplish the RC&IS related rod movement functions is the 3-phase power to the FMCRD motors, associated AC power to the motor built-in brakes, and the holding brakes of the CRD system.

The RC&IS modules that interface with FMCRD instrumentation include the appropriate signal conditioning and conversion components (for example, RDC, discrete contact closure or reed switch input circuitry, and excitation power sources/supplies) for acquisition of the following:

- Resolver A and B position feedback signals (continuous signals);
- Coupling check (overtravel-out) position reed switch (discrete signal);
- Latched full-in and full-in position reed switches (discrete signal; these two reed switches are wired in parallel);
- Buffer contact reed switch (discrete signal); and
- Scram Timing position reed switches (discrete signals) at the following positions:
  - 0% insertion,
  - 10% insertion,
  - 40% insertion,
  - 60% insertion, and
  - 100% insertion.

The induction motor controllers provide the proper 3-phase power to the FMCRD motor, the directly associated motor built-in brake, and the holding brakes of the CRD system to accomplish the RC&IS rod movement functions.

The RC&IS does not directly interface with any other basic plant instrumentation. The other inputs to the RC&IS are by hardwired signal interfaces, data communication links with other systems, or from the RC&IS DOI.

7.7.3 Feedwater Control System

7.7.3.1 System Design Bases

7.7.3.1.1 Safety Design Basis

The FWCS is not a safety-related system and is not required for safe shutdown of the plant. Therefore, the FWCS has no safety-related design basis. In Power Operation Mode, only one of the triple redundant controllers can be removed from service.

The safety-related feedwater isolation function is not included in the FWCS.

The LD&IS performs isolation of the feedwater system following a feedwater line break inside containment by closing the feedwater containment isolation valves and tripping the reactor feedwater pump Adjustable Speed Drive (ASD) motor circuit breaker.

7.7.3.1.2 Power Generation (Non-safety) Design Bases

The FWCS is designed so that the functional capabilities of safety-related systems are not inhibited (IEEE Std. 603, Section 5.6.3). The FWCS regulates the flow of feedwater into the RPV to maintain predetermined water level limits during transients and normal plant operating modes. The desired range of water level during normal power operation is based on steam

separator performance. The requirements include limiting carryover, which can affect turbine performance, and limiting carryunder, which can affect overall plant efficiency.

If the RPV water rises to Level 8, then equipment protective action trips the main turbine and reduce feedwater demand to zero. The feedwater pumps trip if the water continues to rise to Level 9. If the water falls to Level 3, then the RPS shuts down the reactor. The RPS is a fully independent safety-related system (Subsection 7.2.1). If the water continues to drop and reaches Level 2, the high-pressure make-up function of the CRD system initiates (Reference Figure 7.7-1, Water Level Range Definition). The CRD system is fully independent of other plant delivery or injection systems.

7.7.3.2 System Description

7.7.3.2.1 General Description

The FWCS is a power generation (control) system that maintains proper RPV water level in the operating range from high (Level 9) to low (Level 2). During normal operation, feedwater flow is delivered to the RPV through three Reactor Feed Pumps (RFPs) which operate in parallel. Each RFP is driven by an adjustable-speed induction motor that is controlled by an ASD. In normal operation, the fourth RFP is in standby mode and starts automatically if any operating feedwater pump trips while at power. In abnormal operation, the fourth RFP can be set in manual mode or can be removed from service for maintenance.

The FWCS is implemented on the triple redundant, Fault-Tolerant Digital Controller (FTDC) including power supplies and input/output signals. The controller is designed for a Mean Time to Failure (MTTF) of no less than 1000 years. The FTDC consists of three parallel processing channels, each containing the hardware and software for execution of the control algorithms. Each FTDC channel executes the control software for the control modes. Additional information is provided in Mark VIe Control System Guide, N-DCIS Design Documents, GEH-6721B, Vol. 1, Rev C, Chapter 2, System Architecture (Reference 7.7-2). At the operator's discretion, the system operation mode can be selected from the main control console. The FWCS functional diagram is provided as Figure 7.7-3.

During normal operation the FWCS sends three speed-demand signals, each of which reflects a voted FWCS processor output, to each feed pump ASD. The ASD performs a mid value vote and use it to control the speed/frequency of the feed pump motor. The mid value vote is also returned to the FWCS as an analog input and compared with the speed demands sent by the FWCS. If an FTDC channel detects a discrepancy between the field voter output and the FTDC channel output, a “lock-up” signal is sent to a “lock-up” voter and an alarm is activated in the MCR.

7.7.3.2.2 Operation Modes

The following modes of feedwater flow provide level control:

- **Single Element Control** - At less than 25% of rated reactor powers, the FWCS uses single-element control based on RPV water level. In this mode the conditioned level error from the master level (proportional + integral, or PI) controller is used to determine

the demand to either the Low Flow Control Valve (LFCV) or to an individual feed pump ASD. The ASDs control feed-pump-motor-speed and thus feedwater flow. In addition, the FWCS can regulate the RWCU/SDC system Overboard Control Valve (OBCV) flow demand to counter the effects of density changes and purge flows into the reactor during heatup when steam flow is low.

- **Three-Element Control** - During normal power range operation, the three-element control mode uses water level, total feedwater flow, total steam flow, and individual feed pump suction flow signals to determine the feed pump speed demand. The total feedwater flow is subtracted from the total steam flow signal to yield the vessel flow mismatch. The flow mismatch signal is summed with the conditioned level error signal from the master level PI controller to provide the input signal for the master flow (PI) controller. The master flow controller provides the demand signal to the individual RFP loop trim controllers that use the discharge flow signals to balance RFP flows. The trim controllers provide the speed demand signal to the ASDs that control feed pump motor speed and thus feedwater flow.

- **Manual Feed Pump Control** - Each RFP can be controlled manually from the main control console through the FTDC by selecting the manual mode for that feed pump. In manual mode, the RFP speed demand signal that is sent directly to the ASD of the selected feed pump may be increased or decreased. Each feed pump is controlled manually at the manual/automatic transfer station.

The FWCS also provides interlocks and control functions to other systems. If the reactor water reaches Level 8, then the FWCS simultaneously activates a control room alarm and sends a zero-speed demand signal to the feed pump ASDs. At reactor water setpoint Level 8 the main turbine is tripped and at Level 9, a trip signal is sent to the feedwater pump ASD control breaker. Additional feedwater temperature controls, monitoring, and alarms are provided to assist in power maneuvering using the number seven high-pressure feedwater heater and bypass around the high-pressure feedwater heaters. Refer to Section 10.4.

A loss of feedwater heating that results in a significant decrease in feedwater temperature generates a signal that FWCS sends to N-DCIS to initiate a SCRRI and SRI functions. This interlock limits the consequences of a reactor power increase due to cold feedwater. The temperature difference between feedwater lines A and B is monitored and alarmed if excessive.

In addition, the FWCS initiates the signal to open the steam line condensate drain valves when steam flow falls below 40% of rated flow. Finally, the FWCS sends a zero-flow demand signal to the feed pump ASDs on identification of an ATWS condition.

7.7.3.3 Safety Evaluation

The FWCS is not safety-related and is not required for safe shutdown of the plant. It is a power generation system that maintains proper RPV water level. Its operation range is from high water level (Level 9) to low water level (Level 2). If the vessel level rises too high (Level 8), then the main turbine trip and the feed pump ASD flow demand is reduced to zero. Continued rising water level to Level 9 results in a trip of all ASD feed pumps. The vessel water level rising to

Level 8 or falling to Level 3 results in the shutdown of the reactor by the RPS. Refer to Subsection 7.2.1 for the RPS description.

The FWCS initiates a runback of feedwater pump feedwater demand to zero and closes the LFCV and RWCU/SDC overboard flow control valve when it receives an ATWS trip signal from the ATWS/SLC Logic. Refer to Subsection 7.8.1.1.

Table 7.1-1 identifies the FWCS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.7.3.3.1 Code of Federal Regulations

10 CFR 50.62, Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants:

- Conformance: The ATWS mitigation functions are designed in accordance with the requirements of 10 CFR 50.62.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Unresolved and generic safety issues are discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- There are no interface requirements for this section.

7.7.3.3.2 General Design Criteria

GDC 13, 19, and 24:

- Conformance: The FWCS complies with these GDC.

7.7.3.3.3 Regulatory Guides

RG 1.151 - Instrument Sensing Lines:

- Conformance: The FWCS receives signals from sensors on vessel instrument lines in the NBS. Refer to Subsection 7.7.1.3 for a discussion of the criteria of RG 1.151 in relation to the NBS.

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems

RG 1.204 – Guidelines for Lighting Protection of Nuclear Power Plants:

- Conformance: The FWCS system conforms with RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.

7.7.3.3.4 Branch Technical Positions

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail in this subsection conforms with this BTP.

BTP HICB-19, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail in this subsection conforms with this BTP.

7.7.3.4 Testing and Inspection Requirements

The FTDC self-test and on-line diagnostic test features are capable of identifying and isolating failures of process sensors, Input/Output (I/O) cards, power buses, power supplies, processors and inter-processor communication paths. These features identify the presence of a fault and determine the location of the failure down to the module level.

The FWCS components and critical components of interfacing systems are tested to ensure that specified performance requirements are satisfied. Preoperational testing of the FWCS is performed before fuel loading and startup testing to ensure that the system functions as designed and that stated system performance is within specified criteria.

7.7.3.5 Instrumentation and Control Requirements

7.7.3.5.1 Power Sources

Redundant UPS power the FWCS digital controllers and process measurement equipment. No single power source or single power supply failure results in the loss of FWCS functions.

7.7.3.5.2 Equipment

The FWCS consists of the following elements:

- The FTDC that contains the software and processors for execution of the control algorithms;
- Feedwater flow signals that provide for the measurement of the total flow rate of feedwater into the vessel;
- Steam flow signals that provide for the measurement of the total flow rate of steam leaving the vessel;
- Feed pump discharge flow signals that provide for the measurement of the discharge flow rate of each feed pump;

- The LFCV differential pressure transmitters that provide for the measurement of the pressure drop across the LFCV, for LFCV gain control; and
- The LFCV flow transmitters that provide for the measurement of the flow rate through the LFCV, for both LFCV control and low thermal power calculations.

7.7.3.5.3 Reactor Vessel Water Level Measurement

Reactor vessel narrow-range water level is measured by at least three identical, independent sensing systems. For each level measurement channel, a differential pressure transmitter senses the difference between the pressure caused by a constant reference column of water and the pressure caused by the variable height of water in the reactor vessel. The differential pressure transmitters are part of the NBS. (Refer to Subsection 7.7.1.2 for a description of the reactor vessel instrumentation.) The FWCS FTDC determines one validated narrow-range level signal using the multiple level measurements as inputs to a signal validation algorithm. The validated narrow-range water level is indicated on the main control console in the MCR.

7.7.3.5.4 Steam Flow Measurement

The steam flow rate in each of four main steam lines is sensed at each RPV nozzle venturi, part of the NBS. (Refer to Subsection 7.7.1.2 for a description of the reactor vessel instrumentation.) Two flow transmitters per steam line, which are part of the FWCS, sense the venturi differential pressure and send these signals to the FTDC through the multiplexing function of the N-DCIS. The FWCS multiplexing function signal-conditioning algorithms take the square root of the venturi differential pressures and provide eight steam flow rate signals, two for each steam line, to the FTDC for validation. These validated steam line flow measurements are summed in the FTDC to give the total steam flow rate out of the vessel. The total steam flow rate is indicated on the main control console in the MCR.

7.7.3.5.5 Feedwater Flow Rate Measurement

Feedwater flow rate is sensed at a single flow element in each of the two feedwater lines, which are part of the Condensate and Feedwater System (C&FS). Three transmitters per feedwater line, which are part of the FWCS, sense the differential pressure and send these signals to the FTDC through the N-DCIS multiplexing function. The FWCS multiplexing function signal conditioning algorithms take the square root of the differential pressure and provide six feedwater flow rate signals, three for each feedwater line, to the FTDC for validation. These validated feedwater line flow measurements are summed in the FTDC to give the total feedwater flow rate into the vessel. The total feedwater flow rate is indicated on the main control console in the MCR.

Feed pump flow rate is sensed at a single flow element, which is part of the C&FS, downstream of each feed pump. The discharge line flow element differential pressure is sensed by a single transmitter, which is part of the FWCS, and sent to the FTDC through the N-DCIS multiplexing function. The FWCS multiplexing function signal conditioning algorithms take the square root of the differential pressure and provide the discharge flow rate measurements to the FTDC. The feed pump discharge flow rate is compared with the demand flow rate for that pump and the

resulting error is used to adjust the speed demand to the ASD to reduce that error and balance RFP flow rate between operating pumps.

7.7.4 Plant Automation System

7.7.4.1 System Design Bases

7.7.4.1.1 Safety Design Basis

PAS has no safety-related design basis, but is designed so that the functional capabilities of safety-related systems are not hindered. Abnormal events requiring control rod scrams are sensed and controlled by the safety-related RPS, which is fully independent of the PAS. Discussions of the RPS are provided in Subsection 7.2.1.

This system provides the capability for supervisory control of the entire plant. It does this by supplying set-point commands to independent nonsafety-related automatic control systems as changing load demands and plant conditions dictate.

7.7.4.1.2 Power Generation (Non-Safety) Design Bases

The power generation basis of this system provide supervisory control that regulate reactivity during criticality control, provides heatup and pressurization control, regulates reactor power, controls turbine/generator output, controls secondary nonsafety-related systems, and provides reactor startup / shutdown controls.

7.7.4.2 System Description

The primary purposes of the PAS are reactivity control, heatup and pressurization control, reactor power control, generator power control (MWe control), and plant shutdown control. The PAS consists of triple redundant process controllers. The functions of the PAS are accomplished by suitable algorithms for different phases of reactor operation which include approach to criticality, heatup, reactor power increase, automatic load following, reactor power decrease, and shutdown. The N-DCIS accepts one-way communication from the Q-DCIS so that the safety-related information can be monitored, archived, and alarmed seamlessly with the N-DCIS data (IEEE Std. 603, Section 5.6.3).

Through the N-DCIS, the PAS receives input from the following major safety-related systems: NMS and the RPS (Subsection 7.2.2). Through the N-DCIS, the PAS receives input from the following major non-safety systems: the RC&IS (Subsection 7.7.2), SB&PC (Subsection 7.7.5), FWCS (Subsection 7.7.3), RWCU/SDC (Subsection 7.4.3), and the Turbine Generator Control System (TGCS). The output demand request signals from the PAS are to the RC&IS to position the control rods, to the SB&CS for pressure setpoints, and to the TGCS for load following operation. A simplified functional block diagram of the PAS is provided in Figure 7.7-4.

The PAS interfaces with the operator's control console to perform its designed functions. From the operator's control console for automatic plant startup, power operation, and shutdown functions, the operator uses the PAS to issue supervisory control commands to nonsafety-related systems. The operator also uses the PAS to adjust set-points of lower level controllers to support automation of the normal plant startup, shutdown, and power range operations. In the automatic

mode, the PAS also issues command signals to the turbine master controller, which contains appropriate algorithms for automated sequences of turbine and related auxiliary systems. The PAS presents the operator with a series of break point controls on the main control console nonsafety-related VDUs for a prescribed plant operation sequence.

When all the prerequisites are satisfied for a prescribed breakpoint in a control sequence, a permissive is requested and upon operator acceptance, the prescribed control sequence is initiated or continued. The PAS then initiates demand signals to various system controllers to carry out the predefined control functions. For non-automated operations that are required during normal startup or shutdown (such as a change of Reactor Mode Switch status), automatic prompts are provided. Automated operations continue after the prompted actions are completed manually. The functions associated with reactor power control are performed by the PAS.

For reactor power control, the PAS contains algorithms that can change reactor power by control rod motions. A prescribed control rod sequence is followed when manipulating control rods for reactor criticality, heatup, power changes, and automatic load following. Each of these functions has its own algorithm to achieve its designed objective. During automatic load following operation, the PAS interfaces with the TGCS to coordinate main turbine and reactor power changes for stable operation and performance.

The normal mode of operation of the PAS is automatic. If any system or component conditions are abnormal during execution of the prescribed sequences, the PAS automatically switches into the manual mode. With the PAS in the manual mode, any in progress operation stops and alarms are activated in the MCR. Also with the PAS in manual mode, the operator can manipulate control rods through the normal controls. A failure of the PAS does not prevent manual control of reactor power, and does not prevent safe shutdown of the reactor.

The triple redundant FTDC and redundant system controllers perform the PAS control functional logic.

7.7.4.3 Safety Evaluation

The PAS does not perform or ensure any safety-related function. This system is designed so that functionalities of safety-related systems in the plant are not affected by it.

Table 7.1-1 identifies the PAS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.7.4.3.1 Code of Federal Regulations

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Resolution of unresolved and generic safety issues for I&C is discussed in Subsection 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- There are no interface requirements for this section.

7.7.4.3.2 General Design Criteria

GDC 13, 19, and 24:

- Conformance: The PAS complies with these GDC.

7.7.4.3.3 Regulatory Guides

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The PAS system conforms with RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.

7.7.4.3.4 Branch Technical Positions

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- The level of detail provided herein for the PAS conforms with this BTP.

7.7.4.4 Testing and Inspection Requirements

The FTDC input and output communication interfaces function continuously during normal power operation. Abnormal functioning of these components can be detected during operation. In addition, FTDC is equipped with self-test and on-line diagnostic capabilities for identifying and isolating failures of input/output signals, buses, power supplies, processors, and inter-processor communications. These on-line tests and diagnostics can be performed without interrupting the normal control operation of the PAS.

7.7.4.5 Instrumentation and Control Requirements

The instrumentation required for the system can be categorized as (1) control room instrumentation, needed for the man-machine interface, (2) hardware and software instrumentation for input/output interfaces and controller functions, and (3) direct non multiplexed sensor inputs needed by the system. The PAS hardware comprises triple redundant master controllers and duplicate system controllers. There is required PAS software for controller functions and input/output interfaces.

7.7.5 Steam Bypass and Pressure Control System

7.7.5.1 System Design Bases

7.7.5.1.1 Safety Design Basis

The SB&PC system does not perform or ensure any safety-related function, is classified as a nonsafety-related system, and has no safety-related design basis. In Power Operation Mode, only one of the three triplicated FTDCs can be removed from service.

7.7.5.1.2 Power Generation (Non-safety) Design Bases

The SB&PC system is designed so that the functional capabilities of safety-related systems are not inhibited (IEEE Std. 603, Section 5.6.3). The SB&PC system is essential to the power generation cycle because it controls reactor pressure during plant startup, power generation, and shutdown modes of operation.

The design objective is to enable a fast and stable response to pressure and system disturbances, and to pressure setpoint changes over the operating range. This is done using Turbine Control Valves (TCVs) through the TGCS and Turbine Bypass Valves (TBVs) for controlling reactor pressure. In addition, the design objective of the SB&PC is to discharge reactor steam directly to the main condenser in order to regulate reactor pressure whenever the turbine cannot use all of the steam generated by the reactor.

7.7.5.2 System Description

7.7.5.2.1 General Description

The purpose of the SB&PC system is to control reactor pressure during plant startup, power generation, and shutdown modes of operation. The SB&PC System is implemented on the triplicated FTDCs. Power supplies and input/output signals are redundant. The controller is designed for a MTTF of no less than 1000 years. Control of reactor pressure is accomplished through control of the TCVs through the TGCS and TBVs, so that susceptibility to reactor trip, turbine-generator trip, main steam isolation, and safety relief valve opening is minimized. Triplicated FTDCs using feedback signals from RPV dome pressure sensors, generate command signals for the TBVs and pressure regulation demand signals used by the TGCS to generate demand signals for the TCVs. For normal operation, the TCVs regulate reactor pressure. However, whenever the total steam flow demand from the SB&PC system exceeds the effective TCV steam flow demand, the SB&PC system sends the excess steam flow directly to the main condenser through the TBVs.

The ability of the plant to load follow the grid-system demands is accomplished by the aid of control rod actions. In response to the resulting steam production demand changes, the SB&PC system adjusts the demand signals sent to the TGCS so that the TGCS adjusts the TCVs to accept the control steam output change, thereby controlling pressure.

Controls and valves are designed so that steam flow is shut off when of control system electrical power or hydraulic system pressure is lost.

Refer to Figure 7.7-5, SB&PC Simplified Functional Block Diagram, and Figure 7.7-6, SB&PC FTDC Block Diagram for an overview of SB&PC functions and interfaces. Additional information is provided in Major Plant Automation System Interfaces (Reference Table 7.7-1).

7.7.5.2.2 Normal Plant Operation

At steady-state plant operation, the SB&PC system maintains RPV pressure at a nearly constant value, to ensure optimum plant performance. During normal operational plant maneuvers (pressure setpoint changes, level setpoint changes), the SB&PC system provides responsive, stable performance to minimize RPV water level and neutron flux transients. During plant startup and heatup, the SB&PC system provides for automatic control of the reactor pressure. Independent control of reactor pressure and power is permitted during RPV heatup by varying the turbine bypass flow as the main turbine is brought up to speed and synchronized. The SB&PC system also controls RPV pressure during normal (main steam isolation valves open) reactor shutdown to control the reactor cooling rate.

7.7.5.2.3 Abnormal Plant Operation

Events that lead to reactor trip present significant transients while the SB&PC system maintains reactor pressure. These transients are characterized by large variations in steam flow and core thermal power output that affect RPV water level. The SB&PC system stabilizes system pressure and thus aids the feedwater/level control systems in maintaining RPV water level.

The SB&PC system is also designed to operate with other reactor control systems to avoid reactor trip after significant plant disturbances. Examples of such disturbances are loss of one feedwater pump, inadvertent opening of safety relief valves or TBVs, main turbine stop/control valve surveillance testing, and steam line isolation valves testing. To protect the condenser the SB&PC inhibits opening of the TBVs when it detects high condenser pressure.

7.7.5.2.4 Operational Considerations

Manual operations permit opening of the main steam lines (up to the steam bypass valves and turbine stop valves) before normal condenser vacuum is obtained and permit cold shutdown testing of the isolation valves. The SB&PC system allows remote manual bypass operation in the normal opening sequence during plant start up and shut down. This facilitates purge of the vessel and main steam lines of accumulated noncondensible gases early on in the start-up process, and controls the rate of cooling during reactor shutdown to atmospheric pressures. When pressure transients increase during such manual operation, the controls provide automatic override of the manual demand signal by the normal bypass demand. The system automatically returns to the manual demand signal when the pressure transient causing the increased bypass demand is relieved.

Triplicated FTDCs perform the SB&PC system functional logic and process control functions. Because of the triple redundancy, it is possible to lose one complete processing channel without affecting the system function. This also facilitates taking one channel out of service for maintenance, repair, or module replacement while the system is on-line.

During operation of the SB&PC, the operator may observe the performance of the plant through nonsafety-related VDUs on the main control console or on the wide display panel in the MCR. As described in Subsection 7.7.5.5 below, the on-line diagnostic provision assures that all detections of transducer/controller failures are indicated to the operator and maintenance personnel. The triplicate logic facilitates on line repair of the controller circuit boards. During abnormal conditions that result in high condenser pressure, the steam bypass valves and Main Steam Isolation Valves (MSIVs) close to prevent positive pressure conditions that would open the main condenser rupture disks. Manually operated provisions permit opening of the MSIVs (that is, inhibit the closure function) during startup operation. This vacuum protection function bypass permits heatup of the main steamlines, up to the steam bypass valves and turbine stop valves, before normal main condenser vacuum is obtained. The bypass also permits cold shutdown testing of the isolation valves. Any plant or component condition that inhibits bypass valve opening is alarmed in the MCR and must be resolved before the TBV inhibit memory can be manually reset by the operator.

The SB&PC has no safety setpoints because it is not a safety-related system. Actual operational setpoints are determined during startup testing.

The SB&PC system and bypass valves are powered by redundant uninterruptible nonsafety-related power supplies and sources. No single power failure results in the loss of any SB&PC system function. Upon detection of a failure of two or more channels in the controller, a turbine trip is initiated.

The pressure control function forces the turbine control valves to remain under pressure control supervision to provide automatic load following. This enables fast bypass opening for transient events that require fast reduction in turbine steam flow.

The steam bypass function controls reactor pressure by responding to the bypass flow demand signal. It modulates the regulating bypass valves, which are automatically operated. This control mode is assumed under the following conditions:

- During reactor vessel heatup to rated pressure;
- While the turbine is brought up to speed and synchronized;
- During power operation when reactor steam generation exceeds the turbine steam flow requirements;
- During plant load rejection and turbine/generator trips; and
- During cooldown of the nuclear reactor.

7.7.5.3 Safety Evaluation

The SB&PC system is classified as a primary power generation system. It is not safety-related, and is not required to operate during or after any design basis accidents. The system is required to operate in the normal plant environment and is essential to the power production cycle. The SB&PC equipment is located in both the MCR area of the CB and the turbine building; and each SB&PC component is subject to the environment of the applicable area. The SB&PC FTDC

panel and its components are designed to retain structural integrity during and after design basis events so that safety-related equipment in its area is able to perform its safety function.

Table 7.1-1 identifies the nonsafety-related control system and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.7.5.3.1 Code of Federal Regulations

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: The SB&PC system is nonsafety-related and conforms in that there are no unresolved issues for the SB&PC system. Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: Test, inspection, analyses, and acceptance criteria of the SB&PC FTDC are identified in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- There are no interface requirements for this section

7.7.5.3.2 General Design Criteria

GDC 13, 19, and 24:

- Conformance: The SB&PC is in conformance with the GDC identified above.

7.7.5.3.3 Regulatory Guides

RG 1.151 - Instrument Sensing Lines:

- Conformance: Not applicable to the SB&PC system. The SB&PC receives reactor dome pressure signals from sensors in the NBS. Refer to Subsection 7.7.1.3 for discussion of the criteria of RG 1.151 in relation to the NBS. The SB&PC also receives condenser absolute pressure signals from sensors in the Main Condenser and Auxiliaries System.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interface in safety-related Instrumentation and Control Systems.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The SB&PC system conforms with RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.

7.7.5.3.4 Branch Technical Positions

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- The level of detail provided in this subsection conforms with this BTP.

7.7.5.4 Testing and Inspection Requirements

The FTDC input and output communication interfaces function continuously during normal power operation. Abnormal operation of these components is detected during operation. FTDC is equipped with on-line diagnostic capabilities to identify and isolate failure of input/output signals, buses, power supplies, processors, and inter-processor communications. On-line diagnostics are performed without interrupting the normal control operation of the SB&PC system.

The SB&PC components and critical components of interfacing systems are tested to ensure the specified performance requirements are satisfied. Preoperational testing of the SB&PC is performed before fuel loading and startup testing to ensure the system functions as designed and stated system performance is within specified criteria.

7.7.5.5 Instrumentation and Control Requirement

7.7.5.5.1 Power Sources

7.7.5.5.1.1 Uninterruptible Nonsafety–Related AC Power Supply

The nonsafety-related inverters of the UPS are powered by rectifiers which are supplied with by AC power. However, if the AC power fails, the inverters receive power from a Direct Current (DC) source (batteries). The SB&PC has three redundant nonsafety-related AC uninterruptible power supplies of 120 ±10% volt AC, 60 Hz. The SB&PC panel is designed so that loss of one power supply or incoming power source does not affect SB&PC system functional operation and thus plant operation.

7.7.5.6 Major Instrument Interfaces with SB&PC System

7.7.5.6.1 Nuclear Boiler System

The NBS provides narrow range dome pressure, wide range dome pressure, inboard MSIV position, and outboard MSIV position signals to SB&PC. The TBVs interface with the NBS to receive main steam supply.

7.7.5.6.1.1 Plant Automation System - Automatic Power Regulator

The SB&PC supplies the following signals to the PAS-Automatic Power Regulator (APR):

- SB&PC Auto/OK status,
- Operating pressure setpoint,

- Total (average) TBV position,
- Pressure regulator output,
- Limited speed regulator output,
- Load reference, and
- First TBV position.

PAS-APR outputs the following signals to SB&PC:

- AFC status,
- Raise pressure setpoint,
- Lower pressure setpoint,
- PAS-APR fatal fault, and
- Reactor thermal power.

7.7.5.6.1.2 N-DCIS - Plant Computer Function

The Performance Monitoring and Control Function (PMCF) of the Plant Computer Function (PCF) within the N-DCIS receives signals from the SB&PC for performance monitoring.

7.7.5.6.1.3 Nonsafety-related Distributed Control and Information System - Multiplexing

The Multiplexing function of the N-DCIS provides the distributed control and instrumentation data communications network that supports the monitoring and control of interfacing plant systems. RMUs are located throughout the plant that support the SB&PC and its interfaces with other systems.

7.7.5.6.1.4 Main Control Room Panels

The MCRP operator interface within the N-DCIS contains controls needed for SB&PC operation and displays variables and alarms from the SB&PC.

7.7.5.6.1.5 Main Control Room Back Panels

The SB&PC's triplicated FTDC panel is mounted in a MCR Back Panel (MCRBP).

7.7.5.6.2 Turbine Bypass System

The TBS provides temperature signals to the SB&PC from thermocouples installed in each TBV discharge pipe, located between the TBV and condenser, for bypass steam leakage detection.

7.7.5.6.2.1 Turbine Generator Control System

The TGCS is a redundant process control system. Only the operator can switch the turbine generator controller to Automatic (remote), but either the operator or the APR can switch the turbine generator controller to Manual (local). The TGCS controls the turbine speed, load, and steam flow for startup and normal operations. The TGCS operates the Turbine Stop Valves TSVs, TCVs, and the intermediate stop and intercept valves. The TGCS also provides automation functions such as sequencing the appropriate turbine support systems and controlling turbine roll, synchronization of the main generator, and initial loading. The SB&PC system sends a steam flow demand to the Turbine Generator (TG) controller.

SB&PC sends the following signals to TGCS:

- Pressure regulation demand, and
- Turbine trip.

TGCS provides the following signals to SB&PC:

- Turbine speed regulator output,
- Load reference,
- Turbine steam flow demand,
- Turbine first stage pressure,
- Power-Load Unbalance (PLU) event,
- TGCS Central Processing Unit (CPU) failure, and
- Turbine trip.

7.7.5.6.2.2 Main Condenser and Auxiliaries

The main condenser receives steam from the TBVs and provides condenser narrow and wide range pressure signals, from all shells of the condenser, to the SB&PC.

7.7.5.6.2.3 Auxiliary Boiler

The SB&PC sends signals to start the electric auxiliary boiler. Additionally, the SB&SC sends signals to increase auxiliary boiler steam production rate upon a MSIV closure condition

7.7.6 Neutron Monitoring System - Nonsafety-Related Subsystems

7.7.6.1 System Design Basis

7.7.6.1.1 Safety Design Basis

The NMS has two nonsafety-related subsystems, the Automatic Fixed In Core Probe (AFIP) subsystem and the MRBM subsystem. Neither the AFIP subsystem nor the MRBM subsystem

performs or ensures any safety-related function; therefore the AFIP and Multi-Channel Rod Block Monitor (MBRM) subsystems have no safety-related design basis.

7.7.6.1.2 Power Generation (Non-Safety) Design Bases

The AFIP has the following power generation design bases:

- To provide a signal proportional to the axial neutron flux distribution at the radial core locations of the LPRM detectors. This signal allows calibration of the LPRM;
- To provide sufficient axial neutron flux monitoring with corresponding axial position and indication to allow point-wise measurement of the axial neutron flux distribution to support the determination of three-dimension core power distribution; and
- To provide a totally automated mode of LPRM calibration by direct interface with the plant computer function of the N-DCIS.

The MRBM has the following power generation design bases:

- To provide a signal to the RC&IS to block rod movement if the MRBM signal exceeds a preset rod block setpoint to prevent fuel damage;
- To provide MRBM values to the N-DCIS;
- To provide bypass capability of one-out-of-two MRBM channels;
- To provide bypass of individual LPRM channels in its calculations;
- To provide online test and diagnostic capability to validate proper operation of its microprocessor-based system; and
- To provide rod block status to the MCR alarm system.

7.7.6.2 System Description

7.7.6.2.1 Automated Fixed In-Core Probe

7.7.6.2.1.1 General Description

The AFIP subsystem comprises AFIP sensors and their associated cables, as well as the signal processing electronic unit. The AFIP sensors are installed permanently within the LPRM assemblies. In each LPRM assembly in the core, there are seven AFIP sensors evenly distributed axially along the LPRM assembly. Consequently, there are AFIP sensors at and between all LPRM locations. The AFIP sensor cables are routed within the LPRM assembly and then out of the RPV through the LPRM assembly penetration to the vessel. The AFIP subsystem generates signals proportional to the axial power distribution at the radial core locations of the LPRM detector assemblies. The AFIP signal range is sufficiently wide to accommodate the corresponding local power range from approximately 1% to 125% of reactor rated power.

During core power and LPRM calibration, the AFIP signals are automatically collected and sent to the AFIP data processing and control unit. The data are properly amplified and compensated by applying correct sensor calibration adjustment factors. The data are sent to the PCF of the N-DCIS for core local power and thermal limits calculations. The calculated local power data are then used for LPRM calibration. The AFIP data collection and processing sequences are fully automated, with manual control available.

The AFIP sensor has near constant, very stable detector sensitivity due to its operating principle. Its sensitivity does not depend upon fissile material depletion or radiation exposure. The AFIP sensor, however, can be calibrated manually or automatically by using a built-in calibration device inside the LPRM assembly. The calibrated new sensitivity data of the AFIP sensors are stored in the AFIP control unit and are readily applied to the newly collected AFIP data to provide accurate local power information.

The AFIP sensors in an LPRM assembly are replaced together with the LPRM detectors when the whole LPRM assembly is replaced. The AFIP detectors within the LPRM assembly are installed so that physical separation is maintained between the LPRM detectors and the AFIP detectors. The AFIP cables are also routed within the LPRM assembly separately from the LPRM detector cables, with separate external connectors.

7.7.6.2.1.2 Classification

The AFIP is nonsafety-related. It is an operational subsystem and has no safety-related function.

7.7.6.2.1.3 Power Supply

The power for the AFIP is supplied from the nonsafety-related instrument 120VAC Instrumentation and Control Panel Supply (ICP) power source. The power for the AFIP logic is supplied from redundant nonsafety-related instrument 120VAC uninterruptible power sources.

7.7.6.2.1.4 Environmental Considerations

The AFIP sensor meets BWR environmental requirements. The connectors and cabling located in the drywell are designed for continuous duty (see Appendix 3D). The AFIP instruments are designed to operate under the expected environmental conditions at their locations.

7.7.6.2.1.5 Operational Considerations

The AFIP is operated to provide local power information for three-dimensional power calculations and for calibration of the LPRM channels. The AFIP operation is fully automated including AFIP data collection, AFIP sensor calibration, AFIP data amplification, and data transfer to the PCF. Manual operation capability is available.

7.7.6.2.2 Multi-Channel Rod Block Monitor

7.7.6.2.2.1 General Description

The MRBM subsystem logic issues a rod block signal used in the RC&IS logic to enforce rod blocks. The rod blocks prevent fuel damage by ensuring that the MCPR and MLHGR do not violate fuel thermal safety limits. Once a rod block is initiated, manual action is required by the operator to reset the system.

The MRBM microcomputer-based logic receives input signals from the LPRMs and the APRMs of the NMS. It also receives control rod status data from the RAPI subsystem of the RC&IS to determine when rod withdrawal blocks are required. The MRBM uses the LPRM signals to detect local power change during the rod withdrawal. If the MRBM signal, which is based on averaged LPRM signal, exceeds a preset rod block setpoint, a control rod block demand is issued. The MRBM monitors the core in 4-by-4 fuel bundle regions where control rods are being withdrawn. The MRBM algorithm covers the monitoring of multiple regions simultaneously depending upon the size of the gang of rods being withdrawn. Because it monitors more than one region, it is called the multi-channel rod block monitor. The MRBM is a dual channel system, but it is not a safety-related system.

7.7.6.2.2.2 Classification

The MRBM is nonsafety-related. Its activating interface is through the RC&IS, which is also a nonsafety-related system.

7.7.6.2.2.3 Power Supply

The power supply for the MRBM is from the non-divisional, nonsafety-related 120 VAC uninterruptible buses in two different load groups.

7.7.6.2.2.4 Environmental Considerations

The MRBM is located in the MCR. It is physically and electrically isolated from the safety-related NMS subsystems. All interfaces with the safety-related NMS subsystems are through optical isolators.

7.7.6.3 Safety Evaluation

Table 7.1-1 identifies the nonsafety-related control systems and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.7.6.3.1 Code of Federal Regulations

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Unresolved and generic safety issues are discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- There are no interface requirements for this section.

7.7.6.3.2 General Design Criteria

GDC 13, 19, 24, and 28:

- Conformance: The AFIP and MRBM subsystems are in compliance with these GDC.

7.7.6.3.3 Regulatory Guides

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The systems conform with RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.4.

7.7.6.3.4 Branch Technical Positions

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance : The level of detail provided in this subsection conforms with this BTP.

7.7.6.4 Testing and Inspection Requirements

7.7.6.4.1 Automated Fixed In-Core Probe

The AFIP instruments (not including sensors) are designed such that they can be tested, inspected, and calibrated as required during plant operation without causing plant shutdown or scram, and with easy access for the service personnel.

The AFIP sensor is testable and can be calibrated for its sensitivity. The AFIP instrument unit includes an algorithm that automatically detects and rejects failed AFIP sensor signals. It also includes logic that verifies proper communication with the N-DCIS system PCF.

The duration for AFIP testing and calibration is based on the applicable NMS AFIP design document. Additional information is provided in Gamma Thermometer System for LPRM Calibration and Power Shape Monitoring, NEDE-33197P (Reference 7.7-1).

7.7.6.4.2 Multi-Channel Rod Block Monitor

The MRBM subsystem is designed so that it can be tested, inspected, and calibrated as required during plant operation without causing plant shutdown or reactor scram. It provides easy access for the service personnel. The MRBM subsystem includes logic that verifies proper communication with the N-DCIS system. The duration for MRBM testing and calibration is based on the applicable NMS MRBM design document and the instruction manual for the MRBM subsystem.

7.7.6.5 Instrumentation and Control Requirements

7.7.6.5.1 Automated Fixed In-Core Probe

The AFIP instrument is based on digital measurement and control design practices that include microprocessor-based programmable memory units. It follows a modular design concept so that each unit or its subunit is replaceable during repair service. The instrument has a flexible interface design that accommodates either metal wire or fiber optic communication links. The AFIP instrument is provided with necessary operator-interface functions meeting NMS man-machine interface requirements.

The AFIP includes basic logic such as periodic demand for sensor calibration and data collection, as well as logic that is part of the communication protocol with the PCF. The AFIP instrument cabinets are located in appropriate areas of the CB with physical and electrical separation from the safety-related NMS instruments and with acceptable environmental conditions.

7.7.6.5.2 Multi-Channel Rod Block Monitor

The MRBM subsystem is based on digital measurement and control design practices that include microprocessor-based programmable and memory units. The MRBM follows a modular design concept so that each unit or its subunit is replaceable during repair service. The MRBM has a flexible interface design to accommodate either metal wire or fiber optic communication links. The MRBM instrument is provided with necessary operator-interface functions meeting NMS man-machine interface requirements.

The MRBM includes basic logic such as continuous LPRM data collection, MRBM rod block algorithm calculation, MRBM setpoint comparison, and communication protocol with the N-DCIS. The MRBM subsystem is located within the nonsafety-related equipment rooms of the CB with appropriate physical and electrical separation from the safety-related NMS instruments, and with acceptable environmental conditions.

7.7.7 Containment Inerting System

7.7.7.1 System Design Bases

The CIS design bases are discussed in Subsection 9.4.9.

7.7.7.2 System Description

The CIS system description is discussed in Subsection 9.4.9.2.

7.7.7.3 Safety Evaluation

CIS is nonsafety-related except for the containment isolation function. Failure of the nonsafety-related components does not adversely affect any safety-related system. Refer to Subsections 6.2.4 and 9.4.9.

Table 7.1-1 identifies the CIS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.7.7.3.1 Code of Federal Regulations

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

Conformance: There are no interface requirements for this section.

7.7.7.3.2 General Design Criteria

GDC 13, 19, and 24:

- Control and instrumentation is provided to operate the system and monitor process variables during startup, normal, and abnormal reactor operation. The CIS is operable from the MCR.

7.7.7.3.3 Regulatory Guides

There are no RGs other than RG 1.180 and RG 1.204 directly applicable to the nonsafety-related CIS. However, the CIS instrument lines penetrating containment meet the requirements of RG 1.11 and RG 1.151. Sensing lines are Seismic Category I Quality Group B and are provided with redundant isolation valves that can be isolated locally or remote manually from the MCR.

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems:

- Conformance: The CIS system conforms with RG 1.180 as discussed in Subsection 7.1.6.4.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The CIS system conforms with RG 1.204 as discussed in Subsection 7.1.6.4.

7.7.7.3.4 Branch Technical Positions

Only BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52, is applicable to the nonsafety-related CIS. The level of detail provided in this subsection conforms with this BTP.

7.7.7.4 Testing and Inspection Requirements

The CIS testing and inspection requirements are discussed in Subsection 9.4.9.

7.7.7.5 Instrumentation and Control Requirements

7.7.7.5.1 Logic and Interlocks

The CIS operation is manually or automatically activated from the MCR by aligning corresponding valves through remote manual control switches. During the inerting mode, once the steam-heated vaporizer has been activated, a temperature controller accomplishes automatic control of the steam supply. A temperature sensor at the outlet of the steam vaporizer provides input to the temperature controller that then regulates the amount of steam. Low nitrogen temperature in the steam vaporizer outlet causes an alarm and a low-low temperature condition shuts off the main inerting line. The auxiliary steam supply is manually terminated. When the required inert containment pressure is reached, the CIS drywell pressure switch provides a signal to isolate the nitrogen supply shutoff valve.

Upon completion of the initial inerting, the CIS is manually or automatically aligned to its make-up mode. Make-up is accomplished by the automatic modulation of the pressure control valve provided to make-up nitrogen. The opening and closing of the pressure control valve is driven by the pressure controller in response to change of containment pressure. Make-up nitrogen supply is vaporized and heated up to an appropriate temperature by an electric heater that is manually loaded to its power source. Once activated, it continues to operate in automatic on-off mode until manually disconnected. Temperature sensors provide switching signals to start/stop the heater. When the required temperature is reached, the heater automatically cuts off electrical power to the heater elements.

The de-inerting process is manually or automatically activated, by aligning the CIS with the RB Heating, Ventilation and Air Conditioning (HVAC) to replace gases in the containment with breathable air.

During primary containment isolation events, the CIS primary containment isolation valves automatically close upon receipt of the isolation signal from LD&IS. Details of the isolation logic are discussed in Subsection 7.3.3.

The CIS can provide continued nitrogen makeup during isolation events. This is accomplished by overriding, with controlled bypass switches, the isolation signal to the makeup isolation valves.

A simplified system diagram is shown in Figure 9.4-13.

7.7.7.5.2 Instrumentation and Control

Drywell pressure sensors, part of the Containment Monitoring System (CMS), monitor containment pressure. These instruments provide input to the pressure controller that controls makeup flow and provides alarm signals on a high drywell pressure condition.

Permanently installed temperature and humidity sensors are provided in several locations and elevations inside the containment. Outputs from these sensors are transmitted to the PCF for averaging and continuous monitoring of the containment.

Oxygen analyzers monitor oxygen levels in the containment during startup, normal, and abnormal plant operating conditions. Two sample points (one in a high and one in a low location) are provided on opposite sides of each compartment (that is, the upper drywell area, lower drywell area, and wetwell air space). Each air lock is sampled. Oxygen levels in the CIS exhaust line are monitored. A high oxygen level indication is alarmed in the MCR.

A flow-metering device is installed in the makeup line to monitor the amount of nitrogen make up injected into the containment. Total nitrogen make-up flow (make-up flow to containment and make-up flow to the High Pressure Nitrogen Supply System (HPNSS) is also monitored. Total nitrogen flow indicates total containment atmosphere leakage during normal plant operation. Excessive leakage is alarmed in the MCR.

Separate flow metering devices are also provided to both drywell and wetwell inerting and de-inerting flows.

The CIS is described in detail in Section 9.4.

7.7.7.5.3 Alarms and Indications

The following alarms and indications are provided in the MCR:

- High drywell pressure,
- High nitrogen makeup flow,
- Excessive or gross containment leakage,
- High and low make-up flow temperature,
- High and low electric heater temperature,
- Low main vaporizer outlet temperature,
- Low nitrogen storage tank level,
- Keylock switch in override position,
- High oxygen level,

- Wetwell pressure indication,
- Valve position switch status indication,
- Pilot solenoid status indication,
- Drywell temperature, and
- Wetwell temperature.

7.7.8 COL Information

None

7.7.9 References

7.7-1 GE Energy Nuclear, "Gamma Thermometer System for LPRM Calibration and Power Shape Monitoring," NEDE-33197P, Class III (GE Proprietary), September 2005.

7.7-2 GE Energy, "Mark VIe Control System Guide," N-DCIS Design Documents, GEH-6721B, Vol. 1, Rev C, Chapter 2, System Architecture, Class 1 (GE Non-Proprietary), 2004-2005.

Table 7.7-1
Major Plant Automation System Interfaces

APR Functions	Input Signals	Output Signals
Criticality Control	1. SRNM output (NMS) 2. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. Criticality / subcriticality validation check (PCF)
Heatup & Pressurization	1. SRNM output (NMS) 2. Reactor water temperature (PGCS) 3. Reactor heatup schedule (PCF) 4. Reactor mode (PGCS) 5. Dome Pressure (SB&PC)	1. CR control demand (RC&IS) 2. SB&PC pressure setpoint
Reactor Power Control	1. Target generator power (PGCS) 2. Pressure controller output (equivalent load) (SB&PC) 3. Load demand change (SB&PC) 4. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. Load demand (TGCS)
Generator Power Control	1. Generator power feedback signal (PGCS) 2. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. Load demand (TGCS)
Reactor Shutdown Control	1. CR full insert signal (RC&IS) 2. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. SB&PC pressure setpoint

Note: Various status signal interfaces are not shown in this table for brevity.

APR—Automatic Power Regulator

NMS—Neutron Monitoring System

PCF—Plant Computer Function

PGCS—Power Generation Control System

RC&IS—Rod Control and Information System

SB&PC—Steam Bypass and Pressure Control System

TGCS—Turbine Generator Control System

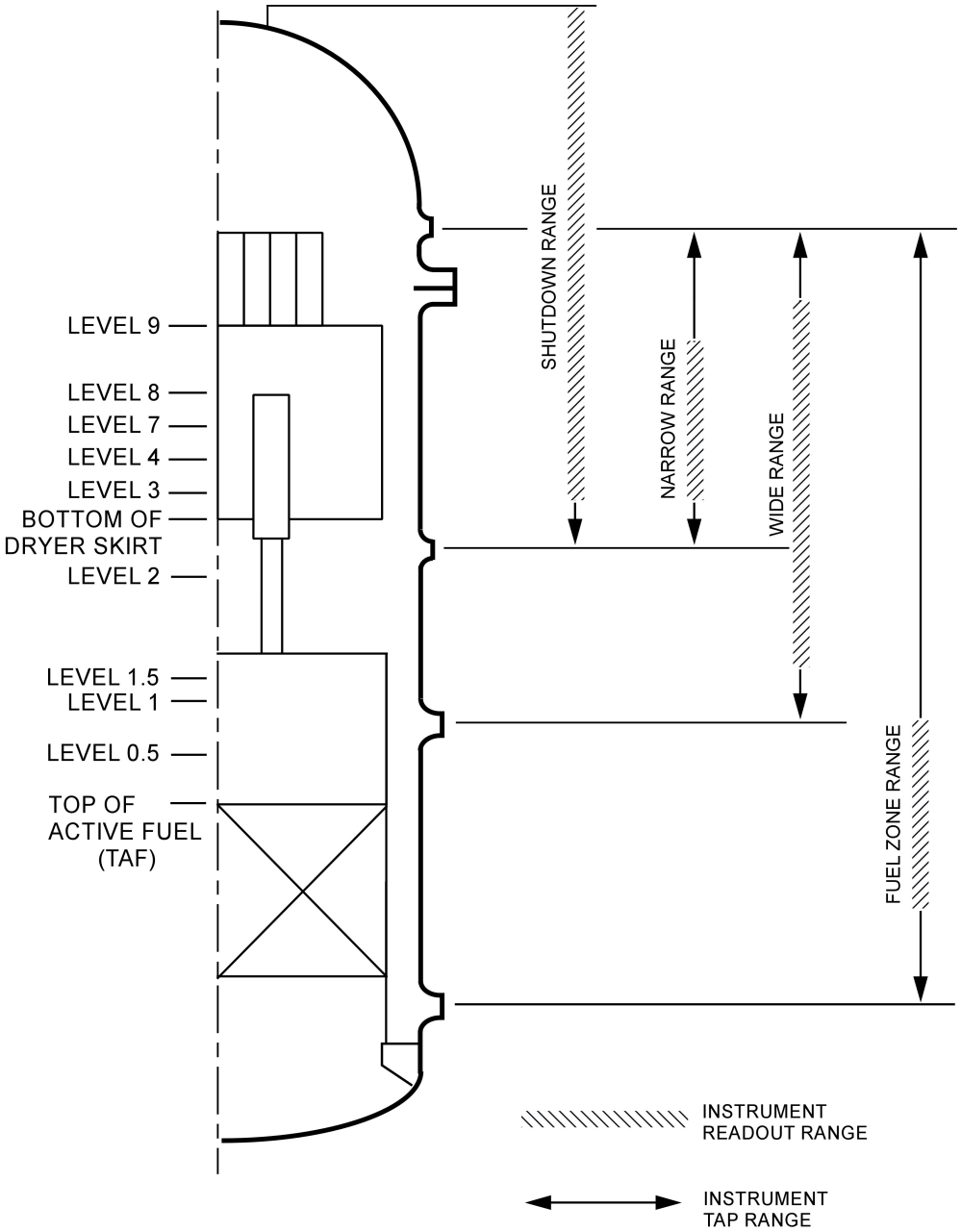


Figure 7.7-1. Water Level Range Definition

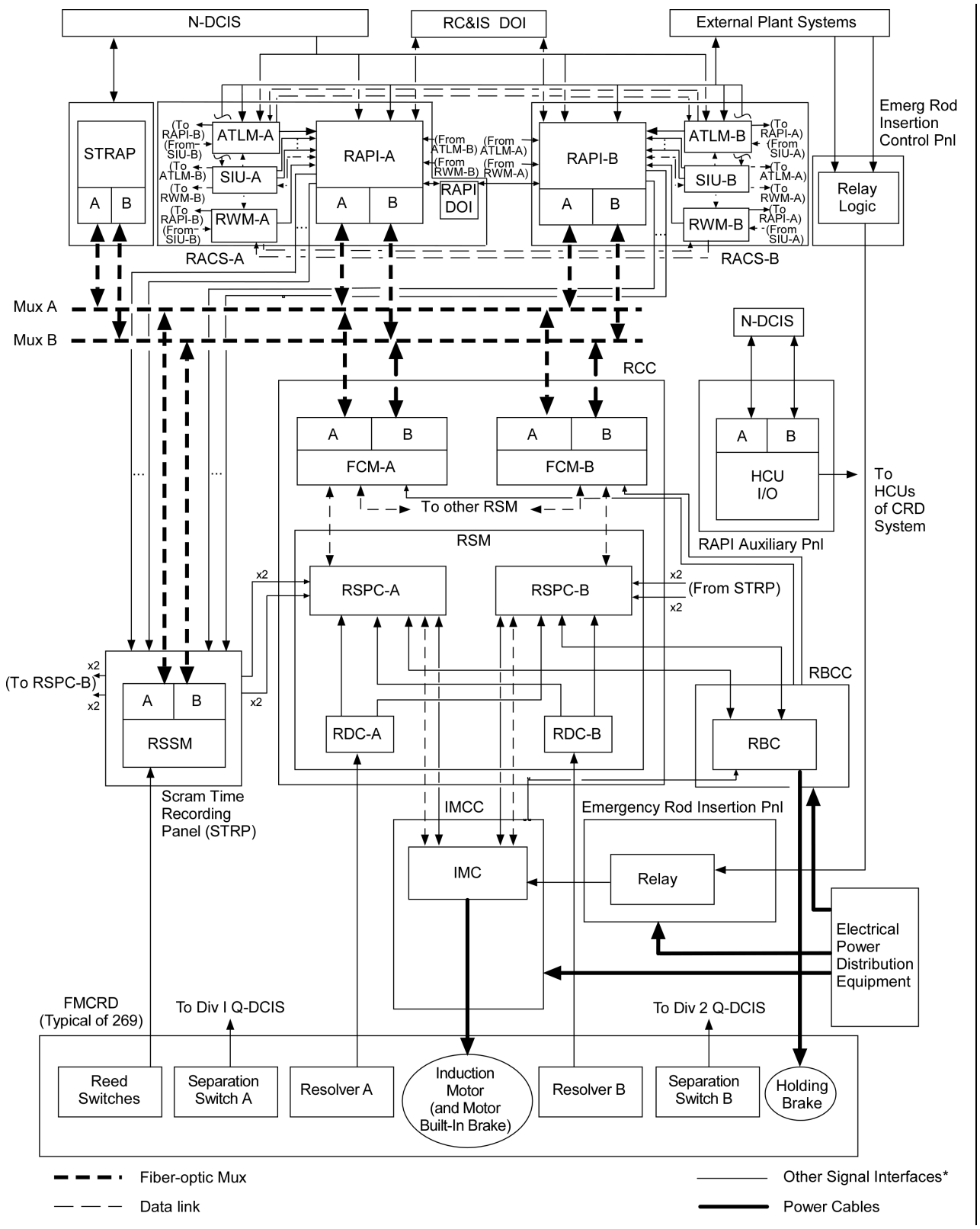


Figure 7.7-2. RC&IS Block Diagram

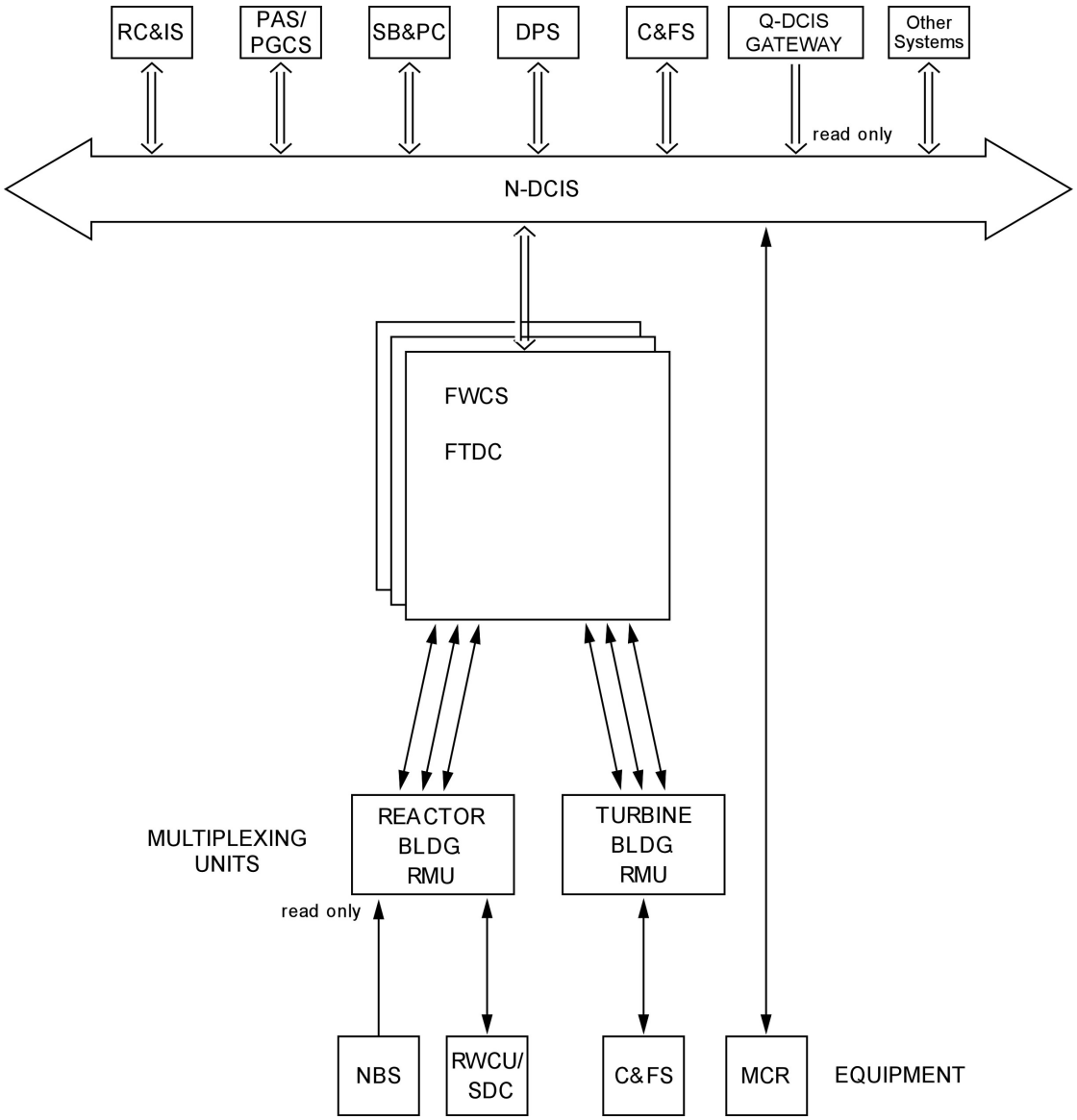


Figure 7.7-3. Feedwater Control System Functional Diagram

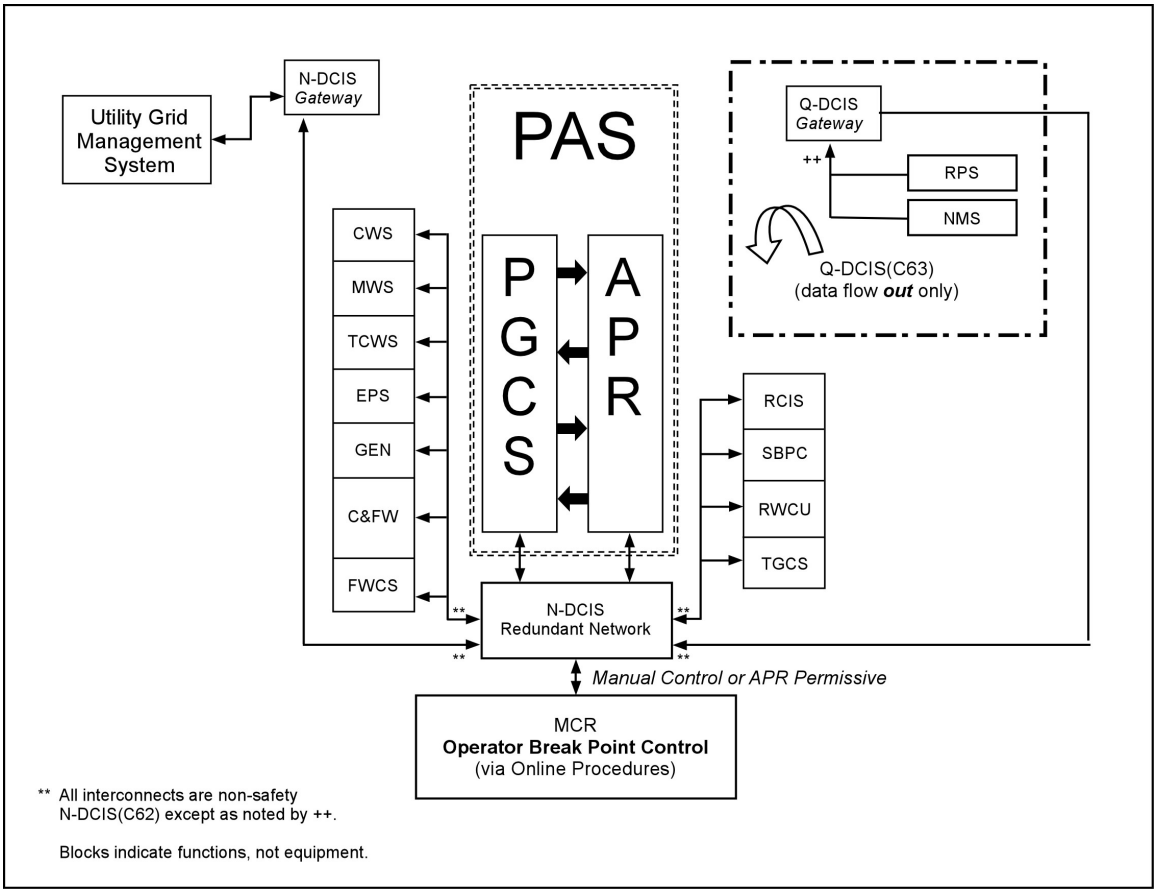


Figure 7.7-4. Plant Automation System Simplified Functional Diagram

(Only major systems are shown)

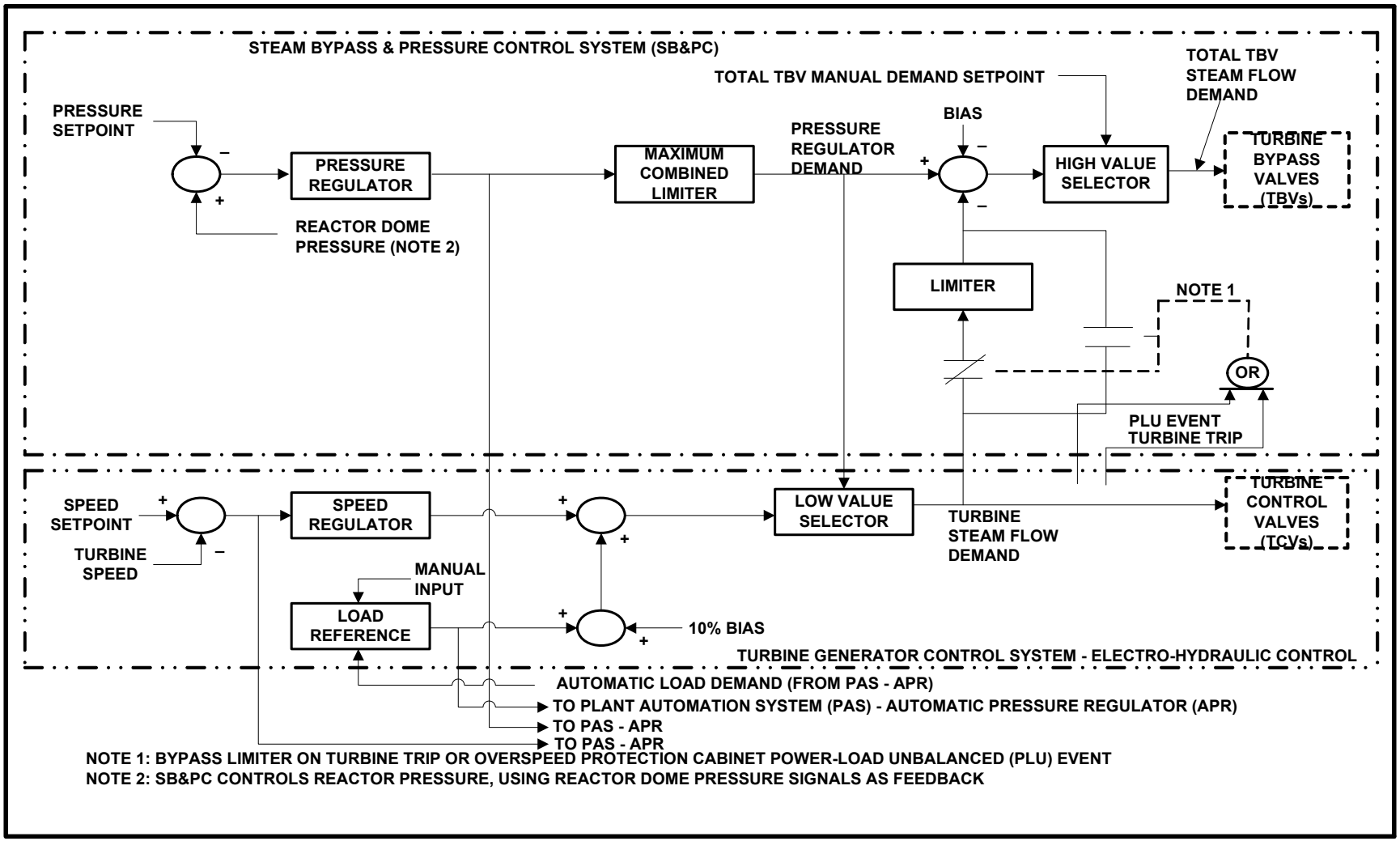


Figure 7.7-5. SB&PC Simplified Functional Block Diagram

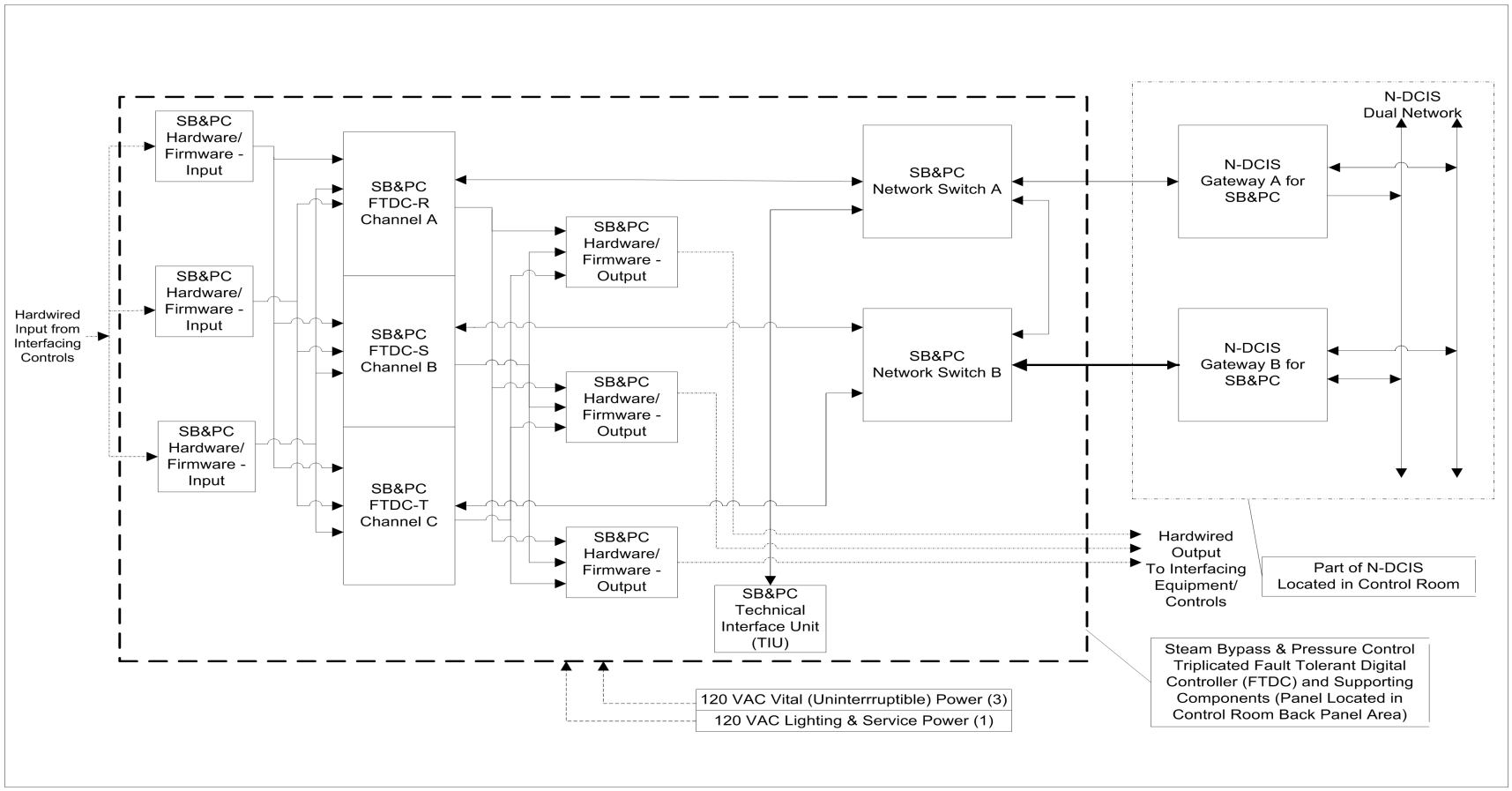


Figure 7.7-6. SB&PC FTDC Block Diagram

7.8 DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS

7.8.1 System Description

The Anticipated Transient Without Scram (ATWS) mitigation system and the Diverse Protection System (DPS) comprise the diverse I&C systems (DICS). The DICS are part of the diversity and defense-in-depth strategy. They provide diverse backup to the Reactor Protection System (RPS) and the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF). The ATWS mitigating logic is designed to meet the diverse shutdown requirements of 10 CFR 50.62, "Requirements For Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants." The ATWS mitigating logic system is implemented with the Safety-Related Distributed Control and Information System (Q-DCIS) and Nonsafety-Related Distributed Control and Information System (N-DCIS).

The nonsafety-related DPS (which is part of the N-DCIS) processes the nonsafety-related portions of the ATWS mitigation logic. It is designed to mitigate the possibility of digital protection system common mode failures discussed in Item II.Q of Commission Paper (Secretary of the Commission, Office of the [NRC]) (SECY) 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs" and Item II.Q of Staff Requirements Memorandum (SRM) on SECY 93-087. Figure 7.8-1 provides a simplified block diagram of the DPS.

The relationships between the ATWS mitigation logic the DPS, the Q-DCIS and the N-DCIS are discussed in Section 7.1. Figure 7.1-1 provides a functional block diagram of the relationship between the Anticipated Transients Without Scram and Standby Liquid Control (ATWS/SLC) and the Q-DCIS, the DPS, and the N-DCIS. Figure 7.1-2 provides a functional network diagram.

The ATWS/SLC mitigation logic provides a diverse means of emergency shutdown using the Standby Liquid Control (SLC) System for soluble boron injection. Alternate Rod Insertion (ARI), which hydraulically scrams the plant using the three sets of air header dump valves of the Control Rod Drive (CRD) System, is also used for ATWS mitigation. This logic is implemented in the DPS. Detailed ATWS mitigation features are described later in this subsection.

The DPS is a nonsafety-related, triple redundant system powered by redundant nonsafety-related load group power sources. The highly reliable, isolated, and independent DPS provides diverse reactor protection using a subset of the RPS scram signals. The DPS provides diverse emergency core cooling by independently actuating the emergency core cooling systems. The DPS performs selected containment isolation functions as part of the diverse Engineered Safety Feature (ESF) function. Additional DPS features are described in Subsection 7.8.1.2. The scope of the DPS functions is based on the diversity and defense-in-depth strategy outlined in Licensing Topical Report (LTR) NEDO-33251, "ESBWR I&C Defense-In-Depth and Diversity Report." (Reference 7.8-1).

Mitigation of common mode failures is provided by the following diverse features:

- Manual scram and Main Steam Isolation Valve (MSIV) isolation by the operator in the Main Control Room (MCR) in response to diverse parameter indications;

- Availability of diverse manual initiation of the passive Emergency Core Cooling System (ECCS) functions including Gravity-Driven Cooling System (GDCS) squib valve initiation, Safety Relief Valve (SRV) initiation, Depressurization Valve (DPV) initiation, Isolation Condenser System (ICS) initiation, and SLC system squib valve initiation. Manual initiation functions are available in the safety-related systems and in the DPS;
- Core makeup water capability from the Feedwater Control System (FWCS), CRD System, and Fuel and Auxiliary Pools Cooling System (FAPCS) in the Low Pressure Coolant Injection (LPCI) mode;
- Long-term shutdown capability in the two redundant Remote Shutdown System (RSS) panels which are equipped with Division 1 and 2 controls for manual scram and MSIV closure, Division 1 and 2 safety-related Video Display Units (VDUs), and a nonsafety-related VDU to allow monitoring and control of all plant systems. Local displays of process variables in the RSS system are continuously powered and are available for monitoring at any time;
- Diverse reactor trip initiation logic, which is different from the safety-related RPS, using separate and independent hardware with diverse software;
- Diverse ESF initiation logic, which is different from the SSLC/ESF, using separate and independent hardware with diverse software;
- ATWS mitigation using liquid boron injection for emergency plant shutdown through the SLC system;
- ATWS mitigation using ARI to hydraulically scram the plant using the three sets of air header dump valves of the CRD system;
- Select Rod Insert (SRI) to hydraulically insert selected control rods; and
- Manual initiation capability of the ATWS mitigation functions (ARI/SLC/Feedwater Runback).

The ATWS/SLC logic mitigates random failures with the divisional sensor channel and/or output trip channel bypass capability. A bypass places the remaining divisions in a two-out-of-three coincident logic condition so that another failure in a remaining division will not disable system operation.

7.8.1.1 Anticipated Transients Without Scram Mitigation Functions

The following ATWS mitigation functions use control logics that are diverse from the primary protection system:

- Automatic SLC system initiation, as shown in Figure 7.8-3. The SLC system is described in Subsection 7.4.1;
- ARI, as shown in Figure 7.8-2 and described in Subsection 7.7.2;

- Fine Motion Control Rod Drive (FMCRD) run-in (or FMCRD Emergency Insertion) associated with the RC&IS, as shown in Figure 7.8-2 and described in Subsection 7.7.2;
- Feedwater runback (FWRB), as shown in Figure 7.8-3 and described in Subsection 7.7.3;
- Inhibition of the Automatic Depressurization System (ADS) and GDCS injection, as described in Subsection 7.8.1.1.2; and
- ARI and diverse scram plus delayed FWRB for events where the RPS scram command has been unsuccessful in shutting down the reactor or when the Selected Control Rod Run-In/Select Rod Insert (SCRRI/SRI) has been unsuccessful in reducing reactor power to an acceptable level, as described in Subsection 7.8.1.1.4.

7.8.1.1.1 ATWS Mitigation Logic Implemented as Safety-Related Logic

The portion of the ATWS mitigation system implemented as safety-related logic is contained within the four divisions of the Reactor Trip and Isolation Function (RTIF) cabinets. The ATWS/SLC logic processing components are separate and diverse from the software-based RPS logic, which is also located in the RTIF cabinets. The RPS is described in Subsection 7.2.1.

ATWS/SLC Analog Trip Modules (ATM), instead of Digital Trip Modules (DTM), perform setpoint comparisons for the automatic trip parameters in each division. Hardware-based discrete digital logic substitutes for software-based trip logic to perform two-out-of-four voting. Therefore, the hardware and software-based logic of this alternate emergency shutdown function is diverse from the hardware and software logic of the RPS function.

7.8.1.1.1.1 Anticipated Transients Without Scram Logic Processors

There is an ATWS logic processor in each of the four divisional RTIF cabinets (Refer to Figure 7.8-3). The ATWS logic processors are separate and diverse from RPS circuitry. Each ATWS logic processor uses discrete programmable logic devices for ATWS mitigation logic processing. The programmable logic devices provide voting logic, control logic, and time delays for evaluating the plant conditions for automatic initiation of SLC boron injection and feedwater runback.

ATWS mitigation functions and trips are described as follows:

- Automatic initiation of the SLC boron injection:
  - High Reactor Pressure Vessel (RPV) dome pressure and a Startup Range Neutron Monitor (SRNM) ATWS permissive (an SRNM signal that is above a specified setpoint) for three minutes or greater; or
  - Low RPV water level (Level 2) and an SRNM ATWS permissive for three minutes or greater.

- Automatic initiation of feedwater runback:
  - High RPV dome pressure and SRNM ATWS permissive. A reset is permitted only when both signals drop below the setpoints. This signal is sent to the DPS for transmission to the FWCS.
- ATWS Mitigation Logic Processor Functions:
  - Performs the two-out-of-four voting function and additional interlock logic using data from ATMs and the Neutron Monitoring System (NMS).
  - Provides isolated hardwired contact closure outputs to SLC system and FWCS, through the DPS.
- ATWS Mitigation Logic Processor Data Handling:
  - Discrete gate logic and hardware timers implement the ATWS mitigation logic. The input signals are hardwired, not multiplexed.
- ATWS Mitigation Logic Processor Status Monitoring and Communication:
  - Programmable logic device in each ATWS mitigation logic division processes the self-test logic. The self-test function is operator initiated and can only be performed with the associated ATWS mitigation logic division bypassed.
  - Fiber optic cables transmit ATWS mitigation logic processor status to external interfaces.
- ATWS Logic Processor Alarms:
  - Instrument Inoperative (INOP) to N-DCIS (operating voltage degraded).
  - Division 1, 2, 3, and 4 ATWS SLC system injection logic tripped.
  - Division 1, 2, 3, and 4 ATWS FWCS runback logic tripped.

Manual initiation capability of the ATWS SLC liquid boron injection is provided in the MCR, with SLC, ARI, and Feedwater runback initiation occurring from the same manual controls.

The actuating signals for the SLC system and FWCS are hardwired, rather than multiplexed, to their respective system controllers. If one of the four ATWS logic processors is inoperable, bypass signals are initiated to bypass the input signals from the out-of-service processor so that the input voting logic changes from two-out-four to two-out-of-three. A manual bypass switch for this function is provided in the MCR.

7.8.1.1.2 ATWS Mitigation Logic to Inhibit the ADS

For ATWS mitigation, the ADS, which is part of the Nuclear Boiler System (NBS), is inhibited automatically. Automatic initiation of ADS is inhibited by the following signals:

- A coincident low RPV water level (Level 2) signal and Average Power Range Monitor (APRM) ATWS permissive signal (i.e., an APRM signal that is above a specified setpoint from the NMS).
- A coincident high RPV pressure and APRM ATWS permissive signal that persists for 60 seconds.

MCR switches manually inhibit the ADS under ATWS conditions. The same inhibit condition applies to the GDCS function.

7.8.1.1.3 DPS ARI ATWS Mitigation Logic

The ARI function of the ATWS mitigation logic is implemented as nonsafety-related logic that is processed by the DPS. The DPS generates the signal to open the ARI air header dump valves in the CRD system based on any of the following command signals:

- High RPV signal, a low RPV water level signal, or a manual ATWS mitigation (ARI/SLC/FWRB initiation) signal;
- RPS scram command;
- SCRRI/SRI command and power levels remaining elevated;
- Manual DPS scram signal;
- On receipt of signals initiating ARI, described above, the DPS generates an additional signal to the Rod Control and Information System (RC&IS) to initiate electrical insertion (that is, FMCRD Run-In) of all operable control; and
- A safety-related manual ATWS mitigation signal initiates the SLC system, ARI and FWCS runback of feedwater flow. It is sent to the nonsafety-related portions of the ATWS mitigation logic through qualified isolation devices.

The ARI and FMCRD Run-In logic resides in the DPS, which is totally separate and independent from the Q-DCIS with diverse hardware and software. The RPV pressure and level input sensors for the ARI logic are independent and separate from the sensors used in the Q-DCIS.

7.8.1.1.4 DPS Scram and SCRRI/SRI ATWS Mitigation Logic

On either SCRRI/SRI command with power remaining elevated (two-out-of-three logic) or RPS scram command (two-out-of-four logic) the DPS will perform the following:

- Initiate a diverse scram (and ARI as indicated previously); and
- Initiate a delayed FWRB if the elevated power levels persist.

For conditions that require SCRRI (processed as two-out-of-three logic) and power levels that remain elevated, the DPS processes an SRI signal to hydraulically scram selected control rods. The DPS will also process an SRI signal if an OPRM trip signal is received from the NMS. It is also possible to initiate SRI and SCRRI manually from the MCR.

7.8.1.2 Diverse Instrumentation and Control

In addition to the ATWS mitigation functions described previously, other DICS functions are included in the DPS.

The DPS has a set of diverse reactor protection and diverse ESF logics that are implemented using hardware and software separate and independent from that of the RPS and SSLC/ESF.

The DPS transmits the feedwater runback signal from the ATWS mitigation logic to the FWCS. The DPS trips the feedwater pumps on high RPV water level (Level 9) after they have been run back to zero flow on high RPV water level (Level 8).

Additionally, the DPS provides diverse monitoring and indication of critical safety functions and process parameters required to support manual operations and assessment of plant status.

7.8.1.2.1 Diverse Reactor Trip Functions

The DPS reactor trip functions provide a diverse means of reactor shutdown and serve as backups to the RPS. A subset of the RPS scram signals is selected for inclusion in the DPS scope, which provides acceptable diverse protection results. This set of diverse protection logics for reactor scram, combined with the ATWS mitigation features, other diverse backup scram protection, and diverse ESF functions provides the necessary diverse protections to meet the required design position. The design position is specified in the SRM on SECY 93-087 and BTP HICB-19 (Referenced in NUREG 0800 Section 7). The following scram signals are selected for inclusion in the DPS::

- High RPV pressure;
- High RPV water level (Level 8);
- Low RPV water level (Level 3);
- High drywell pressure;
- High suppression pool temperature; and
- Closure of the MSIVs.

This diverse set for scram logics resides in hardware and software equipment independent and separate from the RPS. The sensors that provide input are a different set of sensors from those used for the RPS. The diverse logic equipment is nonsafety-related with triple redundant channels processing coincidence logic from four sensor channels.

The power sources of this diverse equipment are from the nonsafety-related load groups. The scram initiation logic is “energize-to-actuate” with the trip signal applied at the return side of the 120 Volts Alternating Current (VAC) circuit for the CRD hydraulic control unit (HCU) scram pilot valve solenoids. The RPS scram initiation signal is applied at the supply side of the 120 VAC circuit.

The trip logic is based on two-out-of-four coincidence logic processed by two-out-of-three triple redundant processors sent through three isolated fiber optic cables to the scram timing panel. A two-out-of-three vote is performed at the scram timing panel to open the solenoid return power switches.

The DPS also provides the ability to initiate a manual scram from either hardwired switches or the DPS VDU.

7.8.1.2.2 Diverse Engineered Safety Features Functions

The ESF functions include core cooling provided by the GDCS and the SLC system and the ADS function using SRVs and DPVs. The pressure relief and core cooling function is also provided by the Isolation Condenser System (ICS). The ESF functions of the GDCS squib valves, SLC system squib valves, ICS, and ADS (SRVs and DPVs) are included in the DPS to provide diverse initiation of emergency core cooling. The initiating logic is based on low RPV water level (Level 1).

The DPS does not provide automatic initiation of the suppression pool equalizing function of the ECCS because it is not required for approximately 30 minutes. Therefore, manual suppression pool equalization capability is provided.

Manual initiation capability is provided in the DPS logic circuitry to initiate the diverse ECCS functions of the GDCS, SLC system, ICS, and ADS (SRVs and DPVs). The DPS also provides the ability to generate diverse manual ECCS actuation from the DPS VDU.

This set of nonsafety-related diverse ESF logics resides in hardware and software equipment separate and independent from the SSLC/ESF system. The process sensors that provide inputs to this diverse set of logics are different from the sensors used in the SSLC/ESF systems. The diverse logic equipment is nonsafety-related with triple redundant channels. The diverse equipment power source is nonsafety-related.

The initiation logic is “energize to actuate” similar to the SSLC/ESF. The diverse ECCS initiation signal is based on two-out-of-four coincidence logic processed by triple redundant processors. If the DPS ECCS initiation signal persists for 10 seconds, the logic seals in and a DPS ECCS start signal is issued. A coincidence logic trip decision is required from two-out-of-three processors to generate the start signal. Redundant output drivers independently process the two-out-of-three voted start signal. A valid initiation signal from both output drivers is required to generate diverse ECCS actuation. Figure 7.8-4 shows the DPS triply modular redundant logic processing.

For the SRV opening function, three of the four SRV solenoids on each SRV are powered by three of the four divisional safety-related power sources in the ESF ADS. A fourth solenoid on each SRV is powered by the nonsafety-related load group, with the trip logic controlled by the DPS. All ten SRVs in the ADS are controlled by the DPS through the fourth solenoid on each valve.

For the DPV opening function, one of the four squib initiators on each DPV is controlled by and connected to the nonsafety-related DPS logic. However, the three squib initiators on all of the

DPVs are controlled simultaneously by the SSLC/ESF ADS logic. The reliability and availability of DPV initiation by the SSLC/ESF ADS function is not affected by the DPS logic. The typical ADS initiation logic arrangements applied in both the SSLC/ESF and DPS functions are illustrated in Figure 7.3-1a and Figure 7.3-1b. As shown in Figure 7.3-1a and Figure 7.3-1b, the logic contact circuit from the DPS is arranged in parallel with the SSLC/ESF circuit.

As described in Subsections 7.3.1 and 7.3.5, it takes three simultaneous SSLC/ESF trip signals to initiate the DPV squib valve opening. It also takes three simultaneous DPS trip signals in a triply redundant logic path to initiate the DPV squib valve opening. This satisfies the single failure criterion for inadvertent squib valve initiation. With this arrangement, the initiation of the DPVs by DPS logic does not affect the reliability and availability of the DPV initiation function controlled by the SSLC/ESF logic.

The logic application to the GDCS squib valves from the SSLC/ESF and from the DPS is similar to that of the DPV logic application described above. Short term injection of the GDCS squib valves can be initiated both by the SSLC/ESF logic and by the DPS logic. For the GDCS squib valve-opening function, one of the four squib initiators on each GDCS valve is controlled by and connected to the nonsafety-related DPS logic. The DPS logic has a dual redundant logic path that requires two simultaneous GDCS trip initiation signals to initiate a GDCS squib valve opening.

The logic application to the SLC system squib valves from the SSLC/ESF and from the DPS is similar to that of the DPV logic application described above, except that there is a dual instead of a triple logic path. However, the SLC system squib valves are actuated by two independent safety-related divisions with one valve per loop that is also actuated by the DPS. This configuration allows the flow path of both SLC system loops to be available through activation from the DPS and from any safety-related division (Refer to Subsection 7.4.1 for a description of the SLC system).

The ICS logic is configured to allow the availability of each ICS loop flow path from the four safety-related divisions and the DPS.

The DPS also provides the following major isolations using two-out-of-four sensor logic and two-out-of-three processing logic. The isolation functions performed as part of the diverse ESF are “energize to actuate.”

- Closure of the MSIVs on detection of high steam flow, low RPV pressure, or low RPV water level (Level 2). The isolation function is performed by contacts in the 120 VAC MSIV solenoid return circuit. The logic is enabled when the reactor is in Run mode;
- Closure of the ICS isolation valves on high steam flow or excessive condensate flow;
- Closure of the Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC) isolation valves on high differential flow; and
- Isolation of the FWCS on a feedwater line break inside containment. The line break is sensed by differential pressure between feedwater lines coincident with high drywell pressure. The DPS trips the main feedwater pump adjustable speed drive motor circuit breakers and closes the feedwater containment isolation valves.

The following additional functions are performed by the DPS:

- With logic similar to the SSLC/ESF, the DPS initiates the ICS on low RPV water level (Level 2) or MSIV closure to provide core cooling.
- The DPS runs back the feedwater pumps on high RPV water level (Level 8). If the water level continues to increase, the DPS trips the feedwater pumps (Level 9).

The diverse protection logics for ESF function initiation, in combination with the ATWS mitigation feature, other diverse backup scram protection, and selected diverse RPS logics provides the diverse protection necessary to satisfy the design position specified in BTP HICB-19.

7.8.1.3 Diverse Manual Controls and Displays

All safety-related systems have displays and controls located in the MCR that provide manual system-level actuation of their safety-related functions and monitoring of parameters that support those safety-related functions.

In addition to the manual controls and displays for the safety-related reactor protection and SSLC/ESF functions, the DPS also has displays and manual control functions that are independent from those of the safety-related protection and SSLC/ESF functions. They are not subject to the same common mode failure as the safety-related protection system components. The manual controls include the manual initiation of the SRV, DPV, GDCS, and SLC system valves, and the ICS.

The operator is provided with a set of diverse displays separate from those supplied through the safety-related software platform. The displays listed below provide independent confirmation of the status of major process parameters:

- Reactor pressure,
- Reactor pressure high alarm,
- Reactor water level,
- Reactor water level high alarm,
- Reactor water level low alarm,
- Drywell pressure,
- Drywell pressure high alarm,
- Suppression pool temperature,
- Suppression pool temperature high alarm,
- SRV solenoid-controlled valves opening,
- DPV squib-initiation valves opening,

- GDCS squib-initiation valves opening,
- SLC system squib injection valves opening, and
- ICS operation.

In addition to the controls provided by the primary safety-related systems, the RSS provides manual control of shutdown cooling functions and continuous local display of monitored process parameters.

7.8.2 Common Mode Failure Defenses Within Safety-Related System Design

7.8.2.1 Design Techniques for Optimizing Safety-Related Hardware and Software

In addition to the DPS, other techniques ensure safety-related system reliability by minimizing both random and common mode failure probabilities. They are outlined below:

- The total amount of hardware is minimized;
- Microprocessors with a simple operating system are used;
- High quality components are used;
- Self-diagnostics are implemented;
- The man-machine interface is implemented so that the equipment is structured into small units with sufficient diagnostics that a user can repair equipment by replacing modules and can operate the equipment by following straightforward instructions;
- The software design process specifies modular code;
- Software modules have one entry and one exit point and are written using a limited number of program constructs;
- Code is segmented by system and function:
  - Program code for each safety-related system resides in independent modules that perform setpoint comparison, voting, and interlock logic;
  - Code for calibration, signal Input / Output (I/O), online-diagnostics, and graphical displays are common to all systems;
  - Fixed message formats are used for plant sensor data, equipment activation data, and diagnostic data. Thus, corrupted messages are readily detected by error-detecting software in each digital instrument;
- Software design uses recognized defensive programming techniques, backed up by self-diagnostic software and hardware watchdog timers;
- Software for control programs is permanently embedded as firmware in controller Read Only Memory (ROM);

- Commercial development tools and languages with a known history of successful applications in similar designs are used for software development;
- Automated software tools aid in verification and validation (V&V), and

Reliable software is implemented by ensuring that the quality of the design and requirements specification is controlled under the formal V&V program which is discussed in the LTR "ESBWR I&C Software Quality Assurance Plan (SQAP)," NEDO-33245, NEDE-33245P. Reference 7.8-3.)

7.8.2.2 Defense Against Common Mode Failure

In addition to the DPS and the ATWS mitigation features, safety-related logic processing systems used in the RPS and SSLC/ESF perform the following simple and repetitive tasks. These tasks are performed continuously and simultaneously in four independent and redundant divisions of logic:

- Setpoint comparison;
- Two-out-of-four voting logic processing;
- Control and interlock logic processing;
- I/O signal processing; and
- Self-testing.

The development of common software modules for many of these functions provides the following advantages:

- Produces reliable programs:
- Promotes standardization and code reusability;
- Minimizes program design errors; and
- Minimizes timing differences among channels.

The V&V program reduces the probability of common mode failure to a very low level. The simple modules used in each division can be thoroughly tested during the validation process. In addition to software V&V, the RPS and SSLC/ESF contain system level and functional level defenses against common mode failure, including defenses within the software itself.

7.8.2.2.1 System Level Defenses

Operational defenses:

- Asynchronous operation of multiple protection divisions. Timing signals are not exchanged among divisions;

- Automatic error checking on all multiplexed transmission paths. Only the last good data is used for logic processing. If a permanent fault is detected, the channel alarms and a trip is initiated for the RPS and MSIV isolation functions;
- Continuous cross-checking of redundant sensor inputs;
- Continuous on-line surveillance of trip functions with divisional bypass capability for the RPS and MSIV isolation functions; and
- Continuous self-test with alarm outputs in all system devices.

Functional defenses:

- Automatic error detection. This permits early safe shutdown or bypass before common mode effects occur. Instantaneous, simultaneous, and undetected failure on a common mode error is unlikely; and
- Separation and independence requirements that protect against global effects resulting from such factors as EMI and thermal conditions.

Software defenses:

The functional program logic in the RPS and SSLC/ESF controllers provides protection against common mode failures, as follows:

- Redundant sensors. Data messages from the sensors have unique identifications in each division;
- Identical modules that provide simple, readily verifiable functions such as setpoint comparison and two-out-of-four; and
- Use of standard protocols for multiplexing and other data transmission functions that are verified to industry standards and are also qualified to safety-related standards.

7.8.3 Safety Evaluation

The DPS is designed as a highly reliable nonsafety-related system that meets the probabilistic risk assessment requirements to minimize failures on demand and to minimize inadvertent operation. The DPS components are designed to ensure that reliability goals and system design requirements are met. The sensors and actuation devices that interface directly with safety-related systems, structures and components (SSCs) are qualified to meet seismic category I classification (IEEE Std. 603, Section 5.4).

Consistent with the guidance in IEEE Std. 603, Section 5.6 and IEEE Std. 384, the nonsafety-related DPS is designed to avoid adverse interaction with the protection systems with which DPS interfaces. Because the DPS logic does not communicate with the RPS logic, credible DPS failure modes do not prevent the RPS from performing a reactor trip. The DPS cannot cause the RPS to initiate a reactor trip prematurely. Credible DPS failure modes cannot prevent the SSLC/ESF actuation system from initiating ECCS functions and/or performing barrier isolation

functions. Additionally, credible failure modes cannot result in premature operation of these protection systems.

The ATWS/SLC logic is designed to mitigate a failure of the normal reactor trip system to function and is diverse from and independent of the Reactor Protection System (RPS). The ATWS/SLC logic platform is designed as a safety-related system with four independent divisions powered from divisionally separated safety-related power sources. Each redundant division of ATWS/SLC logic, which uses two-out-of-four voting logic, is capable of performing ATWS mitigation during reactor operation.

Table 7.1-1 identifies the DICS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses conformance with regulatory requirements, guidelines, and industry standards.

7.8.3.1 Code of Federal Regulations

10 CFR 55a(a)(1), Quality Standards:

- Conformance: The diverse I&C systems are in conformance with this requirement.

10 CFR 50.55a(h), Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: For the diverse I&C systems, the applicable requirements are from IEEE Std. 603, Section 5.6, 'Independence'. The transmission of signals between the divisional equipment of protection system (that is, RPS and SSLC/ESF) or between the ATWS/SLC. The transmission of signals between the equipment of the protection systems or between the equipment of ATWS/SLC and the nonsafety related control systems, including the DPS, is performed via fiber optic cables. The electrical to optical interface provides the required isolation.

  The diverse I&C have electrical surge withstand capability and can withstand the electromagnetic interference, radio frequency, and electrostatic discharge conditions that exist where the diverse I&C equipment is located in the plant.

  The diverse I&C equipment withstands the room ambient temperature, humidity conditions, radiation levels, and seismic accelerations that exist at their locations at the times for which it is required to be operational or required to fail in a safe mode.

10 CFR 50.62, Requirements for reduction of risk from ATWS events for light-water cooled nuclear power plants:

- Conformance: The ATWS mitigation functions described in Subsection 7.8.1.1 are designed in accordance with the requirements of 10 CFR 50.62.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications:

- Conformance: ITAACs are provided for the diverse I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47(a)(2), Level of Detail:

- Conformance: The level of detail provided for the diverse I&C functions within the DCD conforms with this requirement.

7.8.3.2 General Design Criteria

General Design Criteria (GDC) 1, 13, 19, and 24:

- Conformance: The diverse I&C are in conformance with the GDC identified above.

The design of the diverse I&C does not compromise the ability of the RPS and SSLC/ESF actuation system to meet the requirements of 10 CFR 50 Appendix A, "General Design Criteria for Nuclear Power Plants," Section III, "Protection and Reactivity Control Systems."

7.8.3.3 Staff Requirements Memorandum

Item II.Q (Defense Against Common-Mode Failures in Digital Instrument and Control Systems) of SECY-93-087 and SRM on SECY 93-087 (Policy, Technical, and Licensing Issues Pertaining to Evolutionary and ALWR Designs):

- Conformance: The SRM requirements applicable to the diverse I&C functions state that, “If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure as the safety system shall be required to perform either the same function as the safety system function that is vulnerable to common mode failure or a different function.” It also states, “The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary functions under the associated event conditions.” With respect to manual control and display functions, it states, “A set of displays and controls located in the main control room shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer systems.”

  The implementation of the DPS and the ATWS mitigation features as described in Subsection 7.8.1, in conjunction with the RPS and ESF designs, conforms with the above SRM requirements.

7.8.3.4 Regulatory Guides

RG 1.22 – (Safety Guide 22) Periodic Testing of Protection System Actuation Functions:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.22. This RG is not applicable to the nonsafety-related DPS.

RG 1.62 - Manual Initiation of Protection Actions:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.62. This RG is not applicable to the nonsafety-related DPS.

RG 1.75 - Physical Independence of Electric Systems:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.75. This RG is not applicable to the nonsafety-related DPS.

RG 1.105 - Instrument Setpoints for Safety Systems:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.105. This RG is not applicable to the nonsafety-related DPS.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.118. This RG is not applicable to the nonsafety-related DPS.

RG 1.151 – Instrument Sensing Lines:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.151. This RG is not applicable to the nonsafety-related DPS.

RG 1.152 – Criteria for Digital Computers in Safety Systems of Nuclear Power Plants:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.152. This RG is not applicable to the nonsafety-related DPS.

RG 1.153 – Criteria Power Instrumentation and Control Portions of Safety Systems.

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.153. This RG is not applicable to the nonsafety-related DPS.

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

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.168. This RG is not applicable to the nonsafety-related DPS.

RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.169. This RG is not applicable to the nonsafety-related DPS.

RG 1.170 - Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.170. This RG is not applicable to the nonsafety-related DPS.

RG 1.171 - Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.171. This RG is not applicable to the nonsafety-related DPS.

RG 1.172 - Software Requirements Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.172. This RG is not applicable to the nonsafety-related DPS.

RG 1.173 - Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.173. This RG is not applicable to the nonsafety-related DPS.

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in RG 1.180. This RG is not applicable to the nonsafety-related DPS.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The design conforms with the guidance provided in this RG.

7.8.3.5 Branch Technical Position

BTP HICB-8 - Guidance on Application of RG 1.22:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in HICB-8. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-11 - Application and Qualification of Isolation Devices:

- Conformance: The diverse I&C conforms with this BTP.

BTP HICB-12 - Establishing and Maintaining Instrument Setpoints:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in HICB-12. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-14 - Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in HICB-14. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-16 - Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail for the diverse I&C systems conforms with this BTP.

BTP HICB-17 - Self-Test and Surveillance Test for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in HICB-17. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-18 - Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in HICB-18. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-19 – Guidance for evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems:

- Conformance: Reference 7.8-1 details the echelons of defense used in the design. This document also discusses the basis for selection of the DPS functions used as backups for the RPS and SSLC/ESF. A failure modes and effects analysis based on the Guidance in NUREG/CR-6303 (Reference 7.8-2) is performed to ensure the radiation guidelines from 10 CFR 100 are not exceeded in the event of a common mode failure of the RPS or SSLC/ESF software platform during the design basis events discussed in the Safety Analyses.

BTP HICB-21 - Guidance on Digital System Real-Time Performance:

- Conformance: The safety-related ATWS mitigation logic conforms with the guidance in HICB-21. This BTP is not applicable to the nonsafety-related DPS.

7.8.4 Testing and Inspection Requirements

A periodic test to verify proper operation of the ATWS/SLC logic is performed. A periodic test to verify proper operation of the DPS logic is also performed.

7.8.5 Instrumentation and Control Requirements

The ATWS/SLC uses logic that is diverse from the RPS. Logic and controls for ATWS/SLC are located in divisional RTIF cabinets. Operating status is available to the operator in the MCR. Division of sensors bypass capability is provided for the ATWS/SLC logic. Communication to external interfaces is through isolation devices. Provisions are made to allow testing of the ATWS/SLC logic and maintenance of the ATWS/SLC equipment.

The DPS uses triple redundant microprocessor-based automatic actuation logic that is diverse from the RPS and SSLC/ESF automatic actuation logic.

The information available to the operator from the diverse I&C system is described in Subsection 7.8.1.3.

7.8.6 COL Information

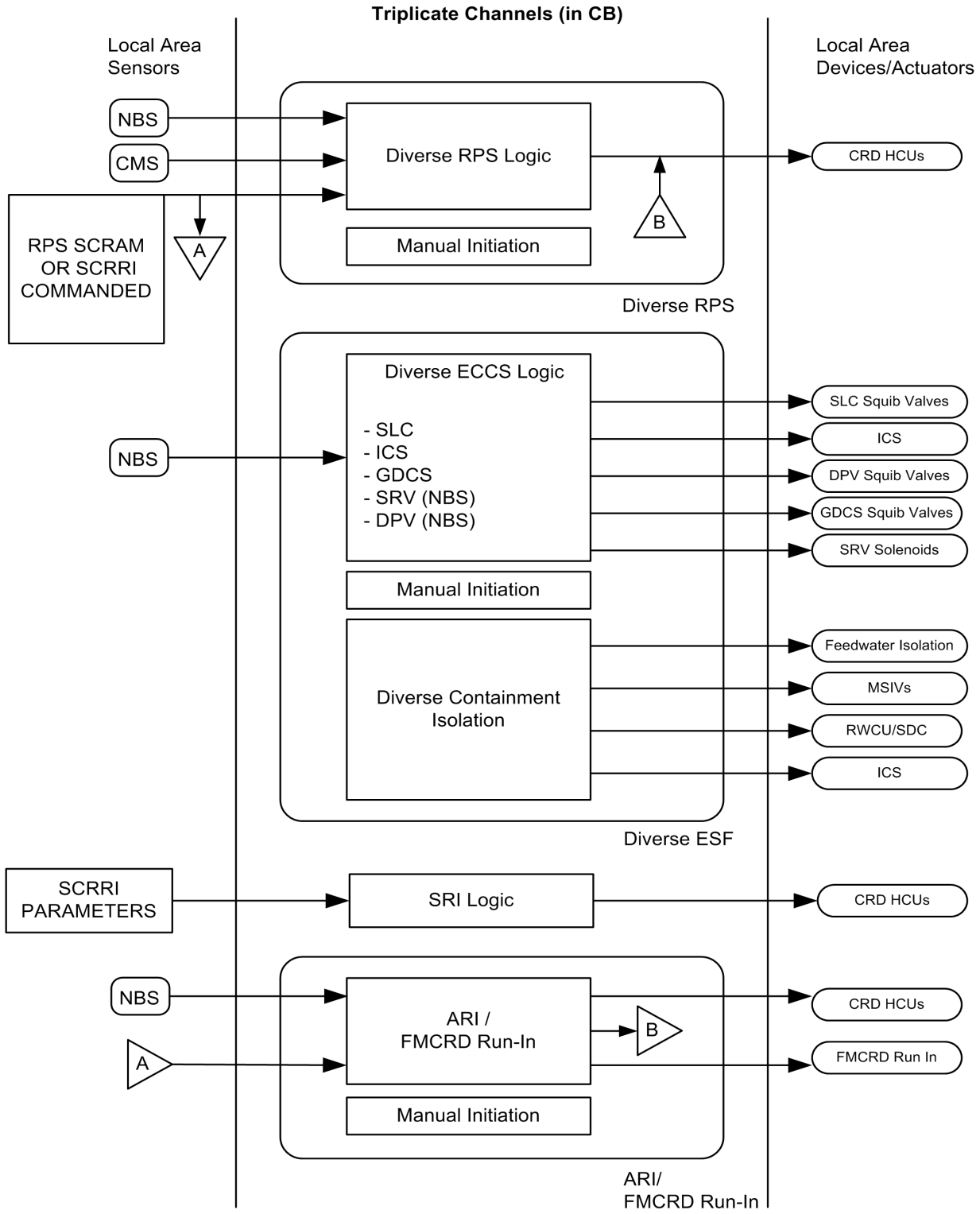
None

7.8.7 References

7.8-1 GE Nuclear Energy, "ESBWR I&C Defense-In-Depth and Diversity Report", NEDO-33251, Class I (Non-proprietary), Revision 0, July 2006.

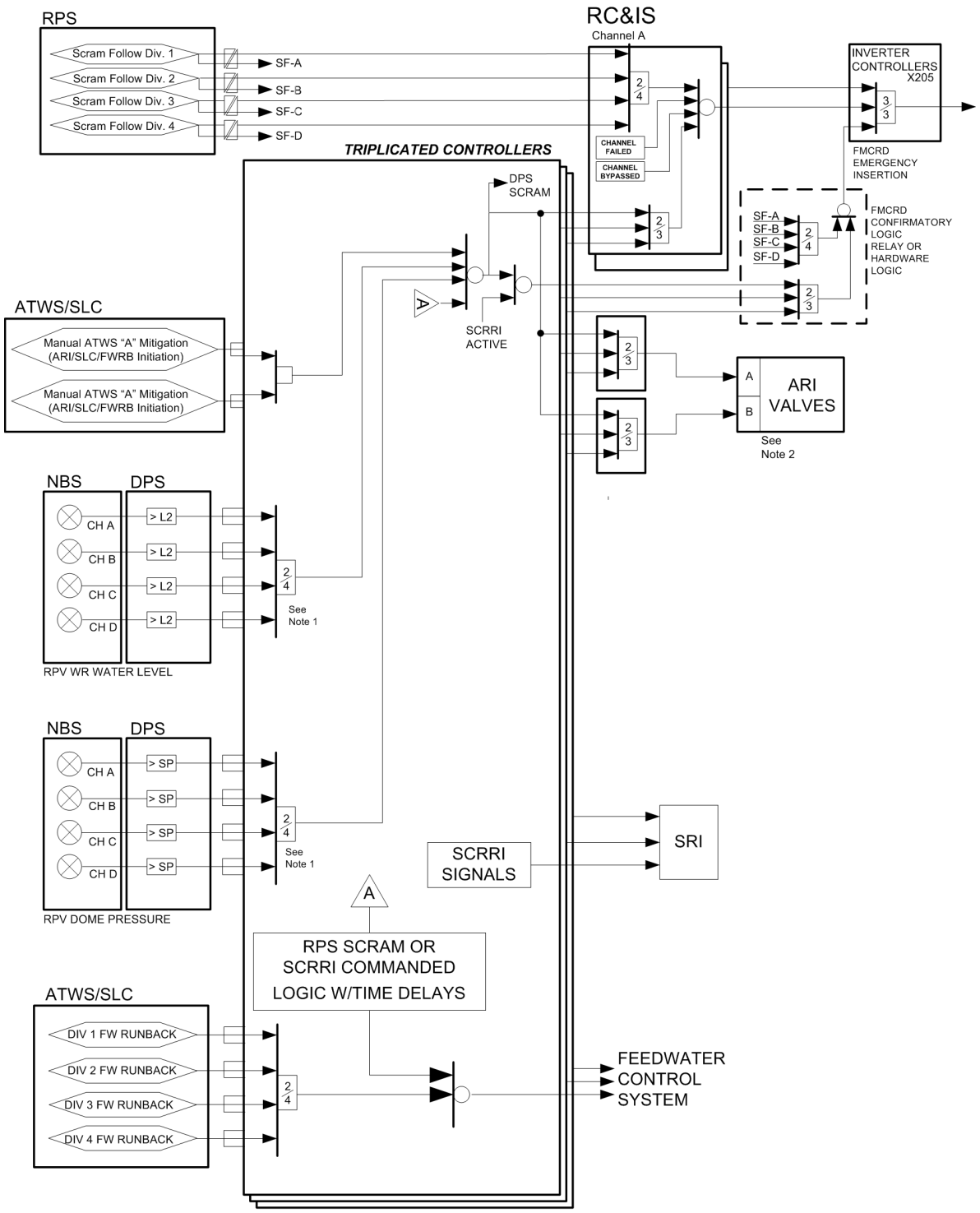
7.8-2 NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, December 1994

7.8-3 GE Nuclear Energy, "ESBWR I&C Software Quality Assurance Plan (SQAP)," NEDO-33245, Class I (Non-proprietary); and "ESBWR I&C Software Quality Assurance Plan (SQAP)," NEDE-33245P, Class III (Proprietary), Revision 2, July 2007.



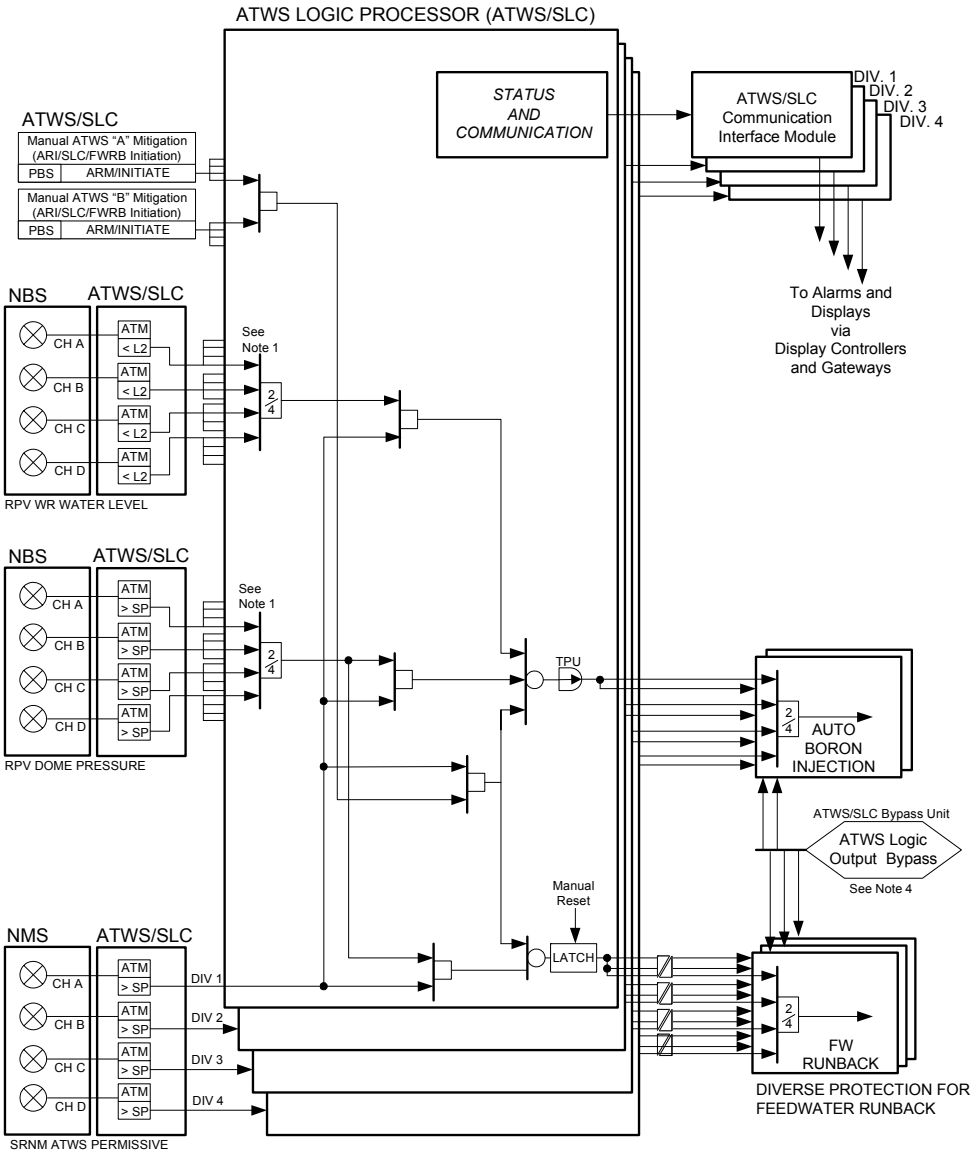
NOTE:
LOCAL AREA SENSORS FOR CONTAINMENT ISOLATION FUNCTIONS NOT SHOWN.

Figure 7.8-1. Simplified DPS Block Diagram



Note:
1. Comparison is part of ARI logic
2. The ARI valves are part of CRD System
3. Both manual pushbutton switches armed to initiate
4. Nonsafety-related sensors from NBS

Figure 7.8-2. ARI & FMCRD Run-In Logic



NOTES:
1. DIVISION-OF-SENSORS BYPASS INPUTS AND LOGIC NOT SHOWN.

2. THE ATWS LOGIC PROCESSOR SHALL INCLUDE DIVISION-OF-SENSORS BYPASS EXCLUSIONARY LOGIC THAT RESULTS IN A "NO BYPASS" CONDITION FOR ALL DIVISIONS IF TWO OR MORE BYPASS INPUTS ARE RECEIVED.

3. THE ATWS LOGIC PROCESSOR SHALL INCLUDE DIVISION-OF-SENSORS BYPASS LOGIC THAT BYPASSES TRIP INPUTS FROM ALL SENSORS IN ONE DIVISION WHEN DIVISION-OF-SENSORS FOR THAT DIVISION IS PRESENT.

4. SEE ATWS/SLC LOGIC DIAGRAM FOR ATWS OUTPUT BYPASS LOGIC.

5. SLC FUNCTIONS IN ATM NOT SHOWN. SEE SLC LOGIC DIAGRAM.

Figure 7.8-3. ATWS Mitigation Logic (SLC System Initiation, Feedwater Runback)

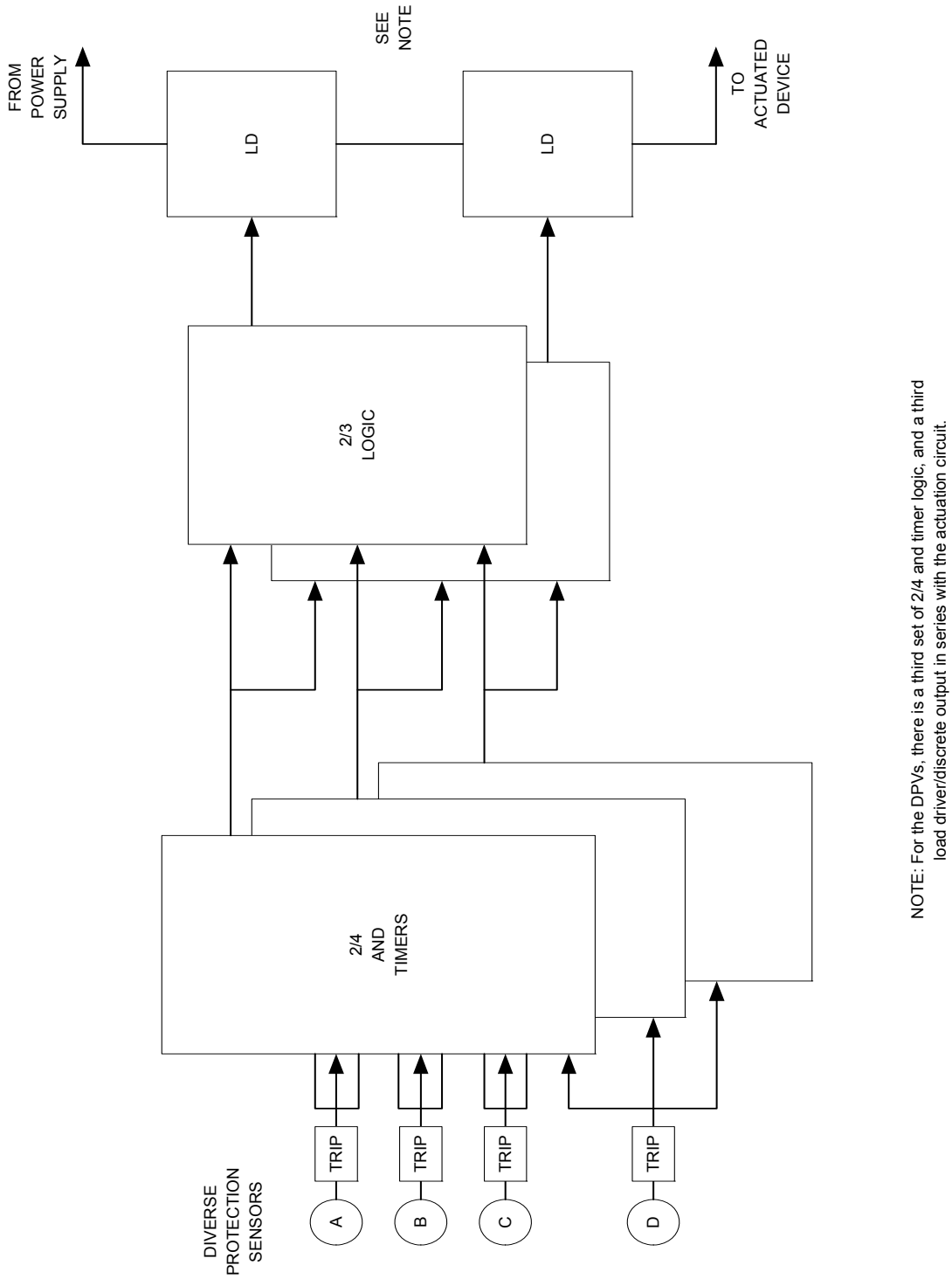


Figure 7.8-4. Diverse ESF Triple Redundant Logic

7.9 DATA COMMUNICATION SYSTEMS - DELETED

Section 7.9 is deleted, and Data Communications is discussed in Section 7.1 as part of the overall DCIS functions.

7A. AUTOMATED FIXED IN-CORE PROBE SUBSYSTEM FOR THE NEUTRON MONITORING SYSTEM - DELETED

7B. SOFTWARE QUALITY PROGRAM FOR SOFTWARE DESIGN AND DEVELOPMENT – DELETED

Appendix 7B was deleted, and Software Quality Program for Software Design and Development is discussed in the following two Licensing Topical Reports:

(1) ESBWR I&C Software Management Plan, NEDO-33226 NEDE-33226P; and

(2) ESBWR I&C Software Quality Assurance Plan, NEDO-33245 NEDE-33245P.

Table 7B-1

Software Requirements Specification – (Deleted)

Table 7B-2

Software Architecture Description– (Deleted)

Table 7B-3

Software Design Specification– (Deleted)

Table 7B-4

Software Source Code Listings– (Deleted)

Table 7B-5

System Build Documents– (Deleted)

Table 7B-6

Installation Configuration Tables– (Deleted)

Table 7B-7

Operations-Maintenance Manuals– (Deleted)

Table 7B-8

Training Manuals– (Deleted)