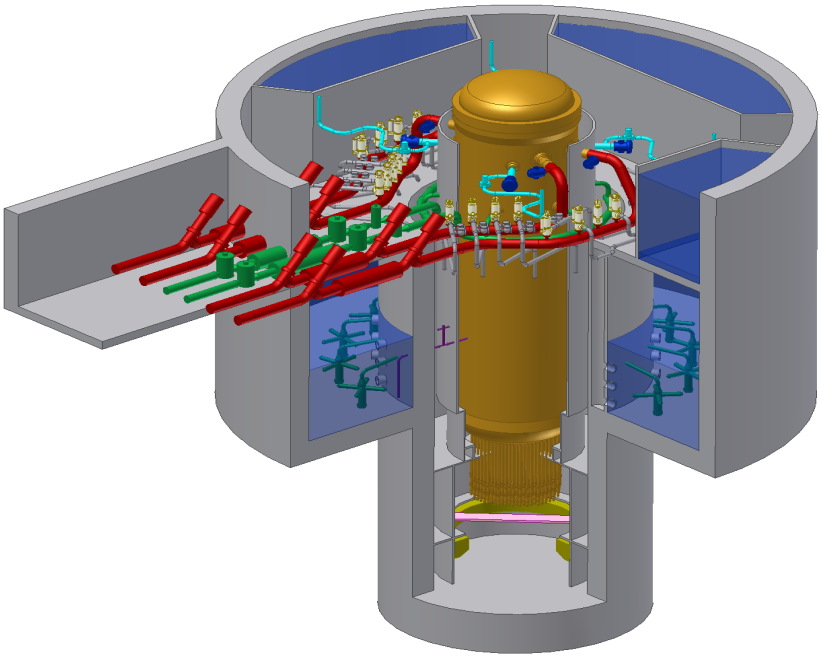
GE Energy Nuclear

26A6642AW
Revision 3
February 2007



ESBWR Design Control Document

Tier 2

Chapter 7

Instrumentation And Control Systems

Contents

List of Tables

List of Illustrations

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 / 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 Proceudres
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
C/C	
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
CRDS	Control Rod Drive System
CRHA	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/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	Electro-magentic Compatibility
EMI	Electro-Magnetic Interference
EOF	Emergency Operations Facility
EOP	Emergency Operating Procedures
EPDS	Electric Power Distribution System
EPG	Emergency Procedures Guidelines
EPRI	Electric Power Research Institute

Abbreviations And Acronyms List

Term	Definition
ERDS	Emergency Response Data System
ERICP	Emergency Rod Insertion Control Panel
ERIP	Emergency Rod Insertion Panel
ESBWR	Enhanced Simple Boiling Water Reactor
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
GENE	General Electric Nuclear Engineering
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
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
ICS	Isolation Condenser System
IEEE	Institute of Electrical and Electronic Engineers

Abbreviations And Acronyms List

Term	Definition
ILRT	Integrated Leak Rate Test
IMC	Induction Motor Controller
IMCC	Induction Motor Controller Cabinet
IP	Implementation Plan
ISA	Instrument Society of America
ISO	International Standards Organization
ITAAC	Inspections, Tests, Analyses and Acceptance Criteria
ITS	Issue Tracking System
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
NBS	Nuclear Boiler System
NDL	Nuclear Data Link
N-DCIS	Nonsafety-related Distributed Control and Information System
NMS	Neutron Monitoring System

Abbreviations And Acronyms List

Term	Definition
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
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
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

Abbreviations And Acronyms List

Term	Definition
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
RPS/RTIF	Reactor Protection System/Reactor Trip and Isolation Function(s)
RPV	Reactor Pressure Vessel System
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	Reactore 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
SBO	Station Blackout
SCM	Software Configuration Management
SCMP	Software Configuration Management Plan
SCRRI	Selected Control Rod Run-in
SCWS	Stator Cooling Water System

Abbreviations And Acronyms List

Term	Definition
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	Source Range Monitor
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
TAF	Top of Active Fuel
TASS	Turbine Auxiliary Steam System
TBS	Turbine Bypass System
TBV	Turbine Bypass Valve
TCCWS	Turbine Component Cooling Water System

Abbreviations And Acronyms List

Term	Definition
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/VAC	Volts Alternating Current
Vdc/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, which are significant for plant operation and are utilized throughout the plant. I&C systems are designated as either safety-related or nonsafety-related. 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 ESBWR Distributed Control and Information System (DCIS):

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

7.1.1 ESBWR Distributed Control And Information System

The ESBWR DCIS is an arrangement of I&C networked components and individual systems that provide processing and logic capability, remote and local data acquisition, gateways/datalinks between systems and components, operator monitoring and control interfaces, firewalls to external computer systems and networks, alarming and archiving functions and communications between the systems.

A simplified functional block diagram of the ESBWR I&C is shown in Figure 7.1-1. The ESBWR DCIS is subdivided into the safety-related DCIS (Q-DCIS) and the nonsafety-related DCIS (N-DCIS). The ESBWR data communication systems are embedded in the ESBWR DCIS that performs the data communication functions that are part of or support the systems described in Sections 7.2 through 7.8. A functional network diagram of the ESBWR DCIS appears as

Figure 7.1-2, which is a functional representation of the current design. The final DCIS design may alter equipment locations and actual hardware components depending on the chosen DCIS vendors.

Q-DCIS and N-DCIS architectures, their relationships, and their acceptance criteria are further described in this section.

Both 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 that are fully discussed in Reference 7.1-4 which is the Licensing Topical Report (LTR) entitled, "ESBWR I&C Defense-In-Depth And Diversity Report", NEDO-33251.

Q-DCIS and N-DCIS will be designed and developed in accordance with Appendix 7B, which describes the software quality program for DCIS and addresses the NRC review guidance described in the SRP.

7.1.2 Q-DCIS General Description Summary

Q-DCIS comprises the safety-related portion of the ESBWR DCIS, which performs the safety-related control and monitoring functions. 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 systems and functions are:

- Reactor Protection System (RPS) which includes Reference Section 7.2.1:
  - Reactor Trip Functions
  - Main Steam Isolation Valve (MSIV) Functions of the Leak Detection And Isolation System (LD&IS)
  - Anticipated Transient Without Scram (ATWS)/Standby Liquid Control (SLC) Functions
- Neutron Monitoring System (NMS) which includes (Reference Section 7.2.1.3):
  - Startup Range Neutron Monitor (SRNM) Functions
  - Power Range Neutron Monitor (PRNM) Functions
    i. Local Power Range Monitor (LPRM) Functions
    ii. Average Power Range Monitor (APRM) Functions
    iii. Oscillation Power Range Monitor (OPRM) Functions
- Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) System which includes Reference Section 7.3.5:
  - Emergency Core Cooling System (ECCS) Functions
    iv. Automatic Depressurization System (ADS) Functions

v. Gravity-Driven Cooling System (GDCS) Functions

vi. Isolation Condenser System (ICS) Functions

vii. Standby Liquid Control (SLC) System Functions

– Leak Detection And Isolation System (LD&IS) Functions (except the Main Steam Isolation Valves [MSIVs] Functions)

– Control Room Habitability System (CRHS) Functions

The Q-DCIS major components include:

- A fiber and hard wired 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)
- Cabinets for housing devices such as power supplies

Q-DCIS provides most of the interface functions for the RPS, NMS, and SSLC/ESF protection systems, such as 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 Q-DCIS is electrically isolated from other Q-DCIS divisions and N-DCIS. Data communication is controlled between Q-DCIS divisions and between Q-DCIS and N-DCIS. Communication between Q-DCIS divisions and between Q-DCIS and N-DCIS is always by optical fiber. Data communication between Q-DCIS and N-DCIS is managed by isolation devices, which are safety-related components within Q-DCIS and nonsafety-related N-DCIS gateways/datalinks. The RPS, NMS, and SSLC/ESF protection systems are designed such that no safety-related function depends on any nonsafety-related component, data, or communication channel.

Q-DCIS uses RMUs for data acquisition for the RPS, NMS, and SSLC/ESF protection systems and provides for safety-related displays in the MCR and Remote Shutdown System (RSS). These units may be distributed (within the division) or actually reside in specific chassis and may 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 status is monitored on divisional Q-DCIS safety-related VDUs, which are connected to the SSLC/ESF. The RPS and NMS process data is 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 even during 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 for manual control and data display for the RPS, NMS, and SSLC/ESF safety-related systems in a Human Factors Engineering (HFE) approved format.

Q-DCIS components, outside the MCR, are located in physically separate DCIS divisional rooms or compartments in the reactor and control buildings that have appropriate fire barriers between them.

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. After 72 hours, Q-DCIS can operate continuously on power from either of the two ESBWR diesel generators or off-site power. Refer to Subsection 8.1.5.2.1 for additional information.

Finally Q-DCIS provides self-diagnostics that monitor communication, power and processors to the replacement 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 Q-DCIS are found in IEEE Std. 603, Sections 4.1, 4.2, 4.5, 4.8, and 4.10 and specifically address reading signals; performing signal conditioning; transmitting data signals and commands; performing safety-related logic independently; providing alarms; and isolating data communication.

7.1.2.2 Q-DCIS Power Generation Design Bases Summary

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

7.1.2.3 Q-DCIS Safety Evaluation Summary

The safety evaluation for Q-DCIS includes the following:

Q-DCIS conforms with IEEE Std. 603. The Licensing Topical Report (LTR), “ESBWR Safety Criteria for Instrumentation & Control Systems,” (Reference 7.1-5) will describe the methods by

which each safety-related system and its platform is expected to meet IEEE Std. 603 criteria. This report will provide the design bases and conformance criteria as they apply to the safety-related I&C associated with the ESBWR. The criteria contained in this report will establish the minimum functional and design requirements for power and I&C portions of the safety-related systems for the ESBWR design. The safety-related systems criteria contained in this report will be applied to those safety-related systems required to protect the public health and safety by functioning to prevent or mitigate the consequences of design basis events. Refer to Reference 7.1-6 and Reference 7.1-7.

The Q-DCIS is arranged into four divisions. The intra-divisional and safety-related to nonsafety-related fiber communication paths are redundant both to support reliability and to allow self-diagnostics to be communicated in the presence of a single failure. Safety-related cabinets and chassis are redundantly and uninterruptedly powered for both reliability and self-diagnostics. For safety-related to safety-related communication, there is no single communication or power failure that will result in the loss of a safety-related function; a dual communication or power failure may result in the loss of a single division but not in the loss of an ESBWR safety-related function. The ESBWR is being designed such that a two division failure (which requires four communications or power failures), does not result in the loss of an ESBWR safety-related function.

7.1.2.4 Q-DCIS Regulatory Requirements Conformance Summary

Q-DCIS conforms with the following regulations and standards:

- 10 CFR 50.34, 10 CFR 50.55, 10 CFR 50.62, 10 CFR 52.47, 10 CFR 52.79
- 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, 1074
- ANSI/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 Memoranda (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, 3, 6, 8, 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, and 21.

Table 7.1-1 identifies DCIS systems and the specific regulatory requirements that apply to them.

7.1.2.5 Q-DCIS Testing And Inspection Requirements Summary

The components of Q-DCIS are accessible for testing purposes. The continuous automatic online-diagnostics of Q-DCIS detect data transmission errors, power supply failure, and

hardware failures at the card or module level. In the Q-DCIS cabinets, continuous self-diagnostics monitor the status of each module or card.

The integrated hardware and software functions of Q-DCIS including the network parameters and data status are checked and tested together. 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. 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.

7.1.2.6 Q-DCIS Operator Interface Requirements Summary

The Q-DCIS VDUs support both operator monitoring and manual control of the safety-related systems; the VDUs also present both process and diagnostic alarm information. The data Input/Output (I/O) and transmission functions do not require any manual operator intervention and have no operator controls. Q-DCIS operates continuously in all modes of plant operation to support the data transmission requirements of the interfacing systems. When one of the two power supplies or communications paths within a division fails, operation continues automatically without operator intervention; a three divisional failure is required before there is a loss of an ESBWR safety-related function. In the event that a channel failure occurs, the failure is alarmed in the MCR, including monitoring of the failed component. The failed segment of the channel can be isolated from the operating segments and can be repaired on-line (IEEE Std. 603, Sections 5.7, 5.10, and 6.5).

The following Q-DCIS monitoring 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

Q-DCIS does not include any components in N-DCIS, nor does Q-DCIS 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 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 via the associated actuation devices (for example., pilot solenoid valves, squib valves, and air operated valves). The RPS is the ESBWR designated reactor trip system. The SSLC/ESF is the ESBWR designated ESF actuation system.

The Q-DCIS systems and components are safety-related entities of the ESBWR DCIS. Summary descriptions of the Q-DCIS major systems and functions follow:

7.1.2.8.1 Reactor Protection System (RPS) Description Summary

The RPS ESBWR implements the reactor trip and MSIV LD&IS 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 for situations that could result in unsafe reactor operations. This action prevents or limits fuel damage, limits system pressure excursions and thus minimizes 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.

The RPS sensors, hardware and logic are diverse from SSLC/ESF logic, ATWS Mitigation logic and Diverse Protection System (DPS) logic. The RPS cabinet houses the equipment that performs the Suppression Pool Temperature Monitoring functions for the Containment Monitoring System (CMS) discussed in Section 7.5.2.

7.1.2.8.2 Neutron Monitoring System (NMS) 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, which 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 SRNM system monitors neutron flux levels from very low average power levels to a power level well above 15% at which the monitoring function is overlapped with LPRM/APRM to assure continuous monitoring of neutron flux levels. However, the SRNM channel still can provide local power information up to 100%. The SRNMs generate trip signals to prevent fuel damage resulting from abnormal positive reactivity insertions under conditions that are not covered by the APRMs. The SRNMs generate both a high neutron flux trip and a high rate of neutron flux increase trip.

- PRNM System - The PRNM system includes the LPRM, the APRM, and the OPRM functions. The LPRM System provides 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 (for example., from 1% to 15% reactor power), the SPRM and PRNM monitoring function overlap.

- Automatic Fixed In-core Probe (AFIP) – This is a nonsafety-related component of the NMS system and has no connections to the Q-DCIS; its function is to calibrate the LPRMs by providing flux information to 3D MONICORE.

- Multi-Channel Rod Block Monitor (MRBM) - This is a nonsafety-related component of the NMS system and is completely isolated from Q-DCIS by one-way optical fiber communication; its function is to provide control rod blocks to RC&IS to prevent core thermal limits violations.

7.1.2.8.3 Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) System Description Summary

The SSLC/ESF is the ESF actuation system for the ESBWR. 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 design basis events. 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. SSLC/ESF provides the automatic decision-making and trip logic to initiate the following protection functions:

- ECCS operation;
- Leak detection, containment isolation and radio activity release barrier defense actuation; and
- Control room habitability functions.

7.1.2.8.3.1 Emergency Core Cooling System (ECCS) Description Summary

The ECCS provides emergency core cooling to respond to events that threaten reactor coolant inventory (for example, a Loss of Coolant Accident (LOCA).) The ECCS comprises the ADS, the Gravity-Driven Cooling System (GDCS), the ICS, and the SLC system. The ECCS function is discussed more fully in Subection 7.3.1.

7.1.2.8.3.2 Automatic Depressurization System (ADS) Description Summary

The ADS resides within the Nuclear Boiler System (NBS) and comprises the 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 on the SSLC/ESF portion of Q-DCIS.

7.1.2.8.3.3 Gravity Driven Cooling System (GDCS) Description Summary

Following the receipt of an actuation signal the GDCS provides emergency core cooling once 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 in the event of a severe accident core melt sequence. The GDCS deluge logic (nonsafety-related except permissives to avoid inadvertent actuation) is separate and diverse from 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 (for example., no operator action required). Manual initiation of GDCS is possible at any time providing a protective permissive has been satisfied.
- 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 (ICS) Description Summary

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 system is unavailable. 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, which can also perform this function. The IC logic resides on the SSLC/ESF portion of Q-DCIS.

7.1.2.8.3.5 Standby Liquid Control (SLC) System Description Summary

The SLC system performs dual functions. It provides additional coolant inventory to respond to a LOCA, and is a backup method to bring the nuclear reactor to subcriticality and to maintain subcriticality as the reactor cools (discussed in the SLC Subection 7.4.1). The SLC logic resides on the SSLC/ESF and ATWS/SLC (RPS) portions of Q-DCIS.

7.1.2.8.3.6 Leak Detection and Isolation System (LD&IS) Description Summary

The LD&IS monitors leakage sources from the reactor coolant pressure boundary, and automatically initiates closure of the appropriate valves that isolate the source of the leak if monitored system variables exceed preset limits. This action limits coolant release from the reactor coolant pressure boundary and the release of radioactive materials to the environment. The LD&IS logic for the non-MSIV isolation valves resides on the SSLC/ESF and the MSIV isolation valve logic resides on the RPS portions of Q-DCIS.

The MSIV isolation logic of the LD&IS is performed as part of the RPS 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 (CRHS) 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 during normal and abnormal conditions. 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 on the SSLC/ESF portion of Q-DCIS.

7.1.2.8.3.8 Anticipated Transient Without Scram Mitigation/Standby Liquid Control (ATWS/SLC) 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. SLC is sized to counteract the positive reactivity effect of 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. The SLC logic resides on the SSLC/ESF and ATWS/SLC (RPS) portions of Q-DCIS.

The nonsafety-related ATWS mitigation logic is implemented in the Diverse Protection System (DPS). (See Subsection 7.8.1.1.3)

7.1.2.8.3.9 Passive Containment Cooling System (PCCS) Description Summary

The PCCS functions to cool the containment following a rise in containment pressure and temperature without requiring any component actuation. The PCCS needs no electric power and does not have instrumentation, control logic, or power actuated valves. The PCCS is only briefly discussed here for completeness.

7.1.2.8.4 Containment Monitoring System (CMS) Description Summary

CMS provides the functions identified in the following Subsections. 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 of the Containment Monitoring System is part of CMS and monitors suppression pool temperatures under all operating accident conditions. The system operates continuously during reactor operation. Should the suppression pool temperature exceed established limits, the Suppression Pool Temperature Monitoring of the Containment Monitoring System 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.

7.1.2.8.4.2 Other CMS Functions Description Summary

Other CMS functions, some of which are nonsafety-related, include the monitoring of key containment fluid levels, radiation levels, pressures, concentrations, and dew point values. 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.

7.1.3 Q-DCIS Specifics

A simplified functional block diagram of DCIS is shown as part of Figure 7.1-1. The Q-DCIS data communication systems are embedded in the ESBWR 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 functional network diagram of DCIS appears as part of Figure 7.1-2, which shows the elements of Q-DCIS and N-DCIS. The figure is a functional representation of the design and the final Q-DCIS design may alter equipment locations and actual hardware components depending on the chosen Q-DCIS vendors.

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

Q-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 that are fully discussed in Reference 7.1-4 which is the Licensing Topical Report (LTR) entitled, “ESBWR I&C Defense-In-Depth And Diversity Report”, NEDO-33251.

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 Q-DCIS are found in IEEE Std. 603, sections 4.1, 4.2, 4.5, 4.8, and 4.10 and specifically include the capability to:

- Read signals from the safety-related instrumentation both locally and via RMUs.
- Perform the required signal conditioning if this function is required, and 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 Main Control Room (MCR) and Remote Shutdown System (RSS) Video Display Units (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 alarm (both self-diagnostic and process) information to the operator.
- 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 Q-DCIS is to transmit plant parameters and other safety-related system data through safety-related isolation devices to the gateways/datalinks to N-DCIS that provide interfaces to nonsafety-related system logic and displays for power generation.

7.1.3.1.3 Q-DCIS Setpoint Methodology

The design considers the range, accuracy, resolution, instrument drift, environmental conditions at the sensor location, changes in the process, testability, and repeatability in the selection of I&C and in the determination of setpoints. 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 since all of the equipment is microprocessor based and discrete setpoints do not drift. The recommended test frequency is greater for instrumentation that demonstrates a stronger tendency to drift.

The actual settings are determined from operating experience and/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 but close enough to the analyzed trip values to assure that appropriate margin is maintained between the actual setting and the limiting safety-related system settings. 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. Establishing setpoints for Q-DCIS systems will be performed in accordance with proven instrument error and setpoint calculation methodology described in Reference 7.1-9, “General Electric Instrument Setpoint Methodology.”

7.1.3.2 Q-DCIS Description

Q-DCIS provides the data processing and transmission network that encompasses the four independent and separate data multiplexing divisions (for example., Divisions 1, 2, 3, and 4) corresponding to the four divisions of safety-related electrical and I&C equipment. Each Q-DCIS division will consist of the RMUs, the fiber optic signal transmission path, the SSLC cabinets, VDUs and safety-related fiber optic Communication Interface Modules (CIMs).

Q-DCIS will contain multiple dual redundant fiber optic networks for each of the four divisions. The networks will connect the RMUs with: divisional safety-related VDUs; RPS and NMS Digital Trip Modules (DTMs); SSLC/ESF CIMs; RPS, NMS, and SSLC/ESF Test Cabinets

located in the safety-related Q-DCIS equipment rooms in the Reactor Building (RB) and Control Building (CB); and N-DCIS through isolated digital gateways/datalinks.

Each Q-DCIS system is housed in a set of uniquely identified cabinets with separate cabinets provided for each of the four divisions and remotely mounted components within divisions. Q-DCIS comprises RMUs, logic cabinets, cabinet power supplies, safety-related displays, and fiber-optic cabling.

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

Each field RMU will format and transmit 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 will receive SSLC/ESF equipment control signals from the network for distribution by hard wired connection to the equipment actuators for actuation 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, and to the other safety-related logic equipment such as the safety-related logic Test Cabinets for control of the functional tests, the CIMs, as well as the isolated divisional gateways/datalinks for communication with N-DCIS.

The components of Q-DCIS in the RB and CB will be located in a controlled environment for safety-related equipment. The RMUs in the RB and safety-related logic cabinets located in the CB will be provided with appropriate cooling to maintain the required environmental conditions. Q-DCIS components including the fiber 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. Control of the electromagnetic environment is paramount to preventing degraded operation of sensitive, software-based, control equipment. Electromagnetic compatibility of the RMUs and Q-DCIS equipment will be assured by conformance with the following program:

- Q-DCIS components are designed to minimize both susceptibility to, and generation of, EMI and RFI
- Q-DCIS components are subjected to tests for EMI, RFI, and surge conditions that conform with guidelines given 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, Q-DCIS electrical equipment will adopt techniques of shielding, grounding and filtering. The equipment will be 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 (RPS)

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 (NMS)

The safety-related NMS monitors the core 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 Suppression Pool Temperature Monitoring of the Containment Monitoring System is provided to monitor suppression pool temperatures under all operating and accident conditions. The system operates continuously during reactor operation. Should the suppression pool temperature exceed established limits, the Suppression Pool Temperature Monitoring of the Containment Monitoring System 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). The Suppression Pool Temperature Monitoring is part of the Containment Monitoring System (CMS). 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 (ECCS)

The safety-related ECCS is an engineered safety feature that provides automatic initiation of the Isolation Condenser System, Automatic Depressurization System, Gravity Driven Cooling System and Standby Liquid Control system to mitigate loss of coolant accidents. Refer to Subsection 7.3.1 for additional information.

7.1.3.2.2.2 Isolation Condenser System (ICS)

The safety-related ICS automatically limits reactor pressure and temperature within an acceptable range so that SRVs will not lift and emergency reactor depressurization action will 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, and with minimal loss of coolant inventory from the reactor when the normal heat removal system is unavailable. Refer to Subsection 7.4.4 for additional information.

7.1.3.2.2.3 Leak Detection and Isolation System (LD&IS)

The safety-related LD&IS monitors leakage sources from the reactor coolant pressure boundary, and automatically initiates closure of the appropriate valves that isolate the source of the leak if 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 (CRHS)

The CRHS is an ESF system that functions to provide a safe environment within the control room to allow 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 control building shielding and area radiation monitoring; a Control Room Habitability Area HVAC System (CRHS); provision for emergency food, and water storage; emergency kitchen and sanitary facilities; provision for protection from and removal of airborne radioactive contaminants; and capability to remove smoke. The Control Room Habitability Area (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 (SSLC/ESF) 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 (for example, pilot solenoid valves, squib valves, etc.) initiate the appropriate plant protection. Refer to Subsection 7.3.5 for additional information.

7.1.3.2.2.6 Passive Containment Cooling System (PCCS)

The safety-related PCCS functions to cool the containment following a rise in containment pressure and temperature, without requiring active component actuation.

The PCCS needs no electric power and does not have instrumentation, control logic, or power actuated valves. The PCCS is briefly described herein for completeness. Refer to Subsection 7.3.2 for additional information.

7.1.3.2.3 Safety Shutdown Systems

7.1.3.2.3.1 Standby Liquid Control (SLC) System

The safety-related SLC system provides a diverse means to shut down the reactor from full power to a sub-critical condition, and maintains the reactor sub-critical 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 loss of coolant accidents as part of the ECCS. Refer to Subsection 7.4.1 for additional information.

7.1.3.2.3.2 Remote Shutdown System (RSS)

The RSS has two redundant and independent panels located in two different areas in the Reactor Building. Should the MCR become inhabitable, all Division 1 and 2 safety-related parameters and all nonsafety-related parameters displayed/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 (PAM) Instrumentation

The PAM instrumentation monitors variables and systems over their anticipated ranges under accident conditions as appropriate to ensure plant and personnel safety. An assessment of ESBWR conformance with RG 1.97 is presented in Subsection 7.5.1.

7.1.3.2.4.2 Containment Monitoring System (CMS)

Safety-related CMS instrumentation measures and records radiation levels and the oxygen/hydrogen concentration levels in the primary containment under post-accident conditions. It 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 (PRMS)

Safety-related (for nonsafety-related, refer to Subsection 7.1.5.2) PRMS instrumentation monitors the main steam lines, fission products in the drywell, discharges from the ICS, vent discharges and liquid and gaseous effluent streams that may contain radioactive materials. MCR display, recording, and alarm capabilities are provided, along with controls which provide automatic trip inputs to the respective systems for isolation of further radiation release. Refer to Subsection 7.5.3 for additional information.

7.1.3.2.5 Interlock Systems

Since interlock functions are embedded in the DCIS logic, ESBWR does not have a separate interlock system. Refer to Subsection 7.6.1 for additional information.

A reactor pressure interlock (embedded in logic) is provided to 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. A high pressure/low pressure interlock is provided to prevent opening of the isolation valve when the reactor pressure is higher than the FAPCS design pressure.

Redundant reactor pressure instruments provide a high-pressure signal to the FAPCS High Pressure/Low Pressure (HP/LP) (embedded in logic) interlock when the reactor pressure exceeds the setpoint determined based on the design pressure of the low-pressure FAPCS piping. Upon receipt of a high reactor pressure signal, the HP/LP interlock circuit initiates a signal to close the isolation valves and prevent them from opening.

Other than the isolation valves, the ESBWR design has no logic that isolates safety-related from nonsafety-related piping during a LOCA, 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 (NBS) Instrumentation

Redundant NBS safety-related instrumentation is provided to monitor reactor vessel water level and reactor vessel pressure for operator monitoring and 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

DCIS data communication functions are embedded within the ESBWR Q-DCIS and N-DCIS architectures. ESBWR does not have separate data communication systems.

7.1.3.3 Q-DCIS Safety Evaluation

Communication from Q-DCIS to N-DCIS elements is via fiber optic cable. Fiber is also used for the limited communication between the Q-DCIS divisions (for example., for two-out-of-four voting logic, data for VDU monitors, and VDU outputs corresponding to manual initiation actions). The use of fiber provides complete electrical isolation between components in addition to noise free communication paths. The fiber optic communication module (which converts safety-related electrical signals to light) on the sending side of the fiber 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; 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 will only result in alarms and loss of data to N-DCIS. Any single divisional data loss to N-DCIS will not affect power generation or safety. The loss of all safety-related data to N-DCIS can potentially affect power generation, but only in the long term (for example, core thermal limits monitoring). As such, the safety-

related/nonsafety-related fibers do not have a safety-related function because 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 and because the communication is not for to safety-related functions. It should also be noted that although this standard applies to electrical cable, the fibers are sheathed in material that meets the IEEE Std. 383 standard addressing fire propagation mitigation.

Q-DCIS is arranged into four divisions. The intra-divisional and safety-related to nonsafety-related fiber communication paths are redundant both 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 redundantly and uninterruptedly powered for both reliability and self-diagnostics. For all safety-related to safety-related communication, safety-related functions will 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. The ESBWR is being designed such that a two division failure (which requires four communications or power failures), does not result in the loss of an ESBWR safety-related function.

Generally, a system of isolators (within the safety-related systems described above) and gateways/datalinks (within N-DCIS) are used to transmit safety-related data to N-DCIS. The gateways are specific to the communication link (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 N-DCIS (the sending sources are different even though the "receivers" are the same). The scheme supports the design basis that whether or not the communications interface is operable or whether or not there is anything functional on the nonsafety-related side of the communications interface does not impact safety-related system operation.

It is also desirable to keep safety-related software as simple as possible so that no Q-DCIS components will have "interrupts" from nonsafety-related devices nor will they have to respond to nonsafety-related component queries for information. 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). It is the nonsafety-related gateway that translates the safety-related information into a format that N-DCIS can understand, will respond to interrupts and queries and will package the safety-related information into the necessary message packets to support specific N-DCIS components for monitoring, alarming and recording purposes. Additionally, there are some safety-related to nonsafety-related communications paths that do not involve gateways because the receiver is designed to receive and extract the safety-related transmitter generated data/signal without the need for data conversion (an example is NMS to Automated Thermal Limit Monitor (ATLM) and MRBM communication). The nonsafety-related gateways (when required) handle the data interface (as opposed to isolation) for communications between Q-DCIS and N-DCIS by packaging the data for the various N-DCIS

functions, responding to N-DCIS requests for information and monitoring communication link status.

The physical communication interface between safety-related and safety-related systems, and safety-related and nonsafety-related systems is always by fiber. Within the safety-related system the electrical to light interface is always safety-related. There is no credible event (for example., seismic, design basis accident, etc.) that can cause a failure of the isolation barrier between the safety-related/safety-related or safety-related/nonsafety-related portions of the isolator (actually, the components at each end of the fiber); although unlikely, the worst case failure is loss of communication. Therefore, the design complies with IEEE 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 either hardware or software protocols, which control the transmission and acceptance of data from outside the division such that these communications cannot adversely affect the operation or safety-related functions of that division. The details of these communication protocols cannot be provided until the actual hardware is chosen; however, they will meet the design principles of Q-DCIS communication interfaces as 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 does not affect safety-related system operation.

The safety-related systems are designed not to depend on nonsafety-related communication for their functioning; 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 Q-DCIS to allow time tagging of data sent to the nonsafety-related components. These time signals are used by the safety-related DCIS only for VDU indication (so that all displays have the same time), but 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 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. (Note that it is not physically possible to simultaneously put more than one division in bypass and both “trips” and “bypasses” are alarmed in the control room). After the chassis has been made “inop”, the operator can review the download as received by the chassis to be calibrated and additionally determine that the "checkback" signal interchange has indicated that the NUMAC chassis has 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 to

carrying the calibration data to the NUMAC chassis and inputting by hand (which is still possible) but more convenient and more accurate. 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 Q-DCIS is from RMUs located in the control, reactor and possibly fuel buildings in areas appropriate to their division; there are no safety-related RMUs located in any other buildings. Data (for example, from transducers, switches, temperatures, and so forth.) is acquired by the RMU, appropriately signal conditioned and, with diagnostic data, sent via the redundant fiber communication links, to the RPS, NMS and SSLC/ESF units. The RPS, NMS, and SSLC/ESF units will either be centralized control processors or distributed through the various cabinets (within the division) but they perform the logic required by the safety-related systems. There are always RPS, NMS, and SSLC/ESF units located in the control room back panel area where there are four Q-DCIS rooms, one per division. The back panel areas are 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 Q-DCIS and N-DCIS. Finally, calculated outputs from the RPS, NMS, and SSLC/ESF units are sent via the redundant communication system to RMUs that provide outputs to the safety-related actuators (for example, solenoids, explosive squib valves, etc.). Note that some outputs are hard wired directly to the final actuators if higher speeds are required.

The dual-redundant, fiber optic, data networks (described above) replace the many conventional, long length, copper conductor cables of existing nuclear plants. This reduces the cost and complexity of divisional cable runs that connect components of the plant protection and safety-related systems such as RPS, MSIV isolation logic functions, LD&IS containment isolation functions, and SSLC/ESF, and safety-related VDUs. 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 and Divisions 1 and 2 each have another VDU located on each remote shutdown 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 and are also 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 RPS or NMS will interpret loss of interdivisional communication as a trip from that division.

The trip will count toward the 2/4 logic initiations unless the failed division is bypassed. Fail as-is systems like ECCS will interpret loss of communications as a non-trip; however the ESBWR has been designed as an N-2 plant, such that more than two of these type failures are required to disable the safety-related functions.

The dual redundant data communication channels per division and the four redundant divisions of 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 and cable and network that are part of Q-DCIS within and between the four redundant divisions satisfy the separation and independence requirements of division equipment including cable routing separation, which meets the requirements of NUREG-0800 SRP 9.5.1, Fire Protection Programs.

DCIS contains continuous online diagnostic functions that monitor transmission path quality and integrity and the integrity of most of the system components; self-diagnostics extend down to the replaceable card or module level. The ability to use 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; Q-DCIS failures are alarmed in the MCR (IEEE Std. 603, Section 5.7 and 6.5).

Finally, all Q-DCIS components and cabinets have redundant power supplies that are supplied by redundant uninterruptible power feeds within each division. These power feeds together will support 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).

Q-DCIS forms an integral part of the safety-related systems and RPS, NMS, and SSLC/ESF protection functions and parallels the four-division design of those systems. No failure of any two divisions can prevent a safety-related action (for example, detection, trip, etc.) from being accomplished successfully. Component self-test reconfigures the system to the approved safe state upon detection of uncorrectable errors. Off-line test and calibration of 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 bypasses are alarmed in the MCR.

7.1.3.3.1 Q-DCIS Summary Of Specific Regulatory And Industry Requirements Conformance

The specific regulatory acceptance criteria and guideline requirements applicable to each of Q-DCIS systems identified in the SRP (Reference 7.1-1) are identified in Table 7.1-1. The regulatory requirements applicability matrix of Table 7.1-1 is followed in Sections 7.2 through Section 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.

7.1.3.4 Q-DCIS Testing and Inspection Requirements

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

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

Because DCIS functions are closely interfaced with the safety-related logic functions, the integrated hardware and software functions of 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 (also the D/A converters if used) in the RMUs are the only components requiring periodic calibration checks. Calibration can be performed automatically. In Q-DCIS, online diagnostics are qualified as safety-related in conjunction with functional software qualification (IEEE Std. 603, Section 5.7).

A 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 provides for the delivery of system data to all nodes in the network (for example, to distributed logics of Q-DCIS RMUs and certain safety-related logic system components), and in certain safety-related systems through dedicated data paths. 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.

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, indicating the failed component. The failed segment of the channel can be isolated from the operating segments and can be 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

  - 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
  - Division 4 Q-DCIS diagnostic displays

7.1.3.6 Q-DCIS Boundaries

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

7.1.4 N-DCIS General Description Summary

N-DCIS comprises the nonsafety-related portion of the ESBWR DCIS. 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 are: (See Reference Subsection 7.1.5 and Figures 7.1-1 and 7.1-2 for more detail.)

- General Electric Nuclear Engineering (GENE) Systems which include:
  - Rod Control and Information
  - Diverse Protection
  - 3D MONICORE
  - Nonsafety-related Gateways/Datalinks
  - Neutron Monitoring (nonsafety-related portion)
- Plant Investment Protection (PIP) Systems (Train A and Train B) which include:
  - Control Rod Drive
  - Reactor Component Cooling Water
  - Fuel and Auxiliary Pools Cooling
  - Reactor Water Cleanup and Shutdown Cooling
  - Drywell Cooling
  - Instrument Air
  - Plant Service Water

  - Plant Service Water Cooling Towers
  - Diesel Generators
  - Nuclear Island Chillers
  - 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
  - Turbine-Generator Control
- Plant Computer Systems Group which includes:
  - Plant Computer Functions
  - MCR and RSS VDUs
  - Transient Recording
  - Core Thermal Power/Flow
  - Data Historian
  - Alarm Systems
  - On-Line Procedures (OLP)

The N-DCIS major components include:

- A fiber and hard wired 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
- Computer peripherals, such as printers and plotters
- Cabinets for housing devices such as power supplies

N-DCIS is both larger and more complex than Q-DCIS but has been designed in segments that can operate independently of one another; redundant automatic network switches manage the network such that during normal operation the segments appear seamless to the operator in the MCR. N-DCIS cannot control any Q-DCIS component. N-DCIS accepts one-way communication from Q-DCIS so that the safety-related information can be monitored, archived and alarmed seamlessly with N-DCIS data.

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

N-DCIS provides the control and monitoring operator interface on 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 N-DCIS. Note that this gives the RSS panels the same control and monitoring capability as the displays in the MCR. N-DCIS provides gateways/datalinks as necessary to allow vendor supplied or prepackaged (“foreign”) control systems to be integrated into the ESBWR DCIS; examples include the Condensate Purification System (CPS) and the Area Radiation Monitoring System (ARMS).

N-DCIS components key for 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, N-DCIS can operate continuously from either of the two ESBWR diesel generators.

Finally, N-DCIS provides extensive self-diagnostics that monitor communication, power, and other failures to the replacement 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

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 N-DCIS include the requirements to:

- Provide functional/operational independence of nonsafety-related divisions important to power generation.
- Perform closed loop control and system logic.
- Be such that no single failure of an N-DCIS component affects power generation.
- Receive selected signals from 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 data through the firewall to the Technical Support Center (TSC), Emergency Operating Facility (EOF), and the Emergency Response Data System (ERDS) and 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 Plant Computer Functions (PCF) to include calculations, displays, and alarms.
- Provide for Report Generation.
- Provide for a Plant Configuration Database (PCD).

7.1.4.3 N-DCIS Safety Evaluation Summary

N-DCIS is classified as a nonsafety-related system and it is used as the primary control, monitoring, and data communication system with power production applications. 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. N-DCIS does provide 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 Q-DCIS.

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 Control Building (MCR and Back Panel areas), Radwaste Building, TSC, EOF, and other auxiliary buildings.

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

7.1.4.4 N-DCIS Regulatory Requirements Conformance Summary

N-DCIS meets applicable sections of the following regulations and standards:

- 10 CFR 50.55, 10 CFR 52.47 and 10 CFR 52.79.
- NUREGs 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, 1050, 1074.
- ANSI/ISA s67.04.01
- General Design Criteria (GDC) 1, 2, 4, 13, 19, and 24.
- Staff Requirements Memoranda (SRM) II.Q to SECY 93-087.
- Regulatory Guides (RGs) 1.22, 1.62, 1.75, 1.97, 1.105, 1.118, 1.152, 1.153, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173, 1.180, and 1.204.
- Branch Technical Positions (BTPs) HICB-8, 10, 11, 12, 14, 16, 17, 18, 19, and 21.

Table 7.1-1 identifies DCIS systems and the specific regulatory requirements that apply to them.

7.1.4.5 N-DCIS Testing And Inspection Requirements Summary

N-DCIS components and critical components of interfacing systems are tested to ensure that the specified performance requirements are satisfied (Reference 7.1-11). Factory, construction, and preoperational testing of 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.

N-DCIS controllers, displays, monitoring and input and output communication interfaces continuously function 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 for identifying and isolating 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 N-DCIS.

7.1.4.6 N-DCIS Operator Interface Requirements Summary

The N-DCIS will provide VDUs to allow operator control and monitoring of the N-DCIS systems and monitoring only of safety-related system data (through appropriate isolation). The VDUs are also segmented such that the network segments can be monitored and controlled independently but in normal operation the segments will not be apparent to the operators. The N-DCIS will also supply alarm and annunciation information to the operator and additionally supply a permanent overview (mimic) display for important plant information.

7.1.4.7 N-DCIS Major Systems Description Summary

N-DCIS does not include any components in Q-DCIS nor does N-DCIS 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

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

7.1.4.8.1 General Electric Nuclear Engineering (GENE) Systems Description Summary

GENE systems include:

- 3D MONICORE that calculates three dimensional power distribution and thermal limits for the reactor core;
- Systems that control and monitor ESBWR Control Rod Motion including Reactor 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 ECCS functions;
- The nonsafety-related gateways/datalinks that both translate and distribute data from Q-DCIS to N-DCIS;
- Operator control and monitoring from the MCR VDUs; and
- The nonsafety-related portion of NMS that provides data to the AFIP subsystem and the Multi-channel Rod Block Monitor (MRBM) subsystem.

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

The N-DCIS for these two systems provides the logic to control the following plant systems: Reactor Water Cleanup and Shutdown Cooling (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, and the diesel generators.

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, 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 (BOP) Systems Description Summary

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

- Reactor pressure (SB&PC)
- Reactor level (FWCS)
- Plant automation (PAS)
- The turbine and generator
- The main condenser and normal heat sink
- The nonsafety-related plant (non-PIP) Electrical system
- Power generation components such as the Moisture Separator Reheater (MSR) and Condensate Purification System (CPS)
- The Condensate / Feedwater System (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 (PCS) Group Description Summary

Functions of the Plant Computer Systems Group include:

- Plant Computer Functions (PCF), distributed throughout the N-DCIS segments in redundant workstations and/or controllers to provide performance monitoring and control, prediction calculations, visual display control, point log and alarm processing, surveillance test support, and automation
- Plant alarm and annunciator systems to alert the operator to process deviations and equipment/instrument malfunctions
- Historian function, which stores data for later analysis and trending
- Control of the main mimic on the MCR Wide Display Panel
- Support functions for printers and the firewall that, in turn, supports the TSC, EOF, Emergency Response Data System (ERDS), and potential links to the Simulator.
- On-Line Procedures (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
- Plant configuration database to document, manage, and configure components of the N-DCIS

- Gateways to foreign nonsafety-related systems such as seismic, meteorological monitoring, radiation monitoring, etc.

7.1.5 N-DCIS Specifics

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

A simple functional block diagram of the ESBWR DCIS is shown as part of Figure 7.1-1. The N-DCIS data communication systems are embedded in the ESBWR 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 Q-DCIS to N-DCIS communications for the safety-related systems described in Sections 7.2 through 7.8. A functional network diagram of DCIS appears as part of Figure 7.1-2, which indicates the elements of N-DCIS and Q-DCIS. The figure is a functional representation of the current design. The final N-DCIS design may alter equipment locations and actual hardware components depending on the chosen N-DCIS vendors.

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

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

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

- Segment N-DCIS display and control of the two PIP Systems (A&B) and the BOP systems so that 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 other and from 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.
- Be such 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” ESBWR control systems and “foreign” (for example. vendor supplied or prepackaged) control systems

such as condensate purification, offgas, radwaste, area radiation monitoring, and meteorological monitoring.

- 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; these 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 Q-DCIS through gateway devices, or workstations, then transmit to nonsafety-related video display units 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 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 Plant Computer Functions (PCF) including Performance Monitoring and Control (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 BOP performance calculations.

- Provide a permanent record and historical perspective for plant operating activities and abnormal events.

- Provide a firewall that is, in turn, used to interface with external computer and monitoring systems (one-way communication, no control capabilities) including the plant simulator (for training and for development and analysis of operational techniques), TSC, EOF, and the ERDS.

- Provide reactor core performance information.

- Provide Safety Parameter Displays of critical plant operating parameters such as power, water level, temperatures, pressure, flows, and status of pumps, valves, etc., to allow 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 Wide Display Panel (WDP).

- Provide MCR displays consisting of overview displays, navigational/top level displays, and system level displays**.**
- Provide TSC and EOF displays.
- Provide an Alarm Management System designed to alert the operator to an alarm condition, informing the operator of its priority, guiding the operator's response, and confirming whether or not the response was effective.
- Display normal, abnormal and emergency operating procedures on operator workstations and other workstations where display of operating procedures is permitted.
- Warn the operator to document that a Technical Specification limit, for example, Limiting Condition of Operation (LCO), is being approached/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% 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 plant configuration database.
- Provide Selected Control Rod Run In (SCRRI) initiation and Select Rod Insertion (SRI), both manually and automatically by the DPS.
- 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 transmission of data from remote locations in the plant to the MCR via both fiber optic 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 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.
- Provide data support functions through the firewall to TSC, EOF, and the ERDS, and provide operator aids provided by the plant computer system of N-DCIS, such as safety parameter displays, transient data recording, analysis, and archiving, alarm processing, and sequence of events processing.

7.1.5.1.3 N-DCIS Setpoint Methodology

The design considers instrument drift, environmental conditions at the sensor location, changes in the process, testability, and repeatability in the selection of instrumentation and controls and in the determination of setpoints. 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 RUM since all of the remaining equipment is microprocessor based and discrete setpoints do not drift. The recommended test frequency is greater on 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 high enough to preclude inadvertent initiation of certain actions but low enough to assure that significant margin is maintained between the actual setting and the limiting system settings. 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. Establishing key N-DCIS setpoints will be a formal process.

7.1.5.2 N-DCIS Description

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

The individual N-DCIS segments are:

- GENE network
- PIP A network

- PIP B network
- BOP network
- Plant Computer network

More specifically, the segments are redundant, managed network switches (sometimes called "level 3" switches) into which are connected the data acquisition, control and displays associated with that segment. Each network switch can have up to several hundred "nodes" and several "uplink" ports, which are connected to the other switches; all connections to these switches are via the fiber optic network. (Note: Fibers used for nonsafety-related applications are also sheathed in material that meets the IEEE-383 standard that addresses fire propogation 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 switches "learn" the addresses of all the nodes connected to them.

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

Each switch "node" (workstation, display, controller, etc.) is connected to redundant switches of the segment and 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 self-diagnostics for the components and data paths; failures are alarmed.

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

The major N-DCIS functions are segmented as defined below; it should be understood, however, that the lists below define functions but not necessarily physical hardware since processor and RMU allocation is part of detailed design:

- GENE
  - Safety-related system gateways
  - Diverse protection system (triple redundant processors)
  - 3D MONICORE
  - ATLM
  - MRBM
  - RWM
  - AFIP
  - RCIS
  - MCR displays
- PIP A (includes the “A” segment of) and PIP B (includes the “B” segment of)
  - FAPCS
  - Control Rod Drive (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
  - 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)
  - Foreign BOP systems/controllers (condensate polishing, offgas, condensate storage and transfer)
  - MCR displays
- Plant computer
  - Core thermal power/flow
  - Performance monitors (BOP, bypass, technical specification monitoring)

- Alarm/annunciator
- On-line and alarm response procedures
- SPDS
- Nonsafety-related post accident (per RG 1.97) displays
- Wide display panel (mimics, etc.)
- Report generators
- Firewall (TSC, EOF, ERDS)
- Printers
- Historian function
- Fire protection system (through gateways/datalinks)
- Area radiation monitoring
- Seismic monitoring
- 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 (RSS)

Each RSS panel includes the ability to operate all of the nonsafety-related PIP equipment and 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 (RWCU/SDC)

The nonsafety-related RWCU/SDC functions to maintain reactor water purity during operation, and to provide normal shutdown cooling by taking suction from the reactor pressure vessel, 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 (FAPCS)

The nonsafety-related FAPCS functions to maintain the various ICS, GDCS and suppression pool temperatures and cleanliness during operation, by pumping pool water through heat exchangers and demineralizers into two 100% cooling and cleaning trains. The FAPCS can also initiate a "Low Pressure Coolant Injection (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 reactor vessel via RMCU/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 (CRD)

The nonsafety-related CRD normally functions to maintain the Hydraulic Control Unit (HCU) accumulators at the required pressure, to provide cooling water flow to the Fine Motion Control Rod Drives (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.

7.1.5.3 Nonsafety-Related Information Systems

7.1.5.3.1 Process Radiation Monitoring System (PRMS)

Nonsafety-related (and safety-related – see Subsection 7.1.3.2.4.3) PRMS instrumentation monitors the main steam lines, fission products in the drywell, discharges from the ICS, vent discharges and liquid and gaseous effluent streams that may contain radioactive materials. MCR display, recording, and alarm capabilities are provided along with controls, which provide automatic trip inputs to the respective systems to prevent further radiation release. Refer to Subsection 7.5.3 for additional information.

7.1.5.3.2 Area Radiation Monitoring System (ARMS)

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

7.1.5.4 Control Systems

7.1.5.4.1 Nuclear Boiler System (NBS) Instrumentation

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

7.1.5.4.2 Rod Control and Information System (RC&IS)

The nonsafety-related RC&IS provides the capability 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.

7.1.5.4.3 Feedwater Control System (FWCS)

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

7.1.5.4.4 Plant Automation System (PAS)

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.

PAS does not involve safety-related systems. PAS is the first of two automation schemes implemented by N-DCIS, namely, 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. PAS uses Automated Program Functions (APF) to coordinate the Automatic Power Regulator (APR) and Power Generation and Control Systems of the PAS.

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. (Note: safety-related systems are never controlled or tasked by the plant automation system.) The automation system covers the tasks involved in criticality, heat-up and pressurization, turbine roll and synchronization, and plant power control.

APR and Power Generation and Control Subsystem of Plant Automation System will, with operator supervision, automatically run the plant from cold non-critical conditions to 100% rated temperature, pressure, and power and back to cold non-critical conditions. Several broad automation sequences will be established;:

- 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)
- 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. A complete list of prerequisite conditions will be established for each system. Some plant systems will never be

shut down (even during refueling outages) and additionally their operating conditions will be independent of plant power.

7.1.5.4.5 Turbine Generator Control System (TGCS)

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
- Related Turbine Generator auxiliary support control functions

7.1.5.4.6 Steam Bypass and Pressure Control System (SB&PC)

A highly reliable and triple redundant nonsafety-related SB&PC controls reactor pressure during plant startup, power generation and shutdown modes of operation. This is accomplished through control of the turbine control valves and/or turbine bypass valves such that 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.

7.1.5.4.7 Neutron Monitoring System - Nonsafety-related Systems

The nonsafety-related AFIP provides a signal proportional to the axial neutron flux distribution at the radial core locations of the LPRM detectors. The signal facilitates fully automated, precise, reliable calibration of LPRM gains and 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 by assuring that the MCPR and MLHGR do not violate fuel thermal safety-related limits. Refer to Subsection 7.7.6 for additional information.

7.1.5.4.8 Containment Inerting System

The nonsafety-related containment inerting system establishes and maintains an inert atmosphere within the Primary Containment Volume (PCV) 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.

7.1.5.4.9 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 Instrumentation and Control 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 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 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 alternate rod insertion (ARI) and associated logics (for example, control rod run-in) via 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.

7.1.5.4.10 Selected Control Rod Run In (SCRRI) / Select Rod Insert (SRI)

N-DCIS will accept the redundant loss of feedwater heating signals from FWCS and the turbine trip and load reject signals from the turbine control system, perform two-out-of-three voting on each and combine them as an “OR” function to become the automatic SRI and SCRRI command signals. It will also be possible to initiate SRI or SCRRI manually from the MCR, which is part of the DPS and RC&IS system’s scope (for example note that the manual SCRRI function is implemented to be independent of the N-DCIS equipment scope). SRI and SCRRI may also be initiated by the diverse protection system (DPS).

The redundant N-DCIS SCRRI command signals will be sent to RC&IS where each of the dual Rod Action and Position Information (RAPI) channels will perform a two-out-of-three vote and initiate RAPI channel logic associated with accomplishing the SCRRI function, which when activated, inserts control rods using the FMCRD motors to pre-defined positions to reduce reactor thermal power to a target power level. This logic will be implemented in a highly reliable redundant control system. The SCRRI command signal is also used in the emergency

rod insertion control logic of N-DCIS, as discussed below. The redundant SRI command signals will be sent from DPS to the nonsafety-related Scram timing panel (RPS); 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 (SRI) the affected HCUs will scram their associated rods. Since the scram timing switches are in the solenoid return and 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.

7.1.5.4.11 Alternate Rods Insertion (ARI)

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

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

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

DPS will not issue an ARI command without issuing a simultaneous Scram command.

7.1.5.4.12 Emergency Rod Insertion

N-DCIS will combine the N-DCIS SCRRI command signal and 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 emergency rod insertion control panel of the RC&IS, which performs two-out-of-three voting. It will initiate associated emergency insertion condition signals in the emergency rod insertion 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 will be implemented in a highly reliable redundant control system.

7.1.5.5 Plant Computer Functions (PCF)

All plant computer functions (PCF) are developed as an integral part of the HFE process (refer to DCD Chapter 18), such that the allocation of functions accommodates human capabilities and limitations, fault detection and recovery capabilities are provided, and an acceptable operator workload is not exceeded.

PCF increases 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 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 a firewall that is, in turn, used to interface with all external computer and monitoring systems (for example, one-way communication, no control capabilities) including 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 Nuclear Steam Supply (NSS) performance module as power in specified axial segments for each fuel bundle in the core.

The calculations performed by N-DCIS [SOC54]include process validation and conversion, combination of points, NSSS performance calculations, and BOP performance calculations.

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

7.1.5.5.1 Safety Parameter Displays (SPDS) System

The SPDS displays provide critical plant operating parameters such as power, water level, temperatures, pressure, flows, and status of pumps, valves, etc., allowing MCR operators to follow the 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 are available in the MCR and parameters are available on the main plant mimic on the MCR Wide Display Panel (WDP).

7.1.5.5.2 MCR Displays

The MCR panel equipment is part of the MCR Panels (MCRP) System or MCRPS. 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) is 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 and status of major equipment and availability of safety-related systems with 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, which are independent of 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 will provide the following navigational or top level displays:
  - Main Menu
  - Safety Parameter Displays
  - Post Accident Monitoring (RG 1.97) Displays
  - Alarms
  - Power Generation Control
  - On-line Procedures
  - Technical Specification Monitor/Reactor Protection System Monitor
  - 3D MONICORE
  - Historian Function
  - Transient Recording and Analysis
  - Thermal Performance Monitor and Diagnostic
  - Report Generator
  - Bypass and Inoperable Status Indication (BISI)
  - System Level Displays (P&IDs, alarms)

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

The RC&IS dedicated operator interface that provides for 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).

7.1.5.5.3 Alarm Management System

The plant Alarm Management System (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, informing the operator of its priority, guiding the operator's response, and confirming whether or not 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, 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;
- 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 will be shown to the operator when the process is operating normally without malfunction at power;
- 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 both basic alarms and high-level (composite) alarms. The generated alarms are subject to potential filtering, alarm suppression, and alarm prioritization techniques

although the plant Historian logs alarms whether or not they are presented to the operator. Alarms are then presented in the MCR using both an annunciator and display function;

- Create temporary operator-defined alarms and associated alarm setpoints; and
- Integrate with other information systems, such as OLP and Technical Specification Monitoring (TSM), to facilitate the operator's tasks.

7.1.5.5.4 On Line Procedures (OLP)

OLP provides for:

- Display of normal, abnormal and emergency operating procedures 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, procedure maintenance, and so forth;
- Maintenance (that is, addition, deletion, 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, 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;
- Logging of discrepancies between operator decisions and actions and recommended procedure execution options;
- Retracing 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; and
- Validation for each operating procedure using the plant simulator.

7.1.5.5.5 Technical Specification Monitoring (TSM)

TSM, when conditions are detectable, provides for:

- Warning the operator when a Technical Specification limit, that is, Limiting Condition of Operation (LCO), is being approached;

- Warning the operator when LCOs are being violated;
- Determining the approach to an LCO based on information on equipment status, core limits and margins and other data;
- Indication, to the extent practical, of appropriate action(s) to avoid violating LCOs;
- Acquisition and processing of available information needed to determine the approach to and existence of an LCO;
- Automatic acquisition of required available information;
- Determination, given available information, of any automatic testing that could impact LCOs;
- Indication, to the extent practical, of the action needed to recover from an LCO;
- Logging of LCO violations;
- Acquisition or calculation, as necessary, of reactor and core parameters required for monitoring LCOs, such as thermal limit margins, power distribution, heat generation rates, etc.;
- Showing the results of calculations of reactor and core parameters on operator displays;
- Manual input capability for LCOs that cannot be monitored automatically by the TSM function;
- Sending alarms to the AMS, which will provide for an acknowledgment function for alarm conditions;
- Showing the operator the availability status of the RPS and safety-related systems;
- RPS and safety-related System Monitoring (RPSM) as a sub-function;
- Monitoring, through RPSM, of support services (for example, voltages, cooling water, oil pressure and levels, etc.) that can affect the availability of the RPS and other safety-related systems;
- Monitoring, through RPSM, of the availability of both the initiating equipment (sensors, control systems, and so forth) and the implementing equipment (for example, pumps, valves, etc.);
- Monitoring, through RPSM, of the availability of both primary and backup sources of services;
- Monitoring, through RPSM, of process parameters (reactor pressure, water storage tank levels, environment, etc.) that can impact the successful operation of the RPS or other safety-related systems; and

- Manual and automatic entry, through the RPSM, of the maintenance, calibration and test data needed to establish RPS and other safety-related system operability.

7.1.5.5.6 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 Historian or in the 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 is able to process algorithms needed to support Turbine Generator (TG) and BOP supplier logs and reports.

7.1.5.5.7 Plant Configuration Database (PCD)

The Plant Configuration Database (PCD) provides overall configuration and management functions for the N-DCIS PCF at an engineering workstation for the PCF.

7.1.5.5.8 3D MONICORE

3D MONICORE provides core performance information and 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 to interface 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, other parameters such as the magnitude and location of minimum margin to thermal limits (such as minimum critical power ratios, peak fuel rod linear powers and average planar heat generation rates), fuel exposure and operating envelope data can be determined.

The 3D MONICORE Monitor is designed to periodically track 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 may 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 provides data to other systems including 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.

7.1.5.5.9 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 historic point data.

- Point data, plant operating activities, and abnormal event sequences are stored, along with their time-tags, for subsequent retrieval and analysis
- The Historian stores third-party generated data, such as 3D MONICORE data, in a format compatible with the display and report system.
- The Historian stores RG 1.97 variables for current trending or later analysis.
- The on-line data storage capability is dependent on plant history and events but is nominally one fuel cycle. The system warns the system operator about remaining disk storage space, leaving enough time for download to an off-line archiving device, preferably optical disks.

7.1.5.5.10 Transient Recording and Analysis (TRA) and Sequence of Events (SOE) Recording

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

7.1.5.5.11 Core Thermal Power and Core Flow Calculation

Real time core thermal power from critical to 100% 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 that bias in the calculation is eliminated. At low thermal power levels the Low Flow (startup level) Control Valve (LFCV) feedwater flow measurement is used to increase 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.

7.1.5.5.12 Thermal Performance Monitor and Diagnostic (TPM&D)

The TPM&D will provide an on-line diagnostic and monitoring program for the thermal heat cycle. It will calculate 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 may be used by utility personnel to identify components that may be contributing to thermal efficiency loss.

The Thermal Performance Monitor 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, temperatures, etc.) 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 (for example, equivalent system parameter such as normalized heat exchanger cleanliness).

7.1.5.6 N-DCIS Hardware

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

- Remote Multiplexing Units (RMUs) are located throughout plant buildings (such as Reactor Building, Control Building, Fuel Building, circulating water system pumphouse, switchyard, Electric Building, Turbine Building, Radwaste Building, etc.). The RMUs acquire and output the same signal types as 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 Control Building; the links are always by redundant fiber.

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

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

- Workstation cabinets, depending on the application, support redundant or single workstations that support VDUs. The workstations are used for dedicated logic functions like the Historian, core thermal power or alarm management, where the use of a control processor is not appropriate.
- N-DCIS gateways/datalinks provide N-DCIS communication with Q-DCIS, foreign controllers, the plant firewall to the TSC/EOF/ERDS, and other nonsafety-related packaged systems such as area radiation monitoring.
- Cabinets that house "packaged" control or monitoring systems such as seismic monitoring, area radiation monitoring, integrated leak rate testing, etc.
- Gateway cabinets 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 optical fiber to support the electrical isolation requirements between Q-DCIS and N-DCIS components. N-DCIS has no control-related inputs to the safety-related systems with the exception of NMS for LPRM and APRM calibration functions. Otherwise, communication is one-way from Q-DCIS to N-DCIS.
- MCR monitoring and control equipment (for 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, etc.). The MCR consoles are part of the MCR, and its monitoring and control equipment is the main operator interface with the various plant processes.
- Display panels whose components and functions include alarm display, mimic, flat panel displays, Closed Circuit Television (CCTV) monitors, large variable display, and their associated computer processors.
- Signal isolators for RMU internal buses and the redundant fiber optic links in the field
- I/O modules to provide interfaces between process sensors/actuators
- Fiber optic modems and media converters to transmit and receive data via the redundant fiber optic links in the field to the redundant control processors
- Computer peripherals, such as printers and plotters, used for data printing capabilities

7.1.5.7 N-DCIS Functions

N-DCIS has no safety-related function and it is not required to be operable during or after any DBE.

N-DCIS provides distribution and control data communication networks to support the monitoring and control of interfacing nonsafety-related plant I&C systems. N-DCIS also processes data from safety-related systems that were originally acquired by Q-DCIS; these data are always transmitted through optical fiber to provide the required isolation between Q-DCIS and 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 for RG 1.97 or for SPDS or for alarms or for a specific system or for the mimic) since data from all sources can be combined to form any coherent function.

N-DCIS controllers, once placed in "auto", can perform closed loop control and system automatic logic independently of operator inputs from the control room N-DCIS VDUs. N-DCIS controllers can also be placed in "manual" for the operator to override automatic control. The remote shutdown panels will 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) that connect field sensors, display devices, controllers, power supplies, and actuators, which are part of the nonsafety-related systems. N-DCIS also includes any associated data acquisition and communications software, if required, to support its data distribution and control function. N-DCIS replaces most conventional, long-length, copper-conductor cables with a dual or triple redundant, fiber optic, data network. The fiber optic 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 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 needed to support power generation (for example, 3D MONICORE) and core thermal power and flow calculations. The nonsafety-related data from sensors are multiplexed at nonsafety-related RMUs and then transferred via the N-DCIS data network to components of N-DCIS. Selected signals from the nonsafety-related instrumentation are transmitted to N-DCIS input cabinets via dedicated hardwired connections as required for faster transmission rates of signals (for example, SB&PC to TGCS control). Similarly, output signals to actuators and controls requiring faster transmission rates also utilize dedicated hard wired connections (for example, manual turbine trip signals). The RMUs and the data communication network for such nonsafety-related data processing and transmission are part of N-DCIS.

There are divisionally separated redundant isolated digital gateways that provide one-way communications from safety-related systems to N-DCIS. The electrical and data isolation functions are part of Q-DCIS and the gateway (data conversion and packaging) functions are part of N-DCIS. The communication from nonsafety-related systems to Q-DCIS is limited to communication from the 3D MONICORE function of N-DCIS to the PRNM (LPRM and APRM) function of the NMS and time tagging.

The local N-DCIS RMUs perform signal conditioning and A/D signal conversion for continuous process signals, and perform signal conditioning and change-of-state detection for discrete signals such as contact closures and openings. The RMU function can be applied for performing both I/O signal processing functions. The RMU formats the acquired signals into data messages and transmits the data via the data network to N-DCIS components for logic processing. The RMU with a system logic function then 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 network (actually segmented network switches). A functional network diagram of N-DCIS with associated components and links is shown in Figure 7.1-2.

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

N-DCIS networks are distributed throughout the plant and are powered by redundant and triply redundant (for specific systems such as DPS, TGCS, FWCS, SB&PC, and PAS) internal power supplies fed from two or three nonsafety-related load groups (as applicable) of the 120 volt AC Uninterruptible Power System (UPS).

7.1.5.8 N-DCIS Safety Evaluation

N-DCIS is classified as nonsafety-related and is not required for safety-related purposes, nor is operability required during or after any DBE. N-DCIS is required to operate in the normal plant environment and is significant for power production applications. N-DCIS does not perform any safety-related functions as a part of its design; however N-DCIS does provide an isolated alternate path for safety-related data from Q-DCIS to N-DCIS to be 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.

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

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

N-DCIS panels and components are designed to retain their structural integrity, during and after DBEs, so as to not prevent any safety-related equipment in its area from performing its safety-related function.

Table 7.1-1 identifies N-DCIS elements and the associated codes and standards applied in accordance with the SRP. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are noted.

7.1.5.8.1 N-DCIS Summary of Specific Regulatory and Industry Requirements Conformance

The following subsections highlight the individual requirements and references to other sections. Following the summary subsection, N-DCIS conformance is discussed in other subsections and in supplemental information, which can be found in Subsection 7.1.6.

7.1.5.8.1.1 N-DCIS Summary of Conformance with Regulatory Requirements

10CFR52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety-Related Issues

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

10CFR52.47(a)(1)(vi) ITAAC in Design Certification Applications

- Conformance: Test, Inspection, Analyses, and Acceptance Criteria of N-DCIS are identified in DCD Tier 1.

10CFR52.47(a)(1)(vii) Interface Requirements

- Conformance: Design interface requirements during the licensing certification and design phases will be commensurate with the detail required to support completion of the final safety-related analysis and design-specific Probabilistic Risk Assessment (PRA).

10CFR52.79(c) ITAAC in Combined Operating License Applications

- Conformance: N-DCIS is nonsafety-related and conforms with those sections applicable for test, inspection, analyses, and acceptance criteria of N-DCIS identified in DCD Tier 1.

7.1.5.8.1.2 N-DCIS Summary of Conformance with General Design Criteria

Criteria: GDC 13, 19, and 24

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

7.1.5.8.1.3 N-DCIS Summary of Conformance with Staff Requirements Memorandum

Staff Requirements Memorandum (SRM), SECY-93-087, Item II.T, Control Room Alarm Reliability.

- Conformance: The N-DCIS Alarm Management System meets the intent of the EPRI document guidance for redundancy, independence, and separation such that the "alarm system" is considered redundant and has its own redundant processors and utilizes signals from distributed and redundant controllers.

Alarm points are sent via a dual network to redundant processors having dual power feeds. The alarm processors are dedicated, redundant and conservatively sized.

The alarms are capable of being displayed on multiple independent VDUs (with dual power supplies on each).

Alarms are driven by redundant data links to the alarm management system. The alarm processors are redundant.

There is one horn and one voice speaker. Test buttons are available to test the horn and the lights.

7.1.5.8.1.4 N-DCIS Summary of Conformance with Regulatory Guides

RG 1.151, Instrument Sensing Lines

- Conformance: Not applicable to N-DCIS. 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.

RG 1.152 - Computer Software Used in Safety-related Systems - Criteria and guidelines stated in ANSI/IEEE-ANS-7-4.3.2, as endorsed by RG 1.152 are used as a basis for design procedures established for programmable digital equipment.

RG 1.152 contains extensive requirements on "security" and endorses IEEE Std. 7-4.3.2.

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

7.1.5.8.1.5 N-DCIS Summary of Conformance with Branch Technical Positions

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

- Conformance: N-DCIS conforms with the intent of this guideline as outlined in ISO 17799 for Security Management of 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 analysis, it is concluded that N-DCIS meets its regulatory and industry design bases.

7.1.5.9 N-DCIS Testing and Inspection Requirements

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

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 (I/O Net) communications. These on-line diagnostics can be performed without interrupting the normal control operation of N-DCIS.

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

7.1.5.10 N-DCIS Instrumentation and Control Requirements

7.1.5.10.1 Power Sources

Uninterruptible Nonsafety-related AC Power Supply

N-DCIS components and cabinets key to power generation are supplied with either dual redundant or triply redundant power supplies and power feeds.

The sources of this power are three independent UPS (inverters) normally supported by AC power. However, if off-site power fails and the diesel generators fail, 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, voltage and current and battery and charger operation, voltages and currents are monitored and alarmed. N-DCIS panel design is such that the loss of one power supply or incoming power source will not affect N-DCIS or its functional operation or plant operation.

Lighting and Servicing Power Supply System (LSP)

LSP supplies 120 VAC to N-DCIS for lighting (including internal cabinet lighting and convenience outlets) and maintenance equipment.

7.1.5.11 N-DCIS Major System Interfaces

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

- ARMS, Auxiliary Boiler System (ABS),
- C&FS, Chilled Water System, Circulating Water system (CIRC), Condensate Storage and Transfer System, Containment Inerting System, Containment Monitoring System (CMS), Control Building 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, Fire Protection System (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, Instrumentation and Control 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, Meterological Observation Station, Moisture Separator Reheater System (MSR),
- NBS, NMS,
- Offgas System (OGS), Oil Storage and Transfer System, Oxygen Injection system (OIS),
- PAS, Passive Contrainment Cooling System (PCCS), Plant Service Water System (PSWS), Process Sampling System (PSS),
- Q-DCIS,
- Radwaste Building HVAC, RC&IS, Reactor Building HVAC, Reactor Component Cooling Water System, Reactor Water Cleanup and Shutdown Cooling System (RWCU/SCS), RPMS, RPS, RSS,
- 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), Turbine Generator Control System (TGCS), Turbine Gland Seal System, Turbine Lube Oil System (TLOS), Turbine Main Steam System (TMSS),
- Uninterruptible AC Power Supply,
- Yard Miscellaneous Drain System
- Zinc Injection System (ZNI), an optional system

7.1.6 Conformance with Regulatory Requirements and Industry Codes and Standards

NUREG 0800, Table 7.1 lists the Code of Federal Regulations, General Design Criteria (GDC), Staff Requirements Memoranda, Regulatory Guides, 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 guidelines 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 Section 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 Conformance with the 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

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 relative to the systems in Table 7.1-1. The applicable systems are generally designed to conform. However, because of the design features of the ESBWR, 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
  - II.K.3.22 - RCIC Automatic Switchover of Suction Supply

For the others, the degree of conformance, along with any clarifications or exceptions, is discussed in the safety evaluation subsections of Sections 7.2 through 7.8. The TMI action items applicable to the I&C systems are:

- 50.34(f)(2)(v) [I.D.3] Bypass and Inoperable Status Indication
- 50.34(f)(2)(xii) [II.E.1.2] Auxiliary Feedwater System Automatic Initiation and Flow Indication
- 50.34(f)(2)(xvii) [II.F.1] Accident Monitoring Instrumentation
- 50.34(f)(2)(xviii) [II.F.2] Inadequate Core Cooling Instrumentation

- 50.34(f)(2)(xiv) [II.E.4.2] Containment Isolation Systems
- 50.34(f)(2)(xix) [II.F.3] Instruments for Monitoring Plant Conditions Following Core Damage
- 50.34(f)(2)(xx) [II.G.1] Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves
- 50.34(f)(2)(xxii) [II.K.2.g] Failure Mode and Effects Analysis of Integrated Control System
- 50.34(f)(2)(xxiii) [II.K.2.10] Anticipatory Trip on Loss of Main Feedwater or Turbine Trip
- 50.34(f)(2)(xxiv) [II.K.3.23] Central Reactor Vessel Water Level Recording

10 CFR 50.62 (ATWS): The ESBWR is designed with 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 Tier 1.

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: Interface material is provided in Tier 1.

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

- Conformance: The level of detail provided for the RPS within the Tier 1 and Tier 2 documents conforms with this regulation.

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

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

10 CFR 52.79(c), ITAAC in Combined Operating License Applications

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

7.1.6.2 Conformance with General Design Criteria (GDC), 10 CFR 50 Appendix A

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

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

- Conformance: 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 Conformance with Staff Requirements Memoranda (SRM)

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

- The ESBWR 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 instrumentation and control system that specifically addresses the requirements of this SRM.

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

- The ESBWR alarm management system meets the intent of the EPRI requirements for redundancy, independence, and separation in that the "alarm system" is considered redundant. Alarm points are sent via dual network 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 (dual power supplies on each). The alarm tiles (or equivalent) are driven by redundant data links (dual power). The alarm processor is redundant. There are no alarms requiring manually controlled actions for safety-related systems to accomplish their safety-related function. Thus the requirements for safety-related equipment and circuits are not applicable.

7.1.6.4 Conformance with Regulatory Guides

A discussion of the general conformance of the I&C equipment to the RGs is provided below. Individual system conformance, along with any clarifications or exceptions, is addressed in the Safety Evaluation subsections within Sections 7.2 through 7.8.

RG 1.22 - Periodic Testing of Protection System Actuation Functions. Safety-related systems have provision for periodic testing. Proper functioning of analog sensors can be verified by channel cross-comparison and is done continuously by the plant computer functions. 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 requirements 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 requirement 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 are designed using 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 ESBWR is being designed to meet N-2.

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

RG 1.75 **-** Physical Independence of Electric Systems**.** The safety-related system designs conform with the physical independence criterion.

The I&C of the safety-related systems complies with the independence and separation criteria for redundant systems in accordance with RG 1.75 or by implementation of the following alternates:

- Associated circuits installed in accordance with IEEE Std. 384, Subsection 5.5.2(1), are subject to the requirements of safety-related circuits for cable derating, environmental qualification, flame retardants, splicing restrictions, and raceway fill unless it is demonstrated that safety-related circuits are not degraded below an acceptable level by the absence of such requirements.

- The method of identification used (IEEE Std. 384, Subsection 6.1.2) preclude the need to frequently consult any reference material to distinguish between safety-related and nonsafety-related circuits, between nonsafety-related circuits associated with different redundant safety-related systems, and between redundant safety-related systems.

- First sentence of IEEE Std. 384, Section 6.8 is implemented as follows:

  - Redundant safety-related sensors and their connections to the process system will be sufficiently separated so that required functional capability of the protection system is maintained despite any single design basis event.

  - Nonsafety-related instrumentation circuits are exempted from the provisions of IEEE 384, Section 5.6, provided they are not routed in the same raceway as power and control cables (unless the cables are optical fiber) or are not routed with associated cables of a redundant division.

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 requirements 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 requirements 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 required "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 both 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 requirements of RG 1.118, with the following clarifications of the RG requirements:

- Position C.6b - Trip of an associated protective channel or actuation of an associated safety-related load group is required on the removal of fuses or the opening of a breaker only for the purpose of deactivating I&C circuits.
- Position C.2 - Insofar as it is practical and safe, response time testing is performed from sensor inputs (at the sensor input connection for process instruments) to and including the actuated equipment.

RG 1.151 - Instrument Sensing Lines. The instrument sensing lines are designed to satisfy the requirements of RG 1.151. Such lines are used to perform both safety-related and nonsafety-related functions. However, there are four redundant and 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 using sensors separate from the safety-related sensors. Therefore, the systems are designed such that no single failure or two division failure could cause an event and at the same time prevent mitigating action for the event.

RG 1.152 - Computer Software Used in Safety-related Systems. Criteria and guidelines stated in ANSI/IEEE-ANS-7-4.3.2, as endorsed by RG 1.152 are used as a basis for design procedures established for programmable digital equipment.

IEEE Std. 7-4.3.2 Summary:

RG 1.152 is the main RG on digital computers in safety-related systems in nuclear power plants. RG-1.152 endorses and refers to IEEE Std. 7-4.3.2 and IEEE Std. 603 for specific criteria details.

One major requirement area in RG 1.152 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. Conditions may exist where some form of diversity may be necessary to provide 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.

RG 1.152 contains extensive requirements on “security” and endorses IEEE Std. 7-4.3.2.

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 (that is, 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 basically unchanged from the 1993 version. This annex provides a methodology for determining the need for diversity. RG 1.152 does not endorse this Annex B.
- Annex C "Dedication of existing commercial computers": This is similar to the 1993 version. The NRC refers to Reference 7.1-11 as a replacement for Annex C.
- Annex E, "Communication Independence": This 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.
- ESBWR Safety I&C System compliance with IEEE Std. 7-4.3.2

RG 1.152 includes additional requirements applicable to Q-DCIS. The ESBWR compliance with these additional requirements is summarized as follows.

Defense against software common mode failures: GE 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: control systems, reactor trip 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 is developed to back 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/Standby Liquid Control system (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 Q-DCIS (including control systems key for plant operation) will follow the guidelines of BTP HICB-14. Software development process plans for the ESBWR DCIS design implementation include the Software Management Plan (SMP), Software Development Plan (SDP), Software Verification and Validation Plan (SVVP), Software Configuration Management Plan (SCMP), and Software Safety Plan (SSP), etc., as required by guidance in BTP HICB-14 and are described in Appendix 7B. 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 specifies that these requirements are applicable to safety-related I&C system equipment. 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 as needed in the DCIS design, both on plant hardware security measures and software security measures. The software development process plans will be developed with the security requirements incorporated for actual detailed design implementation.

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems. Safety-related systems are designed to satisfy the requirements of IEEE Std. 603, as endorsed by RG 1.153. Clarifications or exceptions (if any) for any of the provisions are discussed in the individual systems safety evaluation sections.

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 Software Verification and Validation Plans, 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 Appendix 7B, to develop portions of the overall software development plan 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 Software Configuration Management Plans, 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 Appendix 7B, to develop portions of the overall software development plan 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 requirement 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, as discussed in Appendix 7B, to develop portions of the overall software development plan 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, as discussed in Appendix 7B, to develop portions of the overall software development plan 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 will 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 discussed in Appendix 7B, 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 discussed in Appendix 7B, to develop portions of the overall software development plan and thus comply with this RG.

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems

Electrical and electronic components in the I&C safety-related systems will be qualified for anticipated levels of Electromagnetic Interference (EMI) at their as-installed locations. Electromagnetic compatibility (EMC) of I&C equipment will be verified through factory testing and site-specific testing for both individual equipment and interconnected systems to meet EMC requirements for protection against:

- EMI
- Radio Frequency Interference (RFI)
- Electrostatic Discharge

- Electrical Surge

In the ESBWR design, 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. Reference 7.1-3 is used to define the envelope limits. To that end, EMI qualification for safety-related systems in the ESBWR design meets 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 Conformance with Branch Technical Positions

Applicable BTPs are identified relative to the I&C systems in Table 7.1-1. BTPs are guidance documents and the 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-8 - Guidance on Application of RG 1.22. Q-DCIS is fully-operational during reactor operation and is tested in conjunction with the SSLC/ESF. Therefore, Q-DCIS fully meets this BTP.

BTP HICB-11: Guidance on Application and Qualification of Isolation Devices. Refer to Subsection 7.2.1.12 discussion. Q-DCIS conforms with this BTP.

BTP HICB-12: Guidance on Establishing and Maintaining Instrument Setpoints. Refer to Subsection 7.2.1.12 discussion. Q-DCIS conforms with this BTP.

BTP HICB-14: Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Safety Systems. Refer to Subsections 7.1.2.4 and 7.2.1.12 and Appendix 7B discussion. Q-DCIS conforms with the guidance of this BTP.

Q-DCIS and N-DCIS will follow a development process that is in accordance with BTP HICB-14. Compliance with BTP HICB-14 is explained and summarized in Appendix 7B of this chapter. As part of the ESBWR Certification activity, the software development process plans require NRC review and approval.

ESBWR safety-related I&C systems (RPS and SSLC/ESF) use computers for their logic functions. A description of 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 DCD including this section on Q-DCIS.

In the BTP HICB-16 requirements, it is stated that the application should: (1) describe the resolution of unresolved and generic safety issues applicable to the I&C systems, and (2) 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; and (3) 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 Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) functions should also describe the design of the overall I&C systems with respect to defense-in-depth and diversity requirements.

The ESBWR does not have unresolved or generic safety-related issues applicable to I&C systems. In DCD 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. The above issues either are not applicable to ESBWR safety-related I&C systems design or the ESBWR has addressed those issues in its safety-related I&C design.

Within the scope of the ESBWR DCD submitted for certification application, there are no interface requirements described here that fall into the above category.

The ESBWR 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 ESBWR 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 Instrumentation and Control Systems. Refer to Subsection 7.2.1.12 and 7.3.4.3 discussion. Q-DCIS conforms with this BTP.

BTP HICB-18: Guidance on Use of Programmable Logic Controllers in Digital Computer-based Instrumentation and Control System. Refer to Subsection 7.2.1.12 discussion. 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). Refer to Subsection 7.2.1.12 discussion. Q-DCIS conforms with this BTP.

BTP HICB-21: Guidance on Evaluation of Digital System Architecture and Real-Time Performance. Refer to Subsection 7.2.1.12 discussion. Q-DCIS conforms with this BTP.

7.1.6.6 Conformance with Industry Standards

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

Other codes or standards, not mentioned in the SRP, may be utilized 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 – "Electromagnetic Compatibility (EMC) Testing and Measurement Techniques. This applies to EMI qualification.

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) and remain 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". Independence of safety-related equipment is discussed in Subsection 7.1.6.6.1.

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". This applies to EMI qualification.

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". This applies to EMI qualification and electrical equipment protection.

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, except for the requirement to provide 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 (for example, for accident monitoring instrumentation provided in accordance with RG 1.97). Conformance with the requirements of IEEE Std. 603, is also identified as conforming with the requirements and guidance contained

within the federal regulations, GDC, SRM, RGs, as described. The ESBWR safety-related I&C design, which comprises the Q-DCIS, RPS, NMS, and SSLC/ESF conforms with IEEE Std. 603. ITAACs are provided for the major attributes for compliance with IEEE-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 in part 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 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 as discussed 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 system design basis descriptions are included in the various sections of this chapter as indicated below.

- Reactor Trip System:
  - RPS Subsection 7.2.1
  - 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
  - SSLC/ESF Subsection7.3.5
- SLC Subsection 7.4.1
- RSS Subsection 7.4.2
- RCWU/SDC Subsection 7.4.3

- ICS Subsection 7.4.4
- CMS Subsection 7.5.2

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

The ESBWR safety-related control systems include sufficient redundancy, diversity, and independence to meet system performance requirements even 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 and prevent a single failure from causing either an inadvertent reactor trip or 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 (typically by optical couplers and fiber optic cabling) and one-way. Each division is sufficiently independent from the other divisions such 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, which receive input data from their own division's set of diverse and/or redundant sensors connected to the same process source, sense conditions that require a safety-related trip and they separately broadcast trip signals. The trip actuators go to their trip state whenever they receive concurrent trip signals from any two safety-related logic controller broadcasts. 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 (that is, short circuits, or high voltage) such that the faults cannot propagate into and degrade the performance of any safety-related control function.

Licensing Topical Report (LTR), "ESBWR I&C Defense-In-Depth and Diversity Report," NEDO-33251, (See Reference 7.1-4) describes the type of diversity that exists among the four echelons of defense-in-depth for the ESBWR and identifies the dependencies, 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) will be performed of the complete safety-related reactor protection, ESF, and DPS designs. The methodology for performing the block level FMEA is described in NEDO-33251 (Reference 7.1-4). In addition, the platform specific LTRs for the safety-related system architectures will include analysis summaries of the architecture's conformance with the requirements of IEEE Std. 603. The report, "ESBWR Safety Criteria for Instrumentation & Control Systems," NEDO-33294, (reference 7.1-5) will

describe how the overall ESBWR safety-related system designs conform with IEEE Std. 603, Criterion 5.1, based on the above discussion and the results of the architecture reports.

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, either by the use of 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 upon 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 provided 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 GE's Appendix B quality program. The NRC accepted GE 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, programs and/or firmware conform with the quality requirements described in IEEE 7-4.3.2 as described in the LTR, "ESBWR I&C Software Quality Assurance Plan," NEDO-33245 (Reference 7.1-10).

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

It is required that safety-related system equipment be designed to meet the functional performance requirements over the range of normal 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. Q-DCIS systems are designed to meet the equipment qualification requirements set forth in IEEE Std. 603 and other associated equipment qualification requirements. The qualification was established using qualification methods set forth in GE's Environmental Qualification Program. (See Reference 7.1-2). Q-DCIS components are designed to be qualified to operate in the normal and abnormal environments in which they are located.

For environmental qualification, the following areas are addressed:

Temperature and Humidity: Q-DCIS components are designed to be qualified using type testing and analysis to demonstrate that the components will perform all specified functions correctly when operated within the specified temperature range and relative humidity range. The components will be qualified in accordance with RG 1.89 (IEEE Std. 323 - 1974) and IEEE Std. 323 - 1983. All qualification will be based on type testing. The designers of the HVAC systems

will be required to confirm that the maximum control room temperature plus mounting panel temperature rise, allowing for the heat load of the Q-DCIS equipment, does not exceed the temperature limit, and that control room humidity is maintained within limits.

Pressure: Q-DCIS components are designed to be qualified (by analysis) to perform to specification for any absolute pressure in the range specified. The design of the HVAC systems surrounding the Q-DCIS components ensures that the maximum control room pressure does not exceed the specified limit.

Radiation: Q-DCIS components are designed to be qualified (by analysis) to perform within specification limits 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: Q-DCIS components are designed to be qualified (by type testing and analysis) to demonstrate that the components will perform all specified functions correctly when operated within the specified seismic limits, and when mounted in accordance with the specified mounting methods. Q-DCIS components are to be qualified in accordance with the requirements of RG 1.100 (IEEE Std. 344 - 1975). Qualification is based on type testing. The design ensures that the maximum seismic accelerations at the mounting locations of the equipment do not exceed the allowed limits.

EMI Qualification: Q-DCIS components in conformance with RG 1.180, when mounted in accordance with the specified mounting methods, are designed to be qualified by type testing and analysis to demonstrate that the components will perform all specified functions correctly when operated within the specified EMI limits. Q-DCIS equipment is designed to be not susceptible to electromagnetic disturbances from neighboring modules and does not 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. Q-DCIS equipment is qualified to perform within its specifications continuously while exposed to EMI environmental limits at the hardware mounting location. Reference 7.1-3 is used for the envelope limits. 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)

Q-DCIS systems are required to accomplish their safety-related functions under the full range of applicable conditions enumerated in the design basis. 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.

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 such that the actuated component remains “as-is;” this prevents a control system induced LOCA. Hardware and

software failures detected by self-diagnostics will cause a trip signal to be generated in the division in which the failure occurs in RPS and no signal if the failure occurs in a SSLC/ESF division. Failure of hardware and software will not inhibit manual initiation of protective functions. More descriptions 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 the safety-related systems and the effects of DBEs, and between the 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. Q-DCIS systems have four redundant and independent channels (divisions), which are physically independent and separated, with independent electrical power sources applied to each channel. Unless optical fiber 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 communication interface modules and optic fibers.

Independence between the safety-related systems and the effects of DBEs is achieved through proper equipment qualification. Safety-related equipment is qualified for continued 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 (for example, the communication interface modules and fiber wired network) and data path gateway. Communication from nonsafety-related systems to safety-related systems is prohibited, with only one exception, (that is, the data transmission of LPRM calibration gain adjustment factors which are calculated in the nonsafety-related plant computer function of N-DCIS), 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. RPS and SSLC/ESF protection functions have priority over data transmissions, so that data transmissions do not interfere with RPS or SSLC/ESF protection functions. More descriptions 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 may 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. Q-DCIS meets the requirements outlined in this section. More descriptions 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 will include the necessary steps to ensure compliance with regulatory requirements including 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 for which no automatic control is provided and that are required for safety-related systems to accomplish their safety-related functions for DBEs. Additional discussion on this subject is included in Subsection 7.5.1.

System Status Indication: The ESBWR 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 available to be displayed to the operator upon request. For safety-related systems, such information is available for each division/channel. Certain information, key to plant operation and status monitoring, is permanently displayed (on the large wide display panels) 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. All bypass status information is available to be displayed in accordance with system design requirements; certain bypass information is accompanied with an alarm. More descriptions 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 all displays located in the MCR are either on the main control console or on the large WDP visible and accessible to the operator. The ESBWR 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 the associated references of Chapter 18.

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 control of access such that

qualified plant personnel are allowed to have access to keys (doors, cabinets, 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, logic bypass operation, and access to other plant operation switches. Keys, passwords, and other security devices (per the requirements of RG 1.152) are used by qualified plant personnel to enter specific rooms, open specific equipment cabinets, obtain permission to enter specific electronic instrument for calibration, testing, setpoint changes, and gain access to safety-related system software and data, etc. However, software of safety-related systems is typically not changeable at the plant site. The ESBWR 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 via 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)

Q-DCIS systems are designed to allow the timely recognition (through periodic self-diagnostic functions) of location, replacement (through module replacement), and repair and adjustment of malfunctioning equipment. The self-diagnostic function will locate the failure to the component level. Through individual channel bypassing, the failure component can be replaced or repaired on line without affecting the safety-related system protection function, with the trip logic 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 will support dual divisional failures and still provide all ESBWR safety functions.

7.1.6.6.1.12 Identification (IEEE Std. 603, 5.11)

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 and 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 is implemented to formalize system component and software identification.

7.1.6.6.1.13 Auxiliary Features (IEEE Std. 603, 5.12)

ESBWR safety-related I&C system auxiliary supporting features satisfy the requirements of this standard where applicable, such as safety-related electrical system equipment including batteries, inverters, etc. Q-DCIS is supported by four divisions of safety-related uninterruptible power, and separately, as required, by four divisions of instrument power supply. DC batteries also supply power if there is a loss of both off-site and on-site AC power.

HVAC is a key auxiliary supporting system that maintains the necessary environmental conditions for the safety-related ESBWR I&C equipment. Under normal operating conditions

and whenever the diesel generators are available, HVAC is provided to control the temperature/humidity of all I&C equipment in all of the buildings. Under a loss of power condition including Station Blackout (SBO), batteries are provided for continued safety-related I&C operation for 72 hours, and continued operation of the nonsafety-related I&C equipment for two hours. HVAC will no longer be available to either the control building or reactor building equipment (except the control room area as noted below). The safety-related I&C equipment will be qualified for the expected temperature rise. Battery-operated nonsafety-related HVAC is provided to allow continued operation of the safety-related and nonsafety-related I&C for the approximately two hours of nonsafety-related battery capacity. Should the nonsafety-related HVAC (redundant) not be available, safety-related temperature sensors (with two-out-of-four logic) will trip the control room power that feeds the nonsafety-related I&C; the safety-related I&C is qualified for the resulting temperature rise. This scheme is used to protect the equipment and maximize operator comfort. Additional description of the HVAC design is included in Chapter 9.

Other auxiliary features that support Q-DCIS functions are designed such that these components will not degrade the safety-related system 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 ESBWR standard design. The ESBWR standard design submitted for NRC certification is for a single unit plant.

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

The ESBWR 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 for the ESBWR.

7.1.6.6.1.16 Reliability (IEEE Std. 603, Section 5.15)

The degree of redundancy, diversity, testability, and quality of the ESBWR safety-related I&C design is adequate to achieve the functional reliability necessary to perform its function. Safety-related equipment is provided under GE’s Appendix B quality program. BTP-14 will be followed for software development processes to achieve 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. LTR, “ESBWR I&C Defense-in-Depth and Diversity Report,” NEDO-33251 (Reference 7.1-4), provides specific information on the redundancy and diversity used in ESBWR safety-related I&C systems. Q-DCIS is included in the consideration of the ESBWR PRA. (See Chapter 19)

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

The ESBWR RPS and SSLC/ESF logic is designed to automatically initiate reactor scram trip and actuate the engineered safety features to mitigate the consequences of AOOs and DBEs. Such automatic protection actions are implemented via two-out-of-four voting logic whenever one or more process variables (monitored and measured by each of the RPS and SSLC/ESF divisions) reach the scram or ESF actuation setpoint.

Plant-specific setpoint analyses evaluate whether the protection systems' precision is adequate and thus ensure that the systems' real-time performance is deterministic and known. ESBWR instrument setpoints are determined by setpoint and safety-related analyses described in the GE Setpoint Methodology Licensing Topical Report, NEDC 31336P-A (See Reference 7.1-9). The GE Setpoint Methodology uses plant-specific setpoint analyses to ensure that the characteristics of the instruments (that is, 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.

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

The ESBWR design provides for manual initiation of each protective action 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 must satisfy divisional rules for independence and separation; two manual actions, each in a separate division, are required to satisfy the two-out-of-two system logic or the two-out-of-four division logic that initiates reactor trip and isolation functions (RTIF) in the RPS and ESF functions in the 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 to prevent single failures from firing or inhibiting the firing of the squib valves, that is, the GDCS pool injection valves, the suppression pool injection valves, the GDCS deluge valves, the ADS depressurization valves (DPV), and the SLC injection valves. To initiate the GDCS short-term injection and long-term injection systems manually, 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 with control rods (that is, reactor trip), by any of three different methods using redundant or diverse controls. The reactor trip will occur 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 diverse protection system (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, also 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 such that the information provided, display content and location are taken into consideration for easy operator access and action in the MCR. No single or two division failure will prevent the initiation of the protection action. 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 descriptions 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)

Q-DCIS protection systems are totally separate and independent from the nonsafety-related control systems such that any failure of nonsafety-related systems will not affect and will not prevent the safety-related protection system from performing its safety-related functions. Upon failure of one safety-related channel, 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 only from the protection system to the N-DCIS, thus 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, the technique to provide 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 by nonsafety-related control systems although calculated safety-related signals such as APRMs may be used, after isolation, by nonsafety-related control systems. Q-DCIS meets the requirements of GDC 24. Additional descriptions of 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 LPRM units needs operator acknowledgment for implementation, and does not interfere with reactor protection function or ESF actuation function.)

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 only two RPS sensing inputs that are not direct measures of the variables are the Reactor Pressure Vessel (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 BWR applications. The loss of feedwater flow variable is represented by the loss of the power generation bus signal, because 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 meet the requirements of the safety-related analysis of Chapter 15, since 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.

ESBWR instrument setpoints are determined by setpoint and safety-related analysis using GE Setpoint Methodology, NEDC 31336P-A (Reference 7.1-9). The GE Setpoint Methodology uses plant-specific setpoint analyses to ensure that the characteristics of the instruments (that is, 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. 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.

7.1.6.6.1.21 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 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 cross-checking of monitored variables. The third available channel may also be available for cross-checking 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 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 ESBWR safety-related I&C operating bypass design. Specific descriptions of safety-related system operating bypasses are included in Subsections 7.2.1.1, 7.2.2.2, and 7.3.5.2. Operating bypasses are automatically removed as described in Subsections 7.2.1.1, 7.2.2.2, 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 Q-DCIS. This is mainly to permit equipment maintenance, testing, and repair of one individual division/channel with the plant still operating and without initiating any protection functions. The single failure criterion is maintained under such a bypass condition and, although it is possible to only bypass one division at a time, the ESBWR Q-DCIS design would still 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) where only one channel (out of four channels) is allowed 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 7.2.1.1, 7.2.2.2, and 7.3.5.2.

7.1.6.6.1.24 Setpoints (IEEE Std. 603, Section 6.8)

ESBWR instrument setpoints are determined by setpoint and safety-related analysis using the GE Setpoint Methodology, NEDC 31336P-A (Reference 7.1-9). The GE Setpoint Methodology uses plant-specific setpoint analyses to ensure that the characteristics of the instruments (that is, 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)

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 Subections 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 hydraulic scram, following a signal from the RPS. The Low Control Rod Drive HCU Accumulator Charging Header Pressure (CRD system) sounds an alarm in the MCR when a loss of nitrogen decreases the nitrogen pressure, and actuates a pressure switch. A float type level switch actuates an alarm if water leaks past the piston barrier and collects in the accumulator instrumentation block.

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)

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. After 72 hours, Q-DCIS can operate continuously from either of the two ESBWR diesel

generators or off-site power. This allows for operation of the Q-DCIS when one power supply is in maintenance bypass. 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 both plant hardware and software security measures. The software development process plans will be developed with the security requirements incorporated for actual detailed design implementation.

The comprehensive cyber security program plan identifies security risks and outlines appropriate procedures to ensure that hardware, controls, and data networks comprising the control network cannot be disrupted, interrupted or negatively impacted by unauthorized users or external systems. It also documents the design commitments meeting 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 ESBWR DCD, Tier 1 together with the software development plan.

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 Electric Power Research Institute (EPRI) TR-102323 (TR-1003697), "Guidelines for Electromagnetic Interference Testing of Power Plant Equipment", Revision 3.

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 GE Energy, “ESBWR Safety Criteria for Instrumentation & Control Systems.” NEDO-33294, Class I (Non-proprietary), Revision 0.

7.1-6 GE Energy, “Application of Nuclear Measurement Analysis and Control for a new BWR (NUMAC Platform Architecture.)” NEDC-33288P, Class III (Proprietary), Revision 0

7.1-7 GE Energy, “SSLC/ESF Licensing Topical Report (Platform Architecture.)” Class III (Proprietary), Revision 0

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, "ESBWR I&C Software Quality Assurance Plan," NEDO-33245, Class I (Non-Proprietary).

7.1-11 Electric Power Research Institute (EPRI) TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications".

Table 7.1-1 Regulatory Requirements Applicability Matrix

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

Notes: Q=Q-DCIS, N=N-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 7.1-1 Regulatory Requirements Applicability Matrix

Applicable Criteria Guidelines: SRP NUREG-0800, App. 7.1	General Design Criteria (GDC)												SRM to SECY 93-087	
	1	2	4	13	19	20	21	22	23	24	25	29	II.Q	II.T
Reference Standard		IEEE Std. 603	IEEE Std.. 603	IEEE Std.. 603		IEEE St.d. 603	IEEE Std. 603 and 338	IEEE Std. 603	IEEE Std. 603	IEEE Std. 603	IEEE Std. 603	IEEE Std. 603	BTP HICB-19	
RPS (Q)	X	X	X	X	X	X	X	X	X	X	X	X	X	
NMS (Q)	X	X	X	X	X	X	X	X	X	X	X	X	X	
SPTM Function (Q)	X	X	X	X	X	X	X	X	X	X	X	X	X	
ADS (Q)	X	X	X	X	X	X	X	X	X	X			X	
GDCS (Q)	X	X	X	X	X	X	X	X	X	X			X	
LD&IS (Q)	X	X	X	X	X	X	X	X	X	X			X	
CRHS (Q)	X	X	X	X	X	X	X	X	X	X			X	
SSLC/ESF (Q)	X	X	X	X	X	X	X	X	X	X			X	
SLC (Q)	X	X	X	X	X					X				
RSS (Q and N)	X	X	X	X	X					X				
RWCU/SDC (N)		X	X	X	X					X				
ICS (Q)	X	X	X	X	X					X				
PAM (Q and N)†	X	X	X	X	X					X				X
CMS (Q and N)	X	X	X	X	X					X				X
PRMS (Q and N)	X	X	X	X	X					X				X
ARMS (N)		X	X	X	X					X				
Interlock Systems (Q and N) †	X	X	X	X	X					X	X			
NBS (Q)	X	X	X	X	X					X			X	
RC&IS (N)				X	X					X		X		
FWCS (N)				X	X					X				
PAS (N)				X	X					X				
SB&PC (N)				X	X					X				
NMS (N)				X	X					X				
Containment Inerting System (N)				X	X					X				
Diverse I&C (N)	X			X	X					X			X	
Q-DCIS (Q)	X	X	X	X	X		X	X	X	X		X	X	X
N-DCIS (N)				X	X					X				

Table 7.1-1 Regulatory Requirements Applicability Matrix

Applicable Criteria Guidelines: SRP NUREG-0800 App. 7.1	Regulatory Guides																		
	1.153	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	1.204
Reference Standard	Refer to RG 1.153	IEEE Std. 603	IEEE Std. 379, IEEE Std. 603	IEEE Std. 603	IEEE Std. 384	IEEE Std. 497	ANSI/ISA S67.04.01	IEEE Std. 338	ANSI/ISA-	IEEE Std. 7-4.3.2	IEEE Std. 603	IEEE Std. 1012, IEEE Std.1028	IEEE Std. 828	IEEE Std. 829	IEEE Std. 1008	IEEE Std. 830	IEEE Std. 1074	IEEE Std. 1050	IEEE Std. 1050
RPS (Q)	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X	X	X
NMS (Q)	X	X	X		X	X	X	X		X	X	X	X	X	X	X	X	X	X
SPTM Function (Q)	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X
ADS (Q)	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X	X	X
GDCS (Q)	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X	X	X
LD&IS (Q)	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X	X	X
CRHS (Q)	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X	X	X
SSLC/ESF (Q)	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X	X	X
SLC (Q)			X		X		X	X			X							X	X
RSS (Q and N)			X		X			X			X							X††	X
RWCU/SDC (N)																		X††	X
ICS (Q)			X		X		X	X		X	X	X	X	X	X	X	X	X	X
PAM (Q and N)†						X												X††	X
CMS (Q and N)		X	X		X		X	X		X	X	X	X	X	X	X	X	X††	X
PRMS (Q and N)		X	X		X		X	X		X	X	X	X	X	X	X	X	X††	X
ARMS (N)																		X††	X
Interlock Systems (Q and N) †		X	X		X		X	X		X	X	X	X	X	X	X	X	X††	X
NBS (Q)					X		X		X	X	X	X	X	X	X	X	X	X	X
RC&IS (N)																		X††	X
FWCS (N)																		X††	X
PAS (N)																		X††	X
SB&PC (N)																		X††	X
NMS (N)																		X††	X
Containment Inerting System (N)																		X††	X
Diverse I&C (N)	X			X	X		X	X		X	X	X	X	X	X	X	X	X††	X
Q-DCIS (Q)	X	X	X		X		X	X		X	X	X	X	X	X	X	X	X	X

Table 7.1-1 Regulatory Requirements Applicability Matrix

Applicable Criteria Guidelines: SRP NUREG-0800 App. 7.1	Regulatory Guides																		
	1.153	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	1.204
Reference Standard	Refer to RG 1.153	IEEE Std. 603	IEEE Std. 379, IEEE Std. 603	IEEE Std. 603	IEEE Std. 384	IEEE Std. 497	ANSI/ISA S67.04.01	IEEE Std. 338	ANSI/ISA-	IEEE Std. 7-4.3.2	IEEE Std. 603	IEEE Std. 1012, IEEE Std.1028	IEEE Std. 828	IEEE Std. 829	IEEE Std. 1008	IEEE Std. 830	IEEE Std. 1074	IEEE Std. 1050	IEEE Std. 1050
N-DCIS (N)																		X††	X

*NOTE: These criteria are addressed in conjunction with the digital computer-related functions of the Q-DCIS; ♀ IEEE Std. 603 provides criteria for the safety-related systems in lieu of the endorsed standard, IEEE Std. 279 that has been withdrawn.. 10 CFR 50.44(c)(4) applies to CMS.

Table 7.1-1 Regulatory Requirements Applicability Matrix

Applicable Criteria Guidelines: SRP NUREG-0800 App 7.1	Branch Technical Positions (BTP) HICB														
	HICB-1	HICB-3	HICB-6	HICB-8	HICB-9	HICB-10	HICB-11	HICB-12	HICB-13	HICB-14*	HICB-16	HICB-17*	HICB-18*	HICB-19*	HICB-21*
Reference Standard	IEEE Std. 603	IEEE Std. 603	IEEE Std. 603	Refer to RG 1.153	Refer to RG 1.153	Refer to RG 1.97	Refer to RG1.75 and RG 1.153	Refer to RG 1.105	Refer toRG 1.153	Refer to RG 1.152		Refer to RG 1.22, 1.47, 1.53, 1.118, 1.152 and 1.153,	Refer to RG 1.152	NUREG/CR-6303	NUREG/CR-6083
RPS (Q)		X		X	X		X	X	X	X	X	X	X	X	X
NMS (Q)		X		X		X	X	X		X	X	X	X	X	X
SPTM Function (Q)		X		X		X	X	X	X	X	X	X	X	X	X
ADS (Q)		X	X	X			X	X		X	X	X	X	X	X
GDCS (Q)	X	X	X	X			X	X	X	X	X	X	X	X	X
LD&IS (Q)				X			X	X	X	X	X	X	X	X	X
CRHS (Q)				X			X	X	X	X	X	X	X	X	X
SSLC/ESF (Q)		X	X	X			X	X	X	X	X	X	X	X	X
SLC (Q)							X	X			X				
RSS (Q and N)							X			X	X	X	X		X
RWCU/SDC (N)											X				
ICS (Q)							X	X	X	X	X	X	X		X
PAM (Q and N)†						X									
CMS (Q and N)							X	X	X	X	X	X	X		X
PRMS (Q and N)							X	X	X	X	X	X	X		X
ARMS (N)											X				
Interlock Systems (Q and N) †	X						X	X		X	X	X	X		X
NBS (Q)							X	X		X	X	X	X	X	X
RC&IS (N)											X				
FWCS (N)											X				
PAS (N)											X				
SB&PC (N)											X				
NMS (N)											X				
Containment Inerting System (N)											X				
Diverse I&C (N)				X			X	X		X	X	X	X	X	X
Q-DCIS (Q)				X			X	X		X	X	X	X	X	X
N-DCIS (N)										X	X				

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std 603 Specific Criteria Compliance

Subject		I&C Systems	RTS	ESF	SS	IS	IL	CS	DICS
		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 (N)	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	7.1.6.6.1.1, 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, 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	7.1.2; 7.1.3; 7.1.6.6.1 (Q-DCIS)	7.1.6.6.1, Table 15.0-2, NEDO-33251; 7.2.1.1, 7.2.1.2.4.1, 7.2.1.2.4.1.2, 7.2.1.14.2 (RPS), 7.2.2.1, 7.2.2.2. et al (NMS), 7.2.3.1, 7.2.3.2 (SPTMS)	7.3.1.1.1 (ADS), 7.3.1.2.1 (GDCS), 7.3.2 (PCCS), 7.3.3.1 (LDIS), 7.4.1.1 (SLC), 7.4.4.1, 7.4.4.5 (ICS)	7.4.2.2.2 (RSS), 7.4.3.1.1 (RWCU / SDC); 7.4.4.1, 7.4.4.5 (ICS)	7.5.1.1 (Q IC Displays), 7.5.1.2 (PAM), 7.5.2.1 (CMS), 7.5.3.1 (PRMS), 7.5.5.1 (PMS), 7.5.6 (WTDVBM)	7.6.1.1 (HP/LPSI)	7.7.1.1.1 (NBS), 7.7.2.1 (RCIS), 7.7.3.1 (FWCS), 7.7.4.2 (PAS), 7.7.5.1 (SB&PC), 7.7.6.1 (NMS), 7.7.7.1 (CIS)	7.8.1.1 (ATWS), 7.8.1.2 (DIC), 7.8.1.3 (DMCD), 7.8.2.1 (CMF defenses within SSD), 7.8.2.2 (SD against CMF)

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std 603 Specific Criteria Compliance

Subject		I&C Systems	RTS	ESF	SS	IS	IL	CS	DICS
4.6	Spatially dependent variables, identification, number and location	-	7.2.1.2.4.2 (RPS); 7.2.2.2, Figure 7.2-6, 7.2-7, 7.2-8, 7.2-9, 7.2-10 (NMS); 7.2.3.2 (SPTMS)	-	-	Figure 7.2-7, 7.5-2 (PRMS), Figure 7.5-1 (CMS)	-	-	-
4.7	Range of transient and steady-state conditions	-	7.2.1.2.3 (RPS); 7.2.2 (NMS); 7.2.3.2 (SPTMS)	-	-	-	-	-	-
4.8	Adverse environmental conditions	7.1.6.6.1.15 (Q-DCIS)	7.1.6.6.1.15 (RPS); 7.2.2.2 (NMS)	7.4.1.1 (SLC); 7.4.4.3 (ICS)	7.4.1.1 (SLC); 7.4.4.3 (ICS)	-	7.6.1.1 (HP/LPSI)	7.7.1.1.1, 7.7.1.1.3 (NBS)	-
4.10	DBE critical times / conditions	7.1.2, 7.1.3 (Q-DCIS)	Table 4.6-2 (RPS); Table 7.2-2, 7.2-3 (NMS)	-	7.4.1.1 (SLC); 7.4.4.3 (ICS)	-	7.6.1.1 (HP/LPSI)	7.7.1.1.1 (NBS)	-
4.12	Special design basis	-	7.2.2.1.1, Table 7.1-1 (NMS); 7.2.3.1 (SPTMS)	7.4.4.2 (ICS); 7.3.1.1.3.6 (ECCS)	7.4.4.2 (ICS)	-	-	-	-

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std 603 Specific Criteria Compliance

Subject		I&C Systems	RTS	ESF	SS	IS	IL	CS	DICS
5.1	Single failure criterion	7.1.6.6.1.2	7.1.6.6.1.2; 7.1.2.3.6, 7.2.1.2.4, 7.2.1.8 (RPS); 7.2.1.11 (RPS); 7.2.2.1, 7.2.2.1.1, 7.2.2.1.2, 7.2.2.1.3, 7.2.2.1.4, 7.2.2.2.1, 7.2.2.2.2, 7.2.2.2.3, 7.2.2.2.4, 7.2.2.4, 7.2.2.2.4.3, 7.2.2.2.4.6, 7.2.2.2.6.4 (NMS)	7.1.6.6.1.2; 7.3.1.1.2, 7.3.1.1.3, 7.3.1.2.2, 7.3.1.2.3.4, 7.3.1.2.3 (ECCS); 7.3.3.1, 7.3.3.2 (LD&IS); 7.3.4.2 (CRHS); 7.3.5, .2.2 7.3.5.3.4 (SSLC/ESF); 7.4.4.3, 7.4.4.3 (ICS)	7.1.6.6.1.2; 7.4.2.2.1, 7.4.2.3.1.1, 7.4.2.3.3 (RSS)	7.1.6.6.1.2	--	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; 7.1.2.3.6 (RPS); 7.2.1.11 (RPS)	7.1.6.6.1.3; 7.3.1.1.2 (ECCS); 7.3.3.3 (LD&IS); 7.3.5.2.2 (SSLC/ESF)	7.1.6.6.1.3	7.1.6.6.1.3	-	7.1.6.6.1.3	7.1.6.6.1.3
5.3	Quality	7.1.6.6.1.4	7.1.6.6.1.4; 7.1.2.3.6 (RPS)	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	7.1.6.6.1.15	7.1.6.6.1.15 (RPS); 7.2.2.2 (NMS); 7.2.1.12 (RPS)	7.1.6.6.1.15; 7.4.4.2 (ICS)	7.1.6.6.1.15; 7.4.4.2 (ICS)	7.1.6.6.1.15	-	7.1.6.6.1.15	7.1.6.6.1.15; 7.8.2.3 (CMF defenses within SSD)
5.5	System Integrity	7.1.6.6.1.6	7.1.6.6.1.6; 7.2.1.1 (RPS)	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
5.6	Independence	7.1.6.6.1.7; 7.1.1.3 (Q-DCIS)	7.1.6.6.1.7; 7.2.1.2.4.1 (RPS); 7.2.1.11 (RPS), 7.2.2.2.4.3, 7.2.2.2.5.3, 7.2.2.2.6.4, 7.2.2.4.3 (NMS); 7.2.3.3.2.1 (SPTMS)	7.1.6.6.1.7; 7.3.1.2.3.1 (ECCS); 7.3.3.1, 7.3.3.2, 7.3.3.3 (LD&IS); 7.3.4.2 (CRHS) 7.3.5.4.2 (SSLC/ESF)	7.1.6.6.1.7; 7.4.2.2.1, 7.4.2.3.1.1, 7.4.2.3.3 (RSS); 7.4.4.3.1.1 (ICS)	7.1.6.6.1.7	-	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 (CMF defenses within SSD); 7.8.3.1.1 (DIC)

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std 603 Specific Criteria Compliance

Subject		I&C Systems	RTS	ESF	SS	IS	IL	CS	DICS
5.7	Capability for test and calibration	7.1.6.6.1.8; 7.1.1.3, 7.1.1.4, 7.1.1.5 (Q-DCIS)	7.1.6.6.1.8, 7.2.1.11 (RPS)	7.1.6.6.1.8; 7.3.1.1.3.6, 7.3.1.2.4 (ECCS); 7.3.3.4.1, 7.3.3.4.2 (LD&IS); 7.3.5.4 (SSLC/ESF); 7.4.1.4 (SLC); 7.4.4.4, 7.4.4.5 (ICS)	7.1.6.6.1.8; 7.4.1.4 (SLC); 7.4.3.4 (RWCU / SDC); 7.4.4.4, 7.4.4.5 (ICS)	7.1.6.6.1.8	-	7.1.6.6.1.8 7.7.1.4 (NBS)	7.1.6.6.1.8
5.8	Information displays	7.1.6.6.1.9; 7.1.1.5 (Q-DCIS)	7.1.6.6.1.9; 7.2.1.7.1.2, 7.2.1.8.1, 7.2.1.11, 7.2.1.13.3 (RPS); 7.2.2.3.2, 7.2.2.6.1 (NMS); Table 7.2-5 (SPTMS); 7.3.4.5 (SSLC/ESF)	7.1.6.6.1.9; 7.3.1.1.2, 7.3.1.2.2 (ECCS); 7.3.1.1.3.7, 7.3.1.2.3.1, 7.3.1.2.4, 7.3.1.2.5 (ECCS GDCS/ADS); 7.3.3.3.1, 7.3.3.5 (5.2.5 and Tables 5.2-8 and 5.2-9, LD&IS); 7.3.4.2 (CRHS); 7.3.5.3.1, 7.3.5.5 (SSLC/ESF); 7.4.1.5 (SLC); 7.4.4.5 (ICS)	7.1.6.6.1.9; 7.4.2.2.1, 7.4.2.5 (RSS); 7.4.1.5 (SLC); 7.4.2.2.1 (RSS); 7.4.3.5 (RWCU / SDC); 7.4.4.3, 7.4.4.5.1 (ICS)	7.1.6.6.1.9; 7.5.2.5 (CMS)	7.6.1.5 (HP/LPSI)	7.1.6.6.1.9; 7.7.1.5 (NBS)	7.1.6.6.1.9; 7.8.1.3 (DMCD)
5.9	Control of Access	7.1.6.6.1.10	7.1.6.6.1.10, 7.2.1.1 (RPS); 7.2.2.2.3 (NMS)	7.1.6.6.1.10	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
5.10.	Repair	7.1.6.6.1.11; 7.1.1.5 (Q-DCIS)	7.1.6.6.1.11, 7.2.1.2.4.4, 7.2.1.7.1.3 (RPS); 7.2.2.2.4.6, 7.2.2.2.6.6 (NMS)	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
5.11	Identification	7.1.6.6.1.12	7.1.6.6.1.12; (RPS)	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; 7.4.1.2.1 (SLC)	7.1.6.6.1.13; 7.4.1.2.1 (SLC)	7.1.6.6.1.13	7.6.1.2.2	7.1.6.6.1.13	7.1.6.6.1.13

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std 603 Specific Criteria Compliance

Subject		I&C Systems	RTS	ESF	SS	IS	IL	CS	DICS
5.13	Multi-unit stations	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
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
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 (ECCS); 7.3.3.1 (LD&IS)	7.1.6.6.1.17	7.1.6.6.1.17	-	7.1.6.6.1.17	7.1.6.6.1.17
6.2	Manual control	7.1.6.6.1.18	7.1.6.6.1.18; 7.2.1.11 (RPS)	7.1.6.6.1.18; 7.3.1.1.2, 7.3.1.2.2 (ECCS); 7.3.1.2.2 (ECCS GDCS/ADS); 7.3.3.3, 7.3.3.3.1 (LD&IS); 7.3.4.2 (CRHS) 7.3.5.3.1 (SSLC/ESF); 7.4.4.5.1 (ICS)	7.1.6.6.1.18; 7.4.4.5.1 (ICS)	7.1.6.6.1.18	-	7.1.6.6.1.18	7.1.6.6.1.18
6.3	Interaction between the sense and command features and other systems	7.1.6.6.1.19; 7.1.1.3 (Q-DCIS)	7.1.6.6.1.19; 7.2.1.8.1 (RPS); 7.2.2.3.2 (NMS); 7.2.3.3.2.1 (SPTMS)	7.1.6.6.1.19	7.1.6.6.1.19; 7.4.2.2.1, 7.4.2.3.1.1, 7.4.2.3.3 (RSS); 7.4.4.3.1.1 (ICS)	7.1.6.6.1.19	-	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

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std 603 Specific Criteria Compliance

Subject		I&C Systems	RTS	ESF	SS	IS	IL	CS	DICS
6.5	Capability for testing and calibration	7.1.6.6.1.21; 7.1.1.3, 7.1.1.4, 7.1.1.5 (Q-DCIS)	7.1.6.6.1.21, 7.2.1.13, 7.2.1.11, 7.2.1.13.3 (RPS), 7.2.2.5.1 (NMS), 7.2.3.4 (SPTMS); 7.3.4.4 (SSLC/ESF)	7.1.6.6.1.21, 7.3.1.1.3.6 (ECCS); 7.3.1.2.4 (ECCS GDCS/ADS); 7.3.3.4; 7.3.3.4.1, 7.3.3.4.2 (LD&IS); 7.3.5.4 (SSLC/ESF); 7.4.1.4 (SLC); 7.4.4.4, 7.4.4.5 (ICS)	7.1.6.6.1.21, 7.4.2.4 (RSS), 7.4.3.4 (RWCU / SDC); 7.4.4.4, 7.4.4.5 (ICS)	7.1.6.6.1.21, 7.5.1.4 (PAM), 7.5.2.4 (CMS)	7.1.6.6.1.21, 7.6.1.4 (HP/LPSI)	7.1.6.6.1.21, 7.7.1.5 (NBS), 7.7.2.4 (RC&IS), 7.7.3.4 (FWCS), 7.7.4.4 (PAS), 7.7.5.5 (SB&PC), 7.7.6.4 (NMS), 7.7.7.4 (CIS)	7.1.6.6.1.21
6.6	Operating bypasses	7.1.6.6.1.22	7.1.6.6.1.22, 7.2.1.14.2 (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, 7.2.1.14.2 (RPS), 7.3.4.2 (SSLC/ESF)	7.1.6.6.1.23, 7.3.5.2 (SSLC/ESF)	-	-	-	7.7.2.2.7.6 (RC&IS)	-
6.8	Setpoints	7.1.6.6.1.24	7.1.6.6.1.24; 7.2.1.3 (RPS), 7.2.2.1.1.1, 7.2.2.2.4.5, 7.2.2.2.4.6 (NMS)	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
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 (ECCS)	7.1.6.6.1.17	7.1.6.6.1.17	-	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 (ECCS); 7.3.1.2.2 (ECCS/GDCS); 7.3.3.3, 7.3.3.3.1 (LD&IS); 7.3.4.2 (CRHS) 7.3.5.3.1 (SSLC/ESF); 7.4.4.5.1 (ICS)	7.1.6.6.1.18; 7.4.4.5.1 (ICS)	7.1.6.6.1.18	--	7.1.6.6.1.18	7.1.6.6.1.18

Table 7.1-2

Section Roadmap of Evaluation of IEEE Std 603 Specific Criteria Compliance

Subject		I&C Systems	RTS	ESF	SS	IS	IL	CS	DICS
7.3	Completion of protective action	-	7.2.1.1, 7.2.1.6, 7.2.1.11, 7.2.1.14.5.2 (RPS)	7.3.1.1.2, 7.3.1.2.2 (ECCS GDCS/ADS); 7.3.3.3 (LD&IS); 7.3.5.2.2 (SSLC/ESF)	-	-	-	-	-
7.4	Operating bypass	7.1.6.6.1.22	7.1.6.6.1.22; 7.2.1.14.2.1 (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	-	7.1.6.6.1.27, 7.2.1.14.2 (RPS), 7.3.4.2 (SSLC/ESF)	7.1.6.6.1.27, 7.3.5.2 (SSLC/ESF)	-	-	-	-	-
8.1	Electrical power sources	7.1.6.6.1.25	7.1.6.6.1.25; 7.2.1.2.4.3 (RPS); 7.2.2.2 (NMS)	7.1.6.6.1.25; 7.4.1.2.1 (SLC); 7.4.4.3 (ICS)	7.1.6.6.1.25; 7.4.1.2.1 (SLC); 7.4.4.3 (ICS)	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	7.2.1.2.4.2 (RPS)	-	7.4.1.2.1 (SLC)	-	7.6.1.2.2	-	-
8.3	Maintenance Bypass	7.1.6.6.1.27; 8.3.1.1.5; 8.3.1.2; 8.3.2.2.2	8.3.1.1.5; 8.3.1.2; 8.3.2.2.2	8.3.1.1.5; 8.3.1.2; 8.3.2.2.2	-	-	-	-	-

(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 CMS, ref. 7.1.1.3.
(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

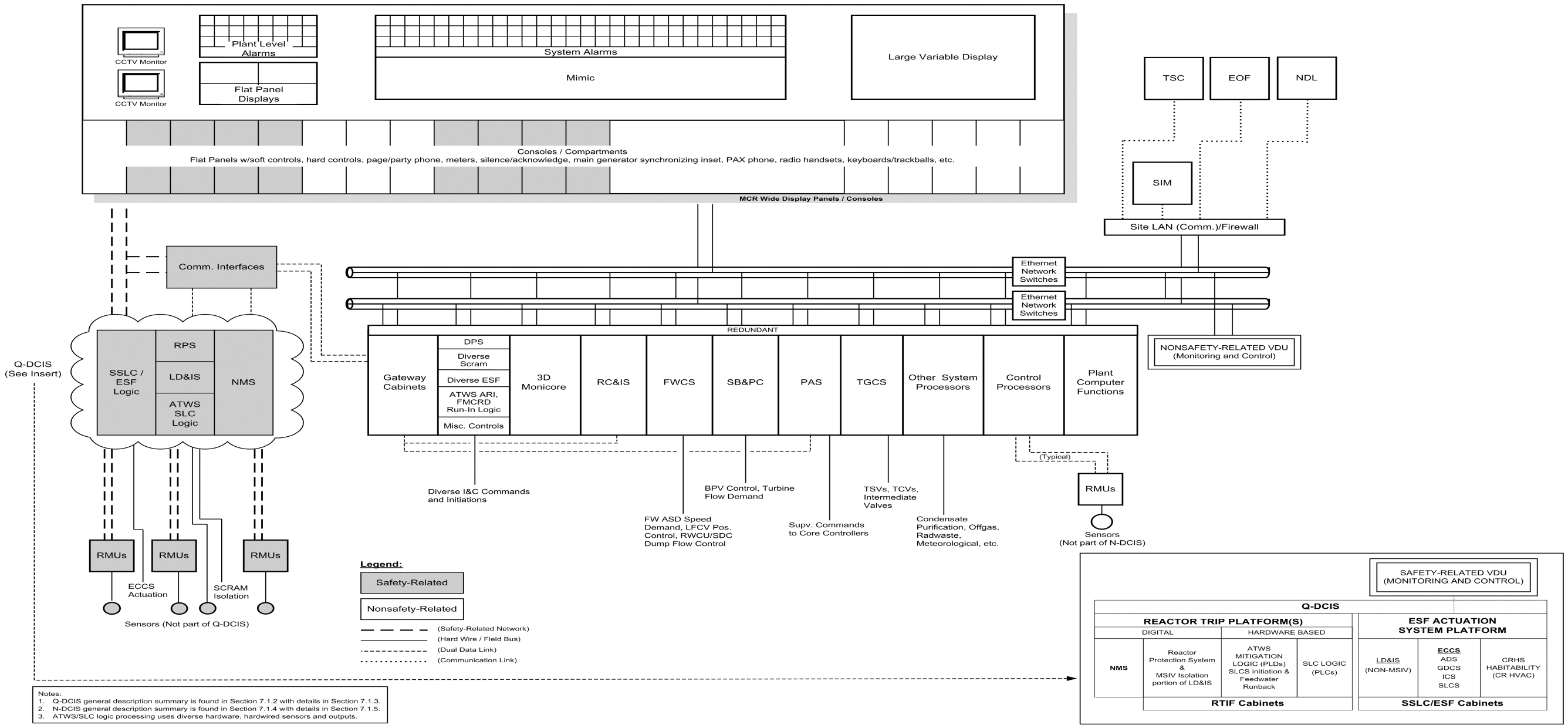


Figure 7.1-1. ESBWR Instrumentation and Control Simplified Block Diagram

ESBWR Distributed Control and Information System (DCIS) Functional Network Diagram

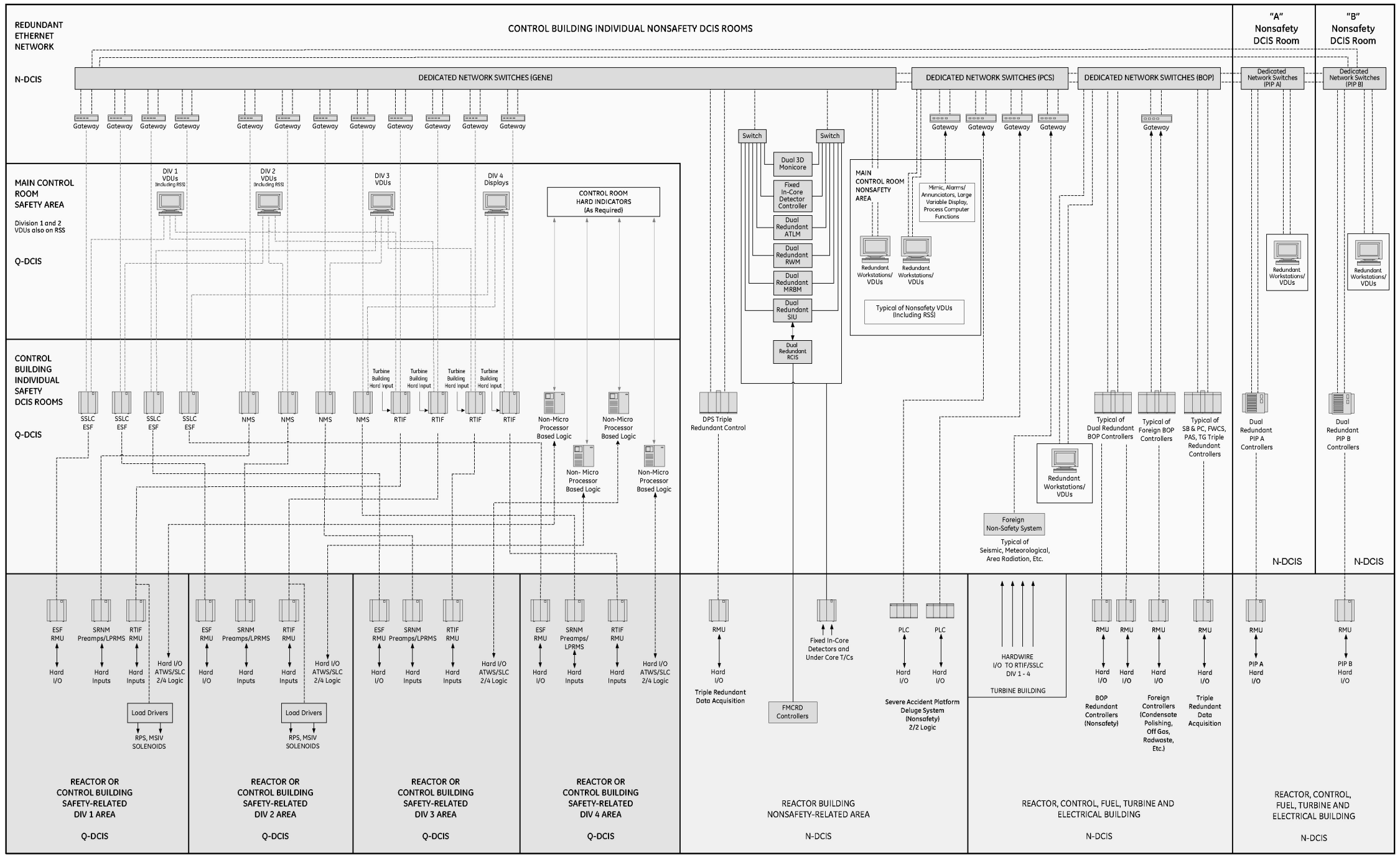
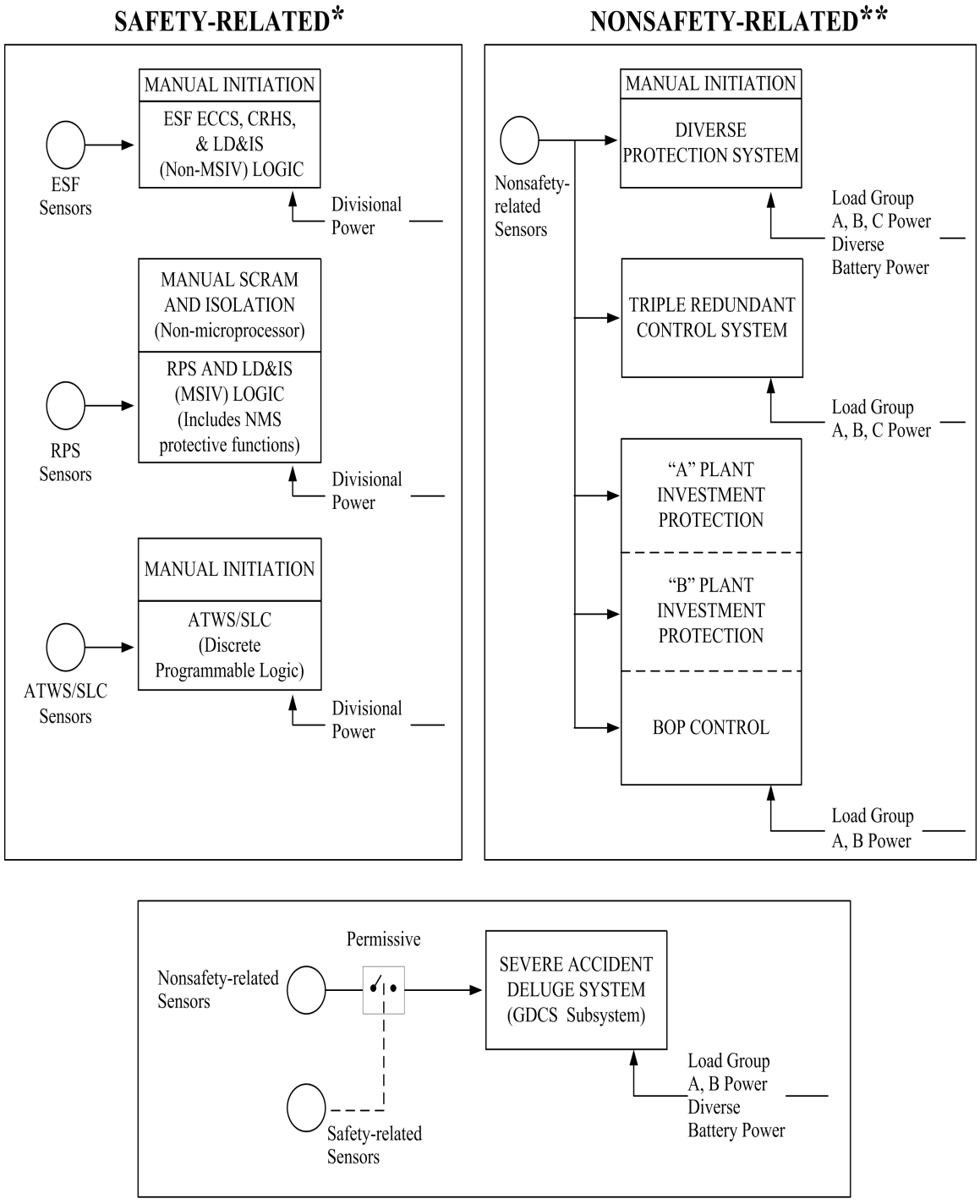


Figure 7.1-2. ESBWR Distributed Control and Information System (DCIS) Functional Network Diagram



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

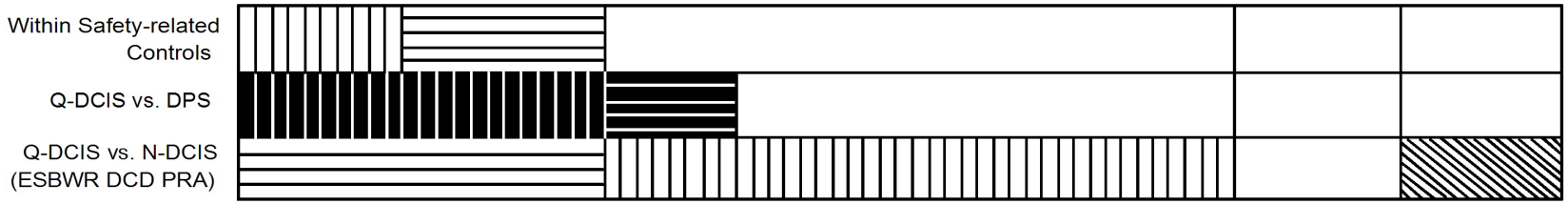
** For nonsafety-related systems, segmented systems are networked but can work independently.

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

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 prompt and safe shutdown of the reactor (also known as reactor trip) by means of rapid hydraulic insertion of all control rods (scram):
  - When anticipated operational occurrence (that is, transient) anomalous states occur, which may impair reactor safety.
  - When errors in operation take place that lead to transients, which may impair reactor safety.
- To initiate prompt reactor power reduction and safe shutdown of the reactor (also known as reactor trip) 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, or the primary containment vessel pressure boundary. This will limit the uncontrolled release of radioactive materials from the fuel assembly or reactor coolant pressure boundary. 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 occurrence (AOO) and accident analyses and instrument setpoint calculation methodology.
- To provide manual 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 that depend upon specific existing or subsequent reactor operating conditions.

- To provide seal-in of specific trip logic paths once trip conditions have been satisfied and also to inhibit the trip reset, as necessary, to ensure subsequent required protective action sequences are completed.

- To provide manual reset capability to permit the restoration of the RPS, and other affected systems, to their normal operational status following the seal-in of any trip logic path or after a full reactor scram.

- To provide isolated outputs to other systems that share instrument channel signals with the RPS, use trip signals generated by the RPS, or require 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 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 5.12):

- 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 avaiable), any failures caused by a single failure, and any failure caused by any design basis event that requires 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 would not cause instrument channel trips or division trips or scram solenoid de-energization that would result in full reactor scram or insertion of any control rod.

- Once initiated, RPS protective actions go in their intended sequence until completion of hydraulic control rod insertion. The RPS trip is sealed-in and must be manually reset. All manual resets are automatically inhibited for ten seconds to allow sufficient time for scram completion.

- The RPS has built-in redundancy in its design that satisfies 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 RPS is provided by separate process instrumentation, separate racks, and separate or independent panels and cabling, and, in the control building, separate equipment rooms.

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

- Access to trip settings, calibration controls, test points, and other terminal points are under the control of operation 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. Physically it ispossible to bypass only one channel at a time from the MCR.
- Selective automatic and manual trip bypasses are provided to permit proper plant operation.
- Manual control switches for initiation of reactor scram, when necessary, by the plant operator, are provided.
- Mode selection switch is provided at the main control console for plant operator to select plant operation mode This switch sends bypass, interlock and actuation signals to the RPS, instruments and hardware.

7.2.1.2 System Description

7.2.1.2.1 RPS Identification

The RPS is the overall complex of instrument channels, trip logics, trip actuators, manual controls and scram logic circuitry that initiate rapid insertion of control rods (scram) to shut down the reactor for situations 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 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 (SBPC) System, Plant Automation System (PAS), Main Control Room Panels, Nonsafety-related DCIS (N-DCIS), Uninterruptible AC Power Supply, Instrumentation and Control Power Supply, DC Power Supply, and Raceway System. The RPS sensors, hardware and logic are diverse from both ECCS logic and from the Diverse Protection System (DPS). The RPS also interfaces with 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 RPS 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 is also classified as Seismic Category I and as IEEE electrical category ssafety-related (RGs 1.26 and 10CFR50.55a(h).

7.2.1.2.3 Power Sources

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

7.2.1.2.4 RPS 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, the redundant sensor channel trip decision logic, and the redundant two-out-of-four trip systems output scram logic. This dual two-out-of-four arrangement utilized 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 on loss of power, loss or disconnection of any input signal, or loss of any internal or external device-to-device connection signal. The failure will not affect trip bypass logic signals and trip bypass permissive logic signals.

The design of RPS includes two operator controlled bypasses; these are the “division of sensors” bypass and “division of logic (division-out-of-service)” bypass. These are independently controlled by separate fiber optic “joystick” switches that allow 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 will always be able to scram the reactor if any two like and un-bypassed parameters exceed their trip value. Even if RPS back panel chassis are keylock disabled (not an operator function), the required scram capability is maintained.

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, and 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. 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 safety-related DCIS. The RMU within each division performs analog-to-digital and signal processing, 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 and for each variable 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 optically isolated using fiber optic links. The DTMs and TLUs are microprocessor-based modules of the RPS. The software associated with RPS channel trip and trip system coincident logic decisions that are installed in these modules are RPS unique. The number of channels utilized in the functional performance of RPS is shown in Table 7.2-1 (IEEE Std. 603, Section 4.4).

Q-DCIS equipment within a single division of sensor channels are 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 totally separated physically and independent from components of other sensor channels, satisfying the independence requirement of IEEE Std. 603, Section 5.6. The RPS equipment is independent and physically separated from other safety or nonsafety systems satisfying 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 that will affect the safety function of the RPS. The application of this non-safety to safety interface is described in detail in the GE NUMAC Licensing Topical Report (NEDC-33288P). This Topical Report explains the CIM function, communication data link, data flow, and isolation requirements of IEEE-603. The CIM has two-way fiber optic communication data links and provides electrical isolation when passing data from non-safety related subsystems to safety-related systems

Divisions of Trip Logic - Equipment within a RPS division of trip logic consists of Trip Logic Units (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 2/4 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, besides 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 electrically isolated using optic fiber 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 bypass units perform bypass and interlock logic for the division of channel sensors bypass, and the division trip logic unit 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 function. Each OLU receives bypass inputs from the RPS BPU, trip inputs from the TLU of the same division, and various 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 that receive inputs from the four divisions of TLU. The load drivers are isolated, solid-state, current-interrupting devices with fast response time 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 solenoids 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 electrically isolated from its input signal. The load driver outputs are arranged in the scram logic circuitry, which is 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 result 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. (Figure 7.2-1).

Relay logic is 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 initiation) to energize. The controllers of the backup scram is

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 to primary scram.

Divisions of Manual Scram Controls - Equipment within a division of manual scram controls includes manual switches, contactors, and relays that provide 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 (which include the scram pilot valves and the scram valves) are components of the CRD system. A full scram of control rods associated with a particular HCU occurs when both A and B solenoid of the HCU are de-energized. The arrangement of equipment groups within the RPS from sensors to actuator loads is shown in the Figure 7.2-1. The RPS functional block diagram showing the RPS interfaces and boundaries diagram with other systems is shown on the 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 within the plant during different conditions of reactor operation. The system monitoring the process condition is indicated in brackets.

- High Drywell Pressure [Containment Monitoring System, (CMS)]
- Turbine Stop Valve Closure (RPS)
- Turbine Control Valve 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)
- Low Control Rod Drive HCU Accumulator Charging Header Pressure (CRD system)
- 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)

- Reactor Mode Switch in "Shutdown" position (RPS)

With the exception of the NMS outputs, the MSIV closure, turbine stop valve closure and turbine control valve fast closure, loss of feedwater flow due to loss of power generation bus, main condenser pressure high, and Manual Scram outputs, all of the other systems provide sensor outputs through the RPS RMU. The MSIV Closure, turbine stop valve closure, turbine control valve 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 that provide trip and scram initiating inputs to the RPS for these conditions are discussed in the following subsections.

7.2.1.3 Neutron Monitoring System

Separate, isolated, and voted in the NMS digital Startup Range Neutron Monitor (SRNM) trip signal and Average Power Range Monitor (APRM) trip signals from each of the four divisions of the Neutron Monitoring System (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 (that is, 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 as follows:

- SRNM upscale (high count rate or high flux level)
- Short (fast) period
- SRNM inoperative

The three trip conditions from every SRNM associated with the same NMS division are combined into a single SRNM trip signal for that division. The specific condition that causes 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 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 as follows:

- APRM high neutron flux
- High simulated thermal power
- 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 that is capable of generating a trip signal in response to core neutron flux oscillation conditions and

thermal-hydraulic instability in time to prevent safety 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 thermal power signal to support the load rejection bypass algorithm.

7.2.1.4 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. 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 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 Water Level - Reactor water level is measured by four physically separate level (differential pressure) transmitters mounted on separate divisional local racks in the safety envelope within the reactor building. 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 Q-DCIS, which in turn provides the equivalent digital signal to the appropriate DTM in one of the four RPS divisional sensor channels. The four 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 mounted on both isolation valves of each MSL provide outputs, which are hard-wired to either the RPS RMU or to the appropriate DTM in one of the four RPS divisional trip channels. On each MSL, two position switches are mounted on each of the inboard isolation valve and the outboard isolation valve. Each of the two position switches on any one MSL isolation valve is associated with a different RPS divisional sensor channel. The eight MSIVs and the sixteen position switches supplied with these valves, for RPS use, are components of the NBS.

7.2.1.5 Control Rod Drive System

Locally mounted pressure transmitters measure the Control Rod Drive (CRD) system accumulator charging header pressure at four physically separated 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 signals before sending it to the appropriate DTM in one of the four RPS divisional trip channels. Similar to other trips, RPS scram initiation signal is generated in the appropriate instruments if the pressure value is below the setpoint value in two (or more) of the four divisions. The four pressure transmitters and associated instrument lines are components of the CRD system.

7.2.1.6 Reactor Protection System

Turbine Stop Valve Closure - Turbine stop valve (TSV) closure is detected by separate valve stem position switches on each of the four turbine stop valves. Each position switch provides

open/close contact output signal through hard-wired connections to the DTM in one of the four RPS divisional trip channels. The turbine stop valves are components of main turbine; however, the position switches are components of the RPS.

Turbine Control Valve Fast Closure - Low hydraulic trip system oil pressure, which is indicative of turbine control valve fast closure, is detected by separate pressure transmitters on each of the four turbine control valve hydraulic mechanisms. Each pressure transmitter provides a 4-20 mA signal through hard-wired connections to the DTM in each of the four RPS divisional trip channels. The turbine control valve (TCV) hydraulic mechanisms are components of the main turbine; however, the pressure transmitters 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 hard-wired 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 to shut off steam flow to the main condenser and protect the main turbine. This is an anticipatory scram in that high condenser pressure will also trip the main turbine and prevent bypass valve operation.

Loss of Power Generation Bus (Loss of Feedwater Flow) —The plant electrical system has four power generation buses that operate at 13.8 kV. Although normally all four buses are energized, the loads on these buses are arranged such that any three buses are required to support power generation. Specifically these buses supply power for the feedwater pumps and circulating water pumps. In Run mode, at least three of the four buses must be powered. If the voltage sensor (one per division) on each bus senses a low voltage, indicating that less than three buses are operating, a two-out-of-four logic will initiate a scram after a preset delay time. This delay time (less than one second) is to allow the auto transfer from the UAT transformer feed to the RAT transformer feed to restore normal bus voltages. Loss of more than three power generation buses is indicative of loss of the feedwater pumps and flow (it is also indicative of loss of condenser vacuum from the loss of the circulating water pumps). The purpose of this scram on loss of the power generation buses is to mitigate the reactor water level drop to Level 1 following the loss of FW pump function. This scram will terminate additional steam production within the vessel before Level 3 is reached.

Manual Scram - Two manual scram switches and the reactor mode switch each provide diverse means to manually initiate a reactor scram independent of conditions within the sensor channels and divisions of trip logic and trip actuators. Each of the two 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 are out of service for power issues (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 are out of service for non-power issues, the manual scram capability remains unaffected. The operability of Divisions 3 and 4 have no effect on the RPS manual scram capability.

The manual scram switches are also provided in the remote shutdown panel to achieve hot shutdown for the reactor from outside the control room. There is a separate manual switch in

each of the four divisions that provides a means to manually trip all trip 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 divisions of manual scram controls. A separate manual switch associated with each division of trip actuators provides 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 ten seconds to allow sufficient time for scram completion. The switch used to reset the manual scram circuitry shall permit resetting of the several scram groups in sequence so that reenergization of only half 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.

7.2.1.7 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 reactor building. 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 each of 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 thermocouples installed evenly (both vertically and azimuthally) inside the suppression pool, provide the suppression pool temperature data for automatic scram initiation. When the established limits of high temperature are exceeded in two of the four divisions, scram initiation is generated. The temperature sensors provide analog output signals 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 are provided along with the suppression pool temperature signals. When water level drops below selected temperature sensors, the exposed sensors are logically bypassed such that only sensors below the water level are utilized to determine the averaged temperature signal to the RPS.)

7.2.1.7.1.1 RPS 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, thus resulting in all control rod insertion and reactor shutdown.

At the same time that 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 functions 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 Rod Control and Information System (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 scram test switch status to the RC&IS, indicating the start of a pair-rod scram test, and provides to the RC&IS the status of Reactor Mode Switch position.

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 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 Leak Detection and Isolation System (LD&IS) for reactor coolant pressure boundary 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. RPS also provides an interlock to LD&IS for bypassing the MSIV isolation when not in Run mode that would otherwise result from high main condenser vacuum pressure and/or low inlet pressure to the turbine, during startup and shutdown.

7.2.1.7.1.2 Outputs to Main Control Room Panels:

Safety-related status and alarm signals are sent from the RPS to the main operator 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 each set of four (one per division) of the different variables or separate processes being monitored. Displays related to RPS scram variables include the following minimum set of signals:

- Reactor vessel pressure
- Reactor water levels
- Primary containment drywell pressures

- CRD HCU accumulator charging header pressures
- Suppression pool (local or bulk) temperatures
- Power Generation Bus voltages
- Main Condenser Pressure
- 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 should any divisional parameter not agree with the other divisions within a predetermined amount. The intent is that channel sensor checks are being 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 by bypassing a scram function. The alarm function is provided through isolated gateways to the plant computer functions.

The following alarms related to RPS status are provided:

- RPS NMS trip (generated in NMS);
- Reactor vessel pressure high;
- Reactor water level low (≤ Level 3);
- Reactor 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, that is, Div. 1, 2, 3, 4 automatic trip);
- RPS divisional manual trip (each of the four, that is, Div. 1, 2, 3, 4 manual trip);
- Manual scram trip (two: both Manual A and/or Manual B);

- Mode switch in Shutdown;
- Shutdown mode trip bypassed;
- NON-COINCIDENT NMS trip mode in effect (in NMS);
- NMS trip mode selection switch still in NON-COINCIDENT position with plant in Run mode (in NMS);
- Division of channel A (or B, C, D) sensors bypassed (four);
- Tripped conditions in Channel A (or B, C, D) and Channel A (or B, C, D) sensors bypassed (four);
- Division 1 (or 2, 3, 4) TLU out-of-service bypass (four);
- CRD accumulator-charging-header-pressure low trip bypass;
- Any CRD accumulator-charging-header trip, bypass switch still in BYPASS position with plant in Startup or Run mode; and
- Auto-scram test switch in TEST mode (manual trip of automatic logic) (four).

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

Outputs to nonsafety-related DCIS (N-DCIS) (Plant Computer Function) - 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, are logged by the plant computer function via isolated gateway connections from the RPS to the N-DCIS. For conditions that cause reactor trip, N-DCIS identifies the specific trip variable, the divisional channel identity, and the specific automatic or manual trip system; these signals are also provided to the sequence of events function of the plant computer functions.

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 Isolation Condenser System to be used as automatic operation signal permissive or inhibits. Automatic operation signal permissive are generated whenever the Reactor Mode Switch is placed in the Run positions, and automatic operation signal inhibits are generated whenever the Reactor Mode Switch is placed in any of the remaining three positionss. The RPS also provides the loss of power generation bus voltage signal (Loss of Feed Water Flow) for automatic initiation of ICS.

Outputs to the Plant Automation System (PAS) - The RPS provides the PAS with separate signals to indicate the position of the reactor mode switch. The RPS also provides the auto scram signal from the output logic unit to the PAS. .

Uninterruptible AC Power Supply —The AC electric power required by the four divisions of RPS logic is delivered from four pair of physically separate and electrically independent

uninterruptible safety-related 120 V AC 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.

7.2.1.7.1.3 System Logic Architecture & 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 concept.

Each divisional trip system processes the trip decisions of plant sensor inputs from the four divisions using a 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 a 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 in that any one division can be bypassed at one time to allow on-line 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; no division depends on the correct operation of another division. There is no combination of main control room initiated bypasses that can degrade RPS protection below that required.

7.2.1.8 Safety Evaluation

7.2.1.8.1 10 CFR Parts 50 and 52:

50.55a(a)(1) "Quality Standards for Systems Important to Safety"

- Conformance: The RPS conforms to these criteria, as shown by the following commitments to applicable RGs and standards.

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 and 7.2.1.2.4

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

- Conformance: The RPS design of bypass and inoperable status indication conforms to these requirements, and is consistent with the conformance of the RPS design with the

RG 1.47 discussed in this Section. It also conforms to the requirements of control and protection system interaction as described in IEEE Std, 603, Sections 5.8 and 6.3.

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.

52.47(a)(1)(vi) ITAAC in Design Certification Applications

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

52.47(a)(1)(vii) Interface Requirements

- Conformance: Interface material is provided in Tier 1.

52.47(a)(2) Level of Detail

- Conformance: The level of detail provided for the RPS within the Tier 1 and Tier 2 documents conforms to this requirement.

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

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

52.79(c), ITAAC in Combined Operating License Applications

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

7.2.1.9 General Design Criteria

In accordance with the SRP and with Table 7.1-1, the following GDC are addressed for the RPS:

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.

7.2.1.10 Staff Requirements Memoranda

Item II.Q of SECY-93-087 (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 as addressed to this SRM, the ESBWR Reactor Trip (Protection) System and Engineered Safety Features (ESF) designs conform with the Item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of an additional Diverse Instrumentation and Control System, described in Section 7.8.

7.2.1.11 Regulatory Guides

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

The system is capable of being tested during plant operation from sensor device to final actuator device. The tests must be performed in overlapping stages so that 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 —

- Automatic indication that a system is out of service is provided in the control room. (IEEE Std, 603, Section 5.8) Indicators indicate which part of a system is not operable.
- Annunciator test switches are provided in the control room.
- Individual indicators are arranged together in the control room 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. 60d, 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 - Compliance with NRC RG 1.53 is satisfied by specifying, designing, and constructing the RPS to meet the single-failure criterion, of IEEE 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 or the decision logic or an actuator would not prevent protective action. Separated channels are employed so that a fault affecting one channel would not prevent the other channels from operating properly.

RG 1.62, Manual Initiation of Protective Actions - Means are provided for manual initiation of reactor scram through the use of two armed pushbutton switches and the reactor mode switch (IEEE Std. 603, Section 6.2). Reactor scram is accomplished by operation of both pushbutton switches, or placing the mode switch in the Shutdown position. These switches are located on the main control console.

The amount of equipment common to 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 603, Section 5.2.

RG 1.75, Physical Independence of Electric Systems - The RPS complies with the criteria set forth in IEEE Std. 603, Section 5.6, and RG 1.75, which endorse 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.

Physical and electrical independence of the instrumentation devices of the system is provided by channel independence for sensors exposed to each process variable. Separate and independent raceways are routed from each device to the respective data acquisition and signal conditioning units (for example, remote multiplexing unit). Each channel utilizes its own divisional separate and independent electronic equipment located in separate equipment rooms. Trip logic outputs are separated in the same manner as the channels. Signals between redundant RPS divisions are electrically and physically isolated by safety-related isolation devices.

RG 1.105, Instrument Setpoints for safety-related Systems - The RPS-initiation setpoints are established consistent with this guide. A licensing topical report (Reference 7.2-1) provides a detailed description of this methodology.

RG 1.118, Periodic Testing of Electric Power and Protection System - The RPS complies with RG 1.118 as amplified in IEEE Std. 338. The RPS is designed so that its individual elements can be periodically and independently tested to demonstrate that the system reliability is being maintained. Safety-related RPS equipment allows for inspection and testing during periodic shutdowns and refueling.

Regulatory Position C.5 for APRM - With respect to conformance to position C.5, the inherent time response of the in-core sensors used for the APRM function (fission detectors operating in the ionization chamber mode) is many orders of magnitude faster than the APRM channel response time requirements and the signal conditioning electronics. The sensors cannot be tested without disconnecting and reconnecting to special equipment.

RG 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants - The RPS fully complies with this RG. The hardware and software for the RPS function and other safety 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 to all software standards referenced in IEEE Std. 7-4.3.2. Hardware and software are integrated into a final assembly that is validated by testing against input requirements.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems - The configuration of RPS and other safety systems regarding independence, separation, and the single-failure criterion conforms to 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 - Refer to Subsection 7.1.6 for compliance discussion.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.6 for compliance discussion.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.6 for compliance discussion.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.6 for compliance discussion.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.6 for compliance discussion.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.6 for compliance discussion.

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

The RPS conforms to RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6).

7.2.1.12 Branch Technical Positions

BTP HICB-3: Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service— The ESBWR has no coolant pump and the BTP Position One does not apply to ESBWR. The ESBWR complies with the BTP Position Two.

BTP HICB-8: Guidance for Application of RG 1.22 - The RPS design conforms to this BTP as discussed in the compliance with RG 1.22 in this Section.

BTP HICB-9: Guidance on Requirements for Reactor Protection System Anticipatory Trips — 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 seismic design requirement as Seismic Category I.

BTP HICB-11: Guidance on Application and Qualification of Isolation Devices— The RPS design conforms to this position. The RPS logic controllers use optical Communications Interface Modules (CIM) and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections from safety-related to 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 - The RPS design conforms to this position. The RPS trip setpoints will be consistent with the requirements of RG 1.105. The setpoints will be established based on instrument accuracy, calibration capability and design drift (estimated) allowance data, and will be within the instrument best accuracy range. The digital RPS trip setpoints do not drift and are reported to the N-DCIS to be 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 will provide margin to satisfy both safety requirements and plant availability objectives. (See reference 7.2-1.)

BTP HICB-13: Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors - The RPS uses sensor inputs for suppression pool temperature monitoring, which is based on thermocouple type temperature sensor. This BTP does not apply to RPS.

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

Development of software for the safety system functions within RPS and NMS conforms to the guidance of this BTP. Discussion of software development is included in the Appendix 7B of this chapter. Safety-related software to be embedded in the memory of the RPS and NMS controllers is developed according to a structured plan as described in Appendix 7B. 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 - This BTP is applicable to all Section of the DCD including this Section on RPS. The RPS Section content conforms to this BTP.

BTP HICB-17: Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based Instrumentation and Control Systems. The RPS and NMS controllers conform to this BTP. Discussions on self-test and surveillance tests of RPS are provided in Subsection 7.2.1.13.

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

Any portions of RPS and NMS design that will use commercial grade programmable logic controllers (PLCs) for safety-related functions conform to this BTP (and to BTPs 14, 17, and 21). Such PLCs will be qualified to a level commensurate with safety 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) - In addition to the design features already incorporated in the design on defense-in-depth and against common mode failures as addressed to this BTP, the ESBWR Reactor Trip (Protection) System and Engineered Safety Features (ESF) designs conform with this BTP by the implementation of an additional diverse instrumentation and control system, the DPS, described in Section 7.8.

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

The real-time performance of RPS and NMS in meeting the requirements for safety system trip and initiation response conforms to this BTP. Each RPS or NMS controller operates independently and asynchronously with respect to other controllers so that timing can readily be evaluated from input to output of each controller. Timing signals are not exchanged between divisions of independent equipment or between controllers within a division.

7.2.1.13 Testing and Inspection Requirements

7.2.1.13.1 System Testing: Operational Verifiability

The RPS is designed so that its individual operating elements can be periodically and independently tested to demonstrate that RPS reliability is being maintained.

The RPS design (and the design of other systems providing the RPS with instrument channel inputs) permits verifying, with a high degree of confidence, and during reactor operation, the operational availability of each of the input sensors utilized by the RPS (that is, channel checks continuously performed by the plant computer function).

The instrument channels are periodically calibrated 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.

7.2.1.13.2 Surveillance Testing and In-Service Inspection

The RPS equipment testing includes the following:

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

7.2.1.13.3 Surveillance Testing

The RPS is designed to permit testing of 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 practicable, the RPS components and testing strategies are designed so that identifiable failures are detectable. Test methods are designed to facilitate recognition and location of malfunctioning components so that 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 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 functions in the division of trip logic and division of actuators, and response time tests in accordance with the established test procedures and as required by Technical Specifications

7.2.1.14 Instrumentation and Control Requirements

7.2.1.14.1 Automatic Scram Variables

Refer to Subsection 7.2.1.2.4.2 for the automatic scram initiating circuits and the systems that supply to them.

7.2.1.14.2 Automatic and Manual Bypass of Selected Scram Functions

7.2.1.14.2.1 Operational Bypasses

Manual or automatic bypass 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 that require automatic or manual bypass of certain reactor trip functions are described below:

The turbine stop valve closure trip bypass and control valve fast closure trip operating bypass - To permit continued reactor operation at low-power levels when the turbine stop or control valves are closed. The main steam TSV closure and the steam governing TCV fast closure scram trip functions are automatically bypassed in each division whenever the reactor mode switch is in either the Shutdown, Refuel or Startup position with the reactor power level below a certain preset power level (bypass setpoint). Also, the TSV closure and TCV fast closure reactor scram is automatically bypassed if a sufficient number of the bypass valves are opened (as indicated by their 10% position sensors) within a preset time delay after the initiation of the reactor trip signal caused by the TCV fast closure or TSV closure. The NMS system sends RPS an analog simulated thermal power signal, which is used to determine both the low power bypass and to determine the required number of bypass valves to open post turbine trip or load rejection. The low power bypass is automatically removed and both scram trip functions 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 main control room.

Bypass of scram trip for CRD-accumulator-charging-header low pressure after scram has occurred (indicated operational bypass) - To permit scram reset, four administratively controlled trip bypass switches are installed in the main control room. This bypass is allowed only when the reactor mode switch is either in Shutdown or Refuel position. When the reactor is in the shutdown or refuel mode, the low CRD HCU accumulator charging header pressure trip can be manually bypassed in each division of trip logic by separate, manual CRD HCU accumulator charging header pressure trip bypass switches. Control of this bypass is achieved with bypass

switches through administrative means. 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 main control room.

The bypass is automatically removed whenever the Reactor Mode Switch is put in either Startup or Run mode, whether or not the CRD charging pressure bypass switches are in the bypass position. However, a separate alarm would result in the main control room if any of the bypass switches were left in the bypass position when the Reactor Mode Switch is in either Startup or Run mode.

Bypass of scram trip for main steam isolation valve closure (alarmed operational bypass) - The MSIV closure scram trip function is automatically bypassed in each division whenever the reactor mode switch is in either the Shutdown, Refuel or Startup position with reactor pressure in the associated sensor channel less than a predetermined setpoint. This bypass condition is indicated in the main control room. This bypass 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 closed or not fully open.

Special Isolated Main Steam Line Operational Bypass (alarmed 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 bypass is alarmed in the MCR.

Bypass of scram trip for Loss of Power Generation Bus (alarmed 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 either the Shutdown, Refuel or Startup position. This bypass condition is alarmed in the main control room. The bypass is automatically removed if the reactor mode switch is moved to the Run position.

Bypass of scram trip on account of mode switch in Shutdown position (alarmed operational bypass) - The RPS 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 bypass permits resetting of the trip actuators and re-energization of the scram pilot valve solenoids.

Bypass of NMS SRNM trip functions in Run mode (not alarmed) - 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 by the main control room. The SRNM rod block functions are also disabled when the reactor mode switch is in the Run mode.

Bypass of non-coincident NMS trips in Run mode - Whenever the reactor mode switch is in the Run position, and if the coincident/non-coincident NMS trip remains in the NON-COINCIDENT position, the non-coincident NMS scram trip functions are automatically disabled (bypassed). This is a NMS function.

The non-coincident NMS trip function is required while core alterations are occurring during initial fuel loading and subsequent refueling operations. During such core alterations, the Reactor Mode Switch is in the Refuel position (or for certain testing conditions, in the Shutdown or Startup positionss). 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 a NMS function.

The non-coincident NMS trip function is automatically removed when the reactor mode switch is in the Run positions. If the coincident/non-coincident NMS trip selection switch were in the NON-COINCIDENT position when the reactor mode switch is in the Run mode, this would result in an alarm in the main control room. When the reactor is in Shutdown, Refuel, or Startup mode, the non-coincident NMS trip can be manually bypassed by a separate "non-coincident trip disable" switch. These logics are NMS functions.

APRM, OPRM, and SRNM trips have manual bypass capabilities within NMS, not RPS.

7.2.1.14.2.2 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 does not affect or eliminate any scram function. Protection functions are available while any RPS equipment is in maintenance bypass. Except where indicated otherwise, any maintenance bypass generates a status alarm at the main control room operator's console.

The following maintenance bypasses are provided**:**

Bypass of detector inputs (Division-Of-Channel-Sensors bypass) (alarmed maintenance bypass) - Manually operated bypass switch with interlock capability (for example, joystick type switch) is installed in the main control room 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, an alarm occurs in the main control room with an indication of the bypassed channel sensor division. The effect of the channel of sensors bypass is to convert the two-out-of-four trip to a two-out-of-three trip logic. A channel of sensors bypass in any channel will bypass all trip initiating input signals at the DTM trip input to the TLU. Bypassing a division of sensors will still allow 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 bypass (Division-Out-Of-Service bypass) (alarmed maintenance bypass) - Manually operated bypass switch with interlock capability (for example, joystick type switch) is installed in the main control room to bypass (take out of service) the RPS trip output logic of one RPS electrical division at a time. This bypass is effective at the TLU trip input to OLU, and permits

the RPS Trip Logic Unit (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, an alarm occurs in the main control room with indication as to which division is out of service. With a division-out-of-service bypass in effect, the operator is still able to manually 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 value.

7.2.1.14.3 Requirements for Manual Controls

Operator action by means of manual controls is limited to:

- Initiation of scram by manual scram switches;
- 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.

7.2.1.14.4 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; namely, Shutdown, Refuel, Startup, and Run. The switch provides both electrical and physical separation between the Sections associated with each of the four separate divisions. The mode switch positions and their related bypass and trip/reset functions are as follows:

- Shutdown
  - Initiate a reactor scram
  - Enable NMS non-coincident trips
  - Enable manual CRD charging pressure trip bypass
  - Automatically bypass Turbine Control Valve fast closure trip

  - Automatically bypass Turbine Stop Valve closure trip
  - Automatically bypass MSIV closure trip
  - Enable automatic bypass of loss of power generation bus trip
- Refuel
  - Enable NMS non-coincident trips
  - Enable manual CRD charging pressure trip bypass
  - Automatically bypass Turbine Control Valve fast closure trip
  - Automatically bypass Turbine Stop Valve closure trip
  - Automatically bypass MSIV closure trip
  - Enable automatic bypass of Power Generation Bus Loss (Loss of Feedwater Flow) trip trip
- Startup
  - Enable NMS non-coincident trips
  - Disable manual CRD charging pressure trip bypass
  - Automatically bypass Turbine Control Valve fast closure trip
  - Automatically bypass Turbine Stop Valve closure trip
  - Enable automatic bypass of loss of power generation bus trip
- Run
  - Disable all trip bypasses enabled by any of the other three modes
  - Enable automatic bypass of NMS SRNM trip

7.2.1.14.5 Manual Scram Switches

Two manual scram switches permit initiating 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; these same switches are included in the RSS panels.

7.2.1.14.5.1 Manual Divisional Trip Switches

Each of the four RPS automatic trip systems has manual trip capability provided by four divisional trip switches that are 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.

7.2.1.14.5.2 Trip Reset Switches

Up to five trip-reset switches 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 that only two groups of "A" and "B" solenoids are re-energized at the same time.

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.

7.2.1.14.5.3 Operational Bypass Switches

Requirements for operational bypass switches for RPS safety-related functions are addressed in Subsection 7.2.1.14.2.2. Operational bypass switches are under administrative control. Four trip-bypass switches implement RPS operational bypass switches for CRD charging header pressure, one for each RPS division. The Reactor Mode Switch provides for several automatic operational bypasses.

7.2.1.14.5.4 Reactor Mode Switch-In Shutdown Scram Bypass Switches

Two manual control switches are used to bypass the scram received when moving the reactor mode switch to shutdown position. This bypass would only be permitted during an outage condition when the reactor is already shutdown.

7.2.1.14.5.5 Maintenance Bypass Switches

Requirements for RPS-related maintenance bypass switches are addressed in Subsection 7.2.1.14.2.2. The following maintenance bypasses are provided:

- Four division-of-channel-sensor maintenance bypass switches; and
- Four division-out-of-service maintenance bypass switches.

7.2.1.14.5.6 Test Switches

Test switches to aid in surveillance testing during reactor operations are provided in the RPS design.

7.2.2 Neutron Monitoring System

7.2.2.1 System Design Bases

The Neutron Monitoring System (NMS) monitors thermal neutron flux from the startup source range to beyond rated power. The NMS is comprised of the following subsystems:

- Startup Range Neutron Monitor (SRNM)
- Power Range Neutron Monitor (PRNM)
- Automatic Fixed In-Core Probe (AFIP)
- Multi-Channel Rod Block Monitor (MRBM)

The PRNM subsystem includes the local power range monitor (LPRM), average power range monitor (APRM) functions, and the oscillation power range monitor (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 the GE NUMAC Licensing Topical Report (NEDC-33288P). This Topical Report explains the CIM function, communication data link, data flow, and isolation requirements of IEEE Std. 603. The CIM has two-way fiber optic communication data links 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 (SRNM) Subsystem

7.2.2.1.1.1 Trip Functions

The SRNM scram trip functions are discussed in Subsection 7.2.1.3, 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 such that the reactor scram (due to the short reactor period caused by excessive rod withdrawal) can be avoided.

- 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 position is in Non-Coincidence, any one of the SRNMs trip can be generated. When the Reactor Mode is in Run, 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 sending 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 provide trips and/or alarms if the original signal exceeds the delayed one. The period alarm and scram setpoints shall be built-in through the period trip circuit or software algorithm.
- A short period warning signal (Period Withdrawal Permissive) is provided to inhibit rod withdrawal in order to avoid inadvertent scram due to excessive rod withdrawal.
- A SRNM interlock signal "ATWS Permissive" is established and sent to the ATWS/SLC logic as a permissive signal to allow the initiation of liquid boron injection of the Standby Liquid Control system.
- The period trip is active except below a fixed power level of approximately (10E-4%) of rated. This power level approximately corresponds to 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 its CALIBRATE-OPERATE switch is not in OPERATE, if any interlock in the instrument is open, if the unit self-test function detects failures, or if the detector polarizing voltage falls below a preset level.

7.2.2.1.1.2 Safety-Related (10 CFR 50.2) Design Bases

The general safety-related functional requirements follow below:

- The SRNMis designed as a safety-related system. The SRNM shall generate a high neutron flux trip signal or a short period trip signal that can be used to initiate 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 is 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 specific regulatory requirements for the NMS are listed in Table 7.1-1.

7.2.2.1.1.3 Nonsafety-Related Design Bases

Neutron sources and neutron detectors together shall result in a signal count rate of at least 3 cps with the control rods fully inserted in a cold unexposed core.

The SRNM is designed to perform the following nonsafety-related functions:

- Indicate measurable increases in output signals with the maximum permitted number SRNM channels out of service during normal reactor startup operations.
- Provide a continuous monitoring of the neutron flux over a range of 10 decades (approximately 1×10^3 nv to 1.5×10^{13} nv).
- Provide a continuous measure of the 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 than or less than preset values or if certain electronic failures occur.
- Generate rod block whenever the period decreases below the preset value.
- The loss of a single power bus would not disable the monitoring and alarming functions of the available monitors.

7.2.2.1.2 Local Power Range Monitor (LPRM)

7.2.2.1.2.1 Safety-Related (10 CFR 50.2) Design Bases

The general safety-related functional requirements are:

- A sufficient overall number of LPRM signals are provided to satisfy the APRM safety-related design bases.
- The LPRM is designed as a safety-related system to satisfy the APRM safety-related design bases.
- The LPRM is qualified to operate under design basis accidents and abnormal environmental conditions.

The specific regulatory requirements applicable to the controls and instrumentation for the NMS are shown in Table 7.1-1.

7.2.2.1.2.2 Nonsafety-Related Design Bases

The LPRM supplies the following nonsafety-related functions:

- Signals to the APRM that are proportional to the local neutron flux at various locations within the reactor core.
- Signals to alarm high or low local neutron flux.
- Signals proportional to the local neutron flux to drive indicators and displays, and for the Plant Computer function used for operator evaluation of power distribution, etc.
- Signals proportional to the local neutron flux for use by other interface systems such as the Rod Control and Information System (RC&IS) for the rod block monitoring function.

7.2.2.1.3 Average Power Range Monitor (APRM)

7.2.2.1.3.1 Safety-Related (10 CFR 50.2) Design Bases

The general safety-related functional requirements are:

- The APRM is designed to safety-related standards. The general functional requirements are that, under the worst permitted input LPRM bypass conditions, the APRM is capable of generating a trip signal in response to excessive average neutron flux increases in time 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 specific regulatory requirements applicable to the controls and instrumentation for the NMS are listed in Table 7.1-1.

7.2.2.1.3.2 Nonsafety-Related Design Bases

The APRM provides the following nonsafety-related functions:

- A 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 to other interfacing systems as core power information.
- Interlock signals for blocking further rod withdrawal to avoid an unnecessary scram actuation.
- A simulated thermal power signal derived from each APRM channel, which approximates the heat dynamic effects of the fuel.
- 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 (OPRM)

7.2.2.1.4.1 Safety-Related (10 CFR 50.2) Design Bases

The general safety-related functional requirements are:

The OPRM is designed to safety-related standards. The general functional requirements are that, under the worst permitted input LPRM bypass conditions, the OPRM is capable of generating a trip signal in response to core neutron flux oscillation conditions and thermal-hydraulic instability in time 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.

7.2.2.1.4.2 Nonsafety-Related Design Bases

The OPRM provides core flux oscillation information for plant computer and for main control room display, and alarm when the OPRM is inoperative or has an with insufficient number of LPRM inputs to OPRM.

7.2.2.2 System Description

The safety-related functions of the Neutron Monitoring System (NMS) consist of the Startup Range Neutron Monitor (SRNM) Subsystem, the Local Power Range Monitor (LPRM), the Average Power Range Monitor (APRM), and the Oscillation Power Range Monitor (OPRM). The Nonsafety-Related Automated Fixed In-Core Probe (AFIP) Subsystem of the Neutron Monitoring System and the Multi-channel Rod Block Monitor (MRBM) are discussed in Subsection 7.7.6. The LPRM and the APRM, with the OPRM, together are also called the Power Range Neutron Monitor (PRNM) Subsystem.

7.2.2.2.1 System Identification

The purpose of the NMS is to monitor power generation and, for the safety-related part of the NMS, to provide trip signals to the RPS to initiate reactor scram under excessive neutron flux (and thermal power) levels, excessive neutron flux oscillation, or fast increases in neutron flux (short period). It also provides power information to the Plant Computer and the automated thermal limit monitor (ATLM) in the Rod Control & Information System (RC&IS) for control of rod block monitoring. The operating range of the various detectors is shown in Figure 7.2-3. A functional block diagram showing a typical SRNM division is shown in Figure 7.2-4. A functional block diagram showing a typical PRNM division is shown in Figure 7.2-5.

7.2.2.2.2 Neutron Flux Monitoring Ranges System Safety Classification

The SRNM, LPRM, APRM, and OPRM perform safety-related functions, and have been designed to meet the applicable design criteria. The system is classified as 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), and 120 VAC Divisional associated Instrument and Control Power Supply (ICP). The power sources for each system are discussed in the individual subsystem descriptions.

7.2.2.2.4 Startup Range Neutron Monitor (SRNM) 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 twelve 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. UPS Bus A (Division 1)
- B, F, K: 120 VAC Div. UPS Bus B (Division 2)
- C, G, L: 120 VAC Div. UPS Bus C (Division 3)
- D, H, M: 120 VAC Div. UPS Bus D (Division 4)

As previously described, each SRNM cabinet is redundantly powered with two uninterruptible divisional 120 VAC power sources from 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 evenly 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 separately routed to the appropriate containment penetration according to divisional assignment. They are connected to their designated preamplifiers located in the different divisional quadrants of the reactor building. The SRNM preamplifier signals are transmitted to the SRNM digital processing equipment units, which provide algorithms for signal processing and calculation to provide neutron flux, power calculations, period trip margin, period calculations, and provide various outputs for local and control console displays, recorders, and to the plant computer function. As shown in Figure 7.2-4, the individual SRNM channel trips are combined to form a SRNM divisional trip in the NMS Trip Logic Unit function. This SRNM divisional trip is sent to the RPS via a safety-related network interface. (This is the logic in Coincidence Mode. Further discussion of SRNM trip logic is included in Subsection 7.2.2.5.2.) alarm and trip outputs are also provided for both high flux and short period trip or alarm conditions. Such outputs also include the instrument inoperative trip. The electronics for the startup range neutron monitors and their designated bypass units are located in four separate cabinets, one in each of the four divisional reactor building quadrants and in each of the control building divisional equipment room locations. The SRNM satisfies the IEEE Std. 603, Section 5.1 single failure criterion that the failure of each individual SRNM channel will not affect the protection function of the SRNM through channel bypasses discussed in the following paragraph

(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 ranges, which covers from lowest 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 ranges, which cover from 1×10^8 nv to 1×10^{13} nv of neutron flux. In the counting range, the discrete pulses produced by the sensors are applied to a discriminator after pre-amplification. 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 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 the two methods are changed over, the SRNM calculates a neutron flux value based on a weighted interpolation of the two flux values calculated by both methods. A continuous and smooth flux reading transfer is achieved in this manner. There is also the calculation algorithm of the period-based trip circuitry that generates 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 such that the reactor scram (due to a shorter reactor period caused by excessive rod withdrawal) can be avoided.

7.2.2.2.4.6 Bypasses and Interlocks

The twelve SRNM channels are divided into four bypass groups. A joystick switch allows only one SRNM at a time to be bypassed in each bypass group; this scheme allows 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 that belong to the same division. 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 RPS to perform 2-out-of-4 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 control room panel. Bypass functions for the SRNM and the APRM in the NMS are separate (that is, there is no single NMS divisional bypass that affects both the SRNM and the APRM). Any APRM bypass does not force a SRNM bypass. The individual SRNM power

signals are not 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 RPS 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-Coindence mode (Table 7.2-2). The SRNM ATWS Permissive signals are sent to the ATWS/SLC system as a permissive signal to control initiation of Standby Liquid Control system boron injection and associated functions (for example, feedwater runback).

7.2.2.2.4.7 Redundancy and Diversity

The signal outputs from the twelve SRNM channels are arranged such that each of the four divisions includes a different set of designated SRNM channels that cover different regions of the core. The SRNM monitoring and protection function is individual channel based. 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 division within the RPS. Bypassing a single SRNM channel does not cause a trip output to the related SRNM division and would not prevent proper operation of the remaining SRNM channels to perform their safety-related functions (Subsection 7.2.1.2).

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 in Reference 7.1-5, Reference 7.1-6, and Reference 7.1-7.

7.2.2.2.5 Local Power Range Monitor

7.2.2.2.5.1 General Description

The Local Power Range Monitor (LPRM) monitors local neutron flux in the power range. The LPRM provides input signals to the APRM (Subsection 7.2.2.6), to the RC&IS (Subsection 7.7.2), and to the plant computer function of the N-DCIS (Subsection 7.1.5).

7.2.2.2.5.2 Uninterruptible Power Supply (UPS)

Alternating current power for the LPRM circuitry is supplied by four pairs of redundant divisional 120 VAC UPS buses (A, B, C and D) that correspond to the four safety-related divisions; the various cabinets can perform their function with either of the 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, which furnishes the detector polarizing potential.

7.2.2.2.5.3 Physical Arrangement

A single division of LPRMs consists of a total of 64 detectors, taking one detector from each LPRM assembly from a total of 64 assemblies in the core; there are a total of 256 LPRM detectors in the ESBWR core. Each assembly consists of four LPRM fission chamber detectors evenly spaced at four axial positions along the fuel bundle vertical direction. The 64 assemblies are distributed throughout the whole core in evenly spaced locations. Within the core, for each square fuel region of four-by-four fuel bundles, there are four LPRM assemblies located at the four corners of this fuel region. The LPRM detector locations in the core are illustrated in Figure 7.2-7. The LPRM detector axial positions along the fuel bundle vertical direction are illustrated in Figure 7.2-8. The LPRM detector at the lowest position in a detector is designated Position A. Detectors above A are designated B and C, and the uppermost detector is designated D.

The LPRM detector is a fission chamber with a polarizing potential of approximately 100 VDC. The four detectors comprising a detector assembly are contained in a common tube that also houses the Automated Fixed In-core Probe (AFIP) sensors (Subsection 7.7.6). The enclosing housing tube contains holes to allow coolant flow for detector cooling. The whole assembly is installed or removed from the top of the reactor vessel, with the reactor vessel head removed. The upper end of the assembly is held under the top fuel guide plate with a spring plunger. A permanently installed in-core guide tube/housing is located below the lower core plate to confine the assembly, and to provide a sealing surface under the reactor vessel. The LPRM assembly also 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 plant computer function of the N-DCIS (Subsection 7.1.9) for core flow determination using the heat balance method. This 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 reactor building 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 total physical separation. This arrangement and wiring practices provide the required electrical isolation and physical separation, and satisfies 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 reactor building, where the signals are processed, amplified, converted to digital data and transmitted by optic fiber to the control building 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 (Subsection 7.2.2.6). Individual LPRM signals are also transmitted through dedicated interface units in the APRM with proper electrical isolation to other systems such as the RC&IS and the Plant Computer, 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 be individually 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 assigned in four divisional APRM channels, with 64 LPRM detector signals in each APRM channel. The redundancy criteria are met such that, in the event of a single failure under permissible APRM bypass conditions, the safety-related protection function can still be 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) at an ambient temperature of approximately 315°C. 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 (Sections 3.10 and 3.11). Additional information on equipment qualification with respect to environmental considerations is in Reference 7.1-5 and Reference 7.1-7.

7.2.2.2.6 Average Power Range Monitor (APRM)

7.2.2.2.6.1 General Description

The APRMs perform a safety-related function. There are four APRM channels, one per division. Each APRM channel receives 64 LPRM signals through fiber cables from the reactor building as primary inputs, averages the inputs and normalizes the result to provide an APRM value that corresponds to the average core thermal power signal. One APRM channel is associated with each division of the RPS. Each of the divisional NMS trip signals is also sent to the other three RPS divisions through optical isolation.

7.2.2.2.6.2 Power Sources

APRM channels are powered as listed below:

- A: Redundant 120 VAC Div UPS Bus A (Division 1)
- B: Redundant 120 VAC Div UPS Bus B (Division 2)

- C: Redundant 120 VAC Div UPS Bus C (Division 3)
- D: Redundant 120 VAC Div UPS Bus D (Division 4)

Either of the two redundant divisional power sources will support 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 consists of 64 LPRM signal inputs. The assignment of individual LPRM sensors to each of the four APRM channel is performed such that an even and uniform selection of LPRM sensors from the whole core is realized for each APRM channel. In this manner, the average value of the 64 LPRM signals from the whole 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 in order 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 that the failure of each individual APRM channel will not affect the protection function of the APRM through channel bypasses discussed in the following paragraph (with any three of the four divisions of safety-related power available). It also satisfies the IEEE Std. 603, Section 5.6, independence requirement, as the redundant portions of the NMS equipment are independent of and physically separated from each other, and that 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 7.2.1.3. 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 still maintaining the required APRM functions. This satisfied the repair requirement of IEEE Std. 603, Section 5.10. When one APRM channel is bypassed, the trip logic in the RPS becomes two-out-of-three instead of two-out-of-four (with any three of the four

divisions of safety-related power available). Each divisional trip signal is sent to all four RPS divisions. All four RPS channels continue to perform the trip logic even if the RPS channel is in the same division as the bypassed APRM input. The bypass of APRM channels is accomplished with a joystick type switch with mutually exclusive positions. The APRM bypass switch is located on the control room 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, assures that no single failure will cause an inadvertent bypass. The bypass function uses physical means and independent logic to assure 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 Run. When any APRM (or OPRM) channel output to the RPS is bypassed, the bypass is indicated on the plant operator's panel. The same channel bypass bypasses both the OPRM and APRM channel.

The APRM ATWS Permissive signals are sent to the ATWS/SLC system as a permissive signal for the ADS initiation inhibit function.

7.2.2.2.6.7 Redundancy

Four independent channels of the APRM monitor neutron flux, each channel being associated with one RPS division but with its trip signal being sent to the other three RPS divisions through optical isolation. The redundancy criteria are met such that in the event of a single failure under permissible APRM bypass conditions, the safety-related protection function can still be 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 in Reference 7.1-5 and Reference 7.1-7.

7.2.2.2.7 Oscillation Power Range Monitor

7.2.2.2.7.1 General Description

The Oscillation Power Range Monitor (OPRM) consists of four independent safety-related channels. The OPRM channel utilizes the same set of LPRM signals used by the associated APRM channel in which this OPRM channel resides. Each OPRM receives the identical LPRM signals from the corresponding APRM channel as inputs, and forms many OPRM cells to monitor the neutron flux behavior of all regions of the core. Assignment of LPRMs to the four OPRM channels are as shown in DCD Figure 7.2-10. The OPRM channel consists of OPRM cells that are formed by grouping LPRM inputs (maximum 4). The OPRM cell signal is the

average of all grouped LPRM input signals 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 to the RPS if the trip setpoint is exceeded.

7.2.2.2.7.2 Power Sources

OPRM function resides in the APRM equipment and receives the same redundant APRM power.

7.2.2.2.7.3 Signal Conditioning

The OPRM function resides in its associated APRM channel equipment. Assignment of LPRMs to the four OPRM channels is shown in Figure 7.2-10. The OPRM channel consists of OPRM cells that are formed by grouping LPRM inputs. Each OPRM cell signal is the average of all grouped LPRM input signals for this cell, 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 RPS. The OPRM function generates an inoperative alarm for an OPRM channel when there is an insufficient number of operating OPRM cells. If the number of operating LPRM inputs to an OPRM cell is less than the minimum required, the cell is considered to be inoperable. Similarly the channel is inoperable if it does not have enough operating cells. Any cell can result in 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 detailed hardware and software design specification document. Any cell can result in an OPRM channel alarm or trip condition.

The OPRM trips are combined with the APRM trips of the same APRM channel, and sent to RPS. The OPRM channel trips are sent to the RPS. The OPRM function shall not generate an inoperative trip, but shall generate an inoperative alarm for an OPRM channel when there is an insufficient number of operating OPRM cells. (An inoperative OPRM cell is defined as a cell that has insufficient number of operating LPRM inputs).

The OPRM alarms and trips are bypassed in all reactor operation modes except Run, and when operating below the required power level (typically 30%). The OPRM channel 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.

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 required 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 can still be 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 follows the same environmental consideration as the APRM.

7.2.2.3 Safety Evaluation

The evaluation for 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.

This evaluation Section covers only the safety-related functions of the NMS. These include the following:

- Startup Range Neutron Monitor (SRNM)
- Local Power Range Monitor (LPRM)
- Average Power Range Monitor (APRM)
- Oscillation Power Range Monitor (OPRM)

7.2.2.3.1 General Functional Requirements Conformance

7.2.2.3.1.1 Startup Range Neutron Monitor

The SRNM is designed as a safety-related subsystem that generates trip signals to prevent fuel damage in the event of any abnormal reactivity insertion transients while operating in the startup power range. This trip signal is generated by either an excessively high neutron flux level, or excessive neutron flux increase rate (that is, 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 are still 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.

7.2.2.3.1.2 Local Power Range Monitor

The LPRM is designed for monitoring the local power level and to provide a sufficient number of LPRM signals to the APRM system such that the safety-related design basis for the APRM is satisfied. The LPRM itself has no safety-related design basis. However, it is qualified to safety-related standards.

7.2.2.3.1.3 Average Power Range Monitor

The APRM provides information for monitoring the average power level of the reactor core when the reactor power is in the power range. The APRM is capable of generating a trip signal to scram the reactor in response to excessive and unacceptable neutron flux increase, in time to prevent fuel damage. Such a trip signal also includes a trip from the simulated thermal power signal, which represents 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 satisfied. If this requirement cannot be met, an inoperative trip signal is generated. The independence and redundancy requirements are incorporated into the design and are consistent with the safety-related design basis of the RPS.

7.2.2.3.1.4 Oscillation Power Range Monitor

The OPRM provides monitoring and protection function for core regional and core wide neutron flux oscillation monitoring, using the same set of LPRM signals used by the associated APRM channel in which the OPRM channel resides. The OPRM is capable of generating a trip signal to scram the reactor in response to excessive and unacceptable neutron flux oscillation, in time to prevent fuel damage. Scram functions are assured when the minimum LPRM input requirement to the OPRM is satisfied. The independence and redundancy requirements are incorporated into the design and are consistent with the safety-related design basis of the RPS.

7.2.2.3.2 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the NMS and the associated codes and standards applied in accordance with the SRP. The following evaluation lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR 50.55a(a)(1) Quality Standard for Systems Important to Safety

- Conformance: The NMS conforms to these criteria, as shown by the following commitments to applicable RGs and standards.

10 CFR 50.55a(h) “Protection and Safety Systems,” compliance with ANS/IEEE Std 603.

Applicable requirements of IEEE Std. 603 are met by the NMS, as described in Subsection 7.1.6, Subsection 7.2.2.2, and in this Section. The safety-related subsystems of the NMS consist of four divisions, which correspond and interface with those of the RPS. This independence and

redundancy assures that no single failure interferes with the system operation (with any three of the four divisions of safety-related power available).[SMS335]

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).

There are 64 LPRM assemblies evenly distributed in the core. There are four LPRM detectors within each LPRM assembly, evenly distributed from near the bottom of the fuel region to near the top of the fuel region (Figure 7.2-8). The 256 detectors are assigned to four divisions that consist of the four APRM channels. Any single LPRM detector is only 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 that represents the average core power. Electrical and physical separation of the division is thus maintained and optimized to satisfy the safety-related system requirement. With the four divisions, redundancy requirements are met because a scram signal can still 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 (Section 3.11). Additional information on NMS equipment qualification is included in Reference 7.1-5

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

The NMS design of bypass and inoperable status indication conforms to this requirement consistent with the conformance of the NMS design with RG 1.47. It also conforms to the requirements of control and protection system interaction as described in IEEE Std. 603, Sections 5.8 and 6.3.

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.

52.47(a)(1)(vi) ITAAC in Design Certification Applications

Conformance: There are no interface requirements for this Section.

- 52.47(a)(1)(vii) Interface Requirements

  Conformance: Interface material is provided in Tier 1.

- 52.47(a)(2) Level of Detail

  Conformance: The level of detail provided for the NMS within the Tier 1 and Tier 2 documents conforms to this requirement.

- 52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

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

- 52.79(c), ITAAC in Combined Operating License Applications

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

7.2.2.4 General Design Criteria

In accordance with the SRP for Chapter 7, and with Table 7.1-1, the following GDC are addressed for the NMS:

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

  Conformance: The NMS complies with these GDC, in part, or as a whole, as applicable. The GDC are generically addressed in Section 3.1.

7.2.2.4.1 Staff Requirements Memoranda:

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

- Conformance: The ESBWR NMS design, as part of the safety-related system, is designed to minimize the likelihood of common mode failures, conforms to this BTP in conjunction with the implementation of an additional Diverse Instrumentation and Control System capabilities as described in Section 7.8, provides additional defense against common mode failures.

7.2.2.4.2 Regulatory Guides

In accordance with the SRP for Chapter 7, and with Table 7.1-1, the following RGs are addressed for the NMS:

- RG 1.22 - Periodic Testing of Protection System Actuation Functions
- 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 Electric Systems
- RG 1.97 - Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident
- RG 1.105 - Instrument Setpoints for safety-related Systems
- RG 1.118 - Periodic Testing of Electric Power and Protection Systems

- RG 1.152 - Criteria for Programmable Digital Computer System Software in safety-related Systems of Nuclear Power Plants
- RG 1.153 - Criteria for Power, Instrumentation and Control Portions of Safety Systems
- RG 1.168 - Verification, Validation, Reviews and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants
- RG 1.169 - Configuration Management Plans for Digital Computer Software used in Safety Systems of Nuclear Power Plants
- RG 1.170 - Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants
- RB 1.171 - Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants
- RG 1.172 - Software Requirements Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants
- RG 1.173 - Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- 11.180 – 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

  The RPS conforms to RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6)

The NMS conforms to all the above-listed RGs, using the same interpretations and clarifications identified in Subsections 7.1.6.

7.2.2.4.3 Branch Technical Positions (BTPs)

In accordance with the SRP for Chapter 7, and with Table 7.1-1, the following BTPs are considered applicable for the NMS:

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

  The ESBWR has no coolant pump and the BTP Position One does not apply to ESBWR. The ESBWR complies with the BTP Position Two.

- BTP HICB-8 - Guidance for Application of RG 1.22

  The NMS is continuously operating during reactor operation. The accuracy of the sensors can be verified by cross-comparison of the various channels within the four redundant divisions and is continuously monitored by and alarmed for inconsistency by the plant computer functions in N-DCIS. A minimum number of channels or one division

can be bypassed for periodical testing during reactor operation without impacting the NMS in performing the safety function. Therefore, the NMS fully meets this BTP.

- BTP HICB-10 - Guidance on Application of RG 1.97

  There are four divisional safety-related subsystems of the NMS. Each division is entirely redundant and identical in design, independent of each other, and capable of providing indication of neutron flux for the required range. The NMS equipment is qualified to requirements of IEEE Std. 323. Hence, the NMS fully meets this BTP.

- BTP HICP-11 - Guidance for Application and Qualification of Isolation Devices

  There are four divisional safety-related subsystems of the NMS. Each division is entirely redundant and identical in design, and independent of each other, meeting requirements of IEEE Std. 603, Section 5.6. The NMS equipment is protected from disturbance from other interfacing systems and electrical power transient by using optical CIMs and fiber optic cables to meet the requirements of RG 1.75 and RG 1.153. The NMS equipment is qualified to requirements of IEEE Std. 323. Hence, the NMS fully meets this BTP.

- BTP HICB-12 - Guidance for Establishing and Maintaining Instrument Setpoints

  The analytical limits of the safety-related setpoints of the NMS are determined from safety analyses for the reactor fuel each cycle to ensure that the reactor core is protected from any rising neutron flux exceeding these values. The nominal setpoints are calculated to be consistent with the GE standard setpoint methodology, which conforms to RG 1.105 and ISA-S67.04. The setpoint margin calculated by this method has also considered additional uncertainties with the calibration interval. Hence, the NMS fully meets this BTP. Most of the uncertainty associated with safety related NMS trip setpoints is associated with the various neutron sensors since the digital electronics in the NMS does not drift and the setpoints are monitored and alarmed by the plant computer function of N-DCIS. The plant technical specifications will set a required calibration interval for LPRM detectors and the APRM signals.

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

  Development of software for the safety-related system functions within NMS conforms to the guidance of this BTP as discussed in Subsection 7.2.1.8 and Appendix 7B. safety-related software to be embedded in the memory of the NMS controllers is developed according to a structures plan as described in Appendix 7B. 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

  This BTP is applicable to all Section of the DCD including this Section on NMS. The NMS Section content conforms to this BTP.

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

The safety-related subsystems of the NMS are designed to support the required periodic testing (Refer to Subsection 7.2.2.5). The NMS system equipment is equipped with self-test design operating in all modes of plant operations. This self-test function provides the operator information of equipment failure modes, which would lead to equipment becoming inoperable. This self-test function does not interfere with the safety functions of the system. The NMS meets this BTP.

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

  Any portions of NMS design that will use commercial grade programmable logic controllers (PLCs) for safety-related functions conform to this BTP. The PLCs will be qualified to a level commensurate with safety system requirements.

- BTP HICB-19 - Guidance for Evaluate of Defense-in-Depth and Diversity in Digital Computer-based Instrumentation and Control Systems

  NMS is a four-division, independent and separated equipment arrangement. Isolation of signal transmission between safety-related divisions and between safety-related and nonsafety-related equipment employs optical CIMs and non-conductive fiber-optic cable. The four NMS divisions operate asynchronously from each other. System functions are segmented among multiple controllers. Control system functions are separated, independent, and diverse from the protection system. Random failures are mitigated by the divisional channel and channel bypass capability of NMS. A divisional bypass places the remaining divisions in a two-out-of-three trip logic condition. The NMS provides trip inputs to the RPS. Design measures to satisfy the Defense-in-Depth and Diversity principles for the RPS and ECCS function are described in Section 7.8.

- BTP HICB-21 - Guidance for Digital Computer Real-Time Performance

  The SRNM/APRM digital subsystems and the OPRM digital subsystem are designed to respond in real time to ensure that the specified fuel limits are not exceeded, and that core power oscillations are detected and suppressed. The NMS meets this BTP.

7.2.2.4.4 TMI Action Plan Requirements

In accordance with the SRP for Chapter 7, and with Table 7.1-1, there are no TMI action plan requirements applicable to the NMS.

- 10 CFR 50.34(f)(2) TMI-Related Requirements: All TMI requirements are addressed within Chapter 1.

7.2.2.5 Testing and Inspection Requirements

7.2.2.5.1 General Requirements

NMS instruments (not including sensors) outside of the containment 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 to the service personnel.

NMS instrument modules, including SRNM and APRM, are designed with the capability of being tested for the normal performance, trip performance, and calibration function, either through an automated process or through a manual process. Routine surveillance functions, including periodic tests and calibration, are automated with minimum operator interference.

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.

7.2.2.5.2 Specific Requirements

7.2.2.5.2.1 SRNM Testability and Calibration

Each SRNM channel is tested and calibrated based on 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.

7.2.2.5.2.2 LPRM Testability and Calibration

LPRM channels are calibrated using data from the AFIP Subsystem and based on plant computer three-dimensional core power distribution calculations. The calibration is based on procedures in the applicable instruction manual.

7.2.2.5.2.3 APRM Testability and Calibration

APRM channels are calibrated using data from the plant computer reactor heat balance calculation. The calibration is based on procedures in the applicable instruction manual. Each APRM channel can be tested individually for the operability of the APRM high neutron flux scram and rod-blocking functions by the introduction of test signals.

7.2.2.5.2.4 OPRM Testability and Calibration

Each OPRM channel can be tested individually for the operability of the OPRM Trip Protection algorithm by the introduction of test signals.

7.2.2.6 Instrumentation & Control Requirements

7.2.2.6.1 Instrumentation Requirements

The NMS instruments are primarily based on the digital instrument and control practices with digital design and digital electronics based programmable and memory units. NMS instruments follow a modular design concept such that each modular unit or its subunit is easily replaceable. The 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 required NMS displays provided at the Main Control Room Panel 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
- AFIP System Operability Status

The required alarms in the MCR include the following as a minimum:

- 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
- OPRM Trip

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

7.2.2.6.2 Basic Control Logic Requirements

The control logic of the safety-related subsystems in the NMS is designed as "fail-safe." That is, a trip signal is initiated if the control logic device fails because of critical hardware failure, power failure, or loss of communication failure.

The minimum required NMS controls located in the main control room 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 will send a trip signal to RPS and cause the reactor scram.

SRNM, LPRM, OPRM or APRM channel can be individually bypassed. Restrictions as to the total number and distribution of bypassed channels (at one time) must be adhered to in order to avoid reactor trip due to inoperative NMS channels.

In the case of SRNM channels, each of the twelve channels belongs to one of the four bypass groups. Each group has one “multiple position” selector switch, so that 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 RPS becomes two-out-of-three instead of two-out-of-four.

There are separate bypass functions for the SRNM and the APRM in the NMS (that is, there is no single NMS divisional bypass which will affect both the SRNM and the APRM). An APRM bypass will not force an SRNM bypass. The SRNM and APRM bypasses are separate logics to RPS, each interfacing with RPS independently. All NMS bypass logic control functions are located within NMS but none are located in RPS.

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 and then can switch it into bypass. The LPRM channel bypassed status is displayed on NMS user interface. When the maximum allowed number of bypassed LPRMs associated with any APRM channel has been 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 Reactor Protection System (RPS).

When the reactor mode switch is in Run mode, this equates to a "Coincident" mode for the NMS. When the reactor mode switch is NOT in Run mode, this equates to a "Non-Coincident" mode for the NMS. The SRNM upscale trip setpoint is lowered in the NMS Non-Coincidence mode (RPS Mode switch in Run). SRNM trips are active only when the reactor mode switch is not in the Run position. When the NMS Coincidence/Non-Coincidence switch position is in Non-Coincidence, any one of the SRNMs channel trips can cause a reactor scram; in the coincidence mode, at least two-out-of-four divisions must be tripped in order to activate the reactor scram.

7.2.2.6.3 Basic Instrument Arrangement Requirements

NMS instruments and equipments are located in appropriate areas in the control building and reactor building, with appropriate divisional physical and electrical separation. Any NMS instruments located in the reactor building are in clean areas.

7.2.3 Suppression Pool Temperature Monitoring

The Suppression Pool Temperature Monitoring (SPTM) function, which is a subsystem of the Containment Monitoring System (CMS), is classified as safety-related because it can control nuclear safety-related systems or equipment.

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 the established limits. It does this by providing the inputs necessary for automatic scram initiation, which then serves to limit the heat addition to the suppression pool.

The SPTM is a safety-related four-divisional subsystem, Seismic Category I. The specific regulatory requirements applicable to this system are listed in Table 7.1-1 and individually addressed in Subsection 7.2.3.3.2.

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 Main Control Room panels.

7.2.3.2 System Description

7.2.3.2.1 General

The SPTM provides the suppression pool temperature data for automatic scram and automatic suppression pool cooling initiation, when established limits of high temperature are exceeded. The SPTM subsystem also provides suppression pool temperature data for operator information and recording and temperature information on 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 suppression pool temperature monitoring hardware is redundantly powered by the appropriate divisional uninterruptible AC power sources, either of which can support the SPTM function.

7.2.3.2.3 Equipment Design

The suppression pool temperature monitoring system is composed of four independent instrumentation divisions. Each safety-related division contains sixteen thermocouples spatially distributed around the suppression pool. The sensor locations are established based upon the following considerations:

- Provide four-divisional, redundant measurement of suppression pool local and bulk-mean temperature, under normal plant operating conditions and under postulated accident and post-accident conditions;

- Provides 16 temperature sensors for use by the diverse protection system (DPS);
- Implementing 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
- Locating sensors away from jet paths of SRV quenchers, horizontal vent discharges, and PCCS vent line discharges. This limits the maximum measurement differences between local and bulk-mean values.

The sensor electrical wiring, encapsulated in bendable, grounded sheathing, is terminated in the wetwell-sealed, moisture-proof junction box for easy sensor replacement or maintenance during the plant outage time. The temperature sensor wiring from the wetwell junction boxes is directed through the suppression pool divisional instrument penetrations to the four-divisional safety-related Distributed Control and Information System (Q-DCIS) 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 are required to be operational and the SPTM logic will automatically compensate for inoperable thermocouples. If less than the required number of thermocouples is available, a trip signal will be generated in that division. These signals are transmitted, via divisional Q-DCIS, to 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

7.2.3.3.1 General Functional Requirements Conformance

Suppression pool temperature monitoring is designed to support the maintenance of suppression pool temperature by providing four-divisional inputs for automatic scram initiation and temperature status display.

Suppression pool temperature monitoring also provides safety-related inputs to the Main Control Room for indication, provides input for nonsafety-related suppression pool automatic cooling mode initiation, and information for display, alarm and recording and inputs to the DPS.

7.2.3.3.2 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the Suppression Pool Temperature Monitoring function and the associated codes and standards applied in accordance with the SRP 7.2. The following analysis lists the applicable criteria and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

7.2.3.3.2.1 10 CFR 50 and 52

- 50.55a(a)(1), Quality Standards for Systems Important to Safety

  Conformance: SPTM complies with this requirement.

- 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, Sections 5.6 and 6.3, and RG 1.75. The SPTM portion of CMS consists of four divisions, which are redundantly designed so that failure of any single temperature elements will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

- 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication

  Conformance: SPTM demonstrates compliance by being able to provide automatic indication of bypassed and operable status.

- 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.

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

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

- 52.47(a)(1)(vii), Interface Requirements

  Conformance: Interface material is provided in Tier 1.

- 52.47(a)(2), Level of Detail

  Conformance: The level of detail provided for the SPTM subsystem within the Tier 1 and Tier 2 documents conforms to this BTP.

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

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

- 52.79(c), ITAAC in Combined Operating License Applications

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

7.2.3.3.2.2 General Design Criteria

In accordance with Table 7.1-1, the following GDC are addressed for the SPTM subsystem:

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

Conformance: The SPTM subsystem complies with the GDC identified. GDC conformance is generically discussed in Subsection 3.1.

7.2.3.3.2.3 Staff Requirements Memoranda

- Item II.Q, (Defense Against Common-Mode Failures in Digital Instrument and Control Systems) of SECY-93-087 (Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs).

  Conformance: The ESBWR SPTM subsystem and Engineered Safety Features (ESF) designs conform to the item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of diverse instrumentation and control, described in Section 7.8.

7.2.3.3.2.4 Regulatory Guides

In accordance with Table 7.1-1, the following RGs are addressed for the SPTM subsystem:

- RG 1.22 - Periodic Testing of Protection System Actuation Function
- RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System
- RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems
- RG 1.62 - Manual Initiation of Protective Actions
- RG 1.75 - Physical Independence of Electric Systems
- RG 1.97 -Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident
- RG 1.105 - Setpoints for safety-related Instrumentation
- RG 1.118 - Periodic Testing of Electric Power and Protection Systems
- RG 1.153 - Power Instrumentation & Control Portions of Safety Systems
- The SPTM subsystem conforms to all of the above listed RGs, with the same interpretations and clarifications identified in Subsection 7.2.1.3 also being applied to SPTM.
- RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 1.173, 1.180 and 1.204 are addressed Subsection 7.1.6.

7.2.3.3.2.5 Branch Technical Positions (BTPs)

In accordance with the SRP for Section 7.4, and with Table 7.1-1, the following BTP is addressed for SPTM:

- HICB-3 - Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service
- HICB-8 - Guidance for Application of RG 1.22
- HICB-10 - Guidance on Application of RG 1.97
- HICB-11 - Guidance on Application and Qualification of Isolation Devices
- HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints
- HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors
- HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
- HICB-17 - Guidance on Self-Test and Surveillance Test Provisions
- HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
- HICB-19 - Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems
- HICB-21 - Guidance on Digital Computer Real-Time Performance

  Conformance: The SPTM complies with all the above HICBs. Discussion of HICBs 14, 17, 18, 19 and 21 are addressed in conjunction with the Engineered Safety Features Safety System Logic and Control System Engineered Safety Features (SSLC/ESF) in Subsection 7.3.5.3 and with the RPS in Subsection 7.2.1.8.

7.2.3.3.2.6 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 above for 10 CFR 50.34(f)(2)(v). However, TMI action plan requirements are generically addressed in Appendix 1A.

7.2.3.4 Testing and Inspection Requirements

Proper functioning of analog temperature sensors is verified by channel cross-comparison during plant normal operation mode; the bulk pool temperatures are continuously compared between divisions and alarmed for inconsistency by the plant computer functions.

Each of four suppression pool temperature monitoring safety-related divisions is testable during plant normal operation to determine the operational availability of the system. Each safety-

related division of suppression pool temperature monitoring has the capability for testing, adjustment, and inspection during plant outage.

7.2.3.5 Instrumentation Requirements

The instrumentation and control requirements related to suppression pool temperature monitoring 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.

Table 7.2-1

Channels Utilized in Functional Performance of RPS

Channel Description	Number of Channels of Sensors
Neutron Monitoring System (APRM)	4
Neutron Monitoring System (SRNM) (Note 1)	4
Nuclear system reactor vessel pressure	4
Drywell pressure	4
Reactor vessel narrow range water level	4
Low charging pressure to control rod hydraulic unit accumulator	4
MSL isolation valve position switches	8
TSV closure	4
TCV fast closure	4
Loss of Power Generation Bus (Loss of FW Flow)	4
High Condenser Pressure	4
Suppression pool temperature monitoring	4

1. In modes other than Run
2. Eight (8) switches

Table 7.2-2

SRNM Trip Function Summary

Trip function	Analytical Limit For Trip Setpoint (Note 1)	Action
SRNM Upscale Flux Trip	45% power (Note 2)	Scram (bypassed in Run)
SRNM Upscale Flux Alarm	35% power (Note 3)	Rod Block (bypassed in Run)
SRNM Short Period Trip	10 second	Scram (Note 4) (bypassed in Run & Refuel) (no scram function in counting range)
SRNM Short Period Alarm	20 second	Rod Block (bypassed in Run)
SRNM Period Control Rod Withdrawal Permissive	55 second	Rod Block (bypassed in Run) (Note 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 (Note 6)
SRNM Intermediate Upscale Flux Alarm	1E+5 cps	Rod Block (Note 6)
SRNM ATWS Permissive	6% power	Permissive signal to ATWS/SLC system (all modes)

Notes:

1. Instrument setpoint accuracy will be determined by safety analyses using GE 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, which is 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 will be 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	

Notes:

(1) No trips are active in Run mode or for a bypassed channel. Otherwise, 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 4.1.1.1.8.f

(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 system requirement.

Table 7.2-4

APRM Trip Function Summary

Trip Function	Analytical Limit For Trip Setpoint (Note 1)	Action
APRM Upscale Flux Trip	120% power 15% power	Scram (only in Run) Scram (not in Run)
APRM Upscale Flux Alarm	108% 12% power	Rod Block (only in Run) Rod Block (not in Run)
APRM Upscale Simulated Thermal Power Trip	115%	Scram
APRM Inoperative	1. LPRM input too few; 2. Module interlocks disconnect	Scram & Rod Block Scram & Rod Block
APRM ATWS Permissive	6%	ADS Permissive signal to SSLC system (all modes)
APRM Downscale	5%	Rod Block (only in Run)

1. Instrument setpoint accuracy will be determined by safety analyses using GE 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** (Note 1)	Action
OPRM Inoperative	LPRM inputs too few	OPRM Cell/Channel Alarm
OPRM Oscillation Detection	Bypassed below 30% and when not in Run	Channel Trip to RPS
OPRM Oscillation Detection	Bypassed below 30% and when not in Run	Channel Alarm
OPRM Bypass	N/A	Controlled by APRM bypass

1. Instrument setpoint accuracy will be determined by safety analyses using GE instrument setpoint methodology of Reference 7.2-1.

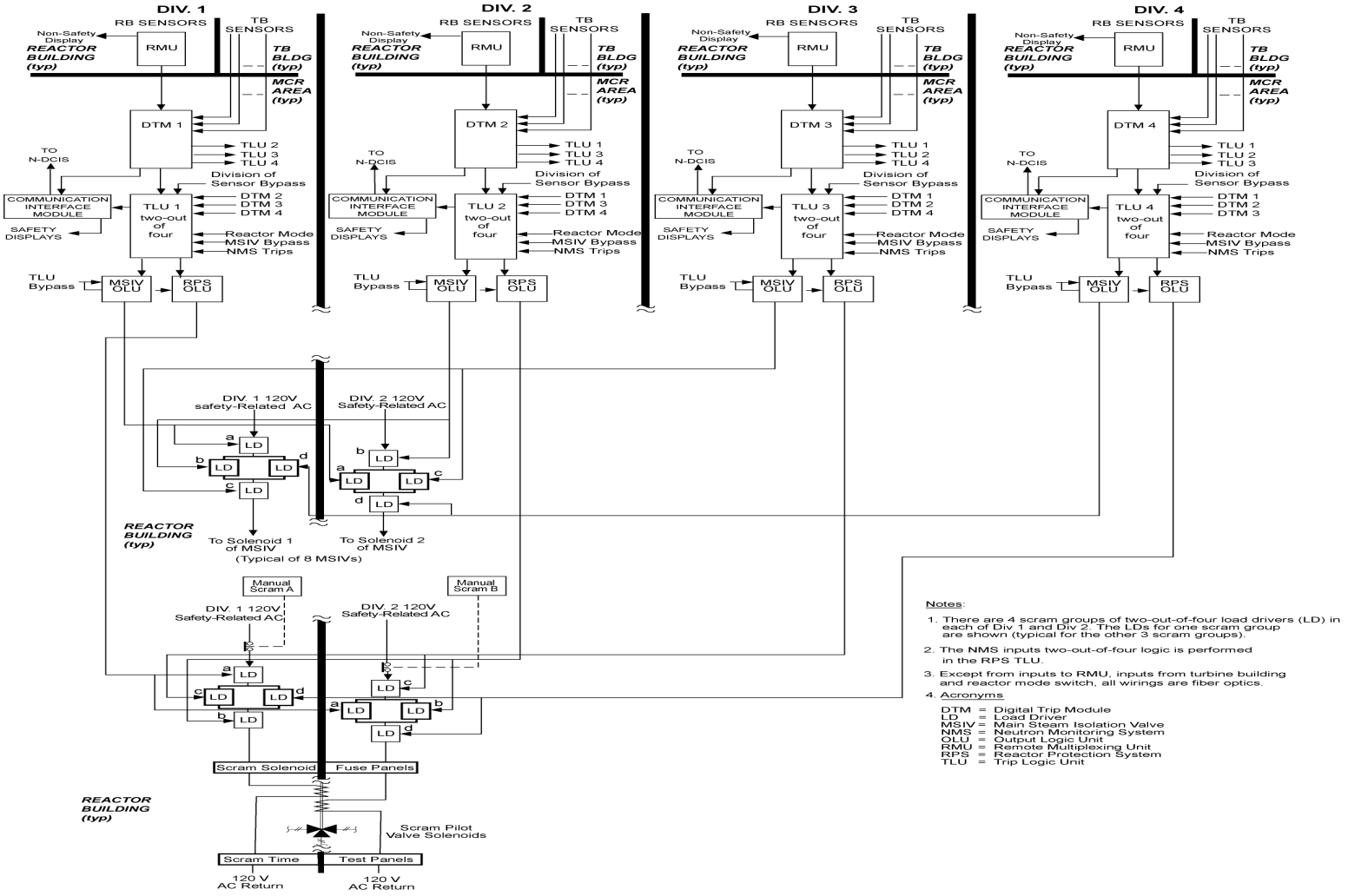


Figure 7.2-1. RPS Functional Block

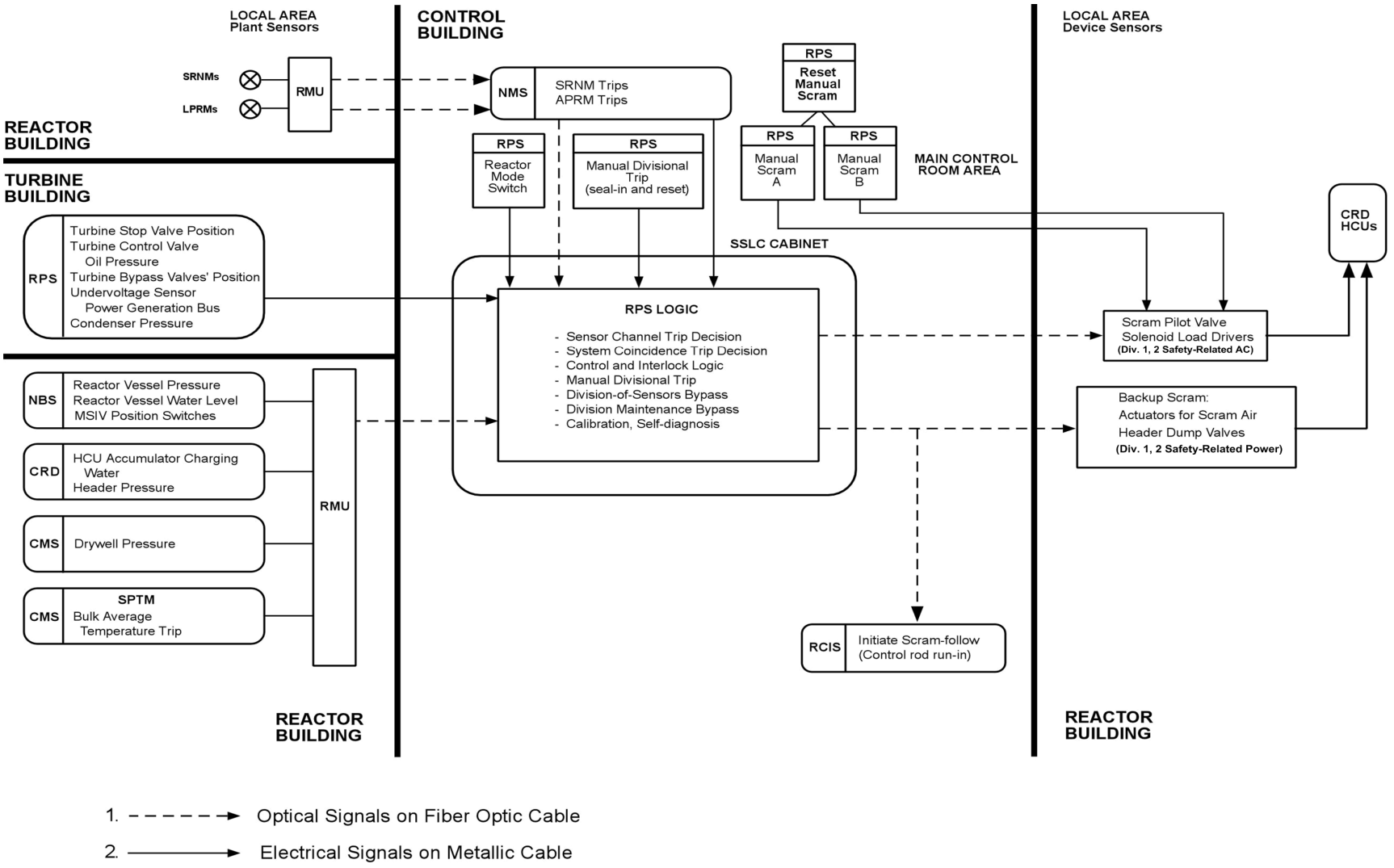


Figure 7.2-2. RPS Interfaces and Boundaries Diagram

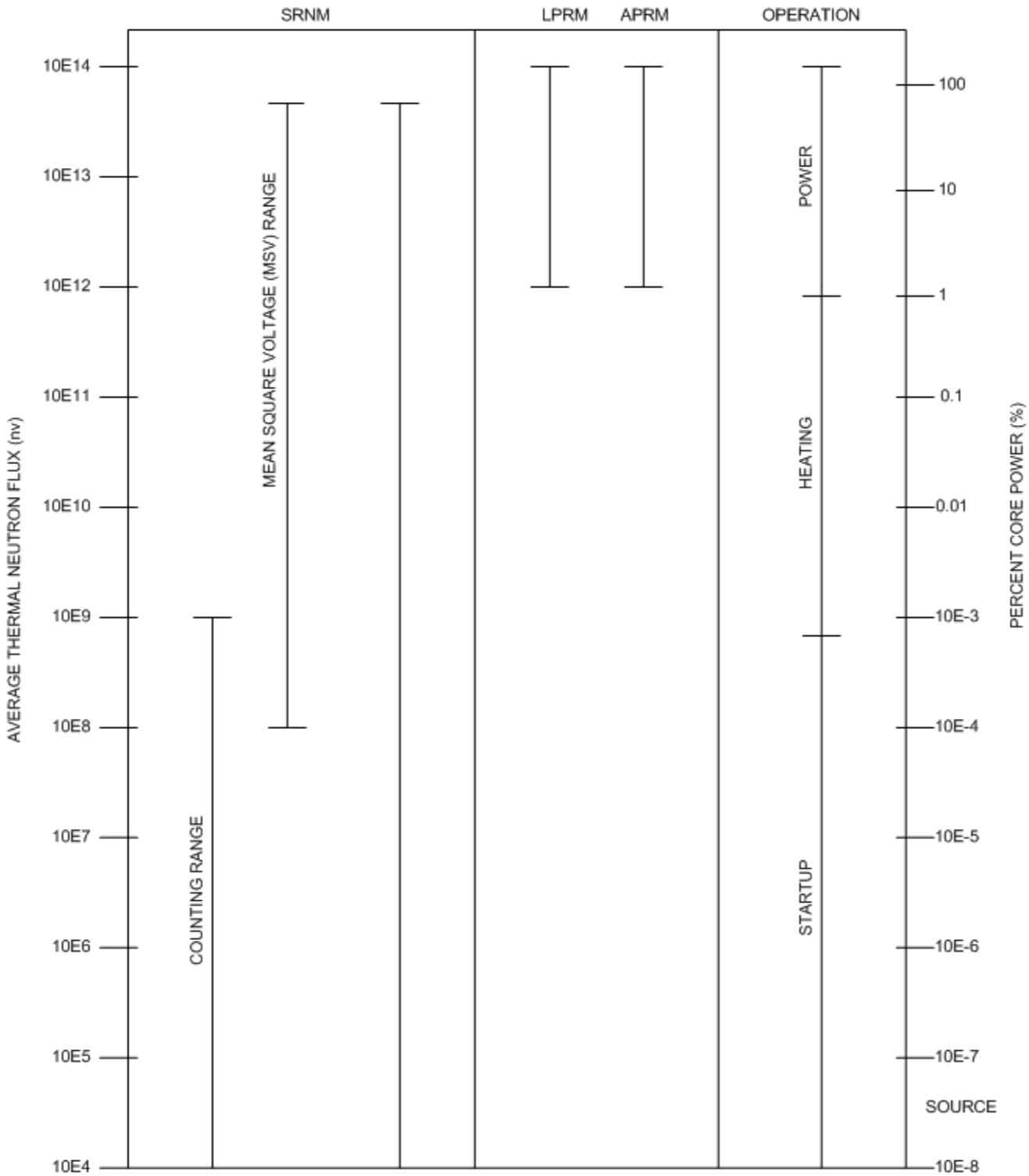


Figure 7.2-3. Neutron Flux Monitoring Ranges

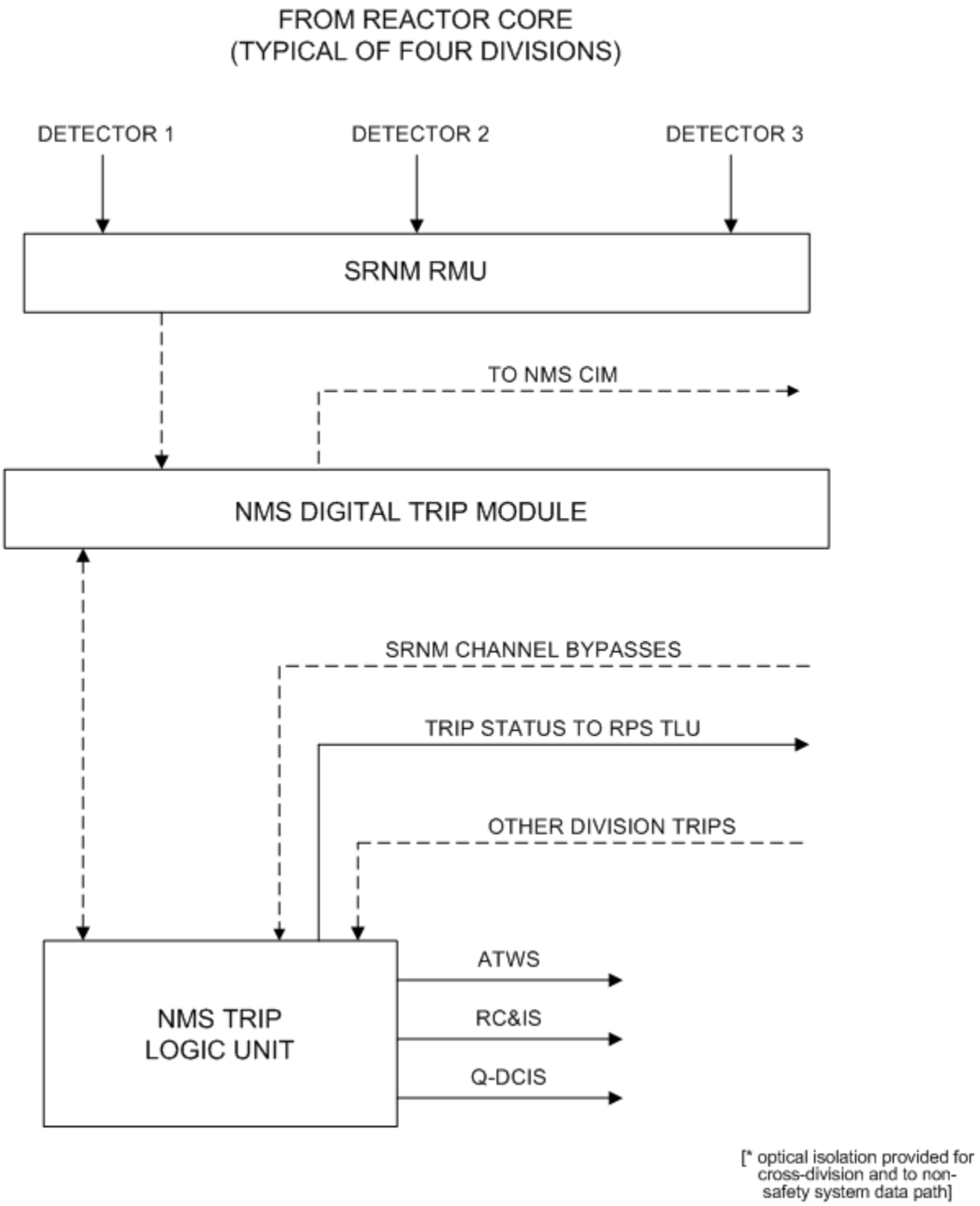


Figure 7.2-4. Basic Configuration of a Typical SRNM Subsystem

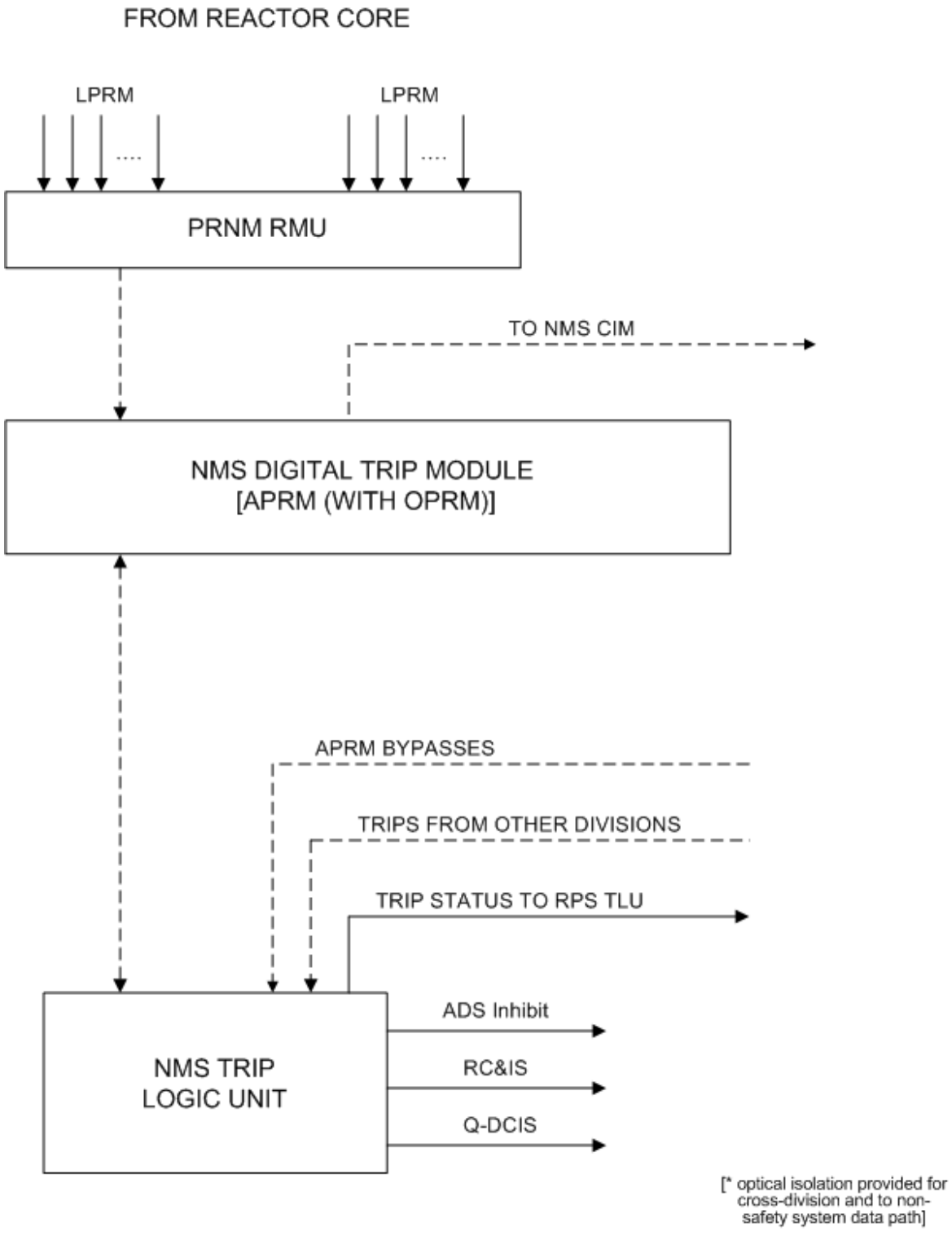


Figure 7.2-5. Basic Configuration of a Typical PRNM Subsystem

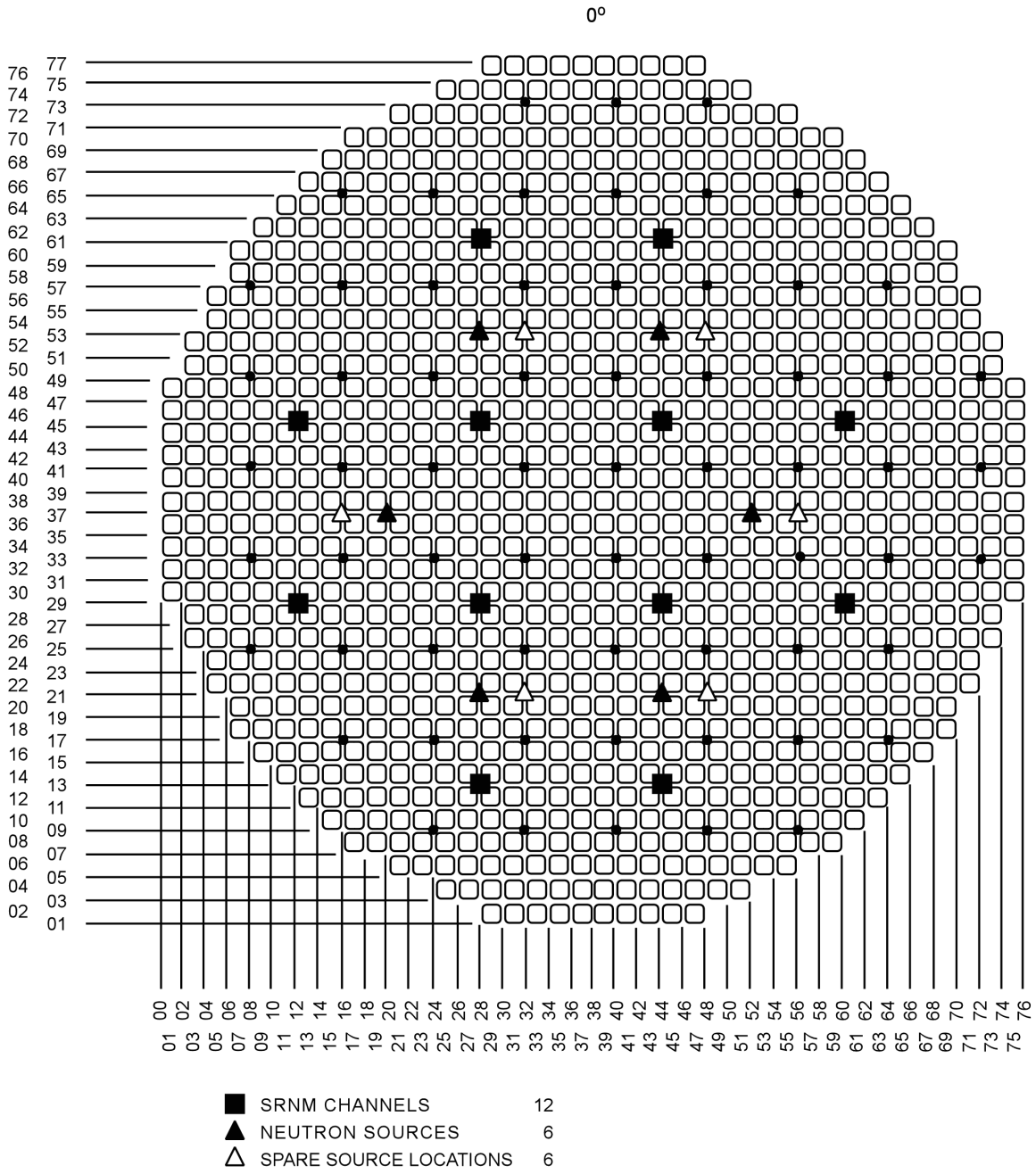


Figure 7.2-6. SRNM Detector Locations

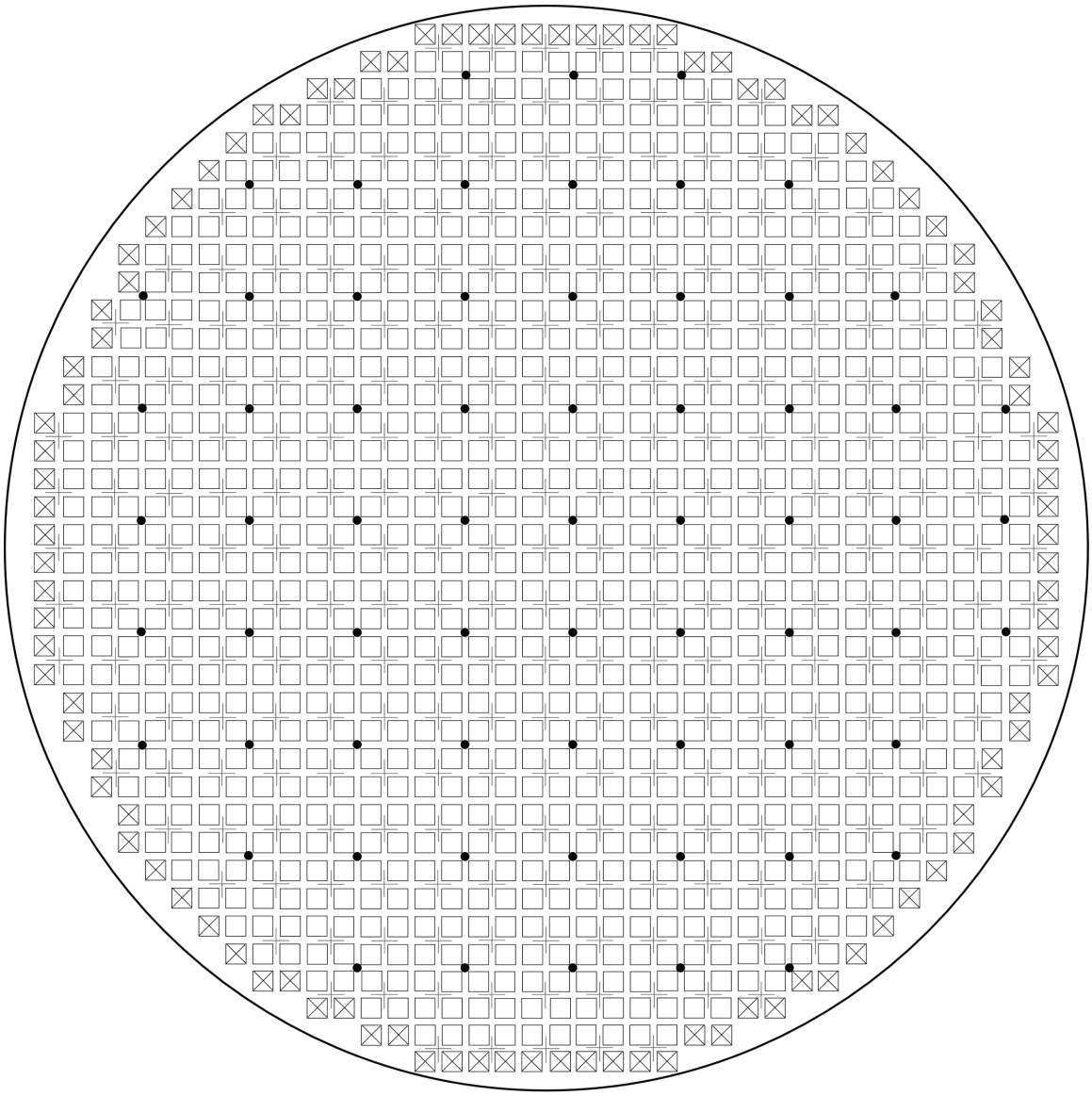
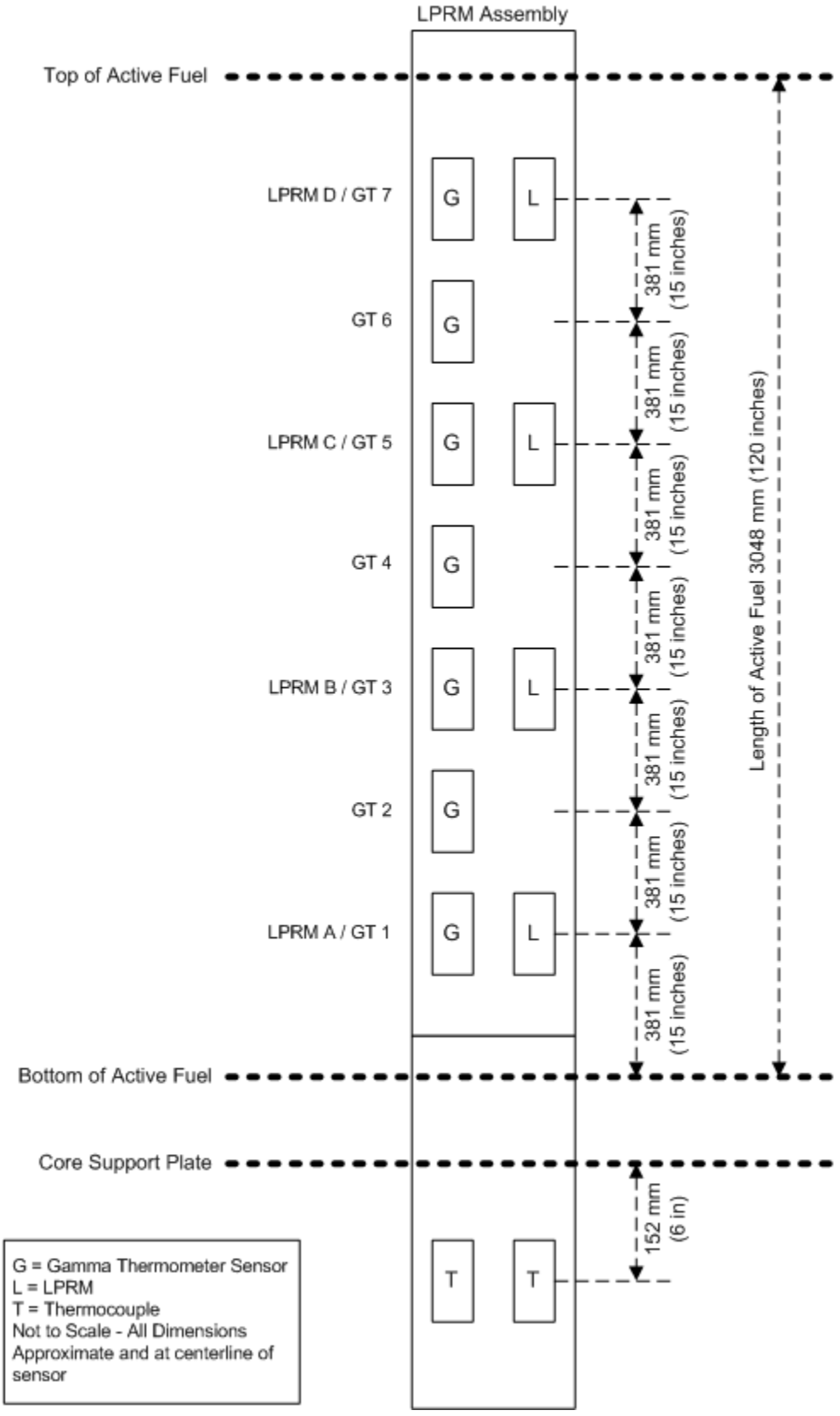


Figure 7.2-7. LPRM Locations in the Core


LPRM Assembly
Top of Active Fuel
LPRM D / GT 7
GT 6
LPRM C / GT 5
GT 4
LPRM B / GT 3
GT 2
LPRM A / GT 1
G
L
381 mm (15 inches)
Length of Active Fuel 3048 mm (120 inches)
Bottom of Active Fuel
Core Support Plate
152 mm (6 in)
T
G = Gamma Thermometer Sensor
L = LPRM
T = Thermocouple
Not to Scale - All Dimensions Approximate and at centerline of sensor

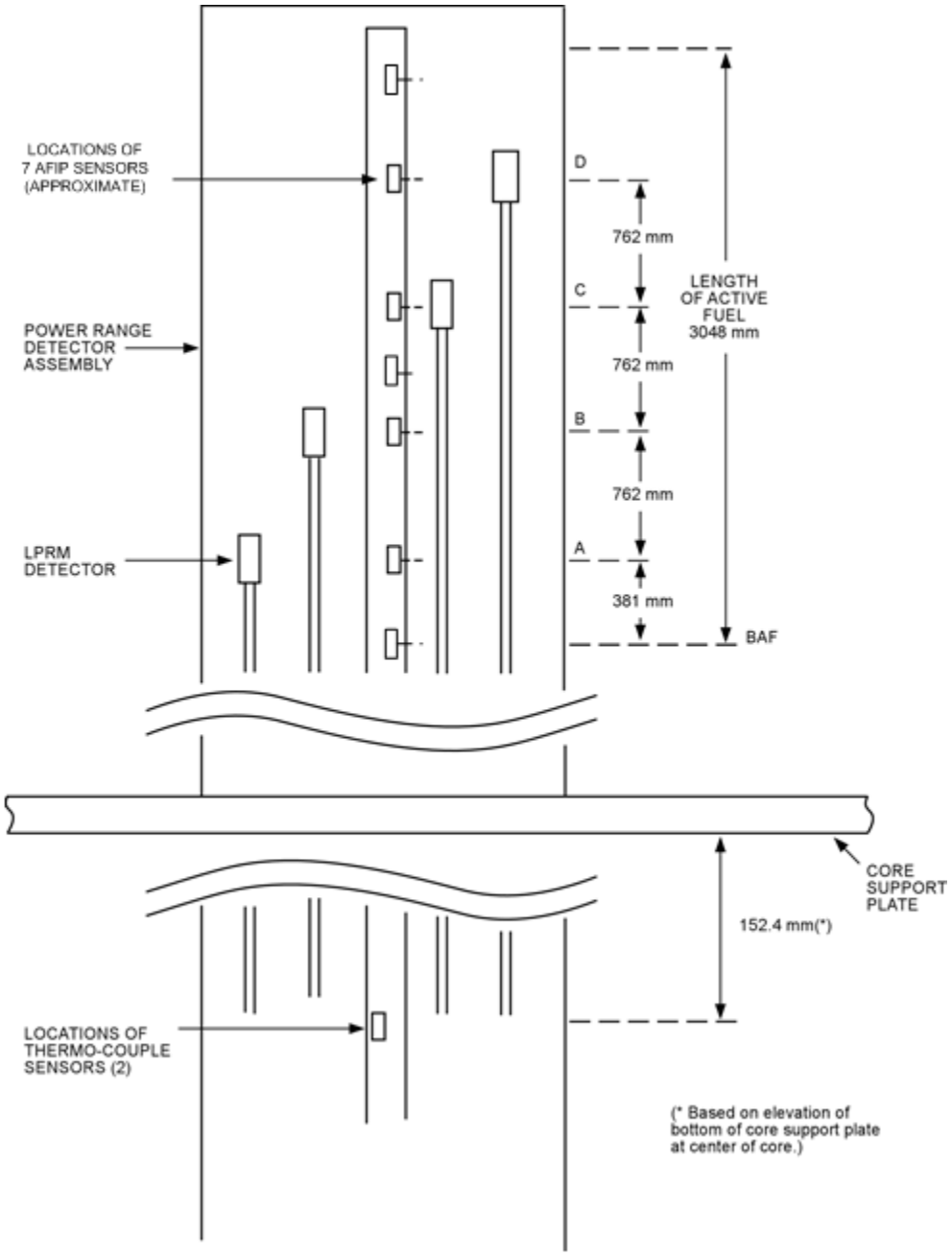


Figure 7.2-8. Axial Distribution of LPRM Detectors

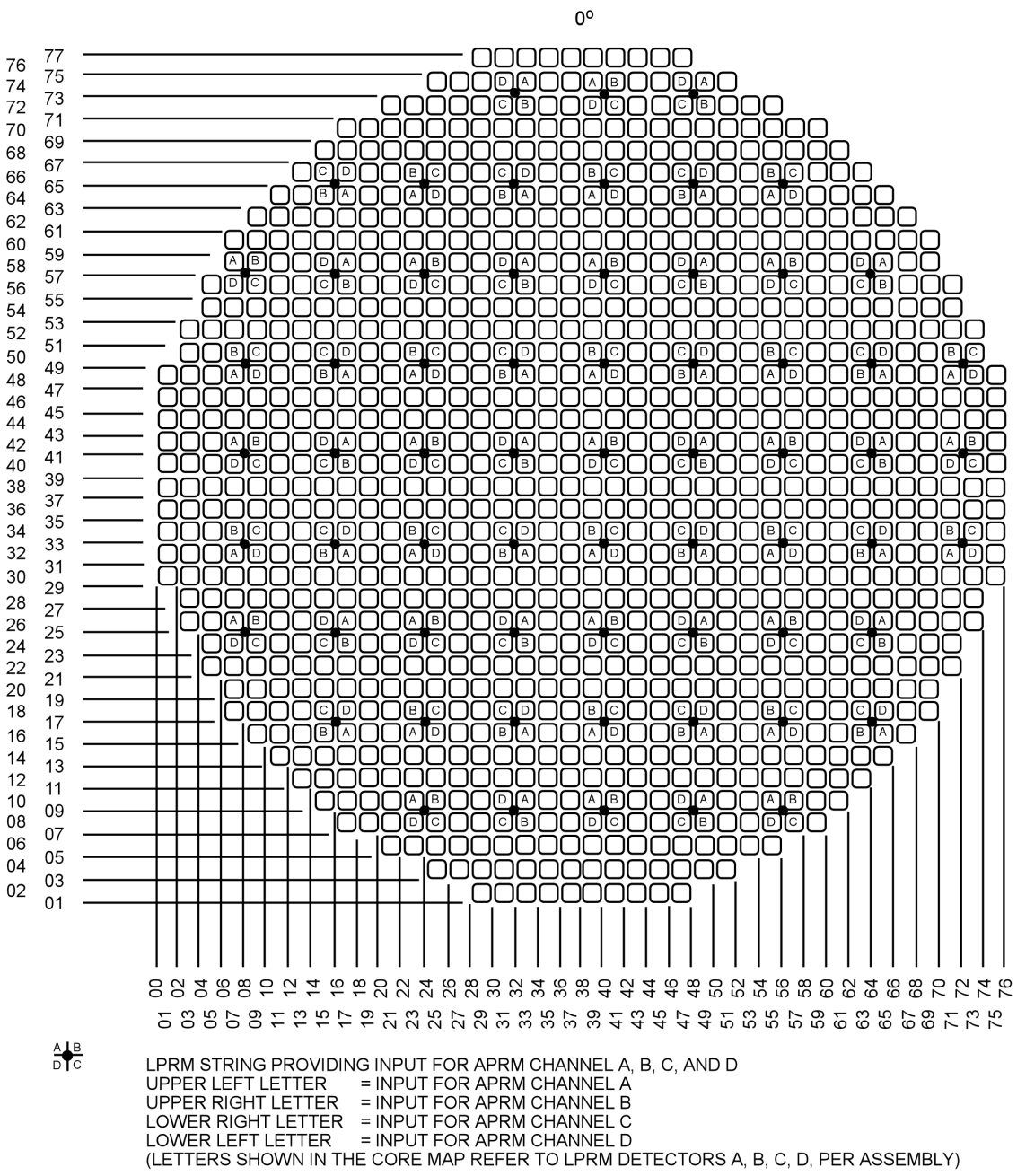


Figure 7.2-9. LPRM Assignments to APRM Channels

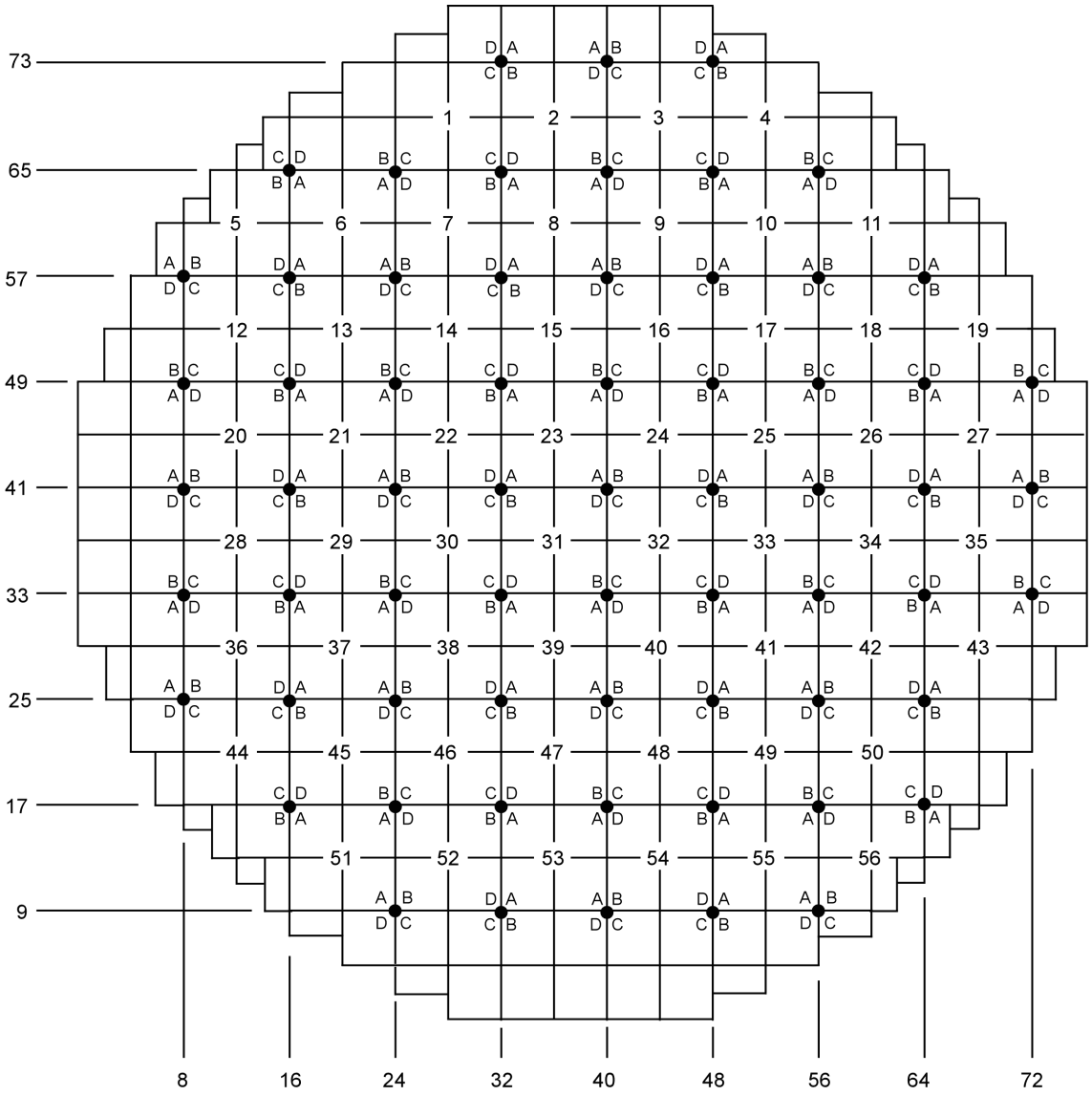


Figure 7.2-10. LPRM Assignment to OPRM Channels

7.3 ENGINEERED SAFETY FEATURES SYSTEMS

The ESF systems are part of a group of systems that are collectively referred to as the Safety-Related Distributed Control and Information System (Q-DCIS). A simplified functional block diagram of Q-DCIS is included as part of Figure 7.1-1 and a detailed 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 that are collectively referred to as N-DCIS. Section 7.1 contains a description of these relationships.

7.3.1 Emergency Core Cooling System

The Emergency Core Cooling System (ECCS) is comprised of the Automatic Depressurization System (ADS), the Gravity-Driven Cooling System (GDCS), the Isolation Condenser System (ICS), and the Standby Liquid Control (SLC) system.

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.

7.3.1.1.1 System Design Bases

Safety-Related Design Bases

The ADS controls and instrumentation meet the following safety-related requirements:

- Detect reactor low water level, Level 1;
- Automatically actuate the safety/relief valves (SRVs) and depressurization valves (DPVs) after Level 1 is reached;
- Actuate the ADS SRVs and DPVs sequentially and in groups to achieve the required depressurization characteristics;
- Any single-failure will not render more than one valve inoperative;
- Have physical and electrical separation and isolation between safety-related divisions and from nonsafety-related circuits and equipment; and
- Indicate the status of ADS SRVs and DPVs in the main control room.
- Nonsafety-Related Design Basis

The ADS instrumentation meets the following nonsafety-related requirements:

- No single control or instrumentation failure will inadvertently open an ADS SRV or a DPV; and
- ADS-parameters alarm provided in the main control room.

7.3.1.1.2 System Description

Summary Description

The ADS comprises 10 safety-relief valves (SRVs), 8 depressurization valves (DPVs) and associated instrumentation and controls. Five (5) ADS SRVs are initially opened to start reducing reactor pressure vessel (RPV) pressure, followed by five more ADS SRVs after a time delay. See Table 7.3-2 for the ADS SRV groups and 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 amount of water lost as a result of level swell in the reactor pressure vessel (RPV) when the RPV pressure is rapidly reduced. The ADS operates independently of the 8 non-ADS SRVs that are also installed on the RPV. See Table 5.2-2 for the ADS SRV and DPV settings and/or capacities.

The NBS function components (including the ADS) are shown on Figure 5.1-2. The mechanical aspects of the ADS function within the ECCS are discussed in Subsection 6.3.3 and the ADS logic and control are shown on Figures 7.3-1A and 7.3-1B.

System Design

The ADS design parameters shown in Table 7.3-1 ensure that no single failure of an ADS division logic, ADS SRV actuation pilot or DPV igniter circuit, with any three of the four divisions of safety-related power available, can prevent successful system operation. This satisfies the single failure criterion of IEEE Std. 603, Section 5.1.

ADS Input Circuits

Actuation of ADS equipment is controlled automatically (IEEE Std. 603, Sections 6.1 and 7.1), without need for operator action. Manual actuation is also provided (IEEE Std. 603, Sections 6.2 and 7.2).

Four wide range reactor level transmitters are used to detect Level 1; these transmitters are separate from those used for RPS functions and diverse to those used for the DPS wide range level transmitters.

Logic and Sequencing

The ADS logic is implemented in four SSLC/ESF ECCS divisions, each of which can make a Level 1 trip decision. Each of the trip decisions is shared between the four divisions. Normally each of the four divisions makes a two-out-of-four trip decision from each of the four divisional trip decisions, however the entire SSLC/ESF ECCS system has a “division of sensors” joystick bypass switch such that any division of sensors can be removed from the two-out-of-four decision process. The bypass is enforced by the switch to allow only one division at a time to be bypassed and can be used for maintenance or calibration activities. The use of the sensor bypass switch reduces the two-out-of-four trip decision process to a two-out-of-three trip decision. Divisional bypasses are alarmed in the MCR and the four divisional water levels and their trip setpoints are continuously monitored and alarmed for consistency by the N-DCIS plant computer functions.

Each division of the SSLC/ESF ECCS 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 do not inadvertently open any ADS valve (SRV or DPV). (See Figures 7.3-1A, 7.3-1B and 7.3-2) 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 will issue the ECCS trip signal if level drops below Level 1.

The ECCS trip signal then starts a timer (see Table 7.3-2); should the trip signal reset (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 the time delay, the logic seals in and issues an "initial start" signal (IEEE Std. 603, Section 5.2). The initial start signal is also sent to the SLC system, ICS and GDCS (these systems are discussed in Subsections 7.3.5 and 7.3.1.2, respectively). The initial start signal specifically initiates five timers in each of the two two-out-of-four trip logic trains (per division) of ADS logic.

These five timers apply to the time delays of six sets of valve openings, (that is, initial start no delay) for Group 1 (5 ADS SRVs), and subsequent delays for Group 2 (5 other ADS SRVs), Group 1 (3 DPVs), Groups 2 and 3 (2 DPVs each) and Group 4 (1 DPV). As such, there is an initial ADS start signal (per train), and then a time delayed second (per train), third (per train), fourth (per train), fifth (per train) and sixth (per train) ADS start signal. The definitions of these ADS group assignments are described in Table 7.3-2 and Table 7.3-3, where the DPVs' number of assigned groups, number of valves per group, and group initiation signal time delays are explained. Once the initial start signal is generated the timers cannot be reset and all six starting signals (per train) will be issued.

The first start (called "initial start") signal opens five ADS SRVs to initially reduce reactor pressure; the second start signal opens the remaining five ADS SRVs. The third start signal, which is also made available to the SLC system (discussed in Subsection 7.3.5) opens three of the DPVs and the fourth through sixth start signals will open the remaining DPVs in groups of two, except Group 4 which is one DPV. This sequential operation facilitates rapid depressurization while minimizing the amount of water lost as a result of level swell in the reactor that occurs when pressure is rapidly reduced.

Each of the trains (per division) of ADS start signals are sent to the load drivers/discrete outputs for the ADS SRVs and DPVs operated by that division. The load drivers/discrete outputs are wired in series for each valve such that each is required for operation; this scheme makes the logic single failure proof against inadvertent actuation. Each ADS SRV and each DPV is connected to three divisions of power (three divisional solenoids for ADS SRVs and three squib initiators for the DPVs) with the solenoids and initiators evenly spread among the four divisions. The logic is such that any of the connected divisions opens the ADS SRV/DPV; this makes the design single failure proof against not opening every valve, with any three of the four divisions of safety-related power available. Every valve will actuate even with the loss of two divisions of power.

Divisional separation is maintained through the use of optical isolators and separated raceway, conduit, penetration wiring to each ADS SRV or DPV. Any two divisions can open all of the valves.

Additionally, as discussed in Subsection 7.8.1.2, the Diverse Protection System (DPS) also has the ability to independently open the same ADS SRVs and DPVs using the same logic but using diverse hardware/software equipment and separate reactor level sensors from those used in the primary ECCS functions. In the case of the ADS SRVs the DPS uses a fourth, nonsafety solenoid on each of the ADS SRVs. In the case of the DPVs the DPS uses a fourth, squib initiator on each of the DPVs.

The SRVs are described in detail in Subsection 5.2.2 and the DPVs are described in detail in Subsection 6.3.2.

The safety-related VDUs in the main control room can provide a display format that will allow the operator to manually open each ADS SRV independently using the primary SSLC/ESF ECCS logic function (IEEE Std. 603, Sections 5.8, 6.2 and 7.2). Any nonsafety-related VDU in the main control room can provide a display format that will allow the operator to individually open each ADS SRV independently using the DPS logic function. Each display utilizes an "arm/fire" configuration that requires at least two deliberate operator actions. Operator use of the "arm" portion of the display will cause a plant alarm. These two manual opening schemes are diverse from one another.

Similar to the ADS SRV manual actuations, the safety-related VDUs in the MCR can provide a display format that allows the operator to manually open each DPV independently using the primary SSLC/ESF ECCS logic function (IEEE Std. 603, Sections 5.8, 6.2 and 7.2). Any nonsafety-related VDU in the MCR can provide a display format that allows the operator to individually open each DPV independently using the DPS logic function. Each display utilizes an "arm/fire" configuration that requires at least two deliberate operator actions. Operator use of the arm portion of the display causes a plant alarm. The two manual opening schemes from the primary SSLC/ESF ECCS and from DPS are diverse from one another.

Finally, each safety-related VDU can provide a display with an "arm/fire" switch (one per division) to manually initiate ADS as a system instead of 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 ADS sequence seals in and starts the ADS valve sequencing (IEEE Std. 603, Section 5.2). This requires at least four deliberate operator actions. For all of the manual initiations, operator use of the "arm" portion of the display causes a plant alarm.

See Figure 7.3-1A for a typical ADS SRV actuation logic and Figure 7.3-1B for a typical DPV actuation logic.

The actual firing circuit for the various squib initiators and ADS SRV solenoids is a series circuit of the two load drivers/discrete output followed by a continuity monitor and then a keylock switch, all located in the appropriate divisional remote multiplexing units and DPS remote multiplexing unit in the Reactor Building. Because there is the division of sensor 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 ECCS logic. It is undesirable to perform this level of bypass activities 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"

(which can be exercised one at a time from the control room) and to indicate that both have closed.

The keylock switch (shown in Figure 7.3-1A and Figure 7.3-1B) that disables the firing circuit is per valve and does not interact with the other valves on that RMU; operation of any keylock switch causes a control room alarm to indicate 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 additionally allows on line surveillance and maintenance activities to be done, with the assurance that the valve will not be opened inadvertently. The operation of a keylock switch in any one division does not disable the ADS SRV or DPV since it may still be opened by it's other divisional solenoid/squib initiator. Additionally it is not possible to lose the single-failure inadvertent actuation protection by any operator or keylock switch action.

Supporting Systems

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 ADS SRV solenoid and DPV squib initiator power is also 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 ADS SRVs is from accumulators located near the SRVs, which are supplied with nitrogen by the High Pressure Nitrogen Supply System.

7.3.1.1.3 Safety Evaluation

Chapter 15 and Subection 6.3 evaluate the individual and combined capabilities of the ECCS systems, including ADS. For the entire range of nuclear process system break sizes, the ECCS systems ensure that the reactor core is always covered.

SSLC/ESF ECCS initiating instrumentation, including the ADS, must respond to the potential inadequacy of core cooling regardless of the location of the breach in the reactor coolant pressure boundary. Reactor vessel low water level, which is completely independent of breach location, is used to initiate 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, logic, and the ADS SRV and DPV initiation circuitry is powered by divisionally separated safety-related power sources.

7.3.1.1.3.1 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the ADS and the applicable codes and standards. These are discussed below:

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

Commitment to RGs and standards, as addressed in this Section, satisfies 10 CFR 50.55a(1).

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 and 7.2.1.2.4.

10 CFR 50.34 (f) (2) (v) (l.D.3)

Commitment to RGs and standards, as addressed in this Section, satisfies 10 CFR 50.34 (f) (2) (v) (I.D.3).

10 CFR 50.34 (f) (2) (xiv) (lI.E.4.2)

Commitment to RGs and standards, as addressed in this Section, satisfies 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

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 I&C systems and equipment.

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 Tier 2 documents conforms to this BTP.

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

The ESBWR I&C design does not use innovative means for accomplishing safety functions.

10 CFR 52.79(c) ITAAC in Combined Operating License Applications

ITAAC are provided for the I&C systems and equipment.

7.3.1.1.3.2 General Design Criterias

In accordance with Table 7.1-1, the following GDCs are addressed for the ADS System:

Criteria: GDC 1, 2, 4, 13, 19, 20, 21, 22, 23 and 24.

Conformance: The ADS complies with these GDCs.

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: In addition to the design features already incorporated in the design on defense-in-depth and against common mode failures as addressed to this SRM, the ADS function and other Engineered Safety Feature (ESF) design conform with the Item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of an additional Diverse Instrumentation and Control System, described in Section 7.8.

7.3.1.1.3.4 Regulatory Guides

RG 1.22 Safety Guide 22 Periodic Testing of Protection System Function - System logic is tested continually as described in Subsection 7.3.1.1.3.6. Components are tested periodically during refueling outages every two years. The ADS fully conforms to 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.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems - The ADS fully meets the guidance of RG 1.47. Automatic indication is provided in the control room to inform the operator that the system is inoperable or a division is bypassed.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems - The ADS 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 - The ADS fully conforms to this RG. Manual actuation of ADS requires the operator to actuate at least two dual action switches. This ensures that the manual initiation of ADS is a deliberate act.

RG 1.75 - Physical Independence of Electric Systems - Physical separation is maintained in accordance with RG 1.75 and is described in Subsection 7.3.1.1.2.

The redundant equipment and circuits within the ADS have divisional separation. Redundant circuits and equipment are located within their respective divisional safety Class enclosures. Separation is achieved by barriers, isolation devices, or physical distance; thus, assuring that a single-failure in one division would not affect the operation of other redundant divisions.

No physical connections are made between divisions except through nonmetallic fiber-optic medium.

Nonsafety-related circuits are in accordance with safety-related circuit requirements up to and including the isolation devices. Circuits beyond the isolation devices do not again become connected with safety-related circuits.

Separation between safety-related and nonsafety-related circuits either satisfies the same minimum requirements as that for the separation between safety-related circuits or they are treated as associated circuits.

RG 1.105 - Instrument Setpoints for Safety Related Systems - The setpoints used to initiate ADS are established 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. The GE design document titled "General Electric Instrument Setpoints Methodology", Reference 7.2-1, provides the detailed description of this methodology.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems - The ADS conforms to the intent of RG 1.118 as amplified in IEEE Std. 338. A full functional test of the ADS is not practical, because a loss-of-coolant event 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 7.3.1.1.3.6.

DPV valve initiators are periodically removed and test fired in a laboratory. Reactor vessel level transmitters are located outside containment and calibration verification can be performed during plant operation.

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems -The ADS fully conforms to RG 1.153.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems

Conformance: ADS conforms to RG 1.180 as discussed in Subsection 7.1.6.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants

Conformance: ADS conforms to RG 1.204 as discussed in Subsection 7.1.6.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are discussed in Subsection 7.1.2.2.

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 ESBWR, in that it has no reactor recirculation pump.

- BTP HICB-6 - Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

  The ESBWR has no recirculation pump and has 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 that is not tested during reactor operation and a discussion of how each conforms to 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 that would allow testing during reactor operation without creating an unacceptable breach of the reactor coolant pressure boundary. The ADS 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 ADS SRVs and DPV initiators can be tested when the reactor is shut down.

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

  ADS conforms to 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 from safety-related to 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 to this BTP. Additional discussion is in Subsection 7.2.2.4.

- 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 Section on ADS. This Section content conforms to this BTP.

- BTP's HICB-14, HICB-17, HICB-18, HICB-19 and HICB-21 are discussed in association with the SSLC/ESF in Subsection 7.3.5.3.

7.3.1.1.3.6 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 ADS SRV pilot solenoids and the bridge wires within the DPV squib valve actuating circuitry. The test current is continuously applied and results in an alarm if the circuit is interrupted. Testing of ADS equipment is conducted during refueling outage. Refer to Subsection 6.3.2.8.4 for a discussion of mechanical tests performed on the ADS. The same continuity test is also applied to the GDCS squib valves described in Subsection 7.3.1.2.

7.3.1.1.3.7 Instrumentation Requirements

System status during normal plant operation and ADS performance monitoring (IEEE Std. 603, Section 5.8) in an accident is based on the following control room indications:

- Status indication of the ADS SRVs and DPVs;
- ADS 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 main control room:
  - Manual arming of ADS;
  - Manual actuation of ADS;
  - Two-out-of-four ADS Level 1 signals;
  - Automatic ADS initiation;
  - Aborted ADS initiation;
  - ADS 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 ADS SRV.

ADS instrumentation located in the drywell that is essential for system operation is designed to operate in an environment resulting from a loss-of-coolant accident. safety-related instruments located outside the containment are also 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

Safety-Related (10 CFR 50.2) Design Bases

The GDCS control and instrumentation is designed to meet the following requirements:

- 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 that causes the need.
- Be completely automatic in operation (that is, no operator action required). Manual initiation of GDCS is possible at any time providing protective interlocks have been satisfied (for example, the reactor is depressurized).
- Prevent the inadvertent actuation of the deluge valves thus preventing inadvertent draining of the GDCS pools.

Nonsafety-Related Design Bases

- 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 are displayed on a mimic of the system in the main control room.
- Alarm GDCS parameters in the main control room

7.3.1.2.2 System Description

The logic elements that provide 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. The logic elements that provide the controls for the actuation of the deluge valves are contained within a separate pair of dedicated nonsafety-related Programmable Logic Controllers (PLCs) and a pair of dedicated safety-related thermocouples and associated temperature switches. The only safety-related function of the deluge logic is the prevention of inadvertent actuation. The deluge logic is independent from all the other plant controls and is also located outside containment. The batteries and uninterruptible power supplies that provide power to operate the injection and equalizing logic and actuate the squib valves are located in separate rooms inside the reactor building. The power for the deluge logic, and squib valves, is backed by batteries, which are separate and independent from all other plant batteries.

The GDCS pools are located within the drywell at an elevation significantly above the top of the active core. The suppression pool is located within the drywell with a water level a few meters above the top of active fuel (TAF).

Redundant safety-related level transmitters, two for each pool, continuously monitor the GDCS pool water level. The GDCS pool levels are continuously available on the safety- related and nonsafety- related displays. Both high and low pool levels are alarmed by the plant computer functions (part of N-DCIS).

RPV Level transmitters used to initiate GDCS are part of the NBS and are located on racks outside the drywell. The thermocouples that initiate the GDCS deluge valves are located in the lower drywell protective layer.

Actuation of GDCS injection sub-system is performed automatically, without need for operator action. It is also possible for the plant operator to manually initiate GDCS injection sub-system or to individually fire the various squib initiators independently by injecting trip signals to the automatic logic; the manual initiation is interlocked with a low reactor pressure signal to ensure that the GDCS pools are capable of flooding the reactor.

As previously described in the ADS logic Section, the SSLC/ESF ECCS logic sends an initial start signal to the GDCS logic that will automatically initiate GDCS following reactor depressurization under LOCA conditions. After seal in, this signal represents Level 1, as shown in ECCS initiation signals of table 6.3-1.

Each of the two trains per division is presented with the initial start signal from the same SSLC/ESF ECCS logic that initiates ADS. The SSLC/ESF ECCS 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.

There are four GDCS injection lines coming from the three GDCS pools to the reactor vessel, one line per division. The squib valves on these lines are called GDCS injection valves and there are two valves on each line and four squib initiators per valve (three divisional initiators and one from the DPS [see Section 7.8]), totaling eight GDCS injection valves and thirty-two squib initiators. With three divisional initiators per valve, the system can suffer the complete loss of two divisions of power and still perform its intended function.

There are four equalizing lines coming from the suppression pool to the reactor vessel, one line per division. The squib valves on these lines are called equalizing valves and there is one valve on each line and four squib initiators per valve (three divisional initiators and one from the DPS [see Section 7.8]), totaling four equalizing valves and sixteen squib initiators. These equalizing valves are used after the GDCS flooded vessel's decay heat has boiled away sufficient vessel inventory to again begin lowering level. After the initial start signal has been given (opening the ADS and GDCS valves) and after a time delay (Table 7.3-4), and when RPV water level drops below RPV Level 0.5 (1 m 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 suffer the complete loss of two divisions of power and still perform its intended function. It is also possible for the operator to manually initiate the equalizing valves or to individually fire the various squib initiators independently by injecting trip signals to the automatic logic.

The GDCS pools also supply the deluge lines, which flood the containment floor after a severe accident. Actuation of the deluge valves is performed automatically with a backup capability for the operator to manually initiate the deluge valves. Automatic actuation of the deluge valves is accomplished via lower drywell high temperature (see Table 7.3-4). Automatic and manual actuation is described later in this Section.

The GDCS injection and equalizing valve logics include the same SSLC/ESF ECCS "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 is also

single-failure proof against inadvertent actuation such that each division of logic has two trains, each of which must operate for the associated valves to fire.

The same wide range level sensors that are used for the ADS logic and fuel zone range reactor level are also used for the equalizing valve logic; these are diverse from the sensors used for RPS functions and from those used by the diverse protection system. Both sets of transmitters belong to the NBS.

The generation of the initial start signal for GDCS has been described in the ADS logic Section. The logic for all squib initiators is similar. The signals are acquired per division by reactor building remote multiplexing units (RMUs) of the same division. The data is sent via fiber optics to the SSLC/ESF cabinets located in the corresponding divisional I&C equipment rooms in the control building. Each division's logic compares the measured parameters to setpoints and outputs a "sensor" trip signal that is sent to its own division and each of the other divisions by appropriately isolated fiber optics.

Each division has access to the 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 and 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 end result is that any two divisions sensing the appropriate trip conditions will result 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 be inadvertently fired by 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 starts an adjustable timer with a preset time delay as specified in Table 7.3-4. After the time delay, each of the two timers will output a trip signal to the GDCS squib load drivers/discrete outputs. There are eight injection squib valves, three divisional squib initiators and one DPS squib initiator per valve.

Within the RMU, per 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 to inadvertently actuate. Because each GDCS injection squib valve always has three squib initiators, powered by three different divisions, the design is also single-failure proof to operate all eight valves and will initiate even with the loss of two divisions of power.

The current monitor continuously verifies squib 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 control room to indicate the squib initiator (not the valve) is inoperable.

For diversity, the DPS also has the ability to fire its squib initiator on each of the eight GDCS injection squib valves using single-failure proof (both to operate and to avoid inadvertent operation) logic. This is accomplished using a completely separate squib initiator connected to the DPS system (See Figure 7.3-1B.). The DPS system uses diverse sensors, hardware and software to operate the GDCS injection valves.

For each GDCS equalization squib valves logic, the initial start signal will initiate a non-resettable equalization squib valve timer (Table 7.3-4). The outputs of the two equalization squib valve timers per division are combined with the two Level 0.5 signals per division such that any time Level 0.5 occurs after the end of equalization squib valve time delay, the logic will output a trip signal to the equalizing valve squib load drivers/diverse outputs. There are four equalizing valves with three divisional squib initiators and one DPS squib initiator per valve. Figure 7.3-2 shows the initiation logic of a typical equalizing squib valve.

Within the RMU, per 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 equalization valve timers and Level 0.5 outputs must transmit a trip signal to the corresponding series load driver/discrete outputs to fire the squib initiator. The effect is that both two-out-of-four trip Level 0.5 voters, both timers and both load drivers/discrete outputs must operate to fire the squib initiator, making the design single-failure proof to inadvertently actuate. Because each equalizing valve always has three divisional squib initiators powered by three different divisions, the design is also single-failure proof to operate all four valves, with any three of the four divisions of safety-related power available. Because the equalizing valves are needed only long term, they are not automatically operated by the DPS system. However, they are included in the manual initiating GDCS valve logic and may also be fired individually via safety-related VDU displays or nonsafety-related DPS VDU displays.

The overall design of the system assures that all eight injection valves and all four equalizing valves will be fired even with a complete failure of any two divisions, but no single-failure will fire any squib.

The safety-related VDUs in the main control room can provide a display format that will allow the operator to manually open each GDCS injection valve independently using the primary SSLC/ESF ECCS logic function (IEEE Std. 603, Sections 5.8, 6.2 and 7.2). Any nonsafety-related VDU in the main control room can provide a display format that will allow the operator to individually open each GDCS injection valve independently using the DPS logic function. Each display utilizes an “arm/fire” configuration that requires at least two deliberate operator actions and is interlocked with a low reactor pressure signal. Operator use of the “arm” portion of the display will cause a plant alarm. These two manual opening schemes are diverse from one another.

Similar to the GDCS injection valve manual actuations, the safety-related VDUs in the main control room can provide a display format that will allow the operator to manually open each GDCS equalizing valve independently using the primary SSLC/ESF ECCS logic function (IEEE Std. 603, Sections 5.8, 6.2 and 7.2). Any nonsafety-related VDU in the main control room can provide a display format that will allow the operator to individually open each GDCS equalizing valve independently using the DPS logic function. Each display utilizes an “arm/fire” configuration that requires at least two deliberate operator actions and is interlocked with a low

reactor pressure signal. Operator use of the "arm" portion of the display will cause a plant alarm. The two manual opening schemes from the primary SSLC/ESF ECCS and from DPS are diverse from one another.

Finally, each safety-related VDU can provide a display with an "arm/fire" switch (one per division for a total of four) to manually initiate the GDCS sequence as a system instead of each valve individually (IEEE Std. 603, Sections 5.8, 6.2 and 7.2). If the operator uses any two of the four switches (this manual actuation is also interlocked with a low reactor pressure signal), the GDCS sequence will seal in and start the GDCS valve sequencing (IEEE Std. 603, Section 5.2). This requires four deliberate operator actions. For all of the manual initiations, operator use of the "arm" portion of the display will cause a plant alarm.

There are 12 deluge valves with two squib initiators (one for automatic actuation and one for manual actuation) on each valve. Each of these valves feeds the 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 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. The deluge logic is completely separate and independent from the Q-DCIS and the N-DCIS. The deluge logic is powered by dedicated batteries supported by battery chargers operating on non-safety power. The deluge valves are also powered by a pair of dedicated batteries that are supported by battery chargers operating on nonsafety-related power. The batteries for the deluge valves are separate and independent from the batteries for the deluge logic. Each of these batteries can fire all twelve deluge valve squibs. All of the deluge batteries are separate and independent of the other plant batteries.

Automatic actuation of the deluge valves is accomplished via lower drywell high temperature. The containment floor is divided into 30 equal area cells, with two thermocouples 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 in any two adjacent cells coincident with the second set of thermocouples in the same two 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 will output a trip signal to the respective deluge valve squib load drivers/discrete outputs. The timers outputs, are wired in series so that each of the two timers must transmit a temperature trip signal to the corresponding series load driver/discrete outputs. Additionally, a pair of dedicated safety-related thermocouples monitors the drywell temperature below the reactor vessel. Each thermocouple outputs to a dedicated, safety-related temperature switch. When temperatures exceed the setpoint, each temperature switch also outputs a trip signal to each deluge valve squib load driver/discrete outputs. The temperature switch outputs are wired in series with the PLC timer outputs. The effect is that both PLC timer outputs, both temperature switch outputs and both load drivers/discrete outputs must operate to fire the squib initiator. The temperature switches serve as permissives for the deluge logic. These temperature switches and the associated thermocouples are safety-related only to prevent inadvertent actuation of the deluge system, which could inadvertently drain the GDCS pools.

Temperature indication and alarms, as well as continuity alarms and valve open/close indication 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 to manually open the twelve 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 GDCS deluge valves. These switches actuate the second squib initiator on each deluge valve. Operator use of the "arm" portion of the switch will cause a plant alarm.

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 ECCSs (ADS and GDCS) ensure that the reactor core is always covered.

Instrumentation that initiates 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 reactor coolant boundary. Such a breach inside or outside the containment is sensed by reactor 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 thermocouples that measure drywell temperature and the associated temperature switches, which are part of the GDCS 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 will cause 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 function.

No operator action is required to initiate the correct response of the GDCS. If the system fails to initiate, the control room operator can manually accomplish GDCS initiation through controls and displays in the control room. 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 are located in the main control room and are under supervision of the control room operator.

No single failure in the initiating trip channel, with any three of the four divisions of safety-related power available, can prevent the initiation of the GDCS injection and equalizing functions when required or inadvertently initiate the GDCS.

The initiation scheme for the GDCS injection and equalizing functions are 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 caused 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 equalizing squib valve logic and initiation circuitry is powered by divisionally separated, safety-related power (see Section 8.3). The mechanical aspects of the GDCS are discussed in Subsection 6.3.2.

7.3.1.2.3.1 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the instrumentation and control systems and the associated codes and standards applied in accordance with the SRP. This table includes the GDCS and covers the codes and standards addressed in its design. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

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

Conformance: GDCS complies with this requirement.

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 the Subsections 7.1.6, and 7.2.1.2.4. 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 so that 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 being able to provide automatic indication of bypassed and 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 the design description.

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 Tier 2 documents conforms to this BTP.

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

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

10 CFR 52.79(c) - ITAAC in Combined Operating License Applications

Conformance: ITAAC are provided for I&C systems and equipment.

7.3.1.2.3.2 General Design Criterias

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following GDCs are addressed for the GDCS:

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 to these criteria in that diverse instrumentation and controls are provided, as described in Section 7.8

7.3.1.2.3.4 Regulatory Guides

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following RGs are addressed for the GDCs:

RG 1.22 - Periodic Testing of Protection System Function - System logic is tested continually as described in Subsection 7.3.1.2.4. Components are tested periodically during refueling outages. The GDCS fully complies with RG 1.22.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems - The GDCS fully meets the requirements of RG 1.47. Automatic indication is provided in the control room to inform the operator that the system is inoperable or a division is bypassed.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems - 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 - The GDCS fully complies with RG 1.62.

Each division of the GDCS has a manual actuation switch in the main control room. Initiation of the two switches initiates the system. The switches ensure that the manual initiation of the

system is a deliberate act. There is an interlock between the manual initiation switches and a low reactor pressure signal that prevents manual initiation of the system if the reactor pressure vessel is not depressurized.

RG 1.75 - Physical Independence of Electric Systems - See Chapter 8 for general discussion of how the ESBWR meets RG 1.75.

Separation within the GDCS for the injection and equalizing sub-systems is such that controls, equipment, and wiring are segregated into four separate logic groups. Four power divisions provide redundant electrical power to the squib valve firing circuits. One power division and two logic divisions are required for each squib valve to open. Refer to Subsection 7.3.1.2.2 for the design description of the GDCS initiation logic. Separation is provided to maintain the independence of the four divisions of the circuits and equipment so that the protection functions required during and following a design basis event can be accomplished.

The redundant equipment and circuits within the GDCS require divisional separation. Pertinent documents and drawings identify separation and safety-related status for each redundant division in a distinctive manner.

Redundant circuits and equipment are located within their respective divisional safety-related Class enclosures. Separation is achieved by barriers, isolation devices or physical distance, which ensures that a single-failure in one division would not affect the operation of the other redundant divisions.

The separation of redundant safety-related circuits and equipment within GDCS is such that no physical connections are made between divisions except through nonmetallic fiber-optic medium.

Associated circuits are in accordance with safety-related circuit requirements up to and including the isolation devices. Circuits beyond the isolation devices do not again become associated with safety-related circuits.

Separation between safety-related and nonsafety-related circuits either satisfies the same minimum requirements as for the separation between safety-related circuits, or the circuits are treated as associated circuits.

RG 1.105 - Instrument Setpoints for safety-related Systems - The setpoints used to initiate GDCS are established consistent with this guide. A licensing topical report (Reference 7.2-1) provides the detailed description of this methodology.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems - The GDCS complies with the intent of RG 1.118 as amplified in IEEE Std. 338. A full functional test of the GDCS is not practical, because it would result in a loss-of-coolant event. Acceptable reliability of equipment operation is demonstrated by alternate test methods. System logic is self-tested every 30 minutes and a low-amperage current continuously tests the continuity of the bridge-wires within the squib valve actuating circuitry. Calibration verification of the GDCS and suppression pool level sensors can be conducted during plant operation because the level transmitters are located outside the drywell.

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems -The GDCS fully complies with RG 1.153.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems

Conformance: GDCS conforms to RG 1.180 as discussed in Subsection 7.1.6.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants

Conformance: GDCS conforms to RG 1.204 as discussed in Subsection 7.1.6.

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 7.1.2.2.

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 - The GDCS design has the low pressure portion of the system properly isolated from the high pressure portion of the system through two valves in series: a squib valve and a biased-open check valve that closes on very low differential pressure. This meets the intent of BTP for a necessary part of the Emergency Core Cooling System.

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 ESBWR, in that it has no reactor recirculation pump.

BTP HICB-6 - Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

The ESBWR has no recirculation pump and has 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 to the provision of Paragraph D.4 of RG 1.22. In the GDCS, the squib valves are not actuated during reactor operation, because actuation of the squib valves would adversely affect the operation of the plant and would result in a reactor shutdown.

Given the GDCS system requirements for zero reactor pressure boundary leakage over the 60-year life of the plant, the only practical solution is for the system actuation valve to be a non-reclosing valve 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 from safety-related to nonsafety-related devices.

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

GDCS logic resides within the SSLC/ESF ECCS. The SSLC/ESF ECCS conforms to this BTP. Additional discussion is in Subsection 7.2.2.4.

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

This BTP does not apply to GDCS or SSLC/ESF ECCS.

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

This BTP is applicable to all Sections of the DCD including this Section on GDCS. This Section content conforms to this BTP.

BTPs 14, 17, 18, 19 and 21 are addressed in conjunction with the SSLC/ESF ECCS in Subsection 7.3.5.3

7.3.1.2.3.6 TMI Action Plan Requirements

In accordance with the SRP for Section 7.3 and Table 7.1-1, only TMIs 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 BWRs and license applicants that potentially could apply to the GDCS. Following each TMI 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 applies to Emergency Core Cooling Systems with steam-driven pumps that use 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 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 GDCS.

TMI II.K.3(22) - Automatic Switchover of RCIC Suction - This TMI 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, may 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 Requirements

The performance and effectiveness of the GDCS in a postulated accident may be verified by observing the following control room indications (IEEE Std. 603, Section 5.8):

- 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 environmental capabilities of the GDCS instrumentation, located in the drywell that is essential for system operation, are designed to operate in a drywell environment resulting from a LOCA. The thermocouples that initiate the deluge valves are qualified to operate in the 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 (IC/PCC pool) outside the containment. A rise in containment (drywell) pressure above the pressure suppression pool (wetwell) pressure, as would occur 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, thus cooling the containment. 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.

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 reactor coolant pressure boundary and to initiate the appropriate safety action to isolate the source of the leak from the containment. The system is designed to automatically initiate the isolation of certain designated process lines that penetrate the containment to prevent release of radiological leakage from the reactor coolant pressure boundary. The initiation of the isolation functions results in the closure of 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 RPS/RTIF platform while all other containment isolation logic functions are performed in the SSLC/ESF system.

7.3.3.1 System Design Bases

The following system design criteria are applicable to the design of LD&IS (IEEE Std. 603, Sections 5.1, 5.6 and 6.1):

- The LD&IS is engineered as a safety system, Seismic Category 1, and conforms to the regulatory codes and 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 reactor coolant pressure boundary.
- The divisional LD&IS logic channels and associated sensors are powered from safety-related divisional power. The loss of one divisional logic power source or one monitoring channel does not cause inadvertent isolation of any containment valves.
- Once isolation is initiated, the isolation action goes to completion. Deliberate operator action is required to return the system to normal and to reopen the isolation valves.
- The LD&IS design meets the single-failure criteria; no single-failure within the system, with any three of the four divisions of safety-related power available, initiates inadvertent isolation or prevent isolation when required.
- Automatic isolation is initiated on a coincidence vote 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 nonsafety-related equipment (see Subsection 7.1.3.3).
- The LD&IS design incorporates provisions to permit bypass of a single division of sensors at any one time.

- LD&IS instrumentation utilizes a diversity of sensed parameters and redundant channels for initiation of containment isolation.
- Manual isolation capability is provided for diversity to the automatic logic.
- The containment leak detection methods that are described in RG 1.45 are adopted in the LD&IS system design.
- Identified and unidentified leakages within the containment are monitored separately for quantifying the flow rates.
- The LD&IS provides different divisional isolation signals to the containment isolation valves.
- The control and isolation logic for the main steamline isolation valves (MSIVs) are provided in the LD&IS system design. The MSIV control logic for each pilot solenoid valve is shown in Figure 7.2-1.

7.3.3.2 System Description

The LD&IS is a four-divisional system designed to detect and monitor leakage from the reactor coolant pressure boundary (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 utilizes two-out-of-four coincidence voting channels for each monitored plant variable for containment isolation. Various plant variables are monitored, such as flow, temperature, pressure, RPV water level, and radiation, and 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 RPS and the SSLC/ESF platforms, where the trip signals are generated to initiate 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 steamlines and drain lines;
- ICS process lines;
- RWCU/SDC System process and sampling lines;
- Fuel and Auxiliary Pools Cooling System suction lines from the GDCS pools;
- Chilled Water System lines to drywell coolers;
- Drywell sumps liquid drain lines;
- Containment purge and vent lines;
- Reactor Building area air supply and exhaust ducts;

- Feedwater process lines

The following leak detection and monitoring functions are implemented in the plant design:

- Condensate flow from the upper and lower drywell air coolers;
- Leakages in the drywell from valves equipped with leak off lines between the two valve stem packings;
- Fission products leakages into the drywell (by PRMS);
- RPV head flange seal pressure leakage;
- Drywell sump levels and flow rates for identified and unidentified leakages.

The LD&IS control functions that initiate automatic isolation functions are classified safety-related, and these functions utilize redundant divisional channels that satisfy both the mechanical and electrical separation criteria and the single-failure criteria (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. Detailed description of detection methods, monitored plant parameters, and the monitoring instrumentation are covered 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 engineered into a safety 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 that are described in Subsection 7.3.3.1 and with the relevant codes and standards that are specified for this system in Table 7.1-1. LD&IS system design utilizes various measurements and redundant instrument channels to detect and monitor reactor coolant leakage in and external to the containment, and detect and isolate the source of the leak to prevent radioactive releases to the environs. The isolation logic utilizes 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 its safety 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 are 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 leakage detection methods associated with LD&IS logic functions generally comply with RG 1.45 with the Process Radiation Monitoring System performing the radiation monitoring of fission products. The RG 1.45 prescribes general guidelines to assure that leakage detection and collection system provides practical identification of leaks from the RCPB. 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 cause the closure of isolation valves. Reset of the isolation logic is required before any isolation valve can be manually 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 function. While in the BYPASS mode, no other division of sensors can be bypassed simultaneously.

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 drywell low conductivity waste (LCW) and high conductivity waste (HCW) sumps instrumentation is designed to satisfy the leakage rate requirements for identified and unidentified sources. The LD&IS includes isolation logic that uses the discharge radiation of the LCW & HCW for the isolation of the drain lines that transfer waste sumps to the liquid radwaste system.

7.3.3.3.1 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the Leak Detection and Isolation System function and the associated codes and standards are applied in accordance with Table 7.1-1. The following analysis lists the applicable criteria and discusses the degree of conformance for each. Exceptions or clarifications are noted.

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

Conformance: LD&IS system complies with this requirement.

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 and 7.2.1.2.4. Separation and isolation is preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6, and RG 1.75. The Leak Detection and Isolation System consists of four divisions, which are redundantly designed so that 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: LD&IS demonstrates compliance by being able to provide automatic indication of bypassed and operable status. (IEEE Std. 603, Subsection 5.8, 6.2 and 7.2).

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: 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.

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 Tier 2 documents conform to this BTP.

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

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

10 CFR 52.79(c) - ITAAC in Combined Operating License Applications

Conformance: ITAAC are provided for I&C systems and equipment.

7.3.3.3.2 General Design Criterias

In accordance with Table 7.1-1, the following GDCs are addressed for the Leak Detection and Isolation System:

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

Conformance: The LD&IS complies with the GDCs identified. GDC conformance is discussed in Section 3.1.

7.3.3.3.3 Staff Requirements Memoranda

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

Conformance: The ESBWR LD&IS and Engineered Safety Features (ESF) designs conform to the item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of diverse instrumentation and control, described in Section 7.8.

7.3.3.3.4 Regulatory Guide

In accordance with Table 7.1-1, the following RGs are addressed for the LD&IS:

- RG 1.22 - Safety Guide 22 Periodic Testing of Protection System Actuation Function;
- RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System;

- RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems;
- RG 1.62 - Manual Initiation of Protective Actions;
- RG 1.75 - Physical Independence of Electric Systems;
- RG 1.105 - Setpoints for safety-related Instrumentation;
- RG 1.118 - Periodic Testing of Electric Power and Protection Systems; and
- RG 1.153 - Power Instrumentation & Control Portions of Safety Systems.

The LD&IS conforms to all of the above listed RGs, with the assumption that the same interpretations and clarifications identified in Subsection 7.2.1.11 also apply to Leak Detection and Isolation System.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the SSLC/ESF in Subsection 7.3.5.3 and 7.1.6.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems

Conformance: LD&IS conforms to RG 1.180 as discussed in Subsection 7.1.6.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants

Conformance: LD&IS conforms to RG 1.204 as discussed in Subsection 7.1.6.

7.3.3.3.5 Branch Technical Positions

In accordance with the SRP for Section 7.3 and with Table 7.1-1, the following BTPs are addressed for the EMC LD&IS:

- BTP HICB-8 - Guidance for Application of RG 1.22
- 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 PLC in Digital Computer-Based Instrumentation and Control Systems
- BTP HICB-19 - Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems
- BTP HICB-21 - Guidance on Digital Computer Real-Time Performance

  Conformance: The LD&IS complies with the above HICBs. Discussion of HICBs 14, 17, 18, 19, and 21 are addressed in conjunction with the SSLC/ESF in Subsection 7.3.5.3, and in Subsection 7.1.6.

7.3.3.3.6 TMI 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. However, TMI action plan requirements are addressed in Appendix 1A.

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 as required instrument channel checks, functional tests, verification of proper sensor and channel calibration, and response time tests in accordance with the established test procedures.

The LD&IS instrument channels utilize conventional sensors for leak detection and monitoring, and require no special or unique testing methods.

The setpoint verifications, the trip logic tests, and the channel integrity tests for the safety-related functions of LD&IS are processed and tested by the RPS and SSLC/ESF systems.

7.3.3.4.2 MSIV 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 periodically tested 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 in accordance with established procedures on the equipment during the time when the channel is out of service or has been deliberately bypassed.

7.3.3.5 Instrumentation Requirements

The LD&IS is an instrumentation system designed to detect and monitor leakage from the reactor coolant pressure boundary, 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 the required trips for the isolation functions.

The LD&IS instrumentation requirements for each specific monitoring and isolation function is described in detail in Subsection 5.2.5. The plant parameters that are 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 Engineered Safety Feature (ESF) system that functions to provide a safe environment within the control room to allow 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 control building shielding and area radiation monitoring; Control Room Habitability Area HVAC System (CRHAVS); provision for emergency food, and water storage; emergency kitchen and sanitary facilities; provision for protection from, and removal of airborne radioactive contaminants; and 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 associated controls are safety-related. Section 6.4 and Subsection 9.4.1 and 9.5.1 provide detailed information on the CRHS.

7.3.4.1 Design Bases

The design bases of the CRHS are detailed in Subsections 6.4.1 and 9.4.1.1.

7.3.4.2 The CRHS Safety-Related Instrumentation and Control

The CRHS safety-related instrumentation is designed to isolate the control room envelope on the following signals and re-align to the emergency filtration mode:

- Detection of high inlet air supply radiation (filtration); and
- Detection of inlet air supply smoke or smoke in the CRHA general area (isolation mode).

The Process Radiation Monitoring System (PRMS) is used to detect high inlet ventilation radiation. The PRMS consists of four redundant channels to monitor the air intake to the control building. The monitoring systems warn of the presence of significant air contamination in inlet air. Each redundant radiation channel consists of a gamma sensitive detector and a radiation monitor that is 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 (or voting logic) on detection of high inlet ventilation radiation. During radiological events, the SSLC/ESF voting logic in each division processes the 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. There are total of 2 pairs of redundant isolation dampers: normal air intake, and restroom exhaust dampers. The two dampers in each redundant pair are in series. Thus, any one of the two dampers will close the airflow path. Each damper will be controlled by two solenoids that are in series electrically, any one of which can be de-energized to close the damper.

The functions of the SSLC/ESF are depicted in Figure 7.3-5 and Subsection 7.3.5 provides detailed information on the SSLC/ESF. The four redundant divisions provide a fault-tolerant architecture that allows single division of sensor bypass for on-line testing, maintenance, and repair without losing reliable trip capability. In such 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 will still be able to generate an actuation signal to close isolation damper(s). At least one of the redundant dampers will be always able to actuate to respond to the sensors detection of high inlet air radiation under all of the postulated design basis failures. This fault-tolerant and single-failure proof arrangement thus conforms to safety system requirements for single-failure proof, fault tolerance, independence, and separation, as required by IEEE Std. 603, Section 5.1, 5.5, and 5.6.

The backup or secondary EFU starts automatically on a low-flow signal or failure of the primary EFU. When both EFUs fail or radiation is detected downstream of the EFUs, the EFUs fans stop and the discharge dampers close to provide CRHA isolation. The CRHA isolation may also 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 the CRHA general areas. The detection subsystems consist of four redundant channels to monitor the air intake to the control building. Each smoke detection channel consists of redundant smoke detectors that are 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) will continue to operate normally to provide the temperature control in the control room. Smoke removal is described in Subsections 9.4.1.2 and 9.5.1.11.

The redundant design of the safety components including the instrumentation and controls (including monitoring channels) in the CRHA, CRHA isolation dampers and EFUs, meets 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 inadvertent actuation of any dampers due to a failed damper. 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, which conforms to the fail-safe principle, in which components or systems are designed to return automatically into their safest condition if they fail or if power is lost.

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 provided in Subsection 9.4.1.5. Alarms for following CRHA/CRHAVS conditions are provided in the Subsection 6.4.8.

7.3.4.3 Safety Evaluation

Safety evaluation of the CRHS is provided in Subsections 6.4.5, and 9.4.1.3. The regulatory requirements and conformance are further addressed in this Subsection:

7.3.4.3.1 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the CRHS and the associated codes and standards applied in accordance with the SRP. The following analysis lists the applicable criteria and discusses the degree of conformance for each. Exceptions or clarifications are noted.

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

Conformance: CRHS complies with this requirement.

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 divisions, which are redundantly designed so that 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: CRHS demonstrates compliance by being able to provide automatic indication of bypassed and operable status.

10 CFR 50.34(f)(2)(xiv)(II.E.4.2) - TMI Action Plan Item IIE.4.2 Containment Isolation Systems

Conformance: 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.

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 requirement provided for the CRHS in the Tier 2 documents conform to this BTP.

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

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

10 CFR 52.79(c) - ITAAC in Combined Operating License Applications

Conformance: ITAACs are provided for I&C systems and equipment.

7.3.4.3.2 General Design Criteria

In accordance with Table 7.1-1, the following GDCs are addressed for the CRHS:

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

Conformance: The CRHS system complies with the GDCs identified. The GDC conformance is discussed in Subsection 3.1.

7.3.4.3.3 Staff Requirements Memoranda

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

Conformance: The ESBWR CRHS system and ESF designs conform to these criteria, as described in Section 7.8.

7.3.4.3.4 Regulatory Guide:

In accordance with Table 7.1-1, the following RGs are addressed for the CRHS:

- RG 1.22 - RG Periodic Testing of Protection System Actuation Function
- RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System
- RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems
- RG 1.62 - Manual Initiation of Protective Actions
- RG 1.75 - Physical Independence of Electric Systems
- RG 1.105 - Setpoints for safety-related Instrumentation
- RG 1.118 - Periodic Testing of Electric Power and Protection Systems
- RG 1.153 - Power Instrumentation & Control Portions of Safety Systems

The CRHS system conforms to all of the above listed RGs, with the assumption that the same interpretations and clarifications identified in Subsections 7.1.6 also applies to the CRHS system.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the SSLC/ESF in Subsections 7.1.6.

RG 1.180 - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems

Conformance: CRHS conforms to RG 1.180 as discussed in Subsection 7.1.6.

RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants

Conformance: CRHS conforms to RG 1.204 as discussed in Subsection 7.1.6.

7.3.4.3.5 Branch Technical Positions

In accordance with the SRP for Section 7.3, and with Table 7.1-1, the following BTPs are addressed for CRHS:

- BTP HICB-8 - Guidance for Application of RG 1.22
- 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-19 - Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems
- BTP HICB-21 - Guidance on Digital Computer Real-Time Performance

  Conformance: The CRHS complies with the above BTPs. The CRHS is part of the SSLC/ESF. These BTPs are addressed in conjunction with the SSLC/ESF in Subsection 7.3.5.3.5, and in Subsection 7.1.6.

7.3.4.3.6 TMI 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 requirements as indicated above. However, TMI action plan requirements are addressed in Appendix 1A.

7.3.4.3.7 Testing and Inspection Requirements

Testing and Inspections requirements are identified in Subsections 6.4.7 and 9.4.1.4.

7.3.4.3.8 Instrumentation Requirements

The required instrumentation for CRHS is provided in Subsection 9.4.1.5 and alarms for following CRHA/CRHAVS conditions are provided in the Subsection 6.4.8.

7.3.5 Engineered Safety Features Safety System Logic and Control

7.3.5.1 System Design Bases

The Engineered Safety Features Safety System Logic and Control (SSLC/ESF) system performs the control logic processing of the plant sensor data and manual control switch signals that activate the functions of the LD&IS, ECCS and CRHS. 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:

- Monitor safety-related signals that provide automatic control of the plant safety protection systems;
- Perform 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;
- Meet 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 initiate necessary system operation;
- Monitor safety-related manual control switches used for system or component test, protection system manual initiation, and individual control of equipment actuators;
- Furnish trip outputs signals to actuators that drive safety system equipment, for example, solenoids and squib explosive-actuated valves;
- Furnish trip or initiation outputs signals to the logic of interfacing functions
- Monitor conditions for ATWS and generate control outputs to systems that provide ATWS prevention and mitigation functions;
- Provide diagnostic facilities for detecting imminent failure of system components and provide an operator interface that facilitates quick repair;
- Provide alarm and status outputs to operator displays, annunciators and the plant computer; and
- Satisfy regulatory requirements for implementation of:

- Single-failure criterion;
- Defense-in-depth protection;
- Testability;
- Separation and independence; and
- Bypass of certain functions and indication of bypass.

7.3.5.2 System Description

SSLC/ESF is the decision-making control logic segment for the ESBWRs engineered safety features (ESF) systems. SSLC/ESF processes automatic and manual demands for ESF system actuations based upon sensed plant process parameters or operator request. The SSLC/ESF includes the controls and instruments that implement the non-MSIV isolation functions of the LD&IS, the ADS functions of the NBS for ADS SRV control and depressurization valve (DPV) control, the ECCS functions of the GDCS and SLC system, and the ECCS and shutdown functions of the ICS.

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 equipment room of the control building. SSLC/ESF runs without interruption in all modes of plant operation to support the 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 ADS SRV and DPV initiation, the GDCS initiation, the SLC initiation, and the core cooling and shutdown cooling logic function of the ICS. There are separate multiplexing networks for RTIF and SSLC/ESF functions within each division. Figure 7.3-4 shows the 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 Section 7.8.

Most SSLC/ESF input data are process variables multiplexed via the safety-related DCIS system (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 feeds 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 is in close proximity to the SSLC/ESF cabinets are directly connected to the divisional cabinets in the safety equipment room in the control building. These signals are derived from 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 is then transmitted through the DCIS network to the SSLC/ESF digital trip module (DTM) function for setpoint comparison. A trip signal is generated from this function. Processed trip signals from its own division and trip signals from the other three divisions are transmitted through communication interface and are processed in the VLU function for two-out-of-four voting. The final trip signal 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 is 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 if any one VLU function has failed, and the failure is alarmed in the MCR. In order to prevent single instrumentation and control 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 and 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.

In summary, at the division level, the four redundant divisions provide a fault-tolerant architecture that allows single division of sensor bypass for on-line maintenance, testing, and repair without losing reliable trip capability. In such bypass condition, the system automatically defaults to two-out-of-three coincident voting when a division of sensor inputs is bypassed. The fault-tolerant arrangement thus conforms to safety system requirements for single-failure tolerance, independence, and separation, as required by IEEE Std. 603, Sections 5.1 and 5.6.

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-critical automatic operations are provided with manual switches in each division for equipment initiation. Key safety RPS and ESF trip logics are duplicated in the DPS, which addresses the common-mode failure concern and protection of digital computer systems performing safety function. The DPS system is described in Section 7.8.

Testing and maintenance activities are supported through the use of manual control switches that can activate the trip logic signal of each safety system. In addition, on-line self-diagnostic tests that check the critical performance of the digital control instrument are performed continuously within SSLC/ESF. An illustration of SSLC/ESF and its relationship to 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 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, which

direct appropriate currents to various devices, such as scram pilot valve solenoids, air-operated valves, and explosive-actuated squib valves. The logic is designed such that once initiated automatically or manually, the intended sequence of protective actions will continue until completion. This satisfies 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.

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 so that only one division of sensors at a time can be placed in bypass, by use of a joystick-type switch. When such a bypass is made, all four divisions of two-out-of-four logic become two-out-of-three logic while bypass is maintained. Bypass permits calibration and repair of sensors or the DTM function. Even though all sensors for all systems are bypassed in one division, the remaining three divisions furnish sufficient redundant sensor data for safe operation and the logic is such that all four divisions can still 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 attempts to bypass simultaneously 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 the 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 there is the division of sensor bypass implemented, and there are multiple trains of two-out-of-four VLU logic, no additional division trip logic bypass is implemented in the SSLC/ESF logic. 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 provides effective bypass function required at the actuator level. (See 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 Engineered Safety Features systems and is therefore 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 that no single equipment failure causes inability to:

- Perform reactor trip;
- Establish containment isolation; or
- Initiate the engineered safety features.

Separation - Physically separate divisions are established by their relationship to the reactor vessel, which is divided into four quadrants. The sensors, logic, and output actuators of the various systems are allocated to these divisions.

Diversity - 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 safety relief valves, squib-actuated depressurization valves, GDCS injection and equalizing valves, ICS valves and SLC squib valves.

For ESBWR, a diverse instrumentation and control system is incorporated which has a totally independent set of selected reactor trip logic functions and ESF initiation logic functions that address the requirements of BTP HICB-19 position. This system is described in Subsection 7.8.

The RPS logic is implemented using a diverse vendor microprocessor-based platform.

Environment - The SSLC/ESF system is designed to operate in a mild environment in clean areas within the control building and reactor building safety envelope. Refer to Chapter 9.4.6 for specific environmental conditions.

Panel internal environment 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, per module).

7.3.5.3.1 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the SSLC/ESF and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

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 603 as discussed in Subsections 7.1.6 and 7.2.1.2.4.

10 CFR 50.34 (f)(2)(v)(I.D.3) - Bypass and Inoperable Status Indication

Conformance: The SSLC/ESF demonstrates compliance by being able to provide automatic indication of bypassed and operable status (IEEE Std. 603, Sections 5.8, 6.2 and 7.2).

10 CFR 50.34 (f)(2)(xiv)

Conformance: The SSLC/ESF logic that controls containment isolation functions conform to this 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..

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 Tier 2 documents conforms to this requirement.

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

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

10 CFR 52.79(c) - ITAAC in Combined Operating License Applications

Conformance: ITAAC are provided for the I&C systems and equipment.

7.3.5.3.2 General Design Criterias

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following GDCs are addressed for the SSLC/ESF:

Criteria: GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24

Conformance: The SSLC/ESF complies with these GDCs.

7.3.5.3.3 Staff Requirements Memoranda

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

Conformance: The ESBWR Reactor Trip (Protection) System and Engineered Safety Features (ESF) designs conform to Item II.Q of SECY-93-087 (BTP HICB-19) in conjunction with the implementation of the Diverse Protection System, described in Section 7.8.

7.3.5.3.4 Regulatory Guides

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following RGs are addressed for the SSLC/ESF:

- RG 1.22 - Safety Guide 22 Periodic Testing of Protection System Actuation FunctionsThe SSLC/ESF fully supports compliance with the guidance of RG 1.22.
- RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems – SSLC/ESF provides bypass capability and status indication that includes Q-DCIS.
- RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems - The SSLC/ESF 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 - The SSLC/ESF meets the requirements of RG 1.62. These signals for manual initiation of protective actions are hardwired to the SSLC/ESF equipment.
- RG 1.75 - Physical Independence of Electric Systems - The SSLC/ESF fully complies with the guidance of RG 1.75 and the requirements of IEEE Std. 384.
- RG 1.105 - Instrument Setpoints for safety-related Systems - The SSLC/ESF fully complies with RG 1.105, as delineated in Subsection 7.1.6.4.
- RG 1.118 - Periodic Testing of Electric Power and Protection Systems - The SSLC/ESF conforms to RG 1.118 as amplified in IEEE Std. 338. Testing of the SSLC/ESF is done in conjunction with the Q-DCIS.
- RG 1.152 - Criteria for Programmable Digital Computer System Software in safety-related Systems of Nuclear Power Plants - The SSLC/ESF meets the requirements of RG 1.152 and IEEE Std. 7-4.3.2. Additional discussion is in Subsection 7.2.1.3 for RPS system compliance.
- RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems - The SSLC/ESF in conjunction with the Q-DCIS fully conforms to RG 1.153.
- RG 1.168 - Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants - The SSLC/ESF fully complies with this 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 - The SSLC/ESF fully 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 - The SSLC/ESF fully 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 - The SSLC/ESF fully complies with RG 1.171, as delineated in Subsection 7.1.4.

- RG 1.172 - Software Requirements Specifications For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants - The SSLC/ESF fully 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 - The SSLC/ESF fully complies with RG 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 as discussed in Subsection 7.1.6.

- RG 1.204 - Guidelines for Lightning Protection of Nuclear Power Plants

  Conformance: SSLC/ESF conforms to RG 1.204 as discussed in Subsection 7.1.6.

7.3.5.3.5 Branch Technical Positions

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following BTPs are addressed for the SSLC/ESF:

- 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 ESBWR, in that it has no reactor recirculation pump.

- BTP HICB-6 - Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

  The ESBWR has no recirculation pump and has no active ECCS pumps. Therefore, this BTP is not applicable.

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

  The SSLC/ESF is fully operational during reactor operation and is tested in conjunction with the Q-DCIS. Therefore, the SSLC/ESF fully meets this BTP.

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

  SSLC/ESF logic controllers use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections from safety-related to nonsafety-related devices. The Q-DCIS provides the communication functions for SSLC/ESF. See Section 7.1.2, 7.1.3.2 and 7.1.3.3 for a description of the Q-DCIS communication system design.

Certain 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 per the guidelines of RG 1.75 and RG 1.153.

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

  The SSLC/ESF conforms to this BTP. Additional discussion is in Subsection 7.2.2.4.3.

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

  This BTP does not apply to SSLC/ESF.

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

  Safety Systems Development of software for the safety system functions within SSLC/ESF conforms to the guidance of this BTP as discussed in Appendix 7B. safety-related software to be embedded in the memory of the SSLC/ESF controllers is developed according to a structured plan outlined in Appendix 7B.

- 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 of the DCD including this Section on SSLC/ESF. This Section content conforms to this BTP.

- BTP-HICB-17 - Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based Instrumentation and Control Systems

  The RPS and SSLC/ESF controllers conform to this BTP. Discussions on self-test and surveillance tests of RPS and ESF are provided in Subsections 7.2.1.13 and 7.3.5.4.

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

  Portions of SSLC/ESF design that use commercial grade PLCs for safety-related functions conform to this BTP (and to BTPs 14, 17, and 21) in that the PLCs will be qualified to a level commensurate with safety system requirements.

- BTP-HICB-19 - Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems

  SSLC/ESF has a 4-division, independent and separated equipment arrangement. Isolation of signal transmission between safety-related divisions and between safety-related and nonsafety-related equipment employs 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. Additional diverse features are included as discussed

in Section 7.8, which describes the diverse instrumentation and control system, specifically addresses the requirements of this BTP.

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

  The real-time performance of SSLC/ESF in meeting the requirements for safety system trip and initiation response conforms to this BTP. Each SSLC/ESF controller operates independently and asynchronously with respect to other controllers. Maximum time delay from input to output is deterministic, based on the control logic design. Timing signals are not exchanged 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-test is to improve system availability by checking and confirming transmission path continuity for safety-critical signals, to verify operation of each two-out-of-four coincidence trip logic function, and to detect, alarm, and record the location of hardware or software faults. Tests verify the basic integrity of each card and the microprocessors. Discrete logic cards contain diagnostic circuitry that monitors critical points within the logic configuration and determines 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 an automatic test sequence 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 main control room 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 in accordance with the established test procedures and as required by Technical Specifications.

All test features adhere to the single-failure criterion, as follows:

- No single-failure in the test circuitry incapacitates an SSLC/ESF safety function.
- 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 Control Requirements

The SSLC/ESF equipment uses microprocessor-based programmable logic and control instrument, with standardized modules interchangeable with similar modules. Discrete solid-state logic is also 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 verification and validation program conforming to applicable codes and standards.

Logic and controls for SSLC/ESF are located on each divisional SSLC/ESF cabinet in the equipment room in the Control Building, with key controls and system operating status available on the operator interface Section in the main control room. The SSLC/ESF controls are used infrequently. Such controls normally 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 to manually bypass a division of sensors or, for RPS/MSIV, 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 Main Control Room (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

None.

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 logics (trains) within a division used to actuate the separate solenoid-operated gas pilots on each ADS SRV	2
Number of logics (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 ADS SRV pilot and open the ADS SRV	2
Minimum number of ADS logic divisions to actuate (energize) one of the igniter circuits and open the DPV	2
ADS trip logic units self-test time interval	continuous

Table 7.3-2

Safety Relief Valve Initiation Parameters

Parameter	Value*
Number of ADS SRV groups	2
Number of ADS SRVs in the first group (Group 1-initial ADS start signal)	5
Number of ADS SRVs in the second group (Group 2 – second ADS start signal)	5
Time delay to confirm ECCS-LOCA signal, sec	10
Time after ECCS-LOCA confirmed initiating signal before signaling Group 1 ADS SRVs to open, sec	0
Time after ECCS-LOCA confirmed initiating signal before signaling Group 2 ADS SRVs to open, sec	10

*The time delay values represent design or analytical limits. The actual setpoints will be determined using an NRC approved setpoint methodology.

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, sec	50
Additional ADS time delay, after Group 1 initiation, before Group 2 DPVs are signaled to open, sec	50
Additional ADS time delay, after Group 2 initiation, before Group 3 DPVs are signaled to open, sec	50
Additional ADS time delay, after Group 3 initiation, before Group 4 DPVs are signaled to open, sec	50

*The time delay values represent design or analytical limits. The actual setpoints will be determined using an NRC approved setpoint methodology.

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 s
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. The actual setpoints will be determined using an NRC approved setpoint methodology.

Table 7.3-5

LD&IS Interfacing Sensor Parameters

Temperatures:

- MSL Tunnel Area Temperature
- Drywell Temperature
- RWCU/SDC Rooms Temperature
- MSL Temperature in Turbine Building (or alternate method)

Pressures:

- MSL Turbine Inlet Pressure
- Main Condenser Pressure
- Reactor Vessel Head Flange Seal Pressure Leakage
- Drywell Pressure
- Feedwater Line Differential Pressure

Radiation Levels:

- RCCWS Intersystem Leakage
- Drywell Fission Product
- Reactor Building HVAC Air Exhaust
- Refueling Handling Area Air Exhaust
- Drywell Sump Low Conductivity Waste (LCW) Drain Line to Radwaste
- Drywell Sump High Conductivity Waste (HCW) Drain Line to Radwaste
- Isolation Condensers Pool Vent Exhaust

Flows:

- MSL Flow
- RWCU/SDC Differential Volume Flow (Temperature Compensated)
- Drywell Air Cooler Condensate Discharge low
- Isolation Condenser Steam Line Flow
- Isolation Condenser Condensate Return Line Flow

Levels:

- Various RPV Water Levels
- Drywell and Containment Sump Levels

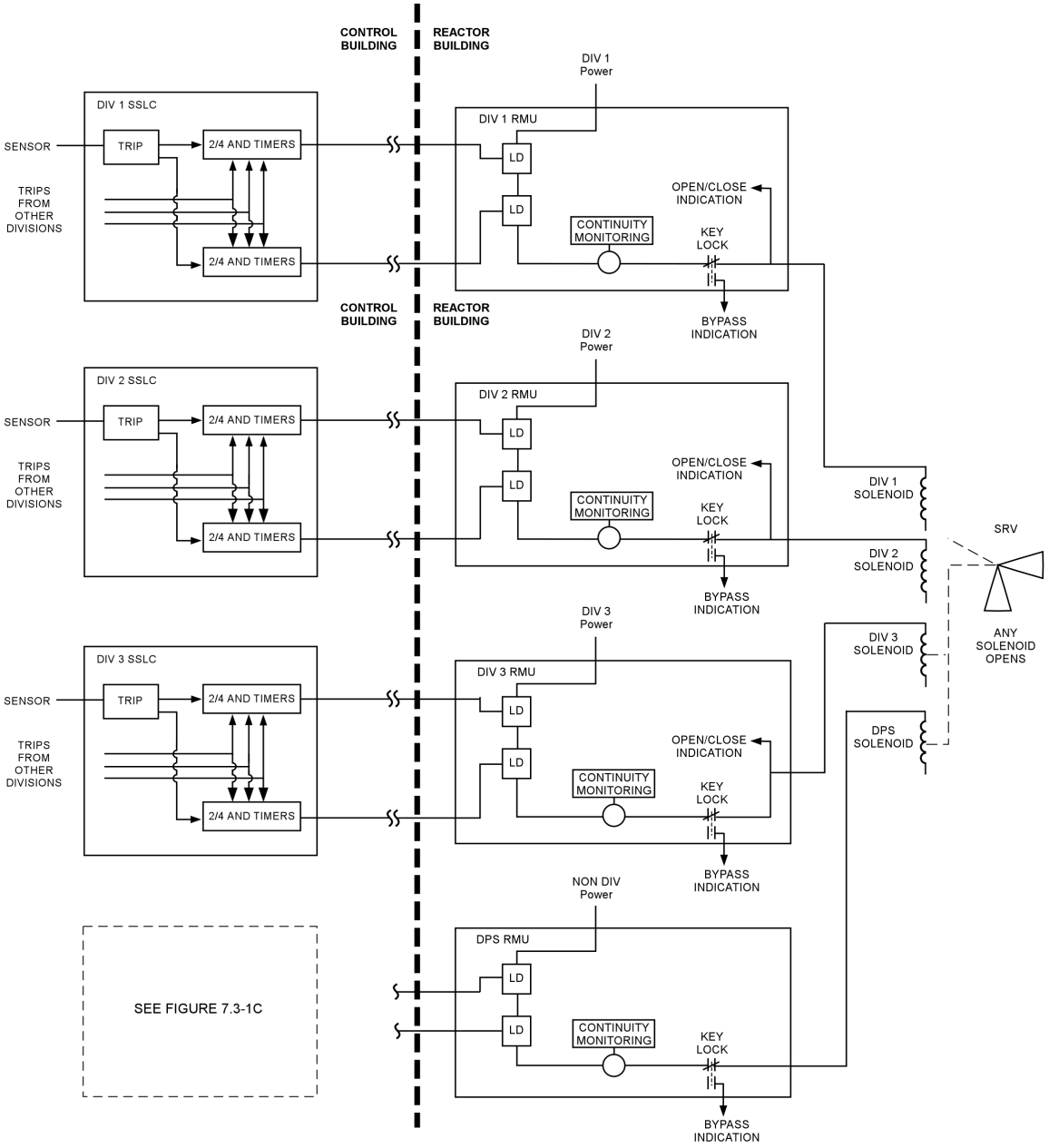
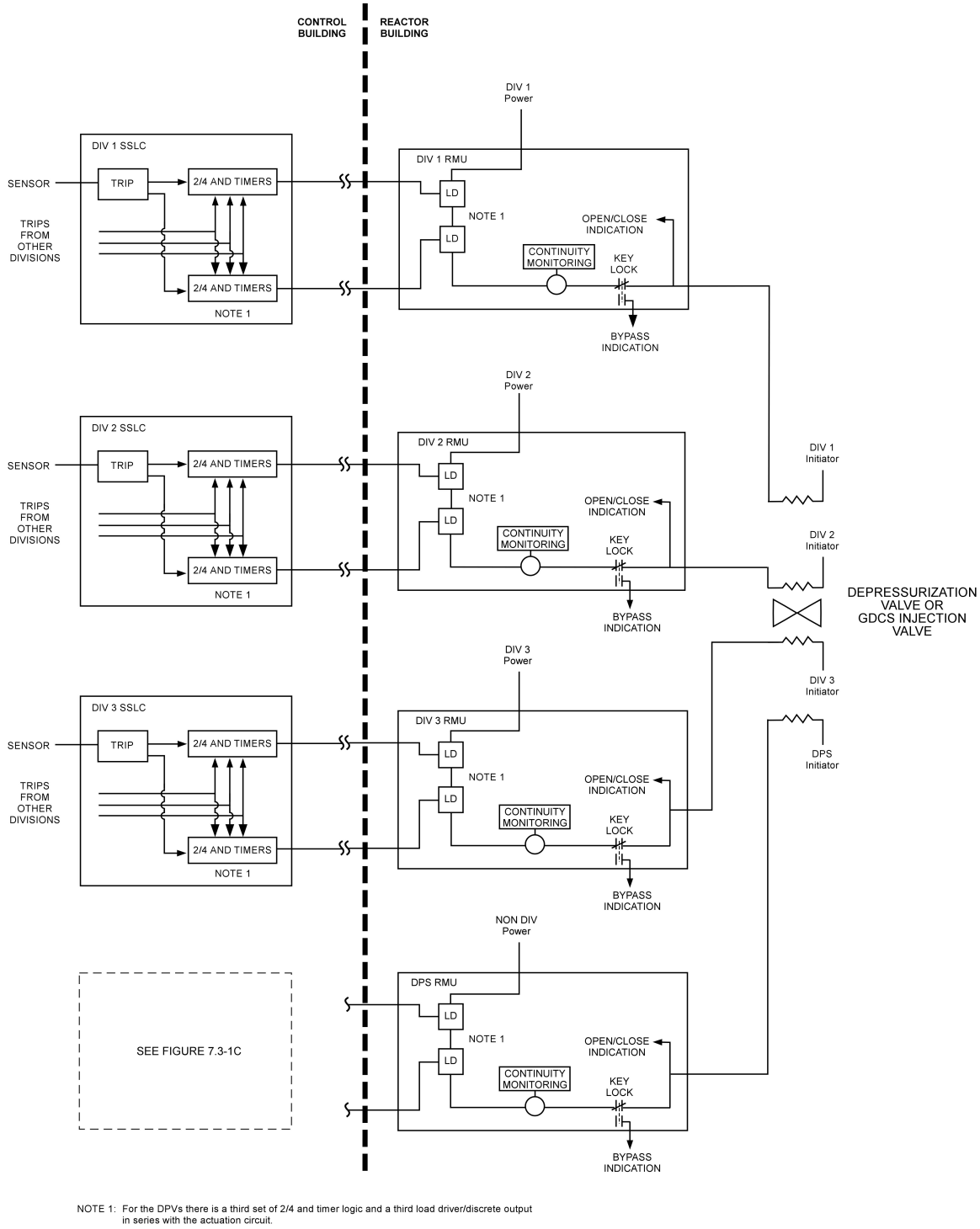


Figure 7.3-1A. ADS SRV Initiation Logics



NOTE 1: For the DPVs there is a third set of 2/4 and timer logic and a third load driver/discrete output in series with the actuation circuit.

Figure 7.3-1B. GDCS and DPV Initiation Logics

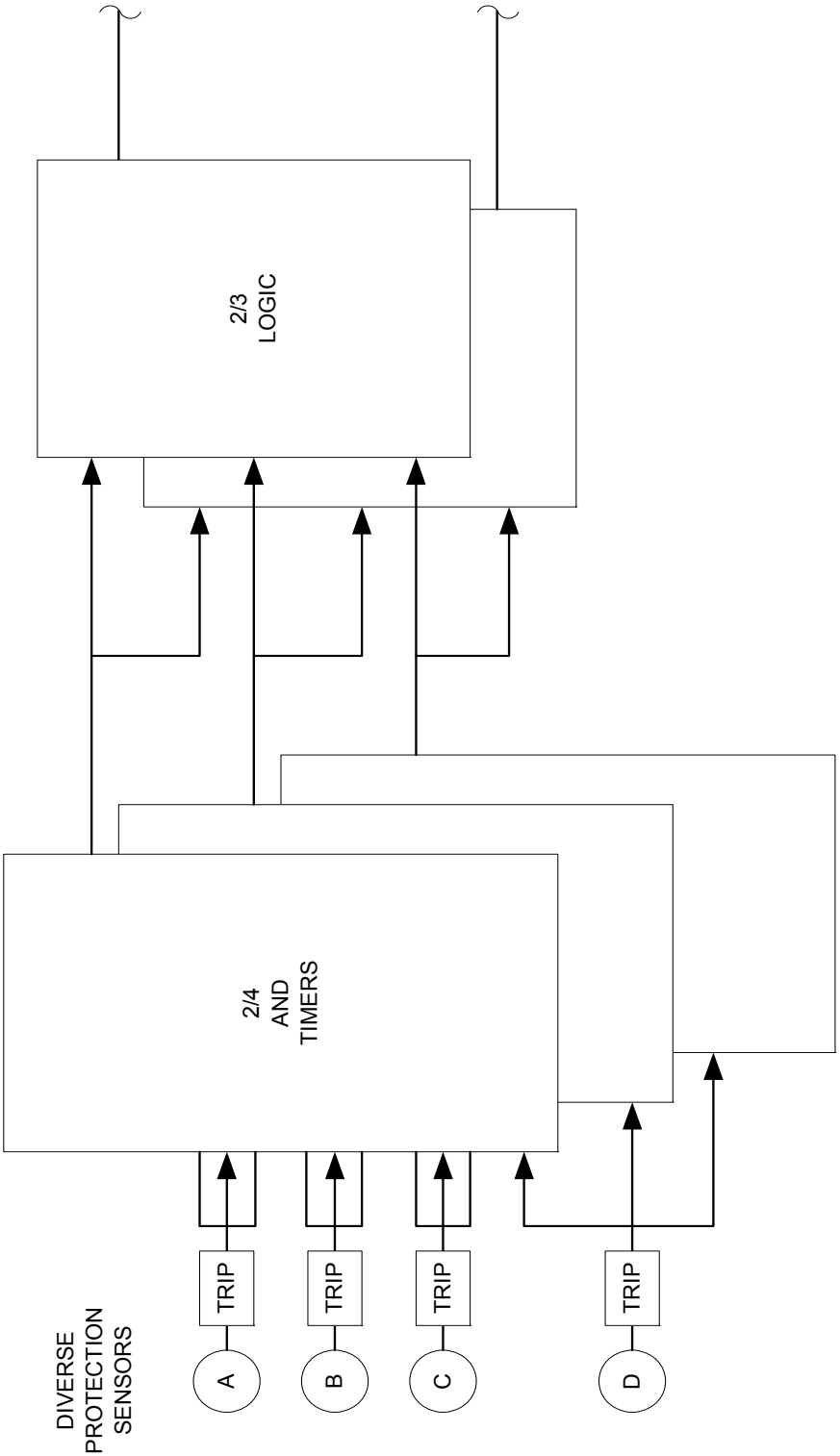


Figure 7.3-1C. DPS Initiation Logic

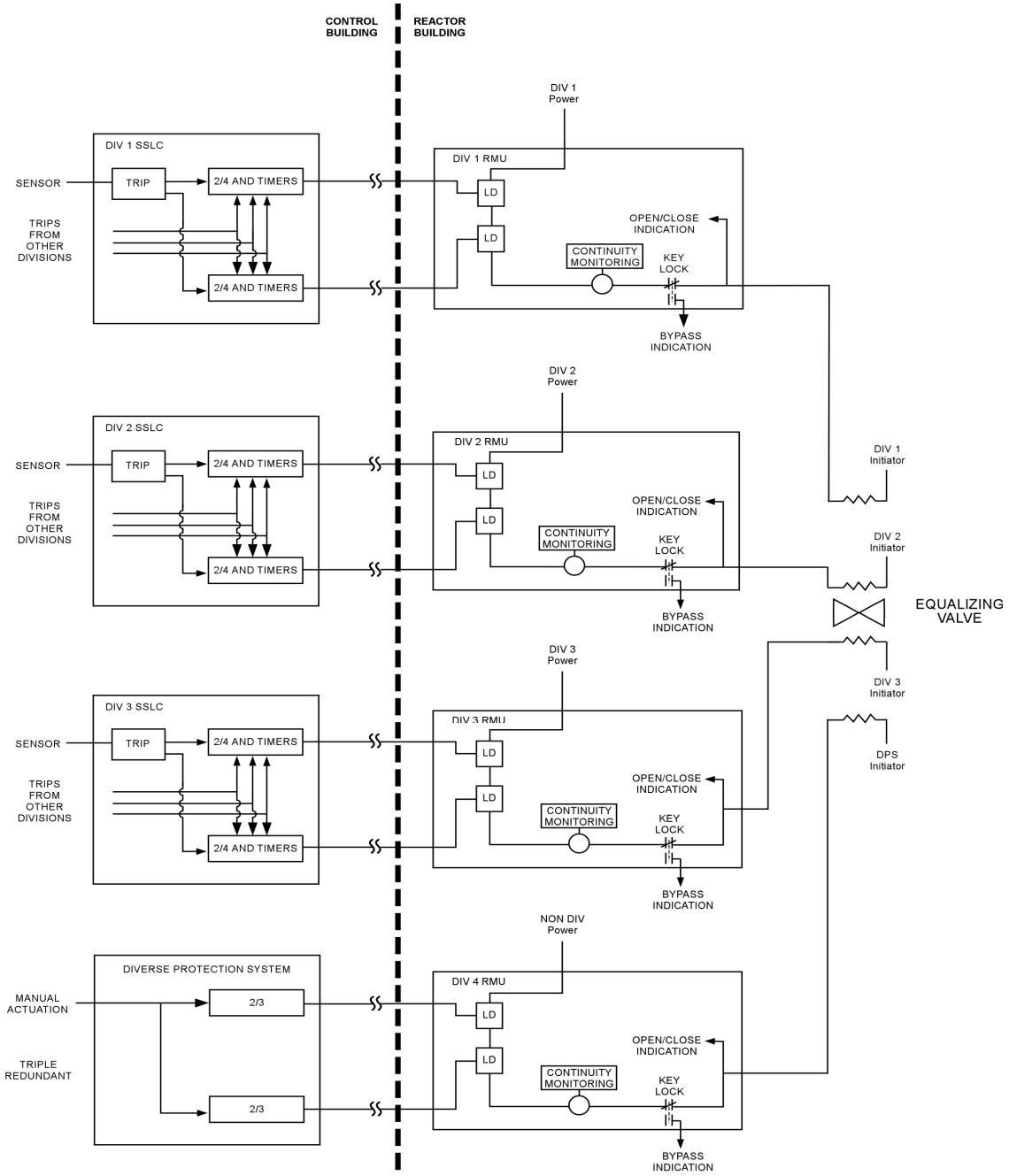


Figure 7.3-2. GDCS Equalizing Valve Initiation Logics

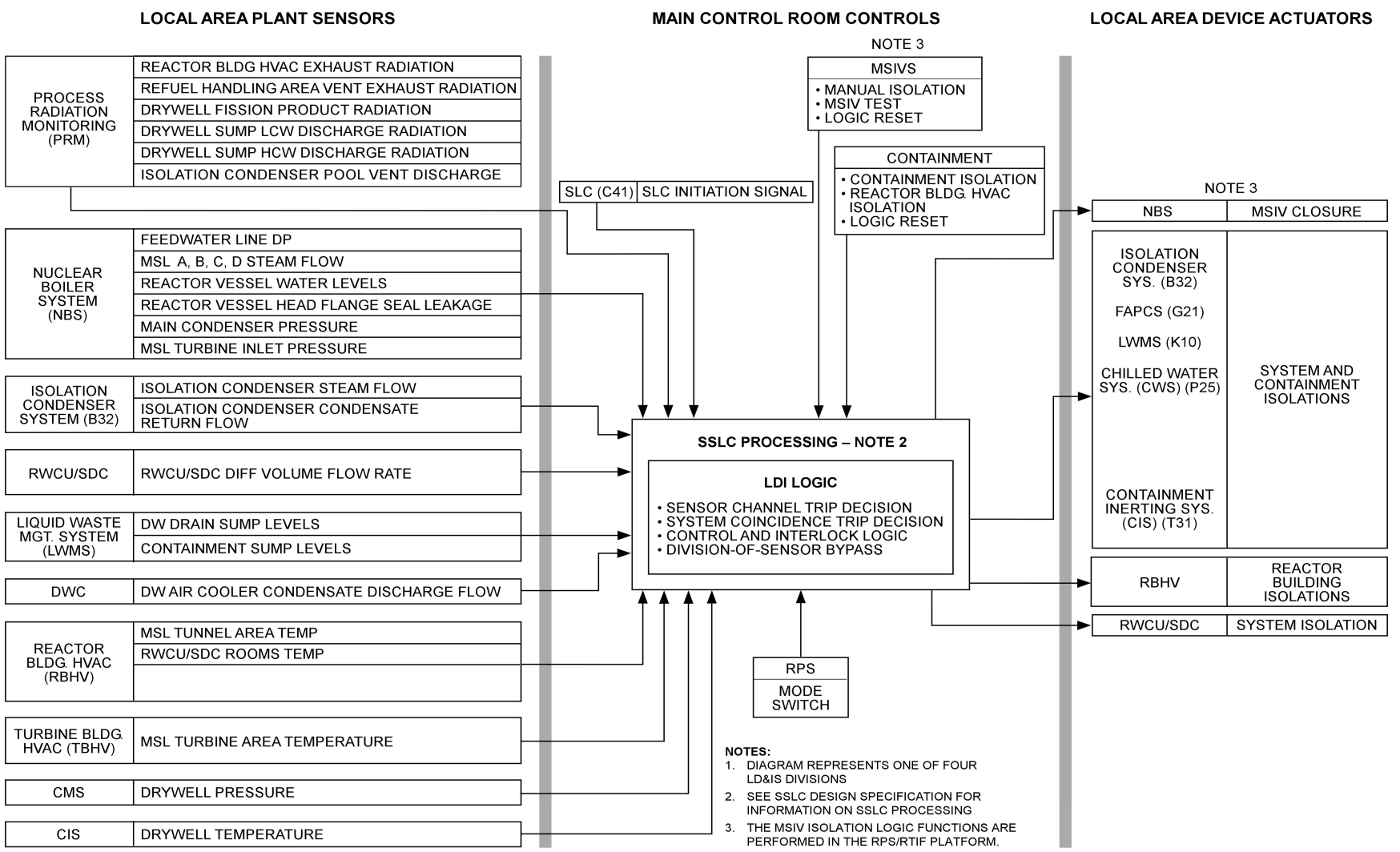
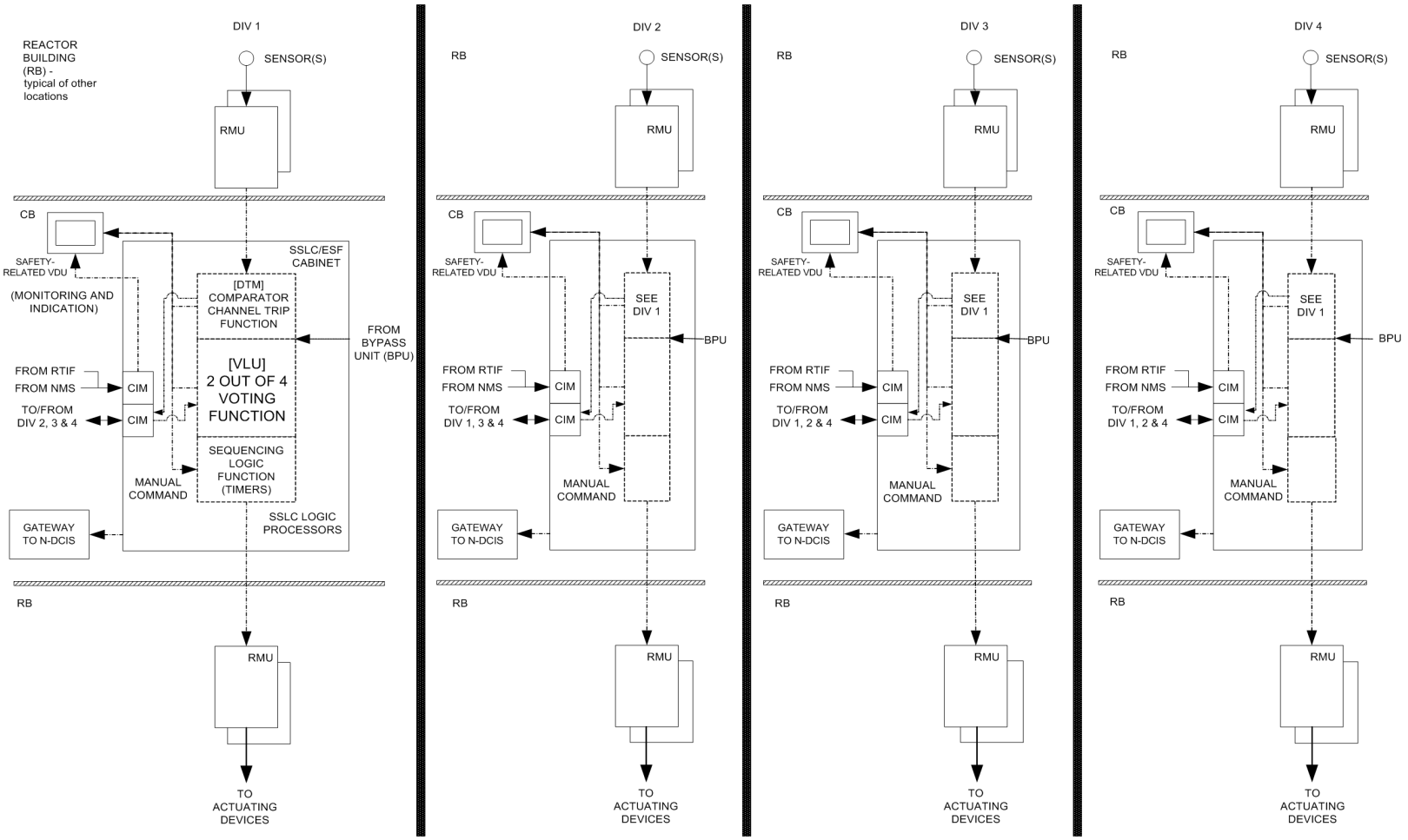
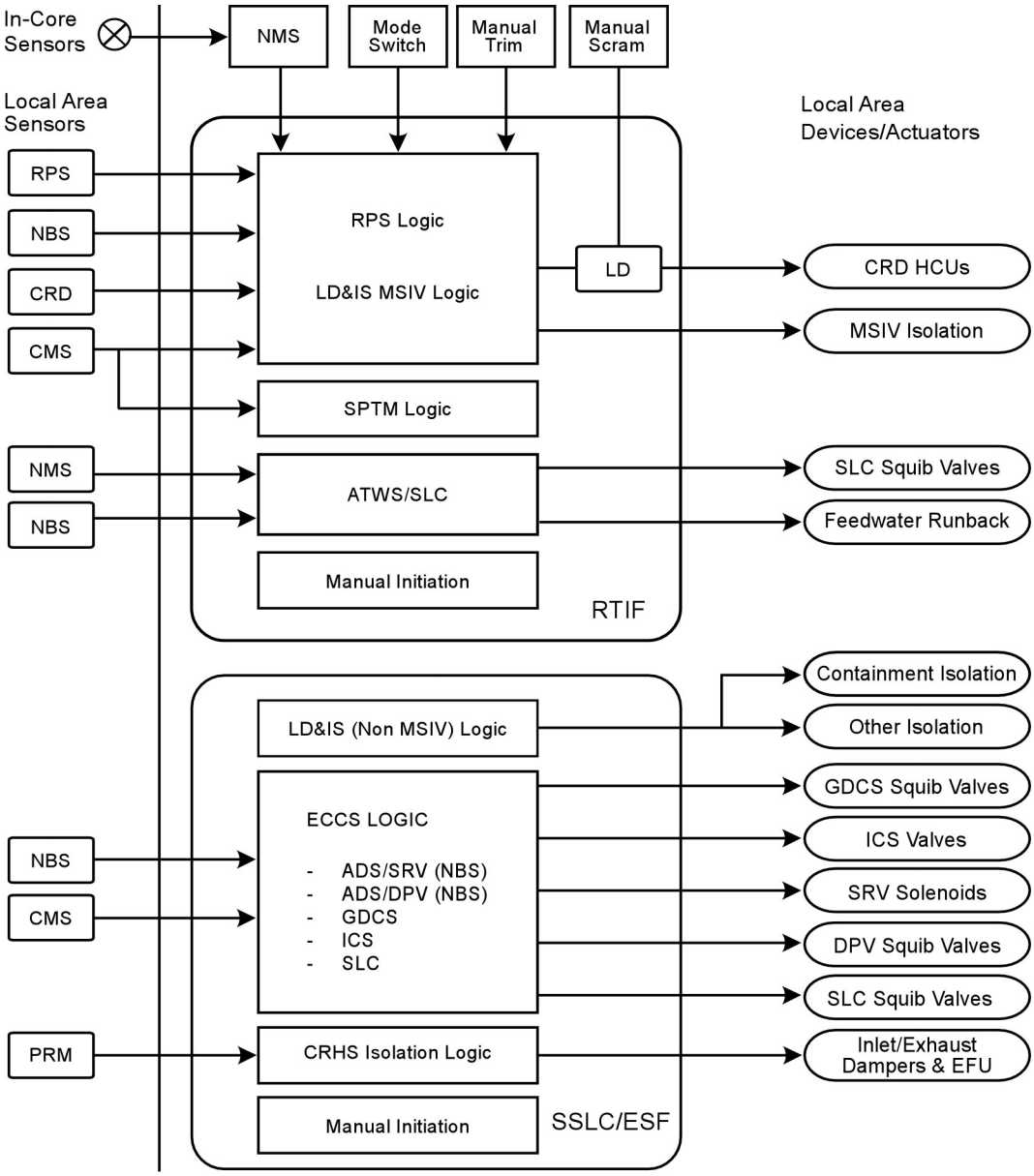


Figure 7.3-3. LD&IS System Design Configuration



(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 circuit
3) LD&IS shares sensor inputs with RTIF (for MSIV isolation) and SSLC/ESF

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, this Section includes "...those instrumentation and control systems used to achieve and maintain a safe shutdown condition of the plant." However, some I&C systems that perform cold shutdown functions are not safety-related. This is justified by the existence of the safety-related systems (ICS, GDCS, SLC system and PCCS), which utilize natural circulation in the performance of their shutdown functions. Additionally, some safety criteria, such as redundant trains and single failure, have been utilized in the design of the nonsafety-related systems. Consequently, both safety-related and nonsafety-related systems that perform either safe shutdown or cold shutdown functions 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 Instrumentation and Controls for Standby Liquid Control System (SLC) supports the passive system capability requirements to perform the following:

- Provide a diverse, backup means to shut down the reactor from full power to a sub-critical condition, using soluble boron injection, and maintain the reactor sub-critical while the reactor 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 the 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 and 4.2, 4.5, 4.8, and 4.10).

The SLC System initiation function is part of a group of systems that are collectively referred to as the Safety-Related Distributed Control and Information System (Q-DCIS). A simple

functional block diagram of Q-DCIS is included as part of Figure 7.1-1 and a detailed functional network diagram appears as Figure 7.1-2. These diagrams indicate the relationships of SLC System with its safety-related peers and with nonsafety-related plant data systems that are collectively referred to as 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 control 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 main control room 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 main control room (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 Emergency Core Cooling System to provide mitigation for LOCA events. SLC receives an actuate command following a confirmed LOCA signal plus a 50 second time delay corresponding to the first depressurization valve actuation (as described in the Automatic Depressurization System (ADS) logic discussion in Subsection 7.3.1). 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), and is described in Section 7.8, Diverse Instrumentation and Control Systems.

The ATWS/SLC initiation logic is depicted on Figure 7.8-3, ATWS Mitigation Logic (SLC System Initiation, Feedwater Runback).

The ATWS/SLC logic uses diverse sensors, hardware and software platforms from the SSLC/ESF, RPS and Diverse Protection System 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 (via the Leak Detection and Isolation System).

To avoid the injection of nitrogen into the reactor vessel, 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 is 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 VAC electrical systems (see Subsection 8.3.1.1.3). Divisional assignments are made to ensure availability of each SLC system loop, assuming a safety-related division of power is not in service in addition to an additional single active failure. Additionally, a squib in each loop may be activated by the DPS as part of the defense-in-depth and diversity 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 main control room. Successful firing of either or both squib valves in each SLC system loop assures adequate SLC system operation.

Control logic is also 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 ensures that at least one valve isolates to prevent nitrogen entry into the reactor vessel

Control logic is also provided for manual venting of the accumulators. Shutdown-off valve isolation. This function is not safety-related. This is assured by provision of serial solenoid valves in each vent line, with each valve separately (jointly) actuated by respective remote manual switches. The initiation signals (switches) are manual from the control room.

Automatic nitrogen makeup to the accumulators is provided to accommodate slow long-term leakage from the system. This makeup function is only required to maintain accumulator pressure, is not required to assure full solution injection, and, therefore, is not safety-related.

7.4.1.3 Safety Evaluation

The SLC system 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 instrumentation and controls are capable of performing their intended safety function based on the following design features. The safety-related SLC instrumentation and controls are designed to operate under the environmental conditions anticipated for the equipment location. Inter-division communication and communication with nonsafety-related interfaces occur through qualified isolation devices. Isolated ECCS initiation signals, as well as isolated ATWS mitigation signals from the DPS is 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 is the low accumulator level isolation signal 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 function with a division removed from service coincident with a single failure. Division of sensors bypass capability allows a safety-related SLC sensor to be removed from service, while maintaining a high level of reliability. Alarmed indication of the bypass conditions provides status monitoring of the off-normal condition. With an SLC accumulator level sensor removed from service, the shut-off valve voting logic changes from 2-out-of-four to two-out-of-three. Redundant signals are used to confirm the demand for squib injection valves 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 are also provided to determines 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 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. Electrical and I&C criteria applicable to the SLC system are identified in Table 7.1-1, and presented below.

7.4.1.3.1 Conformance with Regulatory Requirements

7.4.1.3.1.1 10 CFR Parts 50 and 52

10 CFR 50.55a(a)1), “Quality Standards”

Conformance: The SLC system conforms to this criterion.

10 CFR 50.55a(h), “Protection Systems”

Conformance: The SLC system conforms to this criterion. Separation and isolation is maintained both mechanically and electrically in accordance with IEEE Std. 603 (this replaces IEEE Std. 279) and RG 1.75. The SLC is designed such that a single failure will not interfere with system operation. Electrical separation is maintained between redundant divisions and nonsafety-related portions.

10 CFR 50.62, “Requirements for Reduction of Risk from ATWS Events for light-water Cooled Nuclear Power Plants.”

Conformance: 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 in ESBWR comply 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)(2), "Level of Detail"

Conformance: The level of detail provided for the SLC system within the Tier 1 and Tier 2 documents conforms with this requirement.

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

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

10 CFR 52.79(c), "ITAAC in Combined Operating License Applications"

Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.Conformance with General Design Criteria.

In accordance with Table 7.1-1, the following GDC are addressed for the SLC system:

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

Conformance: The SLC system conforms with these GDC.

7.4.1.3.2 Conformance with Regulatory Guides (RG)

In accordance with Table 7.1-1, the following RGs are addressed for the SLC system.

- RG 1.53 – Application of the Single-Failure Criterion to Nuclear Power Protection Systems. The SLC system is a redundant backup system 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 is also redundant.
- RG 1.62 – Manual Initiation of Protective Actions –The SLC system conforms with this RG. Dual (key-locked) control switches are provided to actuate the SLC system.
- RG 1.75 – Physical Independence of Electric Systems - The SLC system conforms with RG 1.75. See Chapter 8 for general discussion of how the ESBWR meets RG 1.75.
- RG 1.105 – Setpoints for Safety-Related Instrumentation. The SLC system conforms with RG 1.105.
- RG 1.118 – Periodic Testing of Electric Power and Protection Systems -The SLC system conforms with RG 1.118.

- RG 1.153 – Criteria for Power, Instrumentation, and Control Portions of Safety Systems - Consistent with the discussion of other RGs and the General Design Criteria, the SLC system conforms with this RG.

  RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems – The SLC system conforms to RG 1.180 with the assumption that the same interpretations and clarifications identified in Subsection 7.1.6 also apply to the system.

- RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants – The SLC system conforms to RG 1.204 with the assumption that the same interpretations and clarifications identified in Subsection 7.1.6 also apply to the system.

7.4.1.3.3 Conformance with Branch Technical Positions (BTPs)

HICB-11 - The approach to conformance with RG 1.75 and RG 1.153 is discussed above.

HICB-12 - The SLC system conforms with BTP HICB-12.

HICB-16 - The level of detail provided for this system complies with BTP HICB-16.

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 performed as a part of the startup test program. This test is intended to demonstrate that the SLC system performance is in accordance with the data provided in the process flow diagram.

A full test of this system is no longer possible after plant operation. There are, however, no active components in this system other than the two squib valves in each loop and only one valve 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 with critical system parameters (accumulator level and pressure) within their normal range, injection would occur as specified in the process flow diagram.

Routine testing, monitoring of critical system parameters, and Technical Specification surveillances assure 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 indicating 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 assure SLC system operation (IEEE Std. 603, Section 5.8).

Pressure and solution level alarms and indication for each accumulator (IEEE Std. 603, Section 5.8) are provided in the control room to:

- Ensure operability of the system;
- Warn of an out-of-tolerance condition on level or pressure; and
- Provide verification of proper system operation after initiation.

These measurements are redundant to minimize vulnerability to instrument or indicator failure. The level instrumentation for each accumulator is quadruple redundant in order to provide the two-out-of-four initiation signal for closure of the shut-off valve. The pressure indication and alarm is dual redundant, and the signals from both channels are used for makeup of accumulator pressure. These instruments also provide local indication.

Local indication and control room alarm are provided for the nitrogen gas and 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 Remote Shutdown System (RSS) is a safety-related system used to provide operators with the means to safely shutdown the reactor from a place outside the Main Control Room (MCR) if the MCR becomes uninhabitable. RSS provides remote control of the systems that are needed to bring the reactor to a hot shutdown after a scram. RSS also provides the subsequent capability to bring the plant to and maintain the reactor plant in a cold shutdown condition. The specific regulatory requirements applicable to the RSS are listed in Table 7.1-1.

7.4.2.2 System Description

7.4.2.2.1 General

The RSS has two redundant and independent panels. All parameters that are displayed and/or controlled from Division 1 and Division 2 in the MCR are also 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 MSIV Isolation Switch,
- Division 2 Manual MSIV Isolation Switch,
- Division 1 Safety-Related VDU,
- Division 2 Safety-Related VDU,
- Nonsafety-Related VDU,

- Nonsafety-Related Communications Equipment.

Because the VDUs on the RSS panels are connected to Q-DCIS or N-DCIS through the same networks that serve corresponding VDUs at the MCR, all Division 1 and 2 safety-related and nonsafety-related display/control functions at the MCR are also available at the RSS panels. A simplified RSS panel schematic is provided in Figure 7.4-1. A simple functional block diagram of Q-DCIS and N-DCIS is included as part of Figure 7.1-1 and a detailed functional network appears as Figure 7.1-2. These diagrams indicate the relationships of safety-related or nonsafety-related systems to their peers and plant data systems. Section 7.1 contains a description of these relationships. The two RSS panels are located in rooms that are at two different areas 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 is normally similar to the MCR environment. Access to and use of the RSS panels is administratively and procedurally controlled. This satisfies the control access requirement of IEEE Std. 603, Section 5.9.

The RSS provides sufficient redundancy in the control and monitoring capability to accommodate a single failure in the interfacing systems and the RSS controls, in addition to the single-failure event that caused the control room evacuation. RSS is designed such that any failure within RSS 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 main control room 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. The initial plant power is 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 manually scram the reactor before leaving the main control room, or from the manual scram switches on the remote shutdown panel.
- Plant personnel have evacuated the main control room.
- 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 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 main control room.

7.4.2.2.3 System Operation

When evacuation of the main control room 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 vessel 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 1st bullet of Subsection 7.4.2.2.2 Operating Conditions, control of the CRD system from RSS may be utilized. Control of the high-pressure makeup injection capability of the CRD system ensures that the vessel 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 will automatically controls reactor pressure. Because the logic processing equipment for the ICS (or any other safety or nonsafety-related system) is outside the Main Control Room, ICS operation is not affected by an event necessitating control room evacuation, and continued operation of the isolation condensers is assumed. If the event necessitating control room evacuation results in a loss of the pressure regulator, but does not cause main steam line isolation, the ICS would initiate 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 since RSS can control nuclear safety-related systems or equipment.

The RSS provides instrumentation and controls outside the main control room 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 procedures.

7.4.2.3.1 Conformance with Specific Regulatory Requirements

Table 7.1-1 identifies the RSS and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria in order of the

listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

7.4.2.3.1.1 10 CFR Parts 50 and 52

50.55a(a)(1) Design, fabrication, erection, construction, test, and inspection to quality standards commensurate with the importance of the safety function.

Conformance: RSS conforms to 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 to cause the evacuation of the control room. The RSS is designed to accommodate a single failure in the interfacing systems or RSS controls for those 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 ability of the RSS to ultimately facilitate such conditions is not impaired. Each RWCU/SDC loop provides 50% capacity for residual heat removal mode, and each RCCW and PSW train provides approximately 50% capacity for shutdown cooling mode. 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 capacity of the remaining pump can provide sufficient makeup to maintain vessel 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 RSS. 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 the I&C systems and equipment in Tier 1. Test, inspection, analyses, and acceptance criteria of the RSS are identified in Tier 1.

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

Conformance: Design interface requirements during the licensing certification and design phases is be commensurate with the detail required to support the completion of the final safety analysis and design-specific probabilistic risk assessment. Interface material is provided in Tier 1.

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

Conformance: The level of detail provided for the RSS within the Tier 1 and Tier 2 documents conforms with this requirement.

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

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

10 CFR 52.79(c) ITAAC in Combined Operating License Applications

Conformance: ITAAC are provided for I&C systems and equipment in Tier 1. No additional ITAAC for the I&C or RSS are required at the time of COL.

7.4.2.3.2 Conformance with General Design Criteria

In accordance with the SRP for 7.4, and with Table 7.1-1, the following GDCs are addressed for the RSS:

Criteria: GDCs 1, 2, 4, 13, 19, and 24.

Conformance: The RSS conforms with the GDC identified. GDC conformance is generically discussed in Subsection 3.1.

7.4.2.3.3 Conformance with Regulatory Guides

In accordance with the SRP for 7.4, and with Table 7.1-1, the following RGs are addressed for the RSS:

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.

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. With regard to IEEE Std. 603, Section 5.1, a single-failure event is assumed to have occurred to cause the evacuation of the control room. The RSS is designed to accommodate an additional failure in the interfacing systems or RSS controls for those scenarios. 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 ability of the RSS to ultimately facilitate such conditions is not impaired. Each RWCU/SDC loop provides 50% capacity for residual heat removal mode, and each RCCW and PSW train provides approximately 50% capacity for shutdown cooling mode. 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 capacity of the remaining pump can provide sufficient makeup to maintain vessel water level during reactor cooldown.

The RSS conforms with RG 1.53.

RG 1.75 - Physical Independence of Electric Systems

Conformance: The RSS conforms with 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 Instrumentation and Control Systems

Conformance: The RSS conforms with RG 1.180, based on the assumption that the same interpretations and clarifications identified in Subsection 7.1.6 also 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 same interpretations and clarifications identified in Subsection 7.1.6 also apply to the system.

7.4.2.3.4 Conformance with Branch Technical Positions (BTPs)

In accordance with Table 7.1-1, the following BTPs are applicable for the RSS:

- BTP HICB-11 - Guidance on Application and Qualification of Isolation Devices
- 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
- HICB-21 - Guidance on Digital Computer Real-Time Performance

  Conformance: The RSS conforms with all the above HICBs.

7.4.2.4 Conformance with TMI Action Plan Requirements

In accordance with the SRP for 7.4 and with Table 7.1-1, there are no TMI action plan requirements applicable for the RSS. However, TMI action plan requirements are generically addressed in Table 1A-1 of DCD Tier 2 Chapter 1, Appendix 1A.

From the foregoing analysis, it is concluded that the RSS meets its design bases.

7.4.2.5 Testing and Inspection Requirements

The capability to safely shut down the reactor from outside the main control room shall be confirmed during the Initial Plant Test Program (Section 14.2). Testing to confirm the functionality of each RSS control circuit will be performed during each refueling outage.

7.4.2.6 Instrumentation and Control Requirements

All parameters displayed and/or controlled from Division 1 and Division 2 in the MCR are also 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 Reactor Water Cleanup (RWCU) design bases are described further in Subsection 5.4.8.1. The Shutdown Cooling (SDC) design basis is described in further detail in Subsection 5.4.8.2. Figure 5.1-3 shows the basic configuration of RWCU/SDC system.

RWCU/SDC is one of the Dual Redundant Plant Investment Protection (PIP) systems of which the instrumentation belongs to a group of systems collectively referred to as the Nonsafety-Related Distributed Control and Information System (Q-DCIS). A simple functional block diagram of Q-DCIS is included as part of Figure 7.1-1 and a detailed functional network diagram appears as Figure 7.1-2. These diagrams indicate the relationships of RWCU/SDC with its nonsafety-related peers and with safety-related plant data systems that are 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. Therefore, the RWCU/SDC system has no safety-related design bases other than 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 and the water purification equipment of the RWCU/SDC system is also isolated by signals from LD&IS received from the Standby Liquid Control (SLC) system.

7.4.3.1.3 Power Generation Design Bases

The RWCU/SDC system instrumentation shall be designed to provide suitable process indication, alarms, and manual and automatic devices for controlling the system as it:

- Removes impurities;

- Limits excess reactor water level during reactor heatup, startup, shutdown cooling and hot standby modes of plant operation;
- Minimizes reactor temperature gradients;
- Heats the reactor pressure vessel (RPV) for hydrostatic tests; and
- Removes reactor core decay heat during normal plant shutdowns.

7.4.3.2 System Description

7.4.3.2.1 Summary Description

The RWCU/SDC system performs essentially three basic plant functions. It provides a continuous purifying treatment of the reactor water during startup, normal operation, cooldown, hot standby, and shutdown modes of plant operation. It also removes core decay heat in conjunction with the main condenser or the isolation condensers during plant shutdown modes. Thirdly, the system (with the feedwater system) provides reactor vessel heat-up during cold start-up. There are two redundant RWCU/SDC trains. The overall functional description of the RWCU/SDC system is contained in Subsection 5.4.8. The instrumentation maintains the RWCU/SDC system process conditions within the limits necessary to control the system and satisfy the design bases. Protective features include isolating the RWCU/SDC system from the RPV with a LD&IS signal present. The above isolation features protect the reactor core by minimizing the potential loss of RPV coolant inventory or by avoiding removal of boron from the RPV coolant if the SLC system is actuated.

7.4.3.2.2 Detailed System Description

General - The RWCU/SDC system instrumentation for flow, pressure, temperature, and conductivity are recorded or indicated with suitable alarms in the main control room. Valves behind shielding are furnished with on-off air operators that are individually controlled from local panels or by extension stems that penetrate 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.

Pumps - The main process pumps are manually started from the main control room by VDU control with status indication. The pumps are driven by solid-state type adjustable speed drives. Temperature elements located in the Nuclear Boiler System, and a reactor cooldown controller with temperature feedback processor 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 pump from cavitation during shutdown.

The pumps are supplied from separate normal power sources. The pumps' power supplies are automatically switched to separate on-site standby diesel-generators on loss of preferred power (LOPP).

Power-Operated Valves - Motor-operated valves are manually operable from the main control room by a VDU switch. Each valve motor is stopped by limit switches or by torque switches. The positions of air/nitrogen-operated containment isolation valves are indicated in the main control room 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 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 close if:

- SLC system actuation is sent to RWCU/SDC system via LD&IS; and
- LD&IS actuation occurs.

The reactor bottom suction sampling line containment isolation valves isolation signal from LD&IS may be overridden by a manual opening signal when a reactor bottom fluid sample is required for post-accident sampling purpose.

The plant LD&IS, including the portion related to the RWCU/SDC system, is further described in Subsection 7.3.3.

Control Valves - A flow control valve is located on the RWCU/SDC system suction line from the upper RPV nozzle that controls flow from the upper RPV region. These flows are set manually using a flow controller located in the control room. 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 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 is typically overboarded to the main condenser (Subsection 5.4.8). The valve is operated using instrument air and controlled both manually and automatically from the control room using a controller and flow indicator. Pressure switches or transmitters located downstream of the overboarding valve protect low pressure components by alarming in the control room on high pressure and closing the throttle 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 throttle valve fails closed upon loss of power or air pressure.

The demineralizer bypass piping have 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 - 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); hence, conductivity elements are not required to be temperature compensated. Influent and effluent conductivity are continuously measured

and transmitted to control room recorders. Measured values in excess of water quality requirements are alarmed in the control room.

Soluble and insoluble radioisotopic concentrations - The reactor water is manually sampled during cooldown, flood-up, or early period of fuel off-loading when activated corrosion product spiking may occur.

Temperature - 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 flow.

Temperature elements located in the Nuclear Boiler System, and a reactor cooldown controller with a temperature feedback processor, are utilized to provide the necessary signals to control the pump speed during cooldown to maintain the cooldown rate.

Flow - Density compensated system mass flow is measured in the process lines from the reactor bottom and mid-vessel nozzles with venturi-type flow element in each line and are located inside the containment. Flow elements are also provided in the seismic Category I RWCU/SDC return lines to the feedwater lines and the overboarding lines. The flow transmitters for all of these flow elements are arranged in two-out-of-four logic configuration, that are utilized to detect high RWCU/SDC differential mass flow due to a break outside the containment, and 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 Figure 7.4-2E for logic for detection of 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 not safety-related with the exception of containment isolation functions, and providing instruments to detect high differential mass flow to detect RWCU/SDC break outside the containment. Refer to Subsection 6.2.4 for containment isolation functions, and Subsection 7.3.3 for containment isolation and break detection function by LD&IS.

7.4.3.3.1 Conformance with Specific Regulatory Requirements

Table 7.1-1 identifies the RWCU/SDC system and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the criteria in their order of listing in the table and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

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: RSS conforms to these requirements.10 CFR 50.55a(h) (IEEE Std. 603)

10 CFR 50.55a(h) (IEEE Std. 603)

Addressing RG 1.153 and IEEE Std. 603 below covers 10 CFR 50.55a(h).

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 7.1.2.2.

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: Interface material is provided in Tier 1.

10 CFR 52.79(c), ITAAC in Combined Operating License Applications

ITAAC are provided for the I&C equipment in Tier 1.

7.4.3.3.2 Conformance with General Design Criteria

In accordance with Table 7.1-1, the following GDC are addressed for shutdown systems:

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

Conformance: The RWCU/SDC system is not a safety-related system for the ESBWR but is designed in conformance with the listed GDC.

7.4.3.3.3 Conformance with Regulatory Guides

In accordance with Table 7.1-1, RWCU/SDC conforms with the following RGs, based on the assumption that the same interpretations and clarifications identified in Subsection 7.1.6 also apply to the system.

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

7.4.3.3.4 Conformance with Branch Technical Positions (BTPs)

In accordance with Table 7.1-1, only BTP HICB-16 applies to the RWCU/SDC system.

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 RWCU/SDC System conforms to this BTP.

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 are performed at regular intervals in accordance with the plant Technical Specifications (IEEE Std. 603, Section 5.7 and 76.5). Instrumentation requiring regular calibration, testing, and maintenance are mounted on accessible panels or racks located outside high radiation areas to the maximum extent possible.

7.4.3.5 Instrumentation and Control Requirements

Operation of the RWCU/SDC system is from the main control room. The main instrumentation available to the control room operator includes the following:

- Manual and automatic flow controllers for system, demineralizer, and overboarding flow;
- Flow indication for system, demineralizer, and overboarding flow;
- Position indication for containment isolation valves, flow control valves, and all motor-operated valves;
- Temperature indication for demineralizer influent water;
- Conductivity recorder for demineralizer influent and effluent;
- Temperature for the system supply water (from the bottom RPV head);
- Temperature for the system return (to feedwater line) water;
- Temperature for the non-regenerative and regenerative heat exchangers' water (reactor water sides);
- Various 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 Design Basis

Refer to Subsection 5.4.6.1.1 for design bases of Isolation Condenser System (ICS) (IEEE Std. 603, Sections 4.1 and 4.2). Figure 5.1-3 shows the basic configuration of ICS.

ICS is one of the Engineered Safety Feature (ESF) systems of which the instrumentation belongs to a group of systems collectively referred to as the Safety-Related Distributed Control and Information System (Q-DCIS). A simple functional block diagram of Q-DCIS is included as part of Figure 7.1-1 and a detailed functional network diagram appears as Figure 7.1-2. These diagrams indicate relationships of ICS with its safety-related peers and with nonsafety-related

plant data systems that are collectively referred to as 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 Isolation Condenser System is designed as a safety-related system, it fully complies to 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 instrumentation and control is addressed in Subsection 5.4.6.3 (IEEE Std. 603, Sections 4.8 and 4.10). Conformance of ICS instrumentation and control 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 a 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 different safety-related 120 VAC divisional power sources (see Subsection 8.3.1.1.3) than 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 source to automatically start, and 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 will not result in the loss of any one ICS train. However, a second and third source of safety-related power is 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 that starts 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 on loss of electrical power to the solenoids which control its nitrogen-actuated valves.

ICS is initiated automatically as part of the Emergency Core Cooling System to provide mitigation for LOCA events. ICS receives an actuate command following a confirmed LOCA signal plus a time delay corresponding to the first depressurization valve actuation (as described in the Automatic Depressurization System (ADS) logic discussion in Subsection 7.3.1).

The ICS normally starts into operation automatically on high reactor pressure, low reactor water level (Level 2) with time delay, low reactor water level (Level 1.0), loss of power generation buses (same signal that initiates reactor scram), loss of feedwater (loss of power to two-out-of-four feedwater pumps) in reactor run mode, or Main Steamline Isolation Valves (MSIVs) position indication (Indicating closure) whenever the reactor mode switch is in the Run position. Signals that initiate closure of the MSIV are defined in detail in the Sections on the NBS and LD&IS. Each ICS train can also be manually initiated as stated in Subsection 7.4.4.5. The

operator is able to stop any individual ICS train whenever the RPV pressure is below a reset value, overriding ICS automatic actuation signal coming from 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, or by the nonsafety-related RWCU/SDC loops or the make-up function of the CRD system operating in conjunction with safety relief valves and the suppression pool cooling systems.

The Diverse Protection System 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. The following analysis lists the applicable criteria in their order of listing in the table and discusses the degree of conformance for each.

7.4.4.3.1 Conformance with Regulatory Requirements

7.4.4.3.1.1 10 CFR 50.55 and 52

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

Conformance: ICS conforms with this requirement.

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 that failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

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: Interface material is provided in Tier 1.

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

Conformance: The level of detail provided for the ICS within the Tier 1 and Tier 2 documents conforms to this BTP.

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

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

10 CFR 52.79(c), ITAAC in Combined Operating License Applications

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

7.4.4.3.2 Conformance with 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:

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

Conformance: The ICS conforms with these GDC.

7.4.4.3.3 Conformance with Regulatory Guides (RGs)

In accordance with Table 7.1-1, the ICS conforms with the following RGs:

- RG 1.53 - Application of the Single-Failure to Nuclear Power Protection Systems - The ICS meets the requirements of RG 1.53.
- RG 1.75 - Physical Independence of Electric Systems - Separation within the ICS is such that controls, equipment, and wiring are segregated into four separate safety-related logic groups.
- RG 1.105 - Instrument Setpoints for safety-related Systems - The setpoints used to initiate ICS automatic operation or isolation are established consistent with this guide. NRC approved Reference 7.2-1 provides the detailed description of this methodology.
- RG 1.118 - Periodic Testing of Electric Power and Protection Systems - The ICS conforms with RG 1.118.
- RG 1.152 - Criteria for Digital Computers in Safety Systems of Nuclear Power Plants
- RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems.
- RG 1.168 - Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

- RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.173 - Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.180 Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems. Conformance is based on the assumption that the same interpretations and clarifications identified in Subsection 7.1.6 also apply to the system.
- RG 1.204 Guidelines for Lighting Protection of Nuclear Power Plants. Conformance is based on the assumption that the same interpretations and clarifications identified in Subsection 7.1.6 also apply to the system.

7.4.4.3.4 Conformance with Branch Technical Positions (BTP)

In accordance with Table 7.1-1, the following BTPs are addressed for ICS:

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

  SSLC/ESF logic controllers for ICS use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections from safety-related to nonsafety-related devices.

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

  ICS logic resides within the SSLC/ESF. The SSLC/ESF conforms to this BTP. Additional discussion is provided in Subsection 7.2.1.3.

- BTP HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors
- BTP HICB-14 - 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-16 is applicable to the on ICS and conforms to this BTP.
- 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

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).

7.4.4.5.1 Instruments

The following ICS indications are reported in the control room (IEEE Std. 603, Section 5.8):

- Radiation level for each IC pool compartment airspace,
- Mass flow rate in condensate return line,
- Mass flow rate in steam supply line,
- Temperature of steam and condensate return lines,
- Temperature of IC top and bottom vent lines, and
- Valve position indication

The following manual controls are provided by the IC systems (IEEE Std. 603, Sections 6.2 and 7.2):

- Manual control to enable the operator to open/close condensate return valves,
- Manual control to enable the operator to close condensate return isolation valves,
- Manual control to enable the operator to close steam supply isolation valves,
- Manual control to enable the operator to open/close all bottom vent valves,
- Manual control to enable the operator to open/close all top vent valves, and
- Manual control to enable the operator to open/close purge line valve.

7.4.5 COL Information

None.

7.4.6 References

None.

Table 7.4-1

Deleted

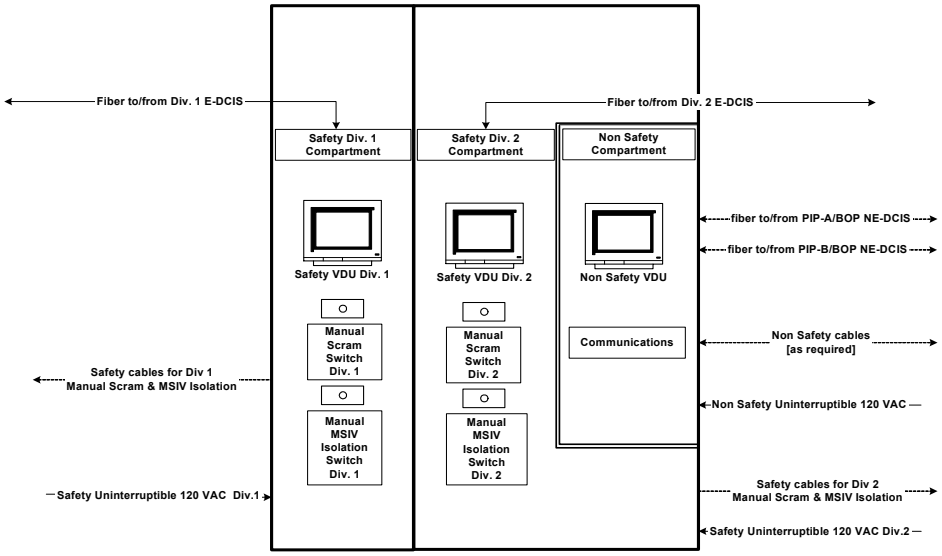


Figure 7.4-1. Remote Shutdown System Panel Schematic

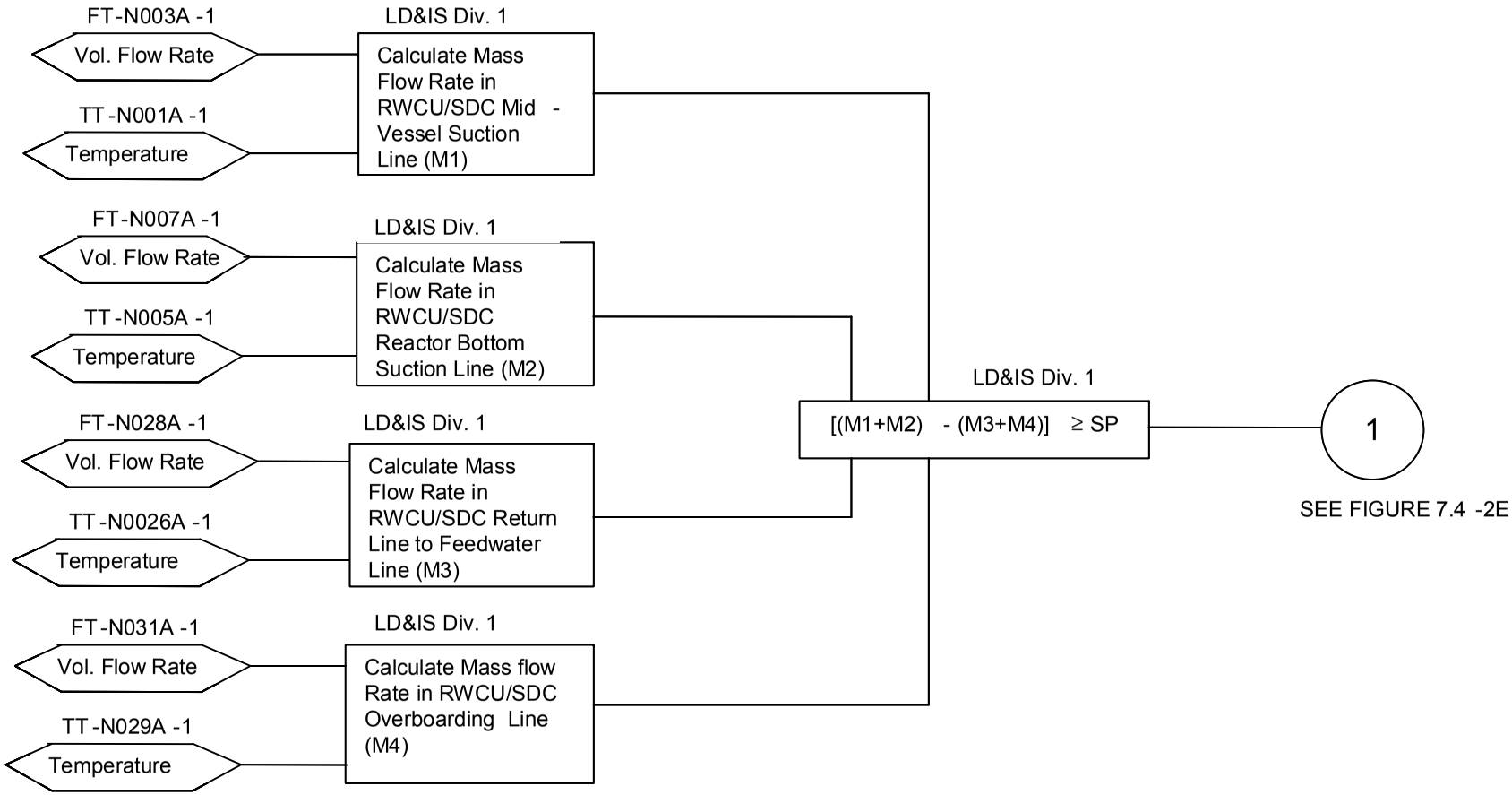


Figure 7.4-2A. RWCU/SDC System Train A Differential Mass Flow Logic- Division 1 (Typical For Train B)

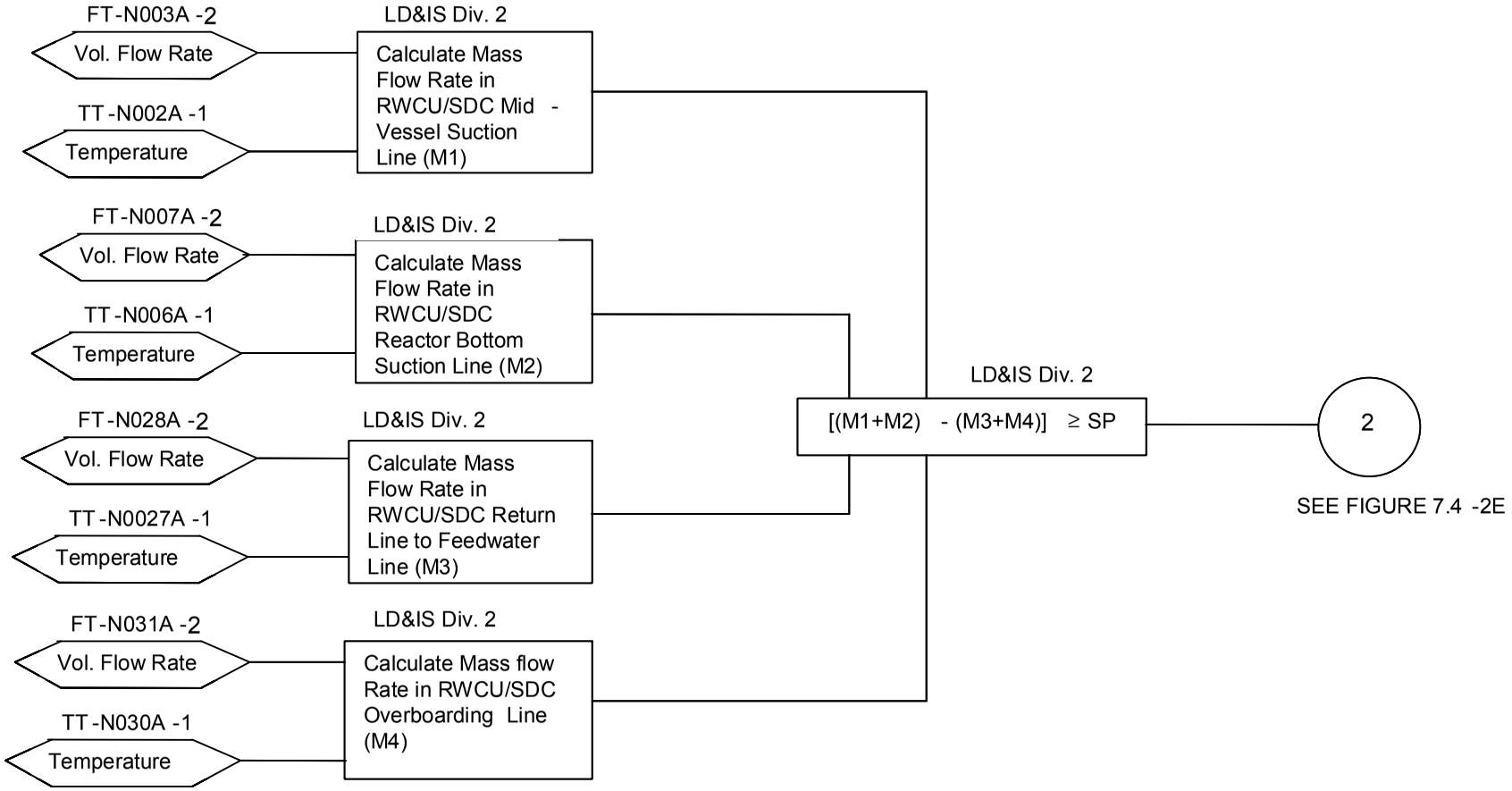


Figure 7.4-2B. RWCU/SDC System Train A Differential Mass Flow Logic- Division 2 (Typical For Train B)

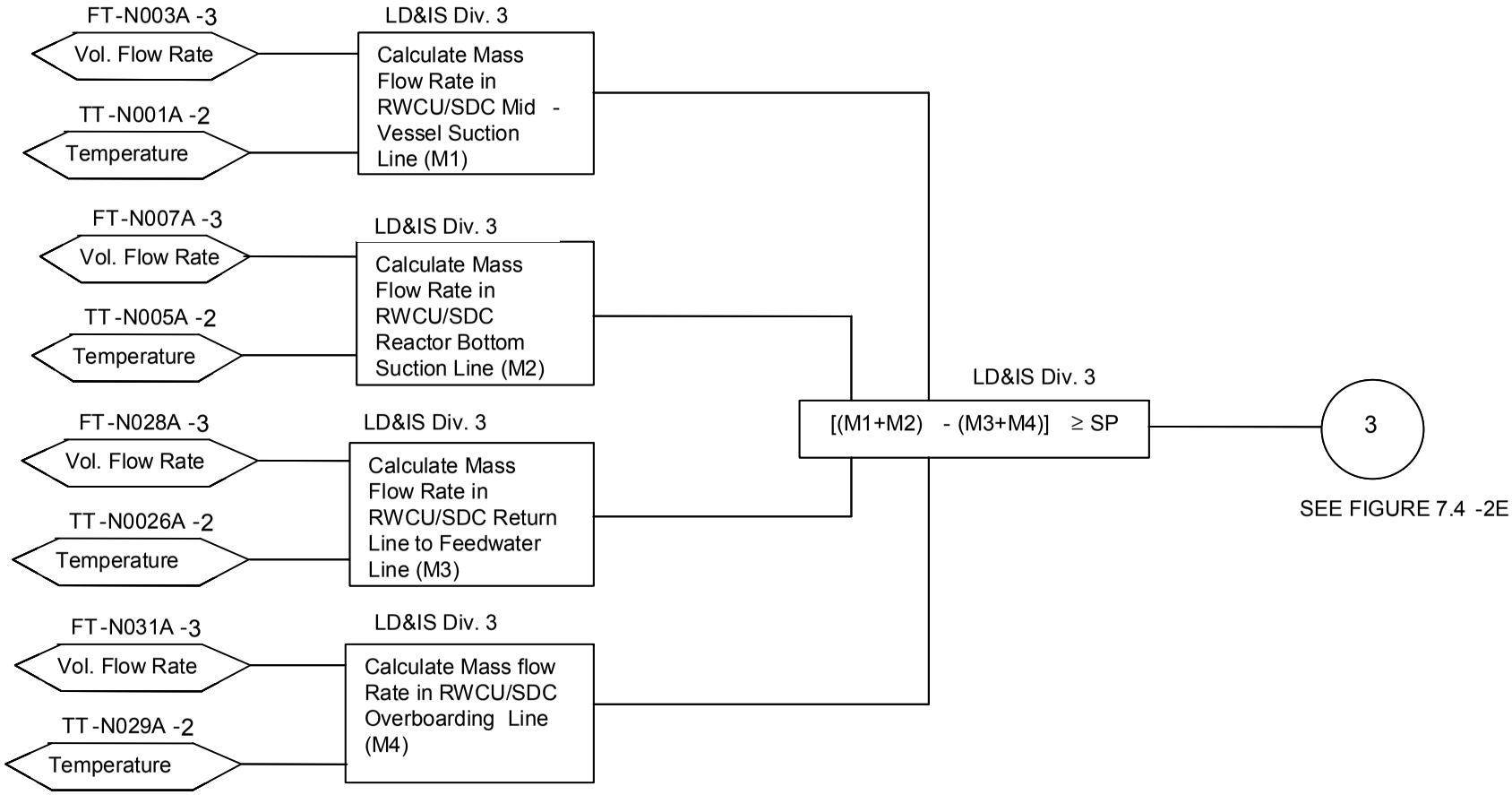


Figure 7.4-2C. RWCU/SDC System Train A Differential Mass Flow Logic- Division 3 (Typical For Train B)

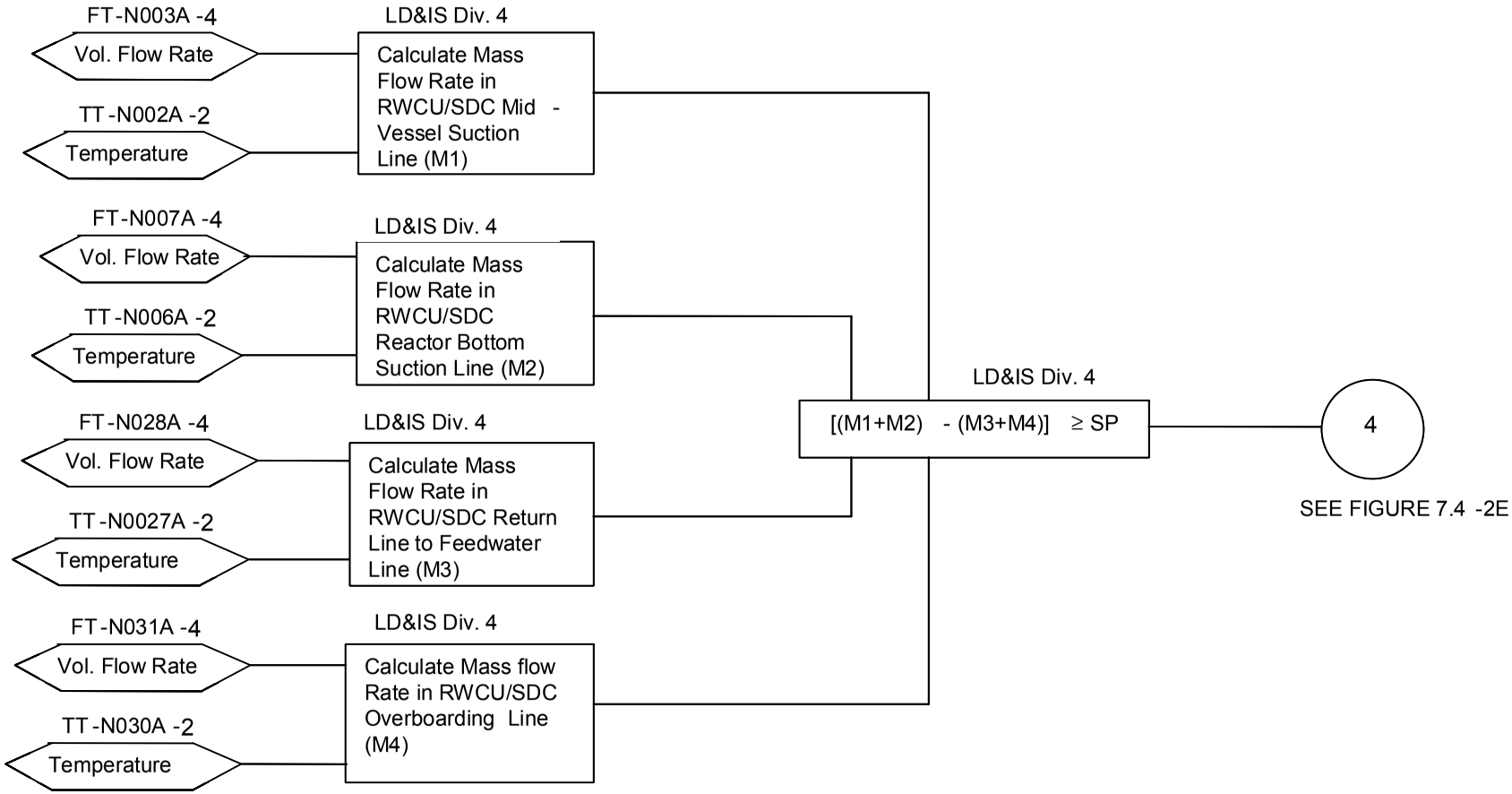


Figure 7.4-2D. RWCU/SDC System Train A Differential Mass Flow Logic- Division 4 (Typical For Train B)

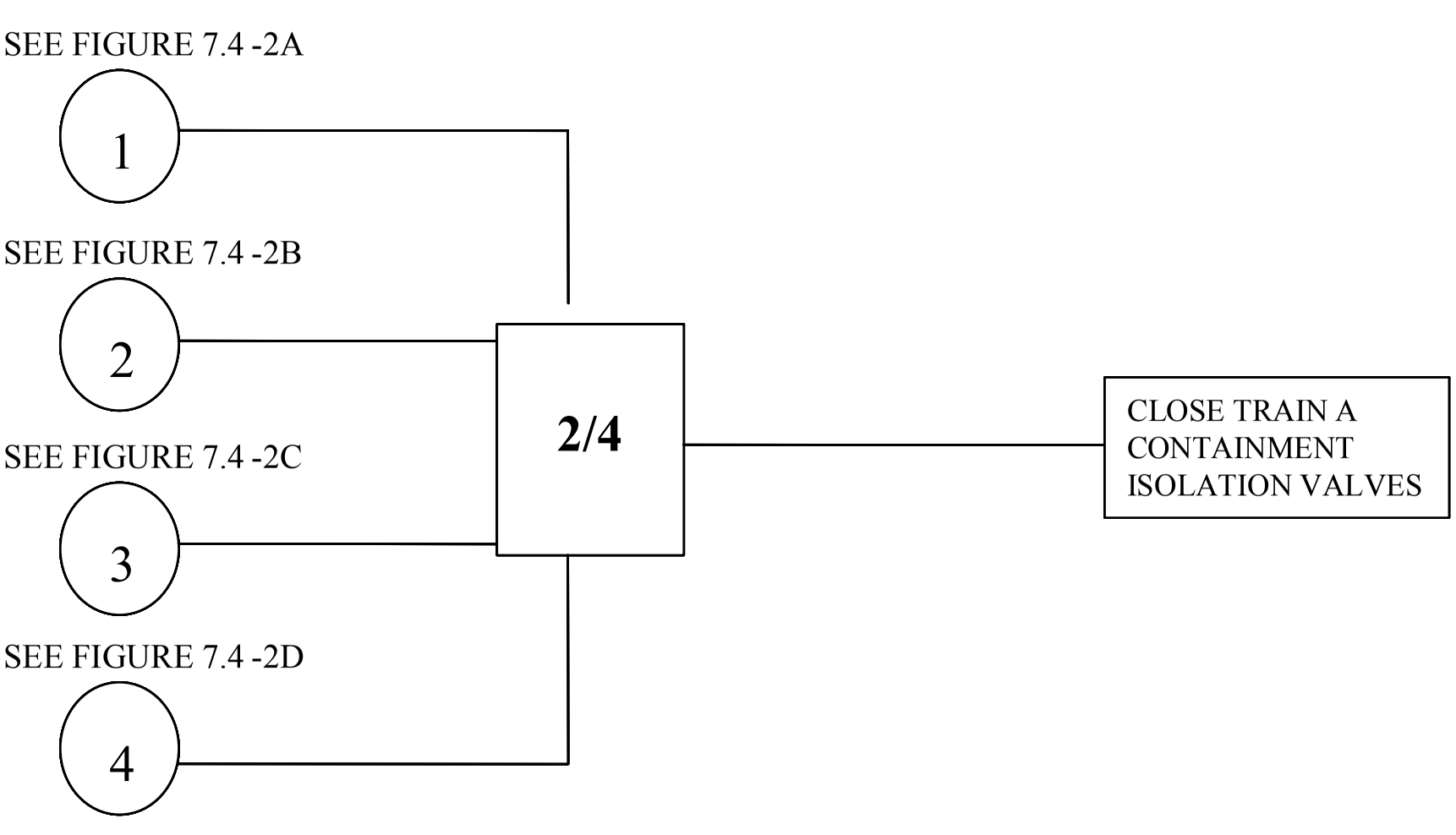


Figure 7.4-2E. RWCU/SDC Line Break Outside Containment Train A Isolation Logic (Typical For Train B)

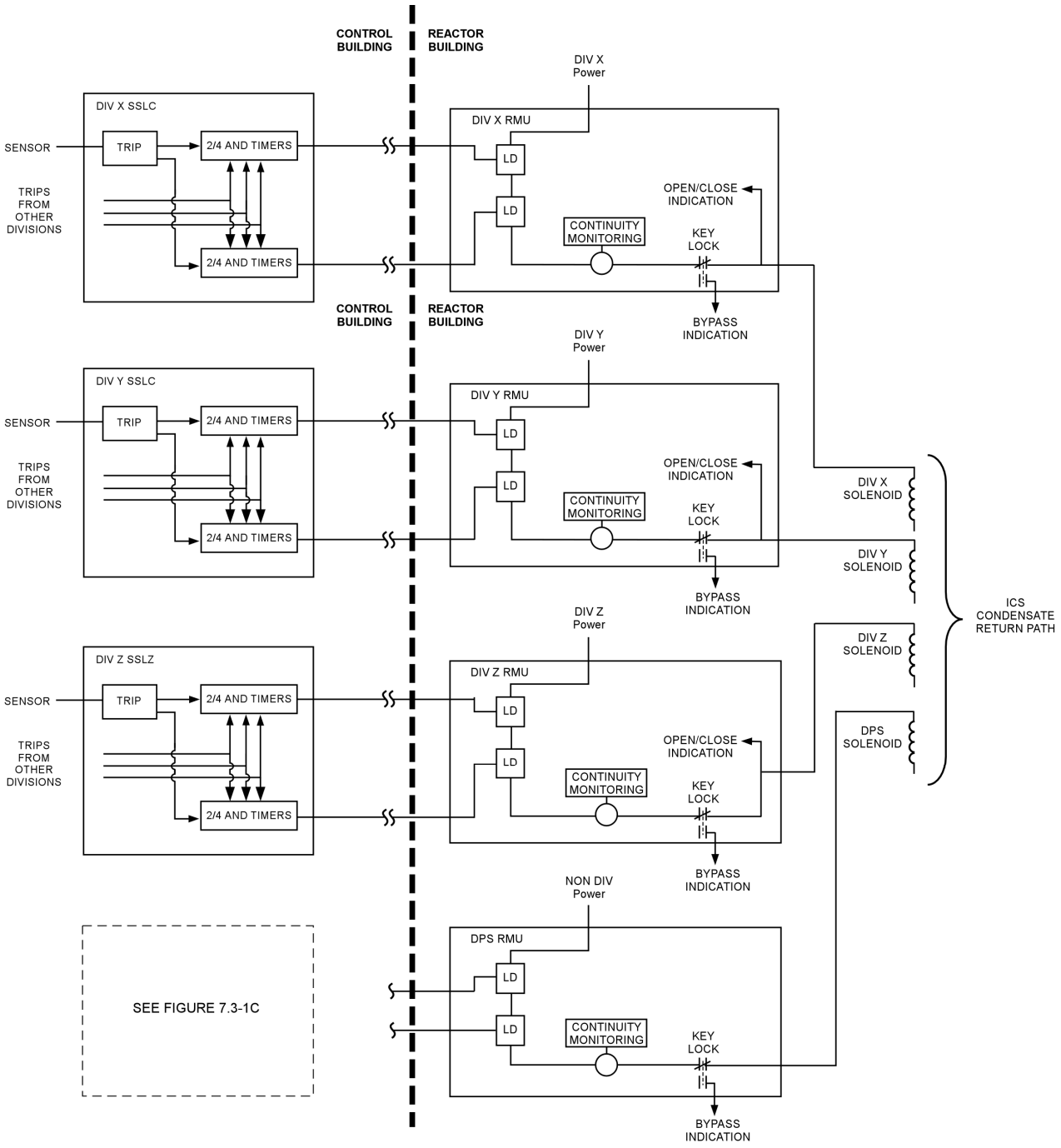


Figure 7.4-3. Isolation Condenser System Initiation and Actuation

7.5 SAFETY-RELATED AND NONSAFETY-RELATED INFORMATION SYSTEMS

This section discusses instrumentation associated with the following information systems:

- Post Accident Monitoring Instrumentation;
- Containment Monitoring System;
- Process Radiation Monitoring System;
- Area Radiation Monitoring System; and
- Pool Monitoring Subsystems.

The safety-related portions of the Post Accident Monitoring Instrumentation, Containment Monitoring System, Process Radiation Monitoring System, Pool Monitoring Subsystems and Wetwell to Drywell Vacuum Breakers are part of a group of systems that are collectively referred to as the Safety-Related Distributed Control and Information System (Q-DCIS). A simple functional block diagram of Q-DCIS is included as part of Figure 7.1-1 and a detailed 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 that are collectively referred to as nonsafety-related plant data systems (N-DCIS). Section 7.1 contains a description of these relationships.

The nonsafety-related portions of the Post Accident Monitoring Instrumentation, Containment Monitoring System, Process Radiation Monitoring System, and Area Radiation Monitoring System are part of a group of systems that are collectively referred to as the N-DCIS. A simple functional block diagram of N-DCIS is included as part of Figure 7.1-1 and a detailed 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 nonsafety-related system with its nonsafety-related peers and with safety-related plant data systems (Q-DCIS). Section 7.1 contains a description of these relationships.

7.5.1 Post Accident Monitoring Instrumentation

7.5.1.1 Design Basis

The Post Accident Monitoring Instrumentation has the following design basis:

Safety (10 CFR 50.2) 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 control room instrumentation and displays to provide the information from which actions can be taken to maintain the ESBWR in a safe condition under accident conditions, including loss-of-cooling accidents (LOCAs).

Provide equipment (including the necessary instrumentation) at appropriate locations outside the control room with a design capability for prompt hot shutdown of the reactor.

Provide the means for monitoring the reactor containment atmosphere, spaces containing components to recirculate LOCA fluids, effluent discharge paths, and the plant environs for radioactivity that may be released as a result of postulated accidents.

7.5.1.2 System Descriptions

Safety-related display 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 that manual safety-related functions are performed. The safety-related information systems include those systems that provide information (1) for manual initiation and control of safety-related systems, (2) to indicate that safety-related plant functions are being accomplished, and (3) to provide information, from which appropriate actions can be taken to mitigate the consequences of accidents. The Safety Parameter Display System, information systems associated with the emergency response facilities and Emergency Response Data System (ERDS), do not perform a safety-related function.

7.5.1.3 Safety Evaluation

The Post Accident Monitoring Instrumentation conforms to the relevant codes and standards that are specified for this instrumentation in Table 7.1-1.

7.5.1.3.1 Regulatory Requirements

7.5.1.3.1.1 10 CFR 50 and 52

50.55a(a)(1), Quality Standards Important to Safety

Conformance: The Post Accident Monitoring Instrumentation complies with this requirement.

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

Conformance: The Post Accident Monitoring Instrumentation complies with this requirement.

50.34a(f)(2)(v) [I.D.3] Bypass and Inoperable Status Indication

Conformance: The Post Accident Monitoring Instrumentation conforms to 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 Post Accident Monitoring Instrumentation to which these requirements apply are defined in Table 7.1-1, general conformance is discussed in Subsection 7.1.6, and specific conformance is discussed in the system specific sections.

50.34(f)(2)(xvii) [II.F.1], Accident Monitoring Instrumentation

Conformance: The Post Accident Monitoring System complies with this requirement.

50.34(f)(2)(xviii) [II.F.2], Inadequate Core Cooling Instrumentation

Conformance: The Post Accident Monitoring Instrumentation complies with this requirement. The detection of conditions indicative of inadequate core cooling is provided in the ESBWR design by the direct water level instrument system (Refer to Table 1.A-1, TMI Action Plan Items).

50.34(f)(2)(xix) [II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage

Conformance: The Post Accident Monitoring Instrumentation meets the intent of this requirement. The Post Accident Monitoring Instrumentation design meets the intent of RG 1.97. Additional information is provided in Subsection 7.5.1.3.1.4.

50.34(f)(2)(xxiv) [II.K.3.23], Recording of Reactor Vessel Water Level

Conformance: The Post Accident Monitoring Instrumentation meets this requirement. (Refer to Table 1.A-1 TMI Action Plan Items).

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.

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

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

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

Conformance: Interface material is provided in Tier 1.

52.47(a)(2), Level of Detail

Conformance: The level of detail provided for the Post Accident Monitoring Instrumentation within Tier 1 and Tier 2 documents conforms to this requirement.

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

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

52.79(c), ITAAC in Combined Operating License Applications

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

7.5.1.3.1.2 General Design Criteria

In accordance with the SRP and with Table 7.1-1, the following General Design Criteria (GDC) are addressed for the Post Accident Monitoring Instrumentation.

GDC 1, 2, 4, 13, 19, 23, 24

The Post Accident Monitoring Instrumentation is in conformance with the GDC identified above.

7.5.1.3.1.3 Staff Requirements Memorandum

Item II.T of SECY 93-087 Control Room Annunciator (Alarm) Reliability

The ESBWR 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, and specific conformance is discussed in the system specific sections.

7.5.1.3.1.4 Regulatory Guides

In accordance with the SRP and with Table 7.1-1, the following RGs are addressed for the Post Accident Monitoring Instrumentation:

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

Conformance: The Post Accident Monitoring Instrumentation conforms to RG 1.180 as discussed in Subsection 7.1.6.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants

Conformance: The Post Accident Monitoring Instrumentation conforms to RG 1.204 as discussed in Subsection 7.1.6.

RG 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants.

Conformance: The ESBWR design meets the intent of RG 1.97 as discussed below.

The ESBWR 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, EPGs or plant specific EOPs and AOPs) related to the variable type.

RG 1.97 has modified Section 1.3 of IEEE Std. 497 by adding the following information:

Regulatory Position (C4): "This standard does not apply to instrumentation required to support plant shutdown from outside the control room."

RG 1.97 has added the following requirement to Section 4.1 of IEEE Std. 497 (the RG provides guidance on the application of this requirement):

Regulatory Position (C4): "Type A variables include those variables that are associated with contingency actions that are within the plan licensing basis and may be identified in written procedures."

The Functional Requirements Analysis (FRA) and Allocation of Functions (AOF) (DCD Chapter 18.4) and Task Analysis (TA) (DCD Chapter 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 HFE process, is compared to the information generated from the design process and the differences are entered into the HFE Issue Tracking System (ITS) for resolution. During the Detailed (second iteration) TA, the RG 1.97 parameters are categorized into the five variable types.

When the EPG/SAG/AOP guidelines are released, they are compared to 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 "Performance Criteria", include:

- Range,
- Accuracy,
- Response Time,
- Required instrument mission duration,
- Reliability, and
- Performance Assessment Documentation.

RG 1.97 has made the following modifications to IEEE Std. 497 Section 5, "Performance Criteria" (the RG provides guidance on the application of these requirements):

Regulatory Position (C3): "The range for type C variables (paragraph 2 of Clause 5.1) shall encompass those limits that would indicate a breach in a fission product barrier. These variables shall have expanded ranges and a source term that consider a damaged core (see NUREG-0660)."

Regulatory Position (C5): "The number of measurement points should be sufficient to adequately indicate the variable value."

Regulatory Position (C7): "Modify paragraph (c) of Clause 5.4 as follows: The operating time for Type C variable instrument channels shall be at least 100 days or the duration for which the measured variable is required by the plants LDB."

Regulatory Position (C8): "Modify Clause 5.4 to replace the term 'post-event operating time' with 'operating time'."

ESBWR performance criteria (identified in IEEE Std. 497, Section 5) are developed during the design process using inputs from the HFE process and 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.

ESBWR performance is verified to meet the as-designed performance criteria per DCD Chapter 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, Criterion 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 has made the following modifications to IEEE Std. 497 Section 6, "Design Criteria":

- Regulatory Position (C2): "Modify the first sentence in the second paragraph of Clause 6.7 as follows: "Means shall be provided for validating instrument calibration during the accident."

The ESBWR design meets the intent of the specific criteria identified in IEEE Std. 497 Criteria, Section 6. Each specific criteria is addressed and documented during the ESBWR detailed

design processes using appropriate inputs from the licensing basis, the design process and the HFE process, identified in Chapter 18.

Qualification Criteria

The ESBWR 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 ESBWR 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 "Display Criteria", 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 ESBWR design meets the intent of the specific Display Criteria identified in IEEE Std. 497 Criteria, Section 8. ESBWR Display Criteria defined in DCD Chapter 18 Human Factors Engineering include all of the display criteria listed above. In addition DCD 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 ESBWR Distributed Control and Information System (DCIS) provides the required signal paths to process the information. The ESBWR DCIS is subdivided into the safety-related DCIS (Q-DCIS) and the nonsafety-related DCIS (N-DCIS). These DCIS systems are described in DCD Section 7.1.

For accident monitoring instrumentation associated with critical safety functions and powered from the safety-related sources, the Q-DCIS provides the required signal path to process this information. This information is then displayed on Q-DCIS divisional safety-related displays. The safety-related information can also be transmitted via isolated safety-related gateways to the N-DCIS for input to nonsafety-related displays, plant computer functions and the Alarm Management System. Type A, Type B, and Type C variables are powered from safety-related sources. Type D and Type E variables will have their power source determined as part of the design process.

The Q-DCIS has four separate divisions, each powered by a different safety-related uninterruptible power source. The safety-related power is discussed in DCD Subsection 8.3.1.1.3. The ESBWR design meets the intent of required instrument duration requirements of IEEE Std. 497, Section 5.4, as modified by RG 1.97.

For accident-monitoring variables that are powered from nonsafety-related sources, the N-DCIS provides the required signal path to process this information. This information is used for input to nonsafety-related displays, plant computer functions, and the Alarm Management System.

The nonsafety-related Alarm Management System, Safety Parameter Displays, and Bypassed and Inoperable Status Indication (BISI) are discussed in Section 7.1.4 and 7.1.5. Subsection 7.1.5 provides the nonsafety-related design basis for the Alarm Management System, Safety Parameter Displays, and plant computer function. Subsection 7.9.2.3 discusses additional acceptance criteria applicable to Annunciator Systems (SECY-93-087, Item II.T). The plant computer function 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 under the GE 10 CFR 50 Appendix B Assurance Quality Program, as accepted by the NRC. The NRC accepted GE Quality Assurance Program, along with its implementing procedures constitute the Quality Assurance system that is applied to the GE ESBWR safety-related I&C system design. It satisfies all applicable requirements of the following:

- 10 CFR 50 Appendix B,
- ANSI/ASME NQA-1, and
- ISO 9001.

PAM Variable List Documentation

The PAM Variable List is not included in DCD Section 7.5.

The PAM Variable List is prepared as a separate document utilizing inputs from the design process, licensing design basis, and HFE process; including the development of the Emergency Procedure Guidelines (EPGs) and/or Plant Specific Emergency Operating Procedures (EOPs) and Abnormal Operating Procedures (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.

7.5.1.3.1.5 Branch Technical Positions

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. Therefore, compliance cannot be specified at this time.

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 to these requirements is addressed during the detailed design phase.

7.5.1.5 Instrumentation Requirements

Instrumentation requirements for RG 1.97 Instrumentation are defined in IEEE Std. 497. Identification of specific instrument requirements and compliance to these requirements is addressed during the detailed design phase.

7.5.2 Containment Monitoring System

The Containment Monitoring System (CMS) provides the instrumentation to monitor:

- Atmosphere in the containment for high gross gamma radiation levels,
- Pressure of the drywell and wetwell,
- Drywell/wetwell differential pressure monitoring,
- Lower drywell pool level monitoring (post-LOCA),
- Temperature of the suppression pool water (Subsection 7.2.3),
- Sppression 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 main control room.

7.5.2.1 System Design Bases

CMS design shall be in conformance with the following system design criteria:

CMS is classified as safety-related and Seismic Category 1 except as noted, and conforms to the relevant codes and standards that are 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 subsystem of CMS is active during normal operation and 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 in the wetwell and provides measurements in the main control room in percent volume for each of the sampled gases. Sampling from the drywell or the wetwell is initiated either manually (locally) or automatically.

Two fully 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 located at widely separated locations to provide representative viewing of the containment volume. The channels measure gross gamma radiation in the drywell and suppression chamber. The signals are provided to the MCR where the signals are continuously displayed. The channels are equipped with upscale alarms to indicate high radiation and an inoperative alarm to indicate channel malfunction.

Main control room alarms are provided for indications of high radiation dose rates, inoperative radiation monitors, high oxygen levels, high hydrogen levels, and abnormal sampling 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 sensors.

The lower drywell water level is monitored to indicate any boiloff from the Isolation Condenser/Passive Containment Cooling System that may accumulate in the lower drywell after a LOCA condition.

The upper drywell water level is monitored with respect to the reactor pressure vessel nozzle elevations.

The drywell 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 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.

Main Control Room alarms and indication are provided for suppression pool temperature (see Subsection 7.2.3).

7.5.2.2 System Description

CMS is a divisionalized and segregated (safety/nonsafety) monitoring system comprised of various subsystems (IEEE Std. 603, Section 5.6-3). The system design 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 is provided for the drywell and for the airspace above the suppression pool.

Each radiation monitoring channel utilizes 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 manually selected 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 two redundant pumps. One is used during normal operation and the other is used for added capacity or backup.

Separate oxygen and hydrogen gas sources are provided in each CMS sampling rack of known compositions for monitor calibration.

CMS piping connections are provided.

The drywell pressure instrumentation consists of pressure transmitters located throughout the containment.

Four drywell pressure transmitters are provided for safety-related signals for use by RPS for reactor scram. These drywell pressure signals also are transmitted to 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 Main Control Room to provide diverse information for operator use.

Two wide-range safety-related pressure transmitters are used for providing safety-related drywell pressure information for meeting the requirements of post-accident monitoring.

Four nonsafety-related drywell pressure transmitters are used by the Diverse Protection System (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 are also provided with two additional safety-related differential pressure transmitters, connected between these two volumes. These channels are also 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 water level on the Remote Shutdown Panels.

Monitoring of suppression pool temperature (see Subsection 7.2.3)

7.5.2.3 Safety Evaluation

The CMS design, including the sensors and the instrumentation channels, are engineered into both safety-related and nonsafety-related subsystems. Safety-related systems are environmentally and seismically qualified for continuous monitoring during reactor operation, and abnormal and accident plant conditions. The system design conforms to the System Design Bases and with the relevant codes and standards that are specified for this system in Table 7.1-1.

7.5.2.3.1 10 CFR 50 and 52

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

Conformance: Containment Monitoring System complies with this requirement.

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 Containment Monitoring System safety-related subsystems are divisionalized and are redundantly designed so that failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

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

Conformance: Containment Monitoring System demonstrates compliance by being able to provide automatic indication of bypassed and operable status.

50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation

Conformance: Containment Monitoring System complies with this requirement.

50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage

Conformance: Containment Monitoring System complies with this requirement.

50.44(c)(4), Combustible Gas Control For Nuclear Power Reactors, Monitoring

Conformance: Containment Monitoring System complies with this requirement.

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.

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

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

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

Conformance: Interface material is provided in Tier 1.

52.47(a)(2), Level of Detail

Conformance: The level of detail provided for the Containment Monitoring System within the Tier 1 and Tier 2 documents conforms to this requirement.

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

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

52.79(c), ITAAC in Combined Operating License Applications

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

7.5.2.3.2 General Design Criteria (GDC)

In accordance with the SRP for Section 7.5, and with Table 7.1-1, the following GDC are addressed:

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

Conformance: The CMS complies with these GDC. The GDC are generically addressed in Subsections 3.1.1, 3.1.2 and 3.1.3.

7.5.2.3.3 Staff Requirements Memorandum (SRM)

SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability

Conformance: The CMS Alarm Management System meets the EPRI requirements 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 on dual power supplies. The processors are dedicated and vastly underutilized as they only do 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 Alarm Management System (dual power). The alarm processor is redundant.
- The horn and voice speaker are not redundant. 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 functions.

7.5.2.3.4 Regulatory Guides

In accordance with the SRP for Section 7.5, and with Table 7.1-1, the following RGs are addressed for the CMS:

- 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 to all of the above listed RGs with the assumption that the same interpretations and clarifications identified in Subsection 7.1.6 also apply to CMS.
- 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.
- RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems

  Conformance: The CMS conforms to RG 1.180 as discussed in Subsection 7.1.6.
- RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants

  Conformance: The CMS conforms to RG 1.204 as discussed in Subsection 7.1.6.

7.5.2.3.5 Branch Technical Positions (BTPs)

In accordance with SRP Section 7.5, and with Table 7.1-1, the following BTP is addressed for Containment Monitoring System:

- HICB-11 - Guidance on Application and Qualification of Isolation Devices
- HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints
- HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors
- HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
- HICB-17 - Guidance on Self-Test and Surveillance Test Provisions
- HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
- HICB-21 - Guidance on Digital Computer Real-Time Performance

  Conformance: The Containment Monitoring System complies with all the above HICBs. Discussion of HICBs 14, 17, 18, and 21 are addressed in conjunction with the SSLC/ESF system in Subsection 7.3.5.3.

7.5.2.3.6 TMI 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 Containment Monitoring System. The CMS complies with these requirements, as indicated above. However, TMI action plan requirements are generically addressed in Appendix 1A.

7.5.2.4 Testing and Inspection Requirements

Inservice and Surveillance Testing - Inservice testing shall be performed periodically on each CMS subsystem to verify operability and to assure its ready status for post accident monitoring (IEEE Std. 603, Section 6.5). Surveillance testing shall include 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 shall be 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 shall be checked and calibrated using a known gamma radiation source with predominant photon energies. Channel response shall be checked for proper measurement and display and for alarm initiation.

Each oxygen and hydrogen gas-sampling channel shall be checked for proper calibration and response using at least two input gas levels per Table 7.5-4.

Sample Gas Leakage Tests - The gas leakage from the sampling lines and associated gas analyzer panel is specified in Table 7.5-4.

7.5.2.5 Instrumentation Requirements

Radiation Level Monitoring - Each compartment in the primary containment is monitored for gross gamma radiation levels by two-divisional channels. 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 measurements 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 main control room 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 identified process and effluents streams:

- Turbine Building,
- Technical Support Center,
- Radwaste Building,
- Control Building,
- Reactor Building,
- Fuel Building, and
- Plant Stack.

The PRMS provides alerts of 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 for excessive radiation levels.

The system design is configured as shown in Figure 11.5-1, and Table 11.5-3, Design Bases, are provided in Subsection 11.5.

7.5.3.1 Safety Evaluation

The safety-related PRMS design, including the sensors and the instrumentation channels, are environmentally and seismically qualified for continuous monitoring during reactor operation and abnormal and accident plant conditions. The system design conforms to the System Design Bases and with the relevant codes and standards that are specified for this system in Table 7.1-1.

7.5.3.1.1 10 CFR 50 and 52

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

Conformance: Process Radiation Monitoring System complies with this requirement.

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 Process Radiation Monitoring System safety-related subsystems are divisionalized and are redundantly designed so that failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

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

Conformance: Process Radiation Monitoring System demonstrates compliance by being able to provide automatic indication of bypassed and inoperable status.

50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation

Conformance: Process Radiation Monitoring System complies with this requirement.

50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage

Conformance: Process Radiation Monitoring System complies with this requirement.

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.

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

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

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

Conformance: Interface material is provided in Tier 1.

52.47(a)(2), Level of Detail

Conformance: The level of detail provided for the Process Radiation Monitoring System within the Tier 1 and Tier 2 documents conforms to this BTP requirement

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

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

52.79(c), ITAAC in Combined Operating License Applications

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

7.5.3.1.2 General Design Criteria (GDC)

In accordance with the SRP for Section 7.5, and with Table 7.1-1, the following GDC are addressed:

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

Conformance: The PRMS are in compliance with these GDC. The GDC are generically addressed in Subsections 3.1.1, 3.1.2 and 3.1.3.

7.5.3.1.3 Staff Requirements Memorandum (SRM)

SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability

Conformance: The PRMS Alarm Management System meets the EPRI requirements 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 on dual power supplies. The processors are dedicated and vastly underutilized as they only do 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 Alarm Management System (dual power). The alarm processor is redundant.

The horn and voice speaker are not redundant. Test buttons are available to test the horn(s) and all the lights.

There are no alarms requiring manually controlled actions for safety systems to accomplish their safety functions.

7.5.3.1.4 Regulatory Guides

In accordance with SRP Section 7.5, and with Table 7.1-1, the following Regulatory Guides (RGs) are addressed for the PRMS:

- 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 to all of the above listed RGs with the assumption that the same interpretations and clarifications identified in Subsection 7.1.6 also apply to PRMS.

- 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.
- RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems.

  Conformance: The PRMS conforms to RG 1.180 as discussed in Subsection 7.1.6.

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

  Conformance: The PRMS conforms to RG 1.204 as discussed in Subsection 7.1.6.

7.5.3.1.5 Branch Technical Positions (BTPs)

In accordance with the SRP Section 7.5, and with Table 7.1-1, the following BTPs are addressed for Process Radiation Monitoring System:

- HICB-11 - Guidance on Application and Qualification of Isolation Devices
- HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints
- HICB-13 - Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors
- HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
- HICB-17 - Guidance on Self-Test and Surveillance Test Provisions
- HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems

- HICB-21 - Guidance on Digital Computer Real-Time Performance

  Conformance: The PRMS complies with the above BTPs. Discussion of BTPs 14, 17, 18, and 21 are addressed in conjunction with the SSLC/ESF in Subsections 7.3.5 and 7.1.6.

7.5.3.1.6 TMI 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 Process Radiation Monitoring System. The PRMS complies with these requirements, as indicated above. However, TMI action plan requirements are generically addressed in Appendix 1A.

7.5.3.2 Testing and Inspection Requirements

See Subsection 11.5.6.1.

7.5.3.3 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 Area Radiation Monitoring System (ARMS) is to continuously monitor the gamma radiation levels within the various areas of the plant and to provide an early warning that predetermined exposure rates are exceeded. The ARMS consists of various area radiation detectors located at accessible areas of the plant and utilizes local and control room alarms for immediate warning. The gross gamma radiation levels are monitored on a continuous basis, any change in exposure rates may be caused by operational transients or maintenance activities. Any high radiation levels are indicated by audible area alarms and control room alarms.

A functional block diagram of the ARMS is as shown in Figure 7.5-3. Design description of this system, together with detector locations, channel ranges, and alarm requirements, are covered in Subsection 12.3.4.

7.5.4.1 Safety Evaluation

The ARMS design, including the sensors and the instrumentation channels, are engineered as a nonsafety-related system designed for continuous monitoring during reactor operation, and additionally during abnormal and accident plant conditions. The system design conforms to the System Design Bases and the relevant codes and standards specified in Table 7.1-1.

7.5.4.1.1 10 CFR 50 and 52

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

Conformance: Area Radiation Monitoring System complies with this requirement.

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 to this system. However, items covered in this regulation are covered by the Containment Monitoring System.

50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation

Conformance: Area Radiation Monitoring System complies with this requirement.

50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage

Conformance: Area Radiation Monitoring System complies with this requirement.

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.

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

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

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

Conformance: Interface material is provided in Tier 1.

52.79(c), ITAAC in Combined Operating License Applications

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

7.5.4.1.2 General Design Criteria (GDC)

In accordance with SRP Section 7.5, and with Table 7.1-1, the following GDC are addressed:

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

Conformance: The ARMS are in compliance with these GDC. The GDC are generically addressed in Subsections 3.1.1, 3.1.2 and 3.1.3.

7.5.4.1.3 Regulatory Guides

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

Conformance: The PARMS conforms to RG 1.180 as discussed in Subsection 7.1.6.

RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants

Conformance: The PRMS conforms to RG 1.204 as discussed in Subsection 7.1.6.

7.5.4.1.4 Branch Technical Positions (BTPs)

In accordance with SRP Section 7.5, and with Table 7.1-1, the following BTP is addressed for Area Radiation Monitoring System:

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

  Conformance: The level of detail for the Area Radiation Monitoring System complies with the above BTP.

7.5.4.1.5 TMI 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 Area Radiation Monitoring System. The ARMS complies with these requirements, as indicated above. However, TMI action plan requirements are generically addressed in Appendix 1A.

7.5.5 Pool Monitoring Subsystems

7.5.5.1 General Functional Requirements Conformance

Instrumentation is provided for automatic reactor scram or 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. This is discussed in Subsection 7.2.3. Refer to Subsection 9.1.3 for additional information on the Fuel and Auxiliary Pools Cooling System.

7.5.5.2 Suppression Pool

The Containment Monitoring System is provided with temperature and water 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 the high pool temperature signal. The water level instrument generates a low water level signal when the suppression pool low level decreases to below 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 the safety-related ECCS function. For this reason, they are classified as safety-related.

7.5.5.3 GDCS Pools

Gravity-Driven Cooling System (GDCS) pools are provided with instruments for monitoring water level in these pools. The instrument generates a high or low water level signal when its water level reading increases above or decreases below the setpoints. The high and low level signal initiates an alarm in the MCR. Additionally the 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 level for the safety function.

These 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.

7.5.5.4 IC/PCC Expansion Pools

Isolation Condenser and Passive Containment Cooling System (IC/PCCS) expansion pools are provided with instruments for monitoring water level in these pools. Each instrument generates a high or low water level signal when its water level reading increases above or decreases below the setpoints. The high or low level signal initiates an alarm in the MCR. Additionally, the low level signal trips the FAPCS system pump operating in the IC/PCCS expansion pool cooling mode. The high 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 level for safety function.

These instruments provide necessary information to the operator for refilling the IC/PCCS pools following an accident. For this reason, it is classified as a safety-related component.

7.5.5.5 Spent Fuel Pool

The skimmer surge tanks are used for receiving overflow water from the spent fuel pool, and as a suction source during the spent fuel pool cooling mode of operation. These tanks are provided with instruments for monitoring water level in the tanks. These instruments generate high, low and low-low water level signals when the water level reading exceeds their setpoints. These 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 level for safety function.

These instruments provide necessary information to the operator for performing a safety-related function of refilling the spent fuel pool following an accident.

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 to monitor their closed position. See Subsection 6.2.1 for further discussion.

7.5.7 COL Information

None.

7.5.8 References

7.5-1 A. Thadani, USNRC, to D. Grace, Chairman BWR Owners' Group, letter "Safety Evaluation of BWR Owners' Group — Emergency Procedure Guidelines, Revision 4, NEDO-31331, March 1987," dated September 12, 1988.

Table 7.5-1

Deleted

Table 7.5-2

Deleted

Table 7.5-3

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

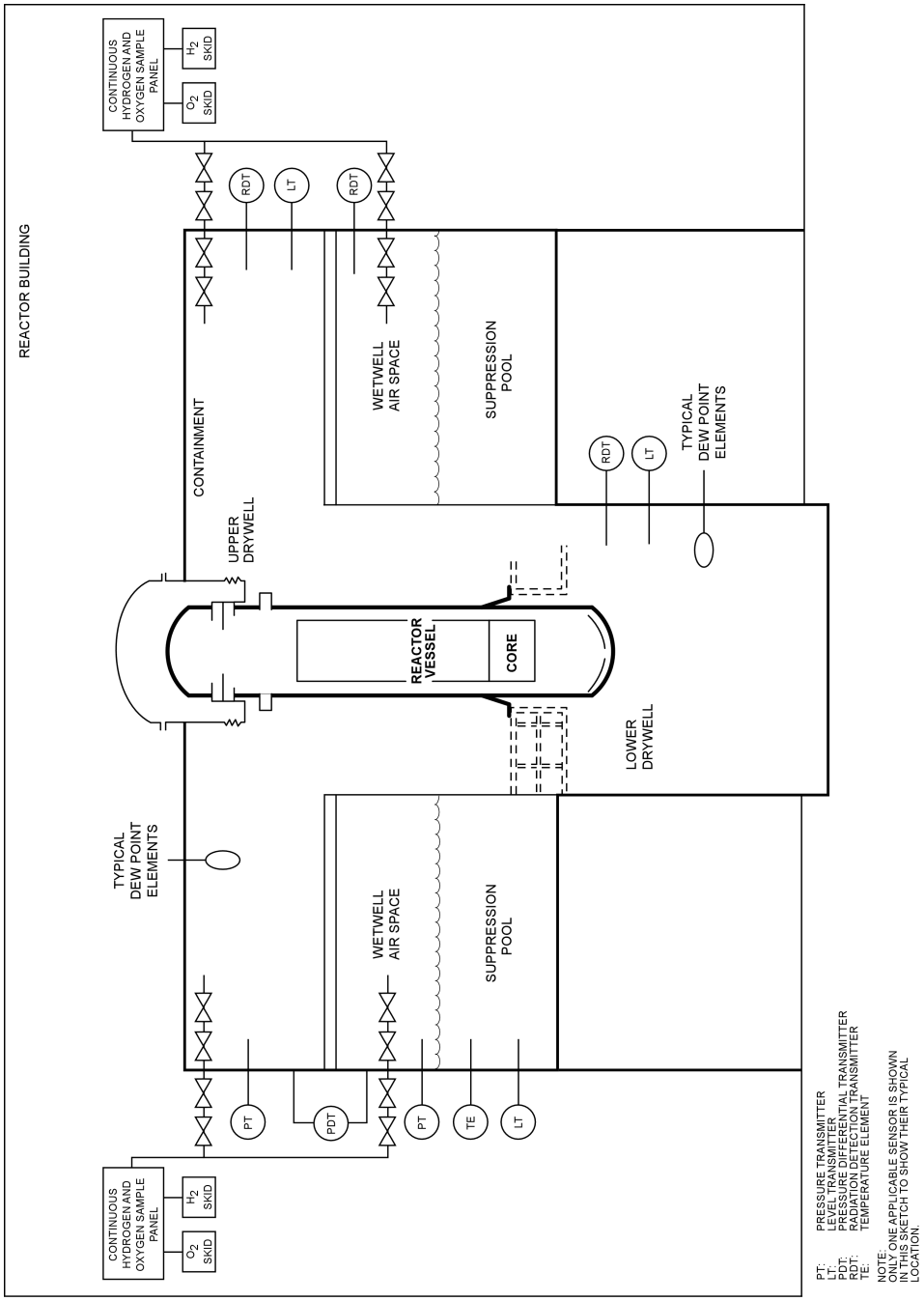


Figure 7.5-1. Containment Monitoring System Design

Figure 7.5-2.
Deleted

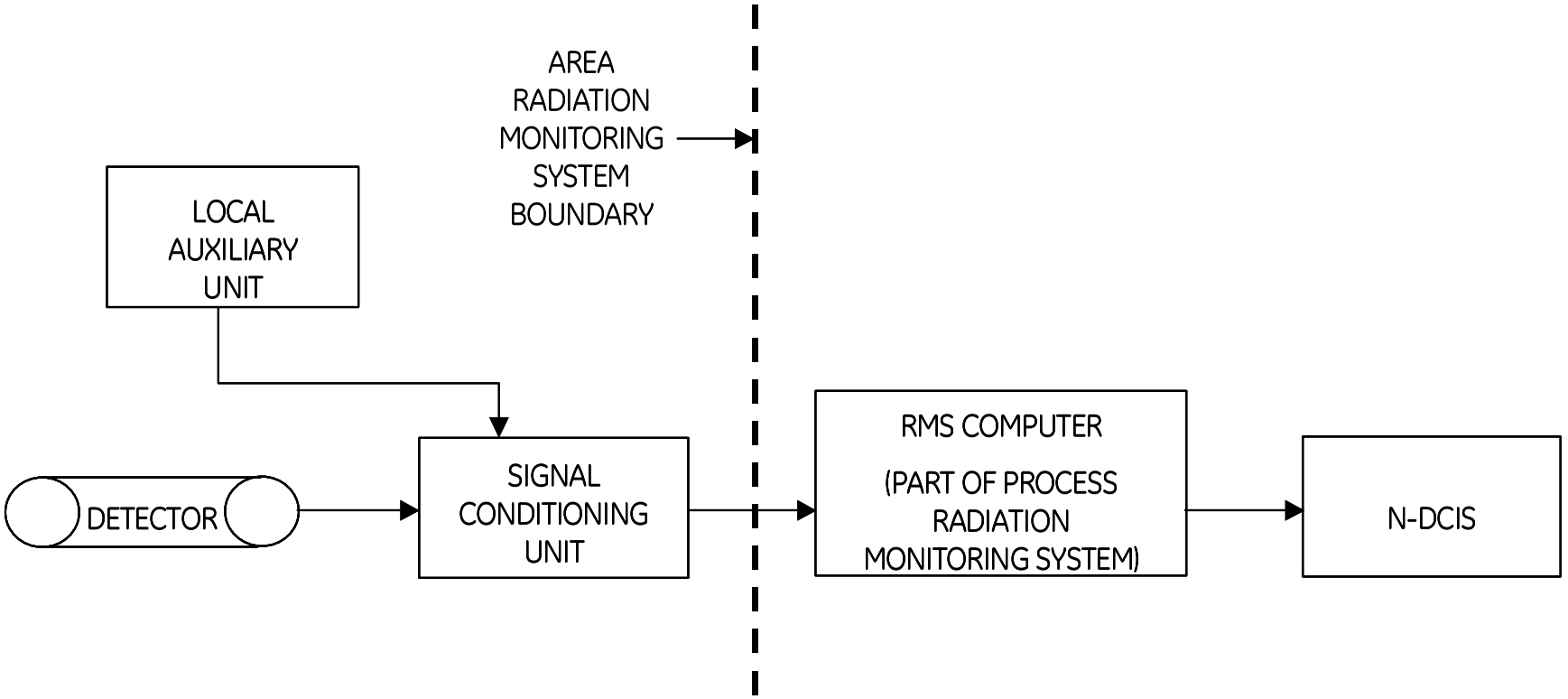


Figure 7.5-3. Area Radiation Monitoring System Functional Block Diagram

7.6 INTERLOCK SYSTEMS

In accordance with the SRP, 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 functions: (1) high pressure/low pressure (HP/LP) interlocks to prevent over-pressurization of low pressure systems (which are connected to high pressure systems), and (2) interlocks to isolate safety-related systems from nonsafety-related systems. Both types of functions are addressed in this Section.

7.6.1 HP/LP System Interlock Function

7.6.1.1 System Design Bases

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 (RWCU/SDC) systems Loop B discharge line, which is connected to the reactor vessel via the Feedwater Loop A discharge line.

During reactor power operation, the high pressure condition in the RWCU/SDC system piping exceeds the design pressure of the low pressure FAPCS piping. This Subsection discusses the reactor pressure interlock design provided to prevent over-pressurization of the FAPCS piping. The FAPCS design is discussed in Subsection 9.1.3. The reactor pressure instruments of 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 low pressure portion of GDCS has a design pressure equivalent to the reactor operating pressure, and its other end is open to the GDCS pools, there is no need for overpressure protection of the low pressure portion. An interlock is provided to prevent inadvertent manual initiation of the system during normal reactor operation. The GDCS design basis is discussed in Subsection 7.3.1.2 (IEEE Std. 603, Sections 4.1, 4.2, 4.5, 4.8 and 4.10).

7.6.1.2 System Description

7.6.1.2.1 Function Identification

Normally closed isolation valves, consisting of two parallel air-operated, testable check valves and two-parallel, air-operated gate valves, are provided to protect the FAPCS low pressure piping from over-pressurization during reactor power operation. Parallel valves are provided for redundancy and fire zone separation. Both sets of parallel valves have identical interlock logic for operation except the power supplies to nonsafety-related solenoids are provided from different sources (PIP A and PIP B buses) for redundancy. The HP/LP interlock prevents the isolation valves from opening, and closes them if opened, whenever a high pressure signal is present 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 opened for testing.

It also prevents operation of LPCI mode of FAPCS. The FAPCS modes are described in DCD Subsection 9.1.3.2.

7.6.1.2.2 Power Sources

The power supplies for the reactor pressure instruments and safety-related valve control logic are provided from the divisional safety-related power supplies, which are backed up by safety-related batteries (IEEE Std. 603, Sections 5.12, 8.1 and 8.2). Nonsafety-related redundant logic is powered by a nonsafety-related power supply, backed up by nonsafety-related batteries. Power supplies to nonsafety-related solenoids are provided from different sources (PIP A and PIP B buses) for redundancy. See DCD 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 reactor vessel sensing lines provide a high pressure signal to the FAPCS HP/LP interlock when the reactor pressure exceeds the setpoint determined, based on the design pressure of the low pressure FAPCS piping. Upon receipt of a high reactor pressure signal, the HP/LP interlock sends a signal to close the isolation valves and testable check valves and prevents them from opening or being tested respectively

7.6.1.2.4 Logic Description

The HP/LP interlock logic is processed in divisionally separate safety-related Q-DCIS and redundant nonsafety-related N-DCIS. See Subsections 7.1.3 and 7.1.5 for Q-DCIS and N-DCIS, respectively. The divisional high reactor pressure signals from NBS are sent to determine whether a high pressure condition exists in the RWCU/SDC discharge line to the RPV feedwater inlet line. If the high pressure condition exists, the safety-related and nonsafety-related interlock logic sends a valve close signal to the divisionally separate safety-related solenoids and redundant nonsafety-related solenoids, respectively to close the isolation valves. This signal prevents testing of the check valves. The high pressure signal also prevents LPCI mode operation of FAPCS.

7.6.1.2.5 Logic Sequencing

Deleted (Provided above)

7.6.1.2.6 Bypasses and Interlocks

The HP/LP interlock design has no bypass.

7.6.1.2.7 Redundancy and Diversity

The LPCI line uses redundant isolation valves (parallel set of air operated valves in series with parallel set of testable check valves) in series for the overpressure protection when the reactor pressure is above the FAPCS design pressure. Diversity is provided by a check valve equipped

with a pneumatic-assist actuator that has a fail close feature, and an air-operated failed close valve. A relief valve down stream of the isolation valve serves to detect any leakage pass 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 that are affected by the HP/LP interlock. Divisionally separated solenoids are used for controlling air to each of the actuator. Nonsafety-related solenoids powered by separate power buses are used for controlling air to each of the actuators. Valves are fail closed on loss of air/power for isolation purpose. Backup air supply is provided by an air bottle for each valve in the event that the normal air supply is not available.

7.6.1.2.9 Separation

Divisionally separate safety-related reactor pressure signals are from separate instruments discussed in Subsection 7.7.1. Safety-related logic is implemented in divisionally separate Q-DCIS and nonsafety-related logic is implemented in redundant N-DCIS. Solenoids provided for actuator action are physically separate. See also Subsection 7.1.3 and Subsection 7.1.5.

7.6.1.2.10 Testability

Testing of the reactor pressure instrument is discussed in Subsection 7.7.1.

Due to the 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 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 ASME Code Section XI.

7.6.1.2.11 Environmental Considerations

The instrumentation and control for the HP/LP interlock classified as safety-related equipment is qualified according to the environmental conditions of the locations of the devices.

7.6.1.2.12 Operational Consideration

The HP/LP interlock prevents manual initiation of the LPCI mode of FAPCS until the reactor vessel has been depressurized to a pressure 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 is also indicated in the MCR.

7.6.1.2.14 Setpoints

The setpoint is based on the highest design pressure of the low pressure FAPCS piping.

7.6.1.3 Safety Evaluation

The ESBWR 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.

7.6.1.3.1 Conformance with General Functional Requirements

The FAPCS HP/LP interlock prevents opening of the isolation valves on the LPCI discharge line. The interlock 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 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 operates automatically, and its status is provided to the reactor operator in the MCR.

7.6.1.3.2 Conformance with Specific Regulatory Requirements

Table 7.1-1 identifies applicable regulatory criteria, and industry codes and standards applied to the interlock system in accordance with the SRP. These are addressed as follows:

7.6.1.3.3 Conformance with Title 10 Code of Federal Regulations 50.55 and 52

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

Conformance: The HP/LP interlocks comply with this requirement.

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. Electrical separation is maintained between the redundant divisions.

50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication

Conformance: The HP/LP interlock does not have a bypass feature.

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.

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

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

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

Conformance: There are no interface requirements for this section.

52.47(a)(2), Level of Detail

Conformance: The level of detail provided for the interlock systems within the Tier 1 and Tier 2 documents conforms with this criterion.

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

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

52.79(c), ITAAC in Combined Operating License Applications

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

7.6.1.3.4 Conformance with General Design Criteria (GDC)

In accordance with the SRP for Section 7.6, and with Table 7.1-1, the following GDC are addressed:

Criteria: GDC 1, 2, 4, 13, 19, 24 and 25

Conformance: The HP/LP interlocks do not involve reactivity control, hence GDC 25 is not applicable. The interlocks are in compliance with the remaining GDC listed above. The GDC are generically addressed in Subsection 3.1.2.

7.6.1.3.5 Conformance with Regulatory Guides

In accordance with the SRP for Section 7.6, and with Table 7.1-1, the following Regulatory Guides are addressed for the H/LP interlocks:

- 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

  Conformance: The LPCI line isolation valves and check valves are stroke-tested only during low reactor pressure conditions due to the interlock.

- RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems

  Conformance: The HP/LP interlocks conform to all of the RGs 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..

7.6.1.3.6 Branch Technical Positions (BTPs)

In accordance with the SRP for Section 7.6, and with Table 7.1-1, the following BTPs are addressed for the HP/LP interlocks:

- HICB-1 - Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System (IEEE Std. 603)
- HICB-11 - Guidance on Application and Qualification of Isolation Devices
- HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints
- HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
- HICB-17 - Guidance on Self-Test and Surveillance Test Provisions
- HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
- HICB-21 - Guidance on Digital Computer Real-Time Performance

  Conformance: The Interlock System complies with all the above BTPs. Discussion of BTPs HICB 14, 17, 18 and 21 are addressed in conjunction with the SSLC/ESF in Subsections 7.3.5.3.5 and 7.1.6.5.

7.6.1.3.7 Conformance with TMI Action Plan Requirements

In accordance with the SRP for 7.6 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) (I.D.3) applies to the HP/LP interlocks and is addressed above. TMI action plan requirements are generically addressed in Appendix 1A.

7.6.1.4 Testing and Inspection Requirements

HP/LP interlock instruments and control functions are calibrated and tested during the preoperational testing program to confirm that the instrumentation is correctly installed and the HP/LP interlock functions as designed (IEEE Std. 603, Section 6.5).

Testing and Inspection of NBS systems' pressure instruments' channels are described in DCD Subsection 7.7.1.4

The LPCI line isolation valves and check valves are stroke-tested during low reactor pressure conditions due to the interlock.

7.6.1.5 Instrumentation and Control Requirements

The following information is available to the reactor operator from the instrumentation and interlock described in this Subsection:

- The reactor pressure is indicated in the MCR and at four local racks in the containment.
- HP/LP interlock status is indicated in the MCR and is alarmed when any valve is open and the interlock is active (IEEE Std. 603, Section 5.8).
- Isolation valves and check valves open and close positions are indicated in the MCR.

7.6.2 Other Interlocks

7.6.2.1 Isolation – Diverse Protection System (DPS) and Safety Systems

The separation/isolation of nonsafety-related Diverse Protection System (DPS) operation and safety-related RPS and SSLC/ESF systems are addressed in Subsection 7.8.2.3. The separation/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 I&C systems for normal plant operation that do not perform plant safety functions, but are those systems that control plant processes that have a significant impact on plant safety. These systems can affect the performance of critical safety functions either through normal operation or through inadvertent operation. The control systems described in this Section include:

- The Nuclear Boiler System (NBS);
- Rod Control and Information System (RC&IS);
- Feedwater Control System (FWCS);
- Plant Automation System (PAS);
- Steam Bypass and Pressure Control System (SB&PC);
- Neutron Monitoring System (NMS) - Nonsafety-Related Subsystems; and
- Containment Inerting System (CIS).

The safety-related portion of the NBS and NMS is part of a group of systems that are collectively referred to as the safety-related Distributed Control and Information System (Q-DCIS). A simple functional block diagram of Q-DCIS is included as part of Figure 7.1-1 and a detailed functional network diagram appears as Figure 7.1-2. These diagrams indicate the relationships of NBS and NMS with their safety-related peers and with nonsafety-related plant data systems that are collectively referred to as N-DCIS. Section 7.1 contains a description of these relationships.

The RC&IS, FWCS, PAS, SB&PC and CIS are part of a group of systems that are collectively referred to as the nonsafety-related Distributed Control and Information System (N-DCIS). A simple functional block diagram of N-DCIS is included as part of Figure 7.1-1 and a detailed 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 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 plant response to accidents. The NBS sensors used for safety-related system actuation and control functions are addressed in the safety-related Sections within this chapter. Described in this Subsection are the safety-related NBS instrumentation that is only used for indication and those instruments that are only used for actuation and control or nonsafety-related systems.

7.7.1.1 System Design Bases

7.7.1.1.1 Safety (10 CFR 50.2) Design Basis

The NBS I&C meet the following safety-related requirements (IEEE Std. 603, Sections 4.1, 4.2, 4.8 and 4.10):

- Provide reactor water level and dome pressure measurements over ranges and to accuracies necessary for adequate operator monitoring of reactor water level during normal, transient, and accident conditions.
- Provide qualification of reactor water level and dome pressure instrumentation 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 such that a single failure would not result in the loss of level and pressure indication.

7.7.1.1.2 Power Generation (Non-safety) Design Bases

The NBS instrumentation meet the following power generation requirements:

Provide indication for the following parameters in support of normal plant operations;

- Reactor coolant and vessel temperatures;
- Reactor vessel water level,
  - Shutdown range,
  - Narrow range,
  - Wide range,
- Fuel zone range;
- Reactor vessel pressure;
- Safety/relief valve discharge line temperature;
- Main Steam Flow; and

To the extent practical, provide for periodic calibration and testing of the 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 plant operation and during transient and accident responses. The instrumentation discussed in this Subsection is also discussed in Section 5.1, and shown on NBS ADS Initiation Logic, Figure 7.3-1.

Safety-related instrumentation is classified and is powered from safety-related 250 VDC plant battery buses and 120 VAC 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 Reactor Pressure Valve System (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 noncondensable gases from the sensing line during calibration procedures.

Level and pressure sensing lines 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 up to the outboard excess flow check valve. The typical arrangement for these sensing lines includes a restricting orifice located inside the containment, and a manual isolation valve located outside the containment followed by an excess flow check valve.

7.7.1.2.2 Detailed System Description

Reactor Coolant and 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 (which in the saturated system infers 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 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 conditions (pressure and liquid temperature) conditions. The reactor water level measurement is

temperature compensated through the thermocouples installed on the sensing line. The reactor water level instrumentation is referenced to a common reference zero - the TAF.

Reactor water level instrumentation that initiates safety-related systems and engineered safeguards 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.

Shutdown Range Water Level - This range is used to monitor the reactor 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. 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 are just below the bottom of the dryer skirt.

Narrow Range Water Level - This 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 the 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.

Wide Range Water Level - This range uses the RPV taps above the top of the active fuel. The upper taps are the same as 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. The RPV wide range water level instrumentation is both safety-related and nonsafety-related (for DPS) and is provided for the range of normal, transient, and accident conditions. Separate sensors and indicators are provided for wide range level indication.

Fuel Zone Range Water Level - This 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 level indication.

Reactor Vessel Pressure

Pressure transmitters detect reactor vessel pressure from the same instrument lines used for measuring reactor vessel water level, and provide indication in the control room. The following lists the Subsections in which other reactor vessel pressure measuring functions are discussed.

Pressure transmitters and trip actuators for initiating scram, and pressure transmitters and trip actuators for bypassing the main steam line isolation valve 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 7.2.1.4.

Safety/Relief Valve (SRV) Leak Detection

Thermocouples are located in the discharge pipes of eight Safety Relief Valves (SRVs). The temperature signals are recorded and temperatures indicative of a leaking SRV are alarmed in the Main Control Room (MCR).

Main Steam Flow

Differential pressure transmitters are used to detect steam flow. Pressure taps from the throat of the RPV steam outlet nozzles, in conjunction with the RPV dome pressure taps measure differential pressure, which is proportional to main steam flow. 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

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 instrumentation ensures that adequate level information is available over the full extent 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 pressures, and ambient pressures and temperatures. Any mechanical interface of nonsafety-related instruments with safety-related instrument piping or the Reactor Coolant Pressure Boundary (RCPB) is classified as safety-related to avoid compromise of the safety-related sensing capability and/or the RCPB. Should a line break occur in a nonsafety-related portion of a sensing line, the excess flow check valve would close to stop the flow of reactor coolant. In the event of a single failure of the excess flow check valve, the restriction orifice limits the flow of coolant to within acceptable bounds.

7.7.1.3.1 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies control systems (including the NBS instrumentation) and the applicable codes and standards are discussed below. Codes and standards applicable to the safety-related monitoring functions of the wide range and fuel zone water level indication are discussed in Section 7.5.

7.7.1.3.1.1 10 CFR Part 50 and 52

The NBS complies with these criteria.

10 CFR 50.55a(1) Quality Standards Important to Safety

Conformance: The RPS conforms to these criteria, as shown by the following commitments to applicable RGs 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 7.1.2.3.3, 7.1.2.3.6 and 7.2.1.2.4.

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 Tier 1.

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 Tier 1 and Tier 2 documents conforms to this regulation.

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

The ESBWR I&C design does not use innovative means for accomplishing safety functions.

10 CFR 52.79(c), ITAAC in Combined Operating License Applications

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

7.7.1.3.2 General Design Criteria

In accordance with the SRP for Subsection 7.7 and Table 7.1-1, the following GDC are addressed for the NBS:

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

  Conformance: The NBS complies with these GDC.

- 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 as addressed to this SRM, the NBS Automatic Depressurization System (ADS) function and other Engineered Safety Features (ESF) designs conform with the Item II.Q of SECY-93-087 (BTP HICB-19) through the implementation of an additional Diverse Instrumentation and Control System, described in Section 7.8

7.7.1.3.3 Regulatory Guides

RG 1.75 - The NBS complies with RG 1.75.

RG 1.105 - The NBS complies with RG 1.105 as delineated in Subsection 7.1.6

RGs 1.151 - RG 1.151 - Instrument Sensing Lines

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 reactor coolant pressure boundary. 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 - Consistent with the discussion of other RGs and the General Design Criteria (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.

RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems.

RG 1.204 – Guidelines for Lighning Protection of Nuclear Power Plants.

Conformance: The NBS system conforms to RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.

7.7.1.3.4 Branch Technical Positions (BTPs)

- HICB-11 - The approach to compliance with RG 1.75 and RG 1.153 is discussed above.
- HICB-12 - The Standby Liquid Control (SLC) system complies with BTP HICB-12.
- HICB-16 - The level of detail provided for this system complies with BTP HICB-16.
- BTP's HICB-14, HICB-17, HICB-18, HICB-19 and HICB-21 are discussed in association with the SSLC/ESF in Subsection 7.3.5.3, and in Subsection 7.1.6.

7.7.1.4 Testing and Inspection Requirements

Calibration and testing of the various instruments are performed during preoperational testing to confirm that the instrumentation is installed correctly and performs as required.

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 Requirements

The following information is available to the reactor operator from the instrumentation discussed in this Subsection (IEEE Std. 603, Section 5.8):

- Reactor 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 racks in the containment.
- The discharge line temperatures of the SRVs are viewed on the 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.
- 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 (10 CFR 50.2) Design Basis

The RC&IS has no functional safety-related design bases and is designed such that functional capabilities of the safety-related systems are not adversely affected.

7.7.2.1.2 Power Generation (Non-safety) Design Bases

The main objective of the RC&IS is to control the FMCRD motors of the 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 brakes of the CRD the RC&IS, acquires status and control rod position information from the FMCRD instrumentation of CRD. It sends purge water valve control signals to and acquires status signals from the HCUs of CRD, as well as sends and receives status and control signals to and from other plant systems and the various 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 plant operator, when the RC&IS is placed in manual or semiautomatic mode of operation
- The automatic rod movement mode of the PAS, when RC&IS is placed in automatic mode of operation.

Displays summary information to the plant operator about positions of the control rods in the core and status of the FMCRDs and RC&IS. This summary information is provided by a RC&IS Dedicated Operator Interface (DOI) on 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 such data (for example, the N-DCIS).

Provides for 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 function is called the scram-follow function.

Automatically enforces rod movement blocks to prevent potentially undesirable rod movements (these blocks do not impact a hydraulic scram insertion function, the scram-follow function, the ARI function, or the selected control rod run-in (SCRRI) function).

Provides for both manual and automatic insertion of all control rods, by an alternate and diverse method. This function is called the ARI motor run-in function. The associated ARI activation signals (that is, activated if either the automatic or manual ARI function is activated by N-DCIS scope logic) are provided to RC&IS from the N-DCIS. RC&IS logic has been designed such that a single failure, only in the single-channel FMCRD control logic and equipment associated with one FMCRD, may result in insertion failure of that rod when the ARI function is activated.

Provides for insertion of selected control rods: 1) for mitigation of a loss of feedwater heating event; or 2) for providing needed power reduction after occurrence of a load rejection event or a turbine trip event (that does not result in scram). This function is called the SCRRI function, which is automatically activated based upon receiving SCRRI command signals from the N-DCIS (manual initiation capability based upon simultaneous actuation of two manual SCRRI pushbuttons located on the main control console in the MCR also exists). RC&IS also sends a SCRRI signal to the Diverse Protection System (DPS) to initiate a Select Rod Insert (SRI).

Insures 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 MCPR and MLHGR when reactor power is above the LPSP. This function is performed by the ATLM subsystem of the RC&IS.

Provides the capability for conducting 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, called the reference Rod Pull Sequence (RRPS) during both 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. This drawing depicts the major components of the RC&IS, their interconnections and interfaces with other plant systems.

7.7.2.2.1 System Configuration

RC&IS utilizes 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 be in agreement. Any sustained disagreement between the two channels would result in a rod block. However, when the conditions for generating a rod block signal in a single channel are satisfied, that channel alone (and independent of the other) can issue 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 logic with the additional input signal coming from the associated emergency rod insertion panels. An automatic single channel bypass feature (only activated when an emergency insertion function is activated) is also provided to assure high availability for the emergency insertion functions when a single channel failure condition exists.

The failure or malfunction of RC&IS has no impact on the hydraulic scram function of CRD. The circuitry for normal insertion and withdrawal of control rods in RC&IS is completely independent of the RPS circuitry controlling the scram valves. This separation of the RPS scram and RC&IS normal rod control functions prevents any failure in the RC&IS circuitry from affecting the scram circuitry.

The RC&IS consists of several different types of cabinets (or panels), which contain special electronic/electrical equipment modules for performing RC&IS logic in the Reactor Building (RB) and Control Building (CB) and 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 and RC&IS status and HCU status. Controls are also provided for performing normal rod movement functions, bypassing of 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 logic functions of the RC&IS:

Rods Action Control Subsystem (RACS) Cabinets

There are two types of cabinets in the back-panel area referred to as the RACS, consisting of Rod Action and Position Information (RAPI) panels and an ATLM/RWM panel, which provide for a dual-redundant architecture. The RAPI panels consist of a RAPI-A panel and RAPI-B panel with the channel A logic in the RAPI-A panel and the channel B logic in the RAPI-B panel. In addition, the RAPI-A panel includes the RAPI DOI, which 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 switch located in the RAPI-A panel is used to change the selection of DOI control operation capability between the RC&IS DOI and the RAPI DOI (that is only one of these DOIs can be selected for control capability at any given time). Normally, the RC&IS DOI is selected for control functions instead of the RAPI DOI. The following Sections describe the normal situation of the RC&IS DOI being selected for control capability.

The two ATLM/RWM panels each contain channel logic for the ATLM, the RWM and the RAPI Signal Interface Unit (SIU).

Remote Communication Cabinets (RCCs)

The RCCs are located in sets such that each set contains 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, via the RC&IS multiplexing network. Each RSM is composed of logic for two Rod Server Processing Channels (RSPCs A and B) so that there is a dual-redundant logic design for each RSM and associated Resolver-to-Digital Converters (RDCs A and B) provide for conversion of 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 RSPC may be implemented in the associated FCM channel equipment or may be located in a separate, replaceable RSPC module located in the RCC. Figure 7.7-2 shows an example 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 and channel A RSPC logic is implemented in separate equipment from the equipment in which the channel B RSPC logic is implemented, to maintain tolerance for single channel failures.

Induction Motor Controller Cabinets (IMCCs)

The IMCCs consist of motor control equipment required for turning on and off the AC power, which is required for energization of the FMCRD 3-Phase motor and its directly associated motor built-in brake for performing 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 Motor Built-in Brake (MBB) provides for more accurate positioning control of each FMCRD because 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 Panel that is used in the logic for providing the emergency rod insertion movement functions (that is scram-follow, ARI or SCRRI).

Rod Brake Controller Cabinets (RBCCs)

The 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 (channel A and channel B) brake status signals to the logic of the associated RSPCs.

Emergency Rod Insertion Control Panel (ERICP)

The ERICP is located in the back-panel area of the MCR. It serves as an additional logic panel to contain relays (or solid-state equivalent) hardware needed to transmit discrete output signals to the emergency rod insertion panels in the RB. The discrete output signals are activated based upon 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 MCRP.

Emergency Rod Insertion Panels (ERIPs)

The ERIPs are located in the Reactor Building and provide discrete output signals to the IMCs in the IMCCs. The discrete output signals are activated based upon 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 (STRPs)

The STRPs, located in the RB, monitor the FMCRD position reed switch status using Reed Switch Sensor Modules (RSSMs) and communicate this information to the RAPI via the RC&IS multiplexing network. Also, the STRPs automatically record and time tag FMCRD scram timing position reed switch status changes either: 1) after initiation of an individual HCU scram test at the RPS Scram Time Test Panel, or 2) 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 (STRAP)

The STRAP, located in the MCR back-panel area, receives scram timing position information from the STRPs and performs scram timing performance analysis against the applicable Technical Specification requirements. 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 Reactor Building, provide output signals to open a purge water valve whenever either FMCRD associated with the corresponding HCU receives an insertion command from RAPI subsystem. These panels also monitor scram valve position status as well as the HCU accumulator water pressure and level status (that is, normal or abnormal). Communication of this information to and from the RAPI subsystem is achieved via the N-DCIS equipment. Two (or more) of the non-safety remote multiplexing unit cabinets of the N-DCIS equipment scope are used as the RAPI auxiliary panels (that is, the RAPI Auxiliary Panels are physically not part of RC&IS equipment scope, even though they provide for the RC&IS related functions described above).

7.7.2.2.2 RC&IS Multiplexing Network

The RC&IS multiplexing network consists of two separate channels. Fiber-optic communication links are used in this multiplexing network to handle communication between the RACS and the RSPCs in the RCCs (via the FCMs), communication between the STRPs and the RACS, and 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) and provides the appropriate status signals to the RACS Cabinets to be 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 Signal Interface Units (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 are not part of the RC&IS equipment scope. Each RAPI SIU transmits these 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 since 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 does not 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 provides the required incoming three-phase AC power for the induction motor controller 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 emergency rod insertion panels and the associated emergency rod insertion control panel. 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 Induction Motor Control Cabinets (IMCCs), RBCCs and ERIPs] is automatically powered from the standby AC diesel generators should the normal power source be lost. Excitation power required for logic in the ERICP is provided directly from the emergency rod insertion panels. 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 such that complete insertion of the FMCRDs (in any two of the three electrical groups to the full-in position) will assure the reactor reaches hot shutdown conditions. This approach provides increased reliability for the capability of the motor run-in ARI function, if activated, to assure 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 DCD Chapter 8) with at least one of the redundant AC power sources being an Uninterruptible AC 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 power source or supply failures, the operator has to perform appropriate bypass of the affected RC&IS equipment in order to restore rod movement capability.

Alternate - On the loss of normal power source, the nonsafety-related standby diesel generators provide for an alternate power source for the IMCCs, RBCCs and emergency rod insertion panels.

7.7.2.2.5 RC&IS 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 emergency rod insertion panels, and the emergency rod insertion control panel. (Note: RAPI auxiliary panels are designated as part of N-DCIS).
- The RC&IS multiplexing network equipment.
- The cross-channel communication links between equipment located in the RACS cabinets.
- The dedicated RC&IS DOI and the communication links from the RACS cabinets to this interface.

7.7.2.2.6 RACS Cabinets Subsystems

As discussed previously, the rod action control subsystem 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 each of these 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 both 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 SRNM and 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 via Divisions 1 and 2 of Q-DCIS communication (required isolation is provided by fiber optic cable and one way communication links to N-DCIS equipment).

- The non-safety dual-channel multi-channel rod block monitor (MRBM) of the NMS.
- 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 BWR plants). Violation of the RRPS causes RAPI logic to issue:
- A switch to manual mode when RC&IS is in the automatic rod movement mode or the Semi-automatic rod movement mode.
- An alarm signal when RC&IS is in the Manual rod movement mode.
- Provides control rod position and FMCRD status information to the N-DCIS; to the NMS; to the RWM; and to the ATLM. The RAPI transmits signals required by the NMS, ATLM and RWM to the associated RAPI SIU. The RAPI SIU which 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 ball nuts 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 electrical 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. RC&IS also sends a SCRRI signal to DPS to initiate the SRI function
- Provides for alternate rod insertion motor run-in of all control rods (that is, ARI), based on the receipt of the ARI initiation signals from the N-DCIS.
- Sends rod movement commands to and receives rod position, FMCRD and RC&IS related status information from the logic of all of the rod server processing channels (A & B) of each RSM in the RCCs, by means of FCMs and the RC&IS multiplexing network. 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 performance of different CRD surveillance tests, including:
  - Scram Time Test;

- Coupling Check Test; and
- Double-Notch Test

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 (only applicable when the RPS reactor mode switch is in either Startup or Run mode). 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 mode 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 Startup mode. This mode allows only a limited set of pre-specified control rods to be withdrawn to perform this special testing.
- The RAPI are responsible for enforcing 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 ATLM issues an internal rod withdrawal block signal 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, that is, MCPR and MLHGR operating limits, had operations stayed in the automatic mode. The ATLM algorithm is based upon input signals from the LPRMs and average power range monitors (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 may be updated based upon calculated inputs from the core monitoring function of N-DCIS. Updates of the ATLM setpoints can occur either automatically or manually by the operator using N-DCIS VDU capabilities (to request a manual ATLM update). Either channel of the ATLM can cause transfer to Manual mode from Automatic mode and rod withdrawal block initiation independently.

7.7.2.2.7 Rod Control and Information System 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 rod movements of individual control rods. To perform this type of rod movement, the operator must establish the manual, single rod movement mode by controls provided at the RC&IS DOI, and select the individual rod to be moved. After confirming the correct rod has been selected, the operator then establishes the desired rod movement mode among step movement (that is 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 has a nominal step distance of 37.5 mm (1.48”), notch movement (that is movement to the next rod position that is an integer multiple of 2 steps movement from being fully- inserted), or continuous mode (for which rod movement continues as long as the operator activates a movement command, then settles to the effective target position after the operator deactivates the movement command). Then, to accomplish the desired movement in the selected movement mode, the operator activates “insert” or “withdraw” movement command (by activating associated hard pushbutton switches located adjacent to the RC&IS DOI on the main control panel in the MCR) and the desired rod movement will occur (provided that no abnormal conditions, such as a rod block, are activated). Should any of the higher priority automatic rod movement actions be activated (for example SCRRI, scram-follow or ARI), these movements will override the operator desired normal movement and will be 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 rod server module, 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; average power range monitor (APRM) subsystems and the multi-channel rod block monitor subsystems of the NMS or from FMCRD separation status signals received from the Q-DCIS via data transmission to the RC&IS. If the status of either separation switch A or B indicates that FMCRD separation has occurred, a rod withdrawal block condition is activated from the corresponding FMCRD if the RPS reactor mode switch is in either Startup or Run mode and 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 (with no abnormal conditions existing), the RAPI of the RC&IS transmits the appropriate rod movement command signals to a dual channel file control module (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 rod server modules (RSMs) of the selected rod and then are 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 rod brake controller (RBC). The induction motor controller then performs two-out-two voting on the command signals received from the logic of both RSPCs and then activates the proper power control signals to accomplish the FMCRD motor movement (that it 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-two voting and energizes (that is mechanically releases) the FMCRD holding brake just prior to the start of FMCRD motor movement and then de-energizes (for example, mechanically engages) the FMCRD holding brake just after the desired normal rod movement is completed.

The RDCs of the RSM also interface with instrumentation of the FMCRD (a subsystem of the CRD), collects 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 for use 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, 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 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 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. By 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 to assure the RRPS sequence is followed.

When the RC&IS is in manual mode and ganged rod movement mode has also been chosen, if the operator selects a specific rod in a gang, the logic will automatically select 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 will have 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 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 dedicated operator interface for automatic rod movement mode must be activated with none of the abnormal conditions that could prevent RC&IS automatic operation mode being active. The operator has the option of discontinuing the automatic operation by either placing the RC&IS mode switches to manual mode or to semi-automatic mode.

7.7.2.2.7.3 Establishment of RRPS

The RRPS is normally established before plant startup and stored in 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 a 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 for confirming successful completion of downloading the RRPS data.

Rod withdrawal block signals are generated whenever selected single or ganged rod movements differ from those allowed by the RRPS, when the RC&IS is in either the automatic or semi-automatic rod movement mode.

The RC&IS provides for activation of an alarm at the operators 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 ganged withdrawal sequence restrictions (GWSR).

Rod block signals to the RC&IS from Safety-related systems are appropriately isolated. This provides required isolation between safety and non-safety systems while keeping electrical failures from propagating into the safety 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 the 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 receive(s) 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 Startup or Run).
- Reactor mode switch in Shutdown (rod withdrawal block for all control rods, applicable when the RPS reactor mode switch is in Shutdown).
- Startup Range Neutron Monitor (SRNM) withdrawal block (rod withdrawal block for all control rods, not applicable when the RPS reactor mode switch is in Run).
- Average Power Range Monitor (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).
- Multi-channel Rod Block Monitor (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 Refuel if a fuel bundle is being handled by the refueling platform while positioned over the reactor pressure vessel).
- Startup mode withdrawal block (rod withdrawal block for all control rods, applicable when the RPS reactor mode switch is in Startup if the refueling platform is positioned over the reactor pressure vessel).
- Rod Action and Position Information (RAPI) trouble (rod withdrawal block and rod insertion block for all control rods).
- RAPI Signal Interface Unit (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 the dual channel configuration in its design that allows its continual operation, when practicable, in the presence of component hardware failures. This is achieved by the operator being 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. The expected frequency of an inadvertent movement of more than one control rod, due to failure, is less than or equal to once in 100 reactor operating years.

The RC&IS design assures 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 is bad, and select resolver B (or resolver A) for providing 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 (except that more control rods can be bypassed when the RPS reactor mode switch is in Refuel mode, as described below). Through operator action, an update in the status of the control rods placed into "inoperable" bypassed 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 into 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 (for example, the N-DCIS). The position substitution status of each FMCRD can also be displayed at the RC&IS DOI and the RAPI DOI.

For purposes of conducting periodical inspections on FMCRD components, RC&IS allows placing up to 54 control rods in "inoperable" bypass condition, only when the RPS reactor mode switch is in Refuel mode.

The RC&IS enforces effective rod movement blocks when the control rod has been placed in an inoperative bypass status. This is accomplished by the RC&IS logic by not sending any rod movement and brake energization power to the associated FMCRD, when this bypass status is active.

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, those control rod(s) are no longer used in determining compliance to 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 a 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 and 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 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 (that is the bypass capabilities described previously), there are additional RC&IS bypass functions provided for the operator to establish bypass 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 these bypass conditions.

The RC&IS logic ensures that associated special restrictions that are placed on the plant operation are enforced as specified in the applicable plant Technical Specifications for 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.
- RAPI channel A or B bypass.

7.7.2.2.7.7 ATLM 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 low power setpoint. One algorithm enforces operating limit minimum critical power ratio (OLMCPR), and the other 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 up into four segments. During a calculation cycle of ATLM rod block setpoints (RBS) are calculated for OLMCPR monitoring and for OLMLHGR monitoring. Then 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 (for example withdrawal and insertion pushbuttons) are the main interfaces for the operator to perform manual or semi-automatic control rod movements, activate (or 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 same 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 Diverse Protection System (DPS) equipment, which provides associated signals to the N-DCIS, which sends associated ARI motor run-in initiation signals to the RC&IS (also 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 in 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 provide for additional operator information to be displayed on other non-safety VDU 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 expected that none or very few of the RC&IS setpoints (besides the continual ATLM rod block setpoint updates) will require adjustment as a result of startup testing results.

7.7.2.3 Safety Evaluation

7.7.2.3.1 General Functional Requirements Conformance

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 rod control and information circuitry from affecting the scram circuitry. The scram circuitry is discussed in Subsection 7.2.1. Because 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.

7.7.2.3.2 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the nonsafety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the SRP for BWRs. The following analysis lists the applicable criteria and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

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

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 subsection.

10 CFR 52.79(c), ITAAC in Combined Operating License Applications

ITAAC are provided for the I&C equipment in Tier 1.

7.7.2.3.3 General Design Criteria

Criteria: GDC 13, 19, 24 and 29 apply.

Conformance: The RC&IS complies with these GDC. Refer to Subsection 3.1.2 for a general discussion of the GDC.

7.7.2.3.4 Regulatory Guides

In accordance with Table 7.1-1 and SRP Table 7-1, there are no RGs applicable to the nonsafety-related RC&IS.

- RG 1.180 – Guideliens for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems
- RG 1.204 – Guidelines for Lighning Protection of Nuclear Power Plants.

  Conformance: The RC&IC system conforms to RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.

7.7.2.3.4.1 Branch Technical Positions (BTP)

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

  The level of detail provided for the RC&IS conforms to this BTP.

7.7.2.3.5 Environmental Considerations

The RC&IS is not required for safety 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 (that is in back-panel area of the MCR and in clean areas of the Reactor Building).

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 dual-channel scope of the RC&IS equipment.

7.7.2.5 Instrumentation 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 is the three-phase power to the FMCRD motors (and associated AC power to the motor built-in brakes) and the holding brakes of the CRD system to accomplish the RC&IS related rod movement functions.

The RC&IS modules that interface with FMCRD instrumentation include the appropriate signal conditioning and conversion components (for example, resolver-to-digital converters, discrete contact closure or reed switch input circuitry, 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);
- Scram Timing position reed switches (discrete signals) at the following positions:
  - 0% insertion.
  - 10% insertion.
  - 40% insertion.
  - 60% insertion.
  - 100% insertion.

The induction motor controllers are designed to provide the proper three-phase power to the FMCRD motor (and power to 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 come either by hardwired signal interfaces or by data communication links with other systems or from the RC&IS dedicated operator interface.

7.7.3 Feedwater Control System

7.7.3.1 System Design Bases

7.7.3.1.1 Safety (10 CFR 50.2) Design Basis

The Feedwater Control System (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 Mode 1, only one of the three triplicated redundant controllers may be removed from service.

Safety-Related feedwater isolation function is not included in the FWCS.

The LD&IS will perform isolation of the feedwater system on feedwater line break inside containment by closing the feedwater containment isolation valves and tripping the main feedwater pump ASD motor safety-related circuit breaker.

7.7.3.1.2 Power Generation (Non-safety) Design Bases

The FWCS is designed such 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 reactor pressure vessel 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 water level rises to Level 8, then equipment protective action would trip the main turbine and reduce feedwater demand to zero. The feedwater pumps would trip if the water level continues to rise to Level 9. If the water level falls to Level 3, then the RPS would shut down the reactor. The RPS is a fully independent safety-related system (Subsection 7.2.1). If the water level continues to drop and reaches Level 2, the high-pressure make-up function of the CRD system would initiate. The CRD system is fully independent from 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 for the purpose of maintaining proper vessel water level in the operating range from high water level (Level 9) to low water level (Level 2). During normal operation, feedwater flow is delivered to the reactor vessel 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 adjustable speed drive (ASD). In normal operation, the fourth RFP is in standby mode and will auto-start 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 triplicate, fault-tolerant digital controller (FTDC). 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. At the operator's discretion, the system operation mode can be selected from the main control console. The 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 adjustable speed drive (ASD). The ASD will perform 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 FWCS as an analog input and compared to the speed demands sent by the FWCS. If an FTDC channel detects a discrepancy between the field voter output and the FTDC channel output, then a “lock-up” signal is sent to a “lock-up” voter and an alarm is activated in the control room.

7.7.3.2.2 Operation Modes

The following modes of feedwater flow control and thus level control are provided:

Single Element Control - At less than 25% of rated reactor powers, the FWCS uses single-element control based on vessel 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 adjustable speed drive (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 utilizes 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 which use the discharge flow signals to balance RFP flows. The trim controllers provide the speed demand signal to the ASDs, which 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.

Operational Considerations - The FWCS also provides interlocks and control functions to other systems. If the reactor water level 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 level 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 high-pressure feedwater heater (no. 7). Refer to subsectrion 10.4,7.2.2.3.

A loss of feedwater heating, resulting in a significant decrease in feedwater temperature, generates a signal that initiates a Selected Control Rod Run-In (SCRRI). This interlock limits the consequences of a reactor power increase due to cold feedwater. In addition, the temperature difference between feedwater lines A and B is monitored and alarmed if found to be 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 for purposes of maintaining proper vessel 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 would trip and the feed pump ASD flow demand would reduce to zero. Continued rising water level to Level 9 would result in a trip of all ASD feed pumps. The vessel water level rising to Level 8 or falling to Level 3 would result in the shutdown of the reactor by the RPS. Refer to Subsection 7.2.1 for RPS description.

FWCS initiates a runback of feedwater pump feedwater demand to zero and closes the LFCV and RWCU.SDC overboard flow control valve upon receipt of ATWS trip signal from ATWS/SLC Logic. Refer to Subsection 7.8.1.1.

7.7.3.3.1 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the nonsafety-related control systems and the associated codes and standards applied in accordance with the SRP. The following analysis lists the applicable criteria and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

- 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 subsection.

- 10 CFR 52.79(c), ITAAC in Combined Operating License Applications

  ITAAC are provided for the I&C equipment in Tier 1.

7.7.3.3.2 General Design Criteria

Criteria: GDC 13, 19, and 24 apply.

Conformance: The FWCS complies with these GDC. Refer to Subsection 3.1.2 for a general discussion of the GDC.

In accordance with RG 1.151, "Instrument Sensing Lines," the FWCS receives signals from sensors on vessel instrument lines in the Nuclear Boiler System. Refer to Subsection 7.7.1.3 for a discussion of the criteria of RG 1.151 in relation to the Nuclear Boiler System.

7.7.3.3.3 Branch Technical Positions (BTP)

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

  The level of detail in this subsection conforms to this BTP.

7.7.3.3.4 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 Lighting Protection of Nuclear Power Plants.

Conformance: The FWCS system conforms to RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.

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 can 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 assure that specified performance requirements are satisfied. Preoperational testing of the FWCS is performed before fuel loading and startup testing to assure that the system functions as designed and that stated system performance is within specified criteria.

7.7.3.5 Instrumentation 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.
- The LFCV flow transmitters that provide for the measurement of the flow 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 control room.

7.7.3.5.4 Steam Flow Measurement

The steam flow in each of four main steam lines is sensed at each reactor pressure vessel nozzle venturi that is 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 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 control room.

7.7.3.5.5 Feedwater Flow Measurement

Feedwater flow is sensed at a single flow element in each of the two feedwater lines, which are part of the Condensate and Feedwater System. 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 control room.

Feed pump flow is sensed at a single flow element, which is part of the Condensate and Feedwater System, 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 to the demand flow 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 between operating pumps.

7.7.4 Plant Automation System

7.7.4.1 System Design Bases

7.7.4.1.1 Safety (10 CFR 50.2) Design Basis

PAS has no safety-related design basis. However, this system is designed in such a manner that the functional capabilities of safety-related systems are not obviated. Abnormal events requiring control rod scrams are sensed and controlled by the safety-related RPS, which is fully independent of Plant Automation System. Discussions on RPS are provided in Subsection 7.2.1.

This system 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.

7.7.4.1.2 Power Generation (Non-Safety) Design Bases

The bases of this system are to provide supervisory control to regulate reactivity during criticality control, provide heatup and pressurization control, regulate reactor power, control turbine/generator output, control secondary nonsafety-related systems and provide reactor startup / shutdown controls.

7.7.4.2 System Description

The primary purpose of the PAS is for reactivity control, heatup and pressurization control, reactor power control, generator power control (MWe control) and plant shutdown control. The PAS consists of redundant, triplicate 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 (Subsection 7.1.5) the PAS receives input from the following major safety-related systems: NMS and the RPS (Subsection 7.2.1). Through the N-DCIS (Subsection 7.1.5), 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 console to perform its designed functions. From the operator's control console for automatic plant startup, power operation, and shutdown functions, the operator uses PAS to issue supervisory control commands to nonsafety-related systems, and adjusts 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 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 (for example, 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 would automatically switch into the manual mode, any operation in progress would stop, and alarms would activate. With the PAS in manual mode, the operator can manipulate control rods through the normal controls. A failure of the PAS would not prevent manual control of reactor power, and would not prevent safe shutdown of the reactor.

The triplicate FTDC and redundant system controllers perform the PAS control functional logic.

7.7.4.3 Safety Evaluation

Plant Automation System does not perform or ensure any safety-related function. This system is designed such that functionalities of safety-related systems in the plant are not affected by it.

7.7.4.3.1 Specific Regulatory Requirements Conformance

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 7.1.2.2.

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 subsection.

10 CFR 52.79(c), ITAAC in Combined Operating License Applications

ITAAC are provided for the I&C equipment in Tier 1.

7.7.4.3.2 General Design Criteria

Criteria: GDC 13, 19, and 24 apply.

Conformance: The PAS complies with these GDC. Refer to Subsection 3.1.2 for a general discussion of the GDC.

7.7.4.3.3 Branch Technical Positions (BTP):

- 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 Plant Automation System conforms to this BTP.

7.7.4.3.4 Regulatory Guides

RG 1.180 – Guideliens for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems

RG 1.204 – Guidelines for Lighning Protection of Nuclear Power Plants.

Conformance: The PAS system conforms to RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.

7.7.4.4 Testing And Inspection Requirement

The FTDC input and output communication interfaces are continuously functioning during normal power operation. Abnormal operation 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 failure 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 Requirements

The instrumentation required for the system can be categorized as (1) control room instrumentation, needed for man-machine interface, (2) hardware and software for input/output interfaces and controller functions, and (3) direct non multiplexed sensor inputs, needed by the system. The control room instrumentation supporting this system would be consistent with the control room design. The PAS consists of triplicate master controllers and duplicated system controllers as hardware, and required 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 (10 CFR 50.2) 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 Mode 1, only one of the three triplicated redundant controllers may be removed from service.

7.7.5.1.2 Power Generation (Non-safety) Design Bases

The SB&PC system is designed such 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 in that SB&PC 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 using Turbine Control Valves (TCVs) through the TGCS and Turbine Bypass Valves (TBVs) for controlling reactor pressure. In addition, the design objective of the steam bypass system is to discharge reactor steam directly to the main condenser in order to regulate reactor pressure whenever the turbine cannot utilize 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. This is accomplished through control of the TCVs through the TGCS and TBVs, such that susceptibility to reactor trip, turbine-generator trip, main steam isolation, and safety/relief valve opening is minimized. Triplicate FTDC using feedback signals from reactor vessel 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 turbine control valve 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 such that steam flow is shut off upon loss of control system electrical power or hydraulic system pressure.

Refer to Figure 7.7-5, SB&PC Simplified Functional Block Diagram, and Figure 7.7-6, SB&PC FTDC Block Diagram, for overview of functions and interfaces.

7.7.5.2.2 Normal Plant Operation

At steady-state plant operation, the SB&PC system maintains reactor vessel 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 vessel 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 reactor-vessel heatup, by varying turbine bypass flow as the main turbine is brought up to speed and synchronized. The SB&PC system also controls 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 leading to reactor trip present significant transients during which the SB&PC system maintains reactor pressure. These transients are characterized by large variations in steam flow and core thermal power output, which affect reactor water level. The SB&PC system is designed to stabilize system pressure and thus aid the feedwater/level control systems in maintaining reactor water level.

The SB&PC system is also designed for operation 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.

The SB&PC inhibits opening of the TBVs upon detection of high condenser pressure, for condenser protection.

7.7.5.2.4 Operational Considerations

Manually operated provisions permit opening of the main steam lines (up to the steam bypass valves and turbine stop valves) before normal condenser vacuum is obtained and permits 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 noncondensable gases early on in the start-up process, and controls the rate of cooling during reactor shutdown to atmospheric pressures. Upon increasing pressure transients 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 pressure transient causing the increased bypass demand is relieved.

Triplicate microprocessor-based FTDC performs 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 via VDUs on the main control console or on large VDUs 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 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 will be determined during startup testing.

Redundant uninterruptible nonsafety-related power supplies and sources power the SB&PC system controls and bypass valves. 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 provides automatic load following by forcing the turbine control valves to remain under pressure control supervision, while enabling fast bypass opening for transient events requiring fast reduction in turbine steam flow.

The steam bypass function controls reactor pressure by modulating automatically operated, regulating bypass valves in response to the bypass flow demand signal. 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
- During cool down of the nuclear boiler

7.7.5.3 Safety Evaluation

The SB&PC system is classified as primary power generation system and is not required for safety purposes, nor is it 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 the main control room area of the control building and in the turbine building and is subject to the environment of that area. The SB&PC FTDC panel and components within are designed for retaining structural integrity as to not impair any safety-related equipment in its area from performing its safety function.

Table 7.1-1 identifies the nonsafety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the SRP. The following analysis lists the applicable criteria, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

7.7.5.3.1 Specific Regulatory Requirements Conformance

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

Conformance: 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.

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.

52.47(a)(1)(vii) Interface Requirements

Conformance: Design interface requirements during the licensing certification and design phases are commensurate with the detail required to support the completion of the final safety analysis and design-specific probabilistic risk assessment. Interface material is provided in Tier 1.

52.79(c) ITAAC in Combined Operating License Applications

Conformance: SB&PC system is nonsafety-related and conforms to those sections applicable for test, inspection, analyses, and acceptance criteria of the SB&PC FTDC, as identified in Tier 1.

7.7.5.4 General Design Criteria

- **Criteria: GDC 13, 19, and 24**

  Conformance: The SB&PC is in conformance with the GDC identified above. Refer to Subsection 3.1.2 for general discussion of the GDC.

7.7.5.4.1 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 RBS. Refer to Subsection 7.7.1.3 for discussion of the criteria of R.G. 1.151 in relation to the RBS. SB&PC also receives condenser absolute pressure signals form sensors in the Main Condenser and Auxiliaries System.

7.7.5.4.2 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 is commensurate with this BTP.

7.7.5.5 Testing and Inspection Requirements

The FTDC input and output communication interfaces are continuously functioning during normal power operation. Abnormal operation of these components can be detected during operation. In addition, FTDC is equipped with on-line diagnostic capabilities for identifying and isolating failure of input/output signals, buses, power supplies, processors, and inter-processor (I/O Net) communications. These on-line diagnostics can be 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 assure that the specified performance requirements are satisfied. Preoperational testing of the SB&PC is performed before fuel loading and startup testing to assure that the system functions as designed and that stated system performance is within specified criteria.

7.7.5.6 Instrumentation Requirement

7.7.5.6.1 Power Sources

7.7.5.6.1.1 Uninterruptible Nonsafety AC Power Supply

The nonsafety inverters of the uninterruptible power source are normally supported by AC power. However, if off-site power fails, it receives power from DC source (batteries). SB&PC has three redundant nonsafety AC uninterruptible power supplies of 120 ±10% volt AC, 60 Hz. SB&PC panel design is such that loss of one power supply or incoming power source will not affect SB&PC system functional operation and thus plant operation.

7.7.5.7 Major Instrument Interfaces with SB&PC

7.7.5.7.1 Nuclear Boiler System (NBS)

NBS provides narrow range dome pressure, wide range dome pressure, inboard MSIV position, and outboard MSIV position signals to SB&PC. TBVs interface with NBS to receive main steam supply.

7.7.5.7.1.1 Plant Automation System (PAS)- Automatic Power Regulator (APR)

SB&PC supplies the following signals to PAS-APR:

- SB&PC Auto/OK status signals
- Operating pressure setpoint signals
- Total (average) TBV position signals

- Pressure regulator output signals
- Limited speed regulator output signals
- Load reference signals
- First TBV position signals

PAS-APR outputs the following signals to SB&PC:

- AFC status signals
- Signals to raise pressure setpoint
- Signals to lower pressure setpoint
- PAS-APR fatal fault signals
- Reactor Thermal Power Signals

7.7.5.7.1.2 N-DCIS - Plant Computer Function (PCF)

The Performance Monitoring and Control Function (PMCF) of PCF within N-DCIS receives signals from SB&PC for performance monitoring.

7.7.5.7.1.3 N-DCIS - Multiplexing

The Multiplexing function of N-DCIS provides the distributed control and instrumentation data communications network to support the monitoring and control of interfacing plant systems. RMUs are located throughout the plant to support SB&PC and its interfaces with other systems.

7.7.5.7.1.4 Main Control Room Panels (MCRP)

The MCRP operator interface within N-DCIS contains controls needed for SB&PC operation and displays variables and alarms from SB&PC.

7.7.5.7.1.5 Main Control Room Back Panels (MCRBP)

The SB&PC's triple-redundant FTDC panel is mounted in a MCRBP.

7.7.5.7.2 Turbine Bypass System (TBS)

TBS provides temperature signals to SB&PC from thermocouples installed in each TBV discharge pipe, located between TBV and condenser, for bypass steam leakage detection.

7.7.5.7.2.1 Turbine Generator Control System (TGCS)

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

flow for startup and normal operations. The TGCS operates the turbine stop valves (TSVs), turbine control valves (TCVs), and the intermediate stop and intercept valves. The TGCS also provides automation functions like 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 TG controller.

SB&PC sends the following signals to TGCS:

- Pressure regulation demand signals
- Signals to trip the turbine

TGCS provides the following signals to SB&PC:

- Turbine speed regulator output signals
- Load reference signals
- Turbine steam flow demand signals
- Turbine first stage pressure signals
- PLU (Power-Load Unbalance) event signals
- TGCS Central Processing Unit (CPU) failure signals
- Turbine trip signals

7.7.5.7.2.2 Main Condenser and Auxiliaries

The main condenser receives steam from TBVs. The Main condenser provides condenser narrow and wide range pressure signals, from all shells of the condenser, to SB&PC.

7.7.5.7.2.3 Auxiliary Boiler (AUXB)

SB&PC sends signals to start the electric auxiliary boiler or increase its steam production rate upon 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 (10 CFR 50.2) Design Basis

Automatic Fixed In-Core Probe (AFIP) and Multi-Channel Rod Block Monitor (MRBM)

The NMS has two nonsafety-related subsystems, the AFIP subsystem and the MRBM subsystem. Neither the AFIP subsystem nor MRBM performs or ensures any safety-related function, and thus, the AFIP and MBRM subsystems have no safety design basis.

7.7.6.1.2 Power Generation (Non-Safety) Design Bases

AFIP

The AFIP has the following power generation design bases:

- Provide a signal proportional to the axial neutron flux distribution at the radial core locations of the LPRM detectors. This signal allows calibration of LPRM;
- 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
- Provide a totally automated mode of LPRM calibration by direct interface with the plant computer function of the N-DCIS.

MRBM

The MRBM has the following power generation design bases:

- Provide a signal to RC&IS to block rod movement if the MRBM signal exceeds a preset rod block setpoint to prevent fuel damage;
- Provide MRBM values to the N-DCIS;
- Provide bypass capability of one-out-of-two MRBM channels;
- Provide bypass of individual LPRM channels in its calculations;
- Provide online test and diagnostic capability to validate proper operation of its microprocessor-based system; and
- Provide rod block status to the main control room alarm system.

7.7.6.2 System Description

7.7.6.2.1 AFIP

7.7.6.2.1.1 General Description

The AFIP subsystem is comprised of 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 (7) gamma thermometer sensors evenly distributed across the LPRM assembly. Consequently, there are AFIP sensors at all LPRM locations. The AFIP sensor cables are routed within the LPRM assembly and then out of the reactor pressure vessel 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 that covers from approximately 1% to 125% of reactor rated power.

During core power and LPRM calibration, the AFIP signals are collected automatically to the AFIP data processing and control unit, where the data are properly amplified and compensated by applying correct sensor calibration adjustment factors. Such data are then sent to the plant computer function of the N-DCIS for core local power and thermal limits calculations. The calculated local power data are then used subsequently 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 operation principle, and its sensitivity does not depend upon fissile material depletion or radiation exposure. The gamma thermometer sensor, however, can be calibrated, either manually or automatically, by using a built-in calibration device inside the LPRM assembly. The calibrated new sensitivity data of the gamma thermometer sensors are stored in the AFIP control unit and are readily applied to the newly collected AFIP data to provide accurate local power information.

With its stable sensitivity and rugged hardware design, the AFIP sensor has a lifetime much longer than that of the LPRM detectors. 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 such that physical separation is maintained between the LPRM detectors and the AFIP detectors. The AFIP cables are also routed separately within the LPRM assembly from the LPRM detector cables, with separate external connectors. More descriptions of the AFIP is included in Reference 7.7.6-1.

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 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 in the areas it resides.

7.7.6.2.1.5 Operational Considerations

The AFIP is operated during reactor operation to provide local power information for three-dimensional power calculation 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 plant computer. Manual operation capability is available. The subsystem has no safety setpoints.

7.7.6.2.2 MRBM

7.7.6.2.2.1 General Description

The MRBM Subsystem logic issues a rod block signal that is used in the RC&IS logic to enforce rod blocks that prevent fuel damage by assuring 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 rod action and position information 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 will be issued. The MRBM monitors the core in 4-by-4 fuel bundle regions in which 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 at any one time, it is called the multi-channel rod block monitor. The MRBM is a dual channel system, but not classified as a safety 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. This nonsafety to safety interface is discussed in Subsection 7.2.2.4.

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 NMS subsystems. All interfaces with the safety NMS subsystems are via optical isolation.

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. The following analysis lists the applicable criteria and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

7.7.6.3.1 Specific Regulatory Requirements Conformance

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

Interface material is provided in Tier 1.

10 CFR 52.79(c), ITAAC in Combined Operating License Applications

ITAAC are provided for the I&C equipment in Tier 1.

7.7.6.3.2 General Design Criteria

Criteria: GDC 13, 19, and 24 apply.

Conformance: The AFIP and MRBM subsystems are in compliance with these GDC. Refer to Subsection 3.1.2 for a general discussion of the GDC.

7.7.6.3.3 Regulatory Guides

RG 1.180 – Guideliens for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems

RG 1.204 – Guidelines for Lighning Protection of Nuclear Power Plants.

Conformance: The system conforms to RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.

7.7.6.3.4 Branch Technical Positions (BTP)

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 to this BTP.

7.7.6.4 Testing And Inspection Requirements

7.7.6.4.1 AFIP

The gamma thermometer instrument (not including sensors) is 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 to the service personnel.

The gamma thermometer sensor is testable and able to be calibrated for its sensitivity. The AFIP instrument unit includes an algorithm that can automatically detect and reject failed AFIP sensor signals. It also includes a logic that can verify proper communication with the plant computer of the N-DCIS system.

The duration for gamma thermometer testing and calibration is based on the applicable NMS AFIP design document and the instruction manual of the AFIP subsystem. Additional information is provided in Reference 7.7-1.

7.7.6.4.2 MRBM

The MRBM subsystem is 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 to the service personnel.

It also includes a logic that can verify 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 of the MRBM subsystem.

7.7.6.5 Instrumentation Requirements

7.7.6.5.1 AFIP

The AFIP instrument is based on the digital measurement and control design practices that use digital design concepts and include microprocessor-based programmable and memory units.

The AFIP instrument follows a modular design concept such that each modular unit or its subunit is replaceable upon repair service.

The instrument has a flexible interface design to accommodate either metal wire or fiber-optic communication links.

The AFIP instrument is provided with necessary operator-interface functions based on adequate NMS man-machine interface requirements.

Basic Control Logic Requirements—The AFIP includes basic logics such as periodic demand for sensor calibration and data collection, as well as logic as part of the communication protocol with the plant computer function.

Basic Instrument Arrangement Requirements—The AFIP instrument cabinets are located in appropriate areas of the reactor building with physical and electrical separation from the safety-related NMS instruments, and with acceptable environmental conditions.

7.7.6.5.2 MRBM

The MRBM subsystem is based on the digital measurement and control design practices that use digital design concepts and include microprocessor-based programmable and memory units. The MRBM follows a modular design concept such that each modular unit or its subunit is replaceable upon 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 based on adequate NMS man-machine interface requirements.

Basic Control Logic Requirements—The MRBM includes basic logics such as continuous LPRM data collection, MRBM rod block algorithm calculation, MRBM setpoint comparison, and communication protocol with the N-DCIS.

Basic Instrument Arrangement Requirements—The MRBM subsystem is located within the nonsafety equipment rooms of the control building 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 would not adversely affect any safety-related system. Refer to Subsections 6.2.4 and 9.4.9.

7.7.7.3.1 Specific Regulatory Requirements Conformance

In accordance with Table 7.1-1, and SRP Section 7.7, the following criteria are addressed:

10 CFR 52.47 and 52.79

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.

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

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

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

Conformance: Interface material is provided in Tier 1.

52.79(c), ITAAC in Combined Operating License Applications

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

7.7.7.3.1.1 General Design Criteria

CIS meets the requirements of GDC 13, 19, and 24. Control and instrumentation is provided to operate the system, monitor process variables during startup, normal, and abnormal reactor operation. The CIS is operable from the main control room.

7.7.7.3.1.2 Regulatory Guides

In accordance with Table 7.1-1, there are no RGs directly applicable to the nonsafety-related CIS. However, the CIS instrument lines penetrating containment meet the requirements of RGs 1.11 and 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 main control room.

7.7.7.3.1.3 Branch Technical Positions

In accordance with Table 7.1-1, 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.

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 CIS system conforms to RG 1.180 and RG 1.204 as discussed in Subsection 7.1.6.

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 Requirements

7.7.7.5.1 Logic and Interlocks

The CIS operation is remote manually or automatically activated from the main control room by aligning corresponding valves through remote manual control switches.

During 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 sounds an alarm and 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 signal to isolate the nitrogen supply shutoff valve.

Upon completion of the initial inerting, CIS is manually or automatically aligned to 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 appropriate temperature by an electric heater. The electric heater 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, heater automatically cuts off electrical power feed into the heater elements.

The de-inerting process is manually or automatically activated, by aligning CIS to the Reactor Building HVAC to rid resident gases in the containment with breathable air supplied by the Reactor Building HVAC.

During primary containment isolation events, CIS primary containment isolation valves automatically close upon receipt of isolation signal from LD&IS. Details of the isolation logic are discussed in Subsection 7.3.2.

The CIS is capable of providing continued nitrogen makeup during isolation events. This is accomplished by overriding the isolation signal to the makeup isolation valves with controlled bypass switches.

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 CMS, are provided for monitoring containment pressure. These instruments provide input to the pressure controller to control makeup flow and provide alarm signals on a high drywell pressure condition.

Permanently installed temperature and humidity sensors are provided in several locations and elevations inside containment. These sensors are fed to the plant computer function for averaging and continuous monitoring of the containment.

Oxygen analyzers are provided to monitor oxygen levels in the containment during startup, normal, and abnormal plant operating conditions. Two sample points in each compartment (that is, upper drywell area, lower drywell area, wetwell air space) are provided (one in a high and one in a low location) on opposite sides of the compartment. Each air lock is also sampled. Oxygen levels in the CIS exhaust line are also monitored. A high oxygen level indication is alarmed in the main control room.

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) are also monitored. Total nitrogen flow indicates total containment atmosphere leakage during normal plant operation. Excessive leakage is alarmed in the main control room.

Separate flow metering devices are also provided to both drywell and wetwell inerting and de-inerting flows.

The CIS is described in Section 9.4.

7.7.7.5.3 Alarms and Indications

The following alarms and indications are also provided in the main control room:

- High drywell pressure,
- High 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," NEDC-33197P, Class III (GE Proprietary), July 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 (plant computer function)
Heatup & Pressurization	1. SRNM output (NMS) 2. Reactor water temperature (PGCS) 3. Reactor heatup schedule (Plant Computer Function) 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

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

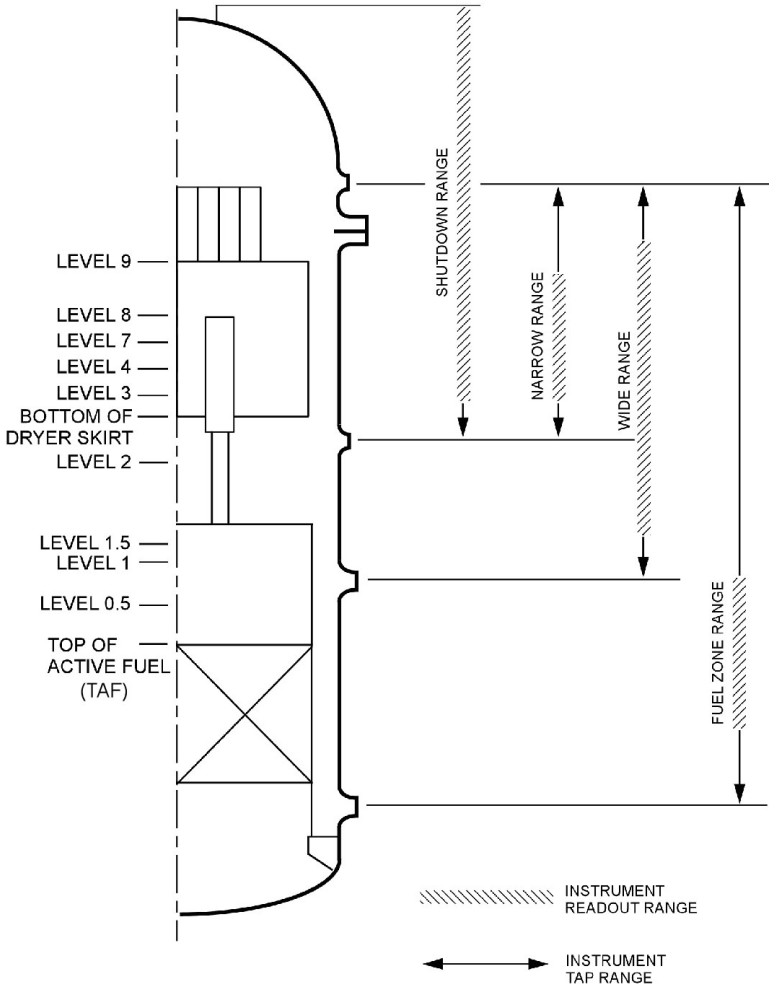
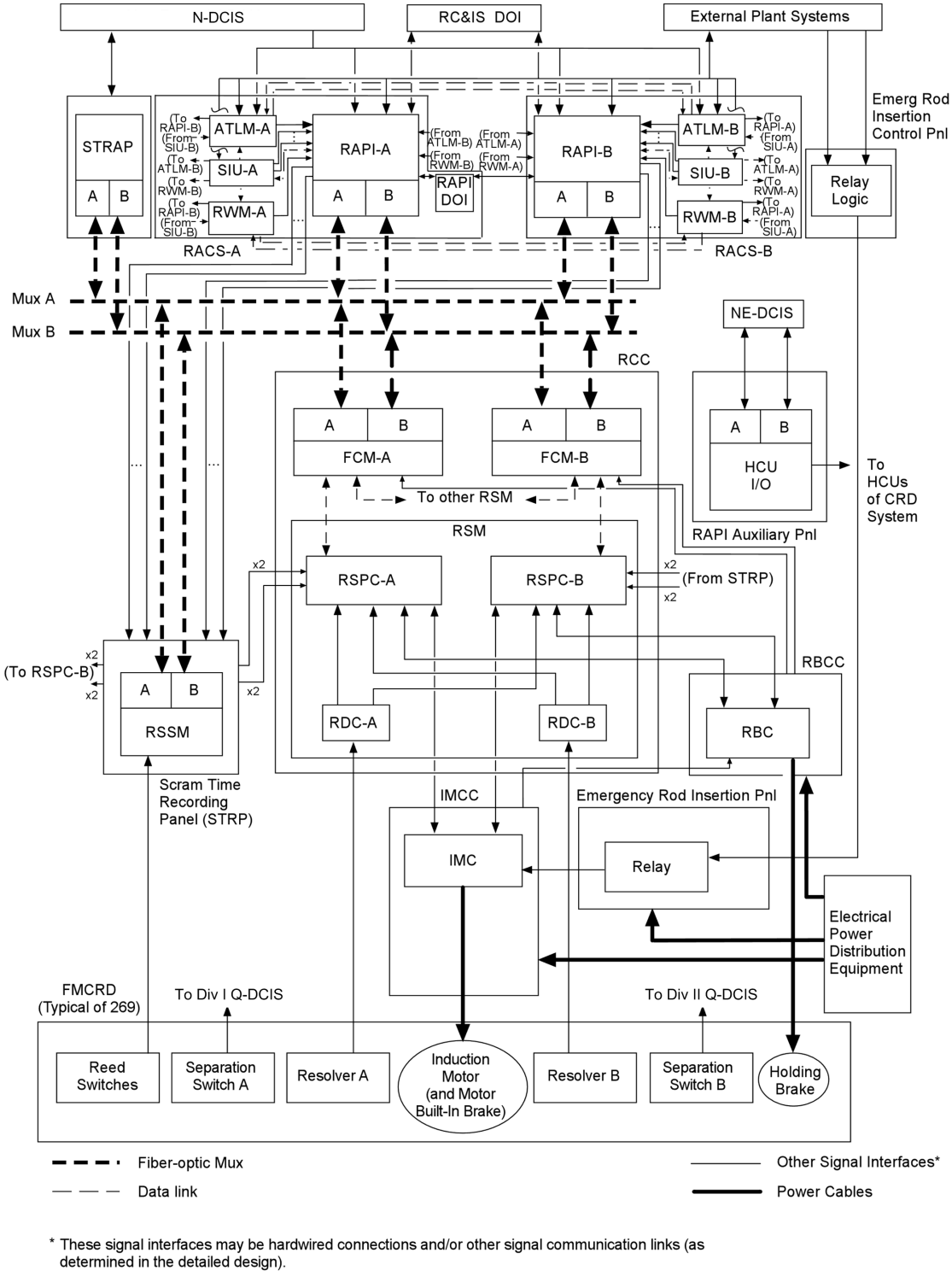


Figure 7.7-1. Water Level Range Definition



* These signal interfaces may be hardwired connections and/or other signal communication links (as determined in the detailed design).

Figure 7.7-2. RC&IS Block Diagram

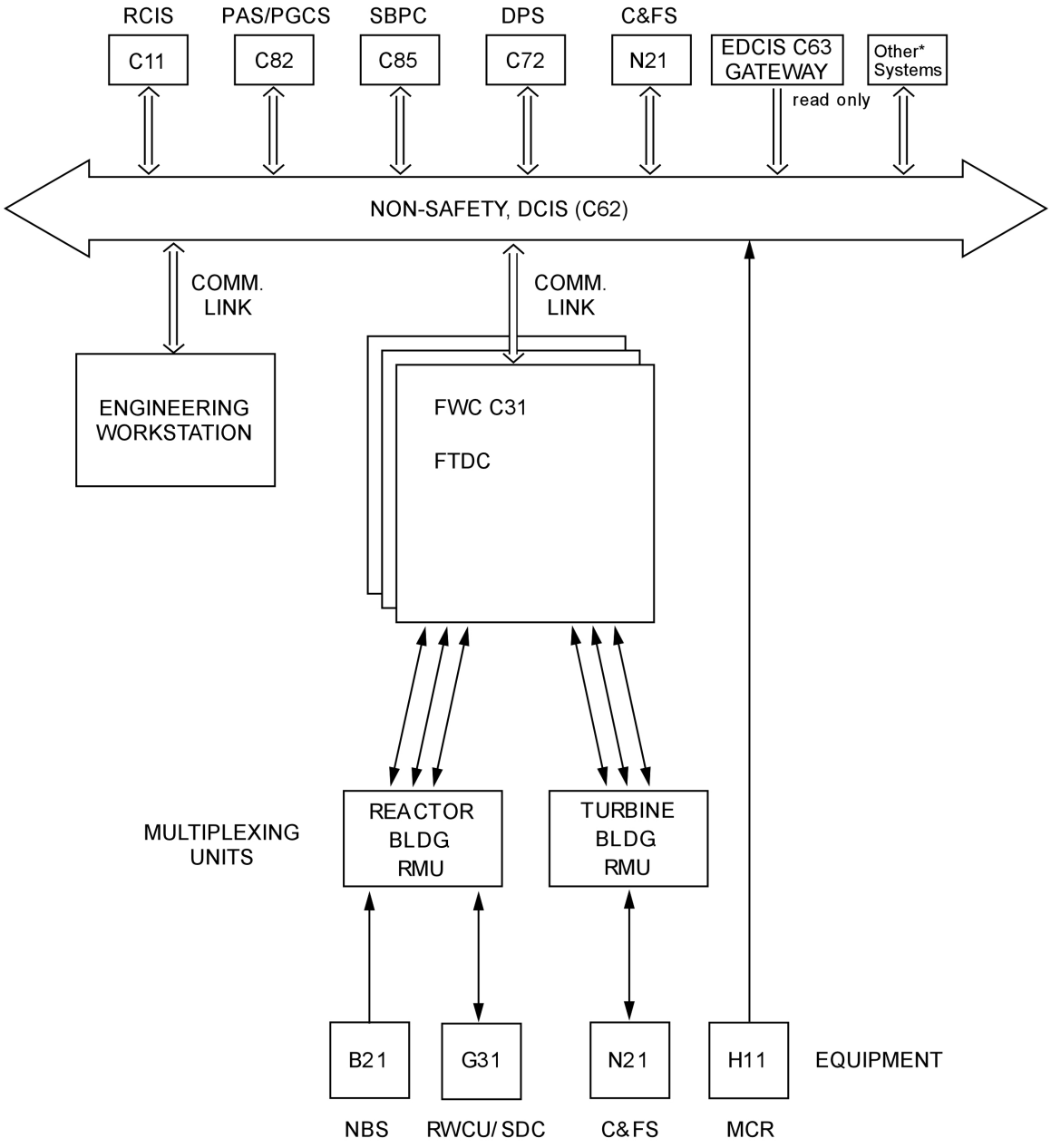


Figure 7.7-3. Feedwater Control System Functional Diagram

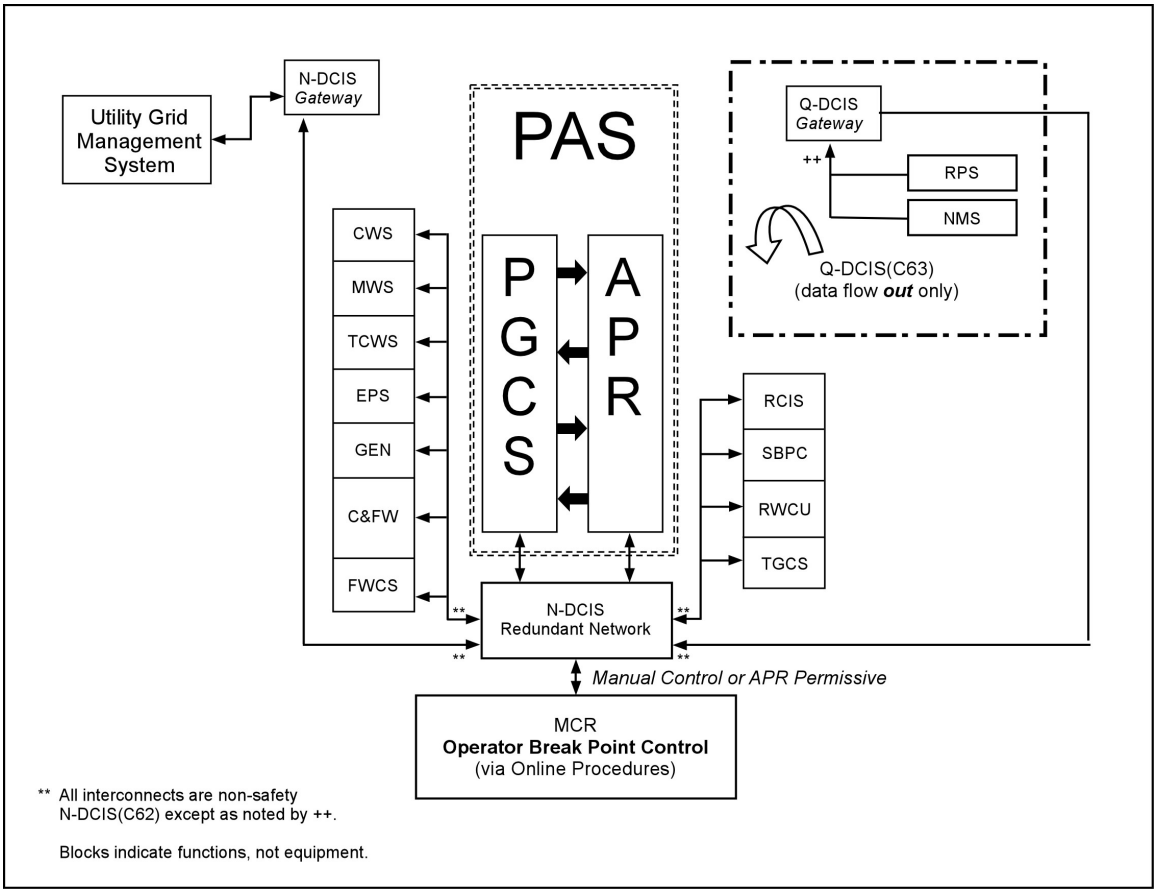


Figure 7.7-4. Plant Automation System Simplified Functional Diagram

(Only major systems are shown)

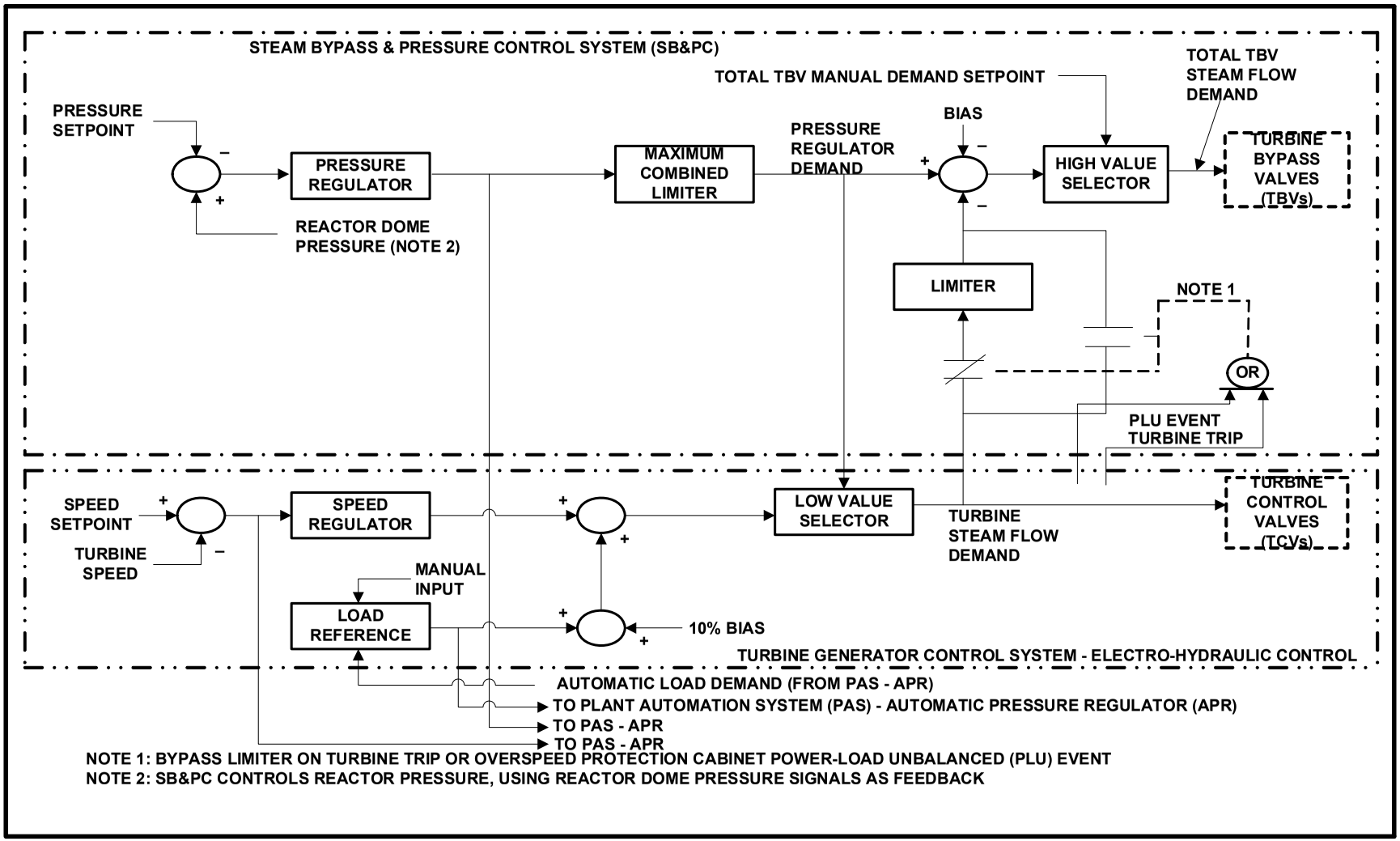


Figure 7.7-5. SB&PC Simplified Functional Block Diagram

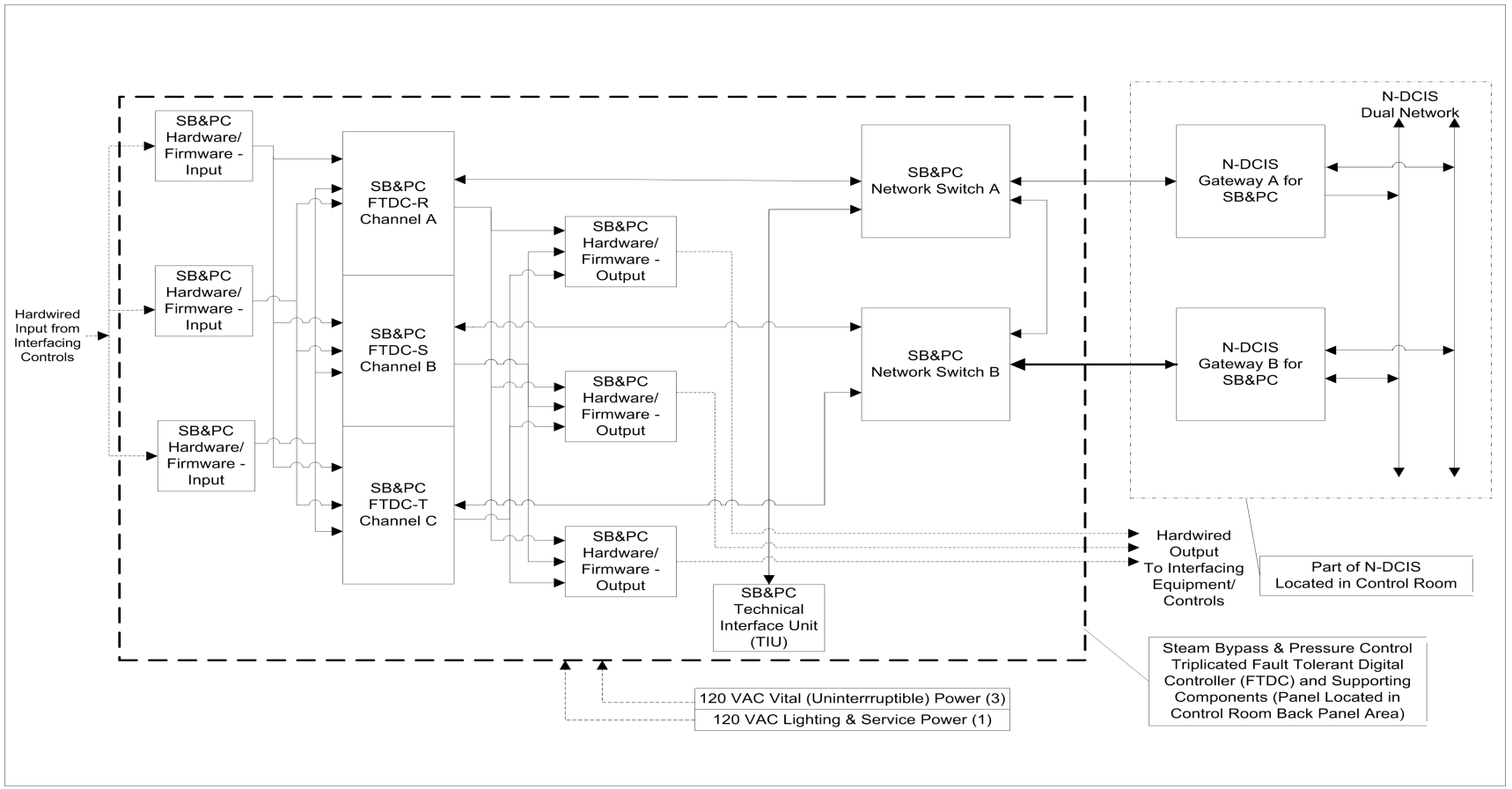


Figure 7.7-6. SB&PC FTDC Block Diagram

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. The diverse I&C systems are part of the ESBWR defense-in-depth and diversity strategy and provide diverse backup to the Reactor Protection System (RPS) and the Safety System Logic and Control for the 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 and nonsafety-related Distributed Control and Information System (that is, Q-DCIS and N-DCIS, respectively). The ATWS mitigation logic is applicable to Modes 1 and 2.

The nonsafety-related DPS (which is part of the N-DCIS) processes the nonsafety-related portions of the ATWS mitigation logic and is designed to mitigate the possibility of digital protection system common mode failures discussed in Item II.Q of Commission Paper (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).

The relationship 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 simple functional block diagram of the relationship between the ATWS/SLC and the Q-DCIS, the DPS, and the N-DCIS. Figure 7.1-2 provides a detailed functional network diagram.

The ATWS/Standby Liquid Control (SLC) mitigation logic provides a diverse means of emergency shutdown using the SLC 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 System (CRD), is also used for ATWS mitigation. This logic is implemented in the DPS. Detailed ATWS mitigation features are described subsequently.

The DPS is a nonsafety-related, triplicate 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 also provides diverse emergency core cooling by independently actuating the emergency core cooling systems. The DPS also performs selected containment isolation functions as part of the diverse ESF function. Additional DPS features are described in Subsection 7.8.1.2. The scope of DPS functions are based on the ESBWR defense-in-depth and diversity strategy outlined in Licensing Topical Report NEDO-33251, "ESBWR I&C Defense-In-Depth and Diversity Report."

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 both in the safety-related systems and in the DPS.

- Core makeup water capability from the feedwater, Control Rod Drive (CRD) System, and Fuel and Auxiliary Pools Cooling System (FAPCS) in Low Pressure Coolant Injection (LPCI) mode.

- Long-term shutdown capability is provided 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 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 via the SLC system.

- ATWS mitigation using ARI to hydraulically scram the plant using the three sets of air header dump valves of the control rod drive system.

- Select Rod Insert (SRI) to hydraulically insert selected control rods.

- Manual initiation capability of the ATWS mitigation functions (ARI/SLC/Feedwater Runback).

With the ATWS/SLC logic, random failures are mitigated by 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 such that another failure in a remaining division will not disable system operation.

7.8.1.1 ATWS Mitigation Functions

The following ATWS mitigation functions (Figures 7.8-2 and 7.8-3) 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 (that is, FMCRD Emergency Insertion), as shown in Figure 7.8-2, and also described in Subsection 7.7.2, associated with the RC&IS.
- Feedwater runback (FWRB), as shown in Figure 7.8-3 and described in Subsection 7.7.3.
- Inhibit of the Automatic Depressurization System (ADS) and GDCS injection as described in Subsection 7.8.1.1.2.
- ARI and diverse scram plus delayed feedwater runback for events where the RPS scram command has been unsuccessful to shutdown the reactor, or Selected Control Rod Run-In (SCRRI)/Select Rod Insert (SRI) has been unsuccessful in reducing reactor power to an acceptable level as described in 7.8.1.1.4).

7.8.1.1.1 ATWS Mitigation Logic of SSLC

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 (ATMs), instead of DTMs, 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. The hardware and software-based logic of this alternate emergency shutdown function is thus diverse from the hardware and software logic of the RPS function.

7.8.1.1.1.1 SSLC ATWS Logic Processors

There is an ATWS logic processor in each of four divisional RTIF cabinets (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 conditions and trips:

- Automatic initiation of the SLC boron injection:
  - High Reactor Pressure Vessel (RPV) dome pressure and a Startup Range Neutron Monitor (SRNM) ATWS permissive (that is, SRNM signal above a specified setpoint) for 3 minutes or greater, or
  - Low RPV water level (L2) and a SRNM ATWS permissive for 3 minutes or greater.
- Automatic initiation of feedwater runback:

- High RPV dome pressure and SRNM ATWS permissive. Reset 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 on data from ATMs and the Neutron Monitoring System (NMS).
  - Provides isolated hardwired contact closure outputs to SLC system and FWCS (via the DPS).

- ATWS Mitigation Logic Processor Data Handling:

  This device uses discrete gate logic and hardware timers to implement the ATWS mitigation logic. The input signals are hardwired (not multiplexed).

- ATWS Mitigation Logic Processor Status Monitoring and Communication

  Each ATWS mitigation logic processor division also has a programmable logical device, which is used to process the self-test logic. The self-test function is operator initiated and can only be performed with the associated ATWS mitigation logic division bypassed.

  ATWS mitigation logic processor status is transmitted via fiber optic cables to external interfaces.

- ATWS Logic Processor Alarms:
  - INOP (instrument inoperative) to N-DCIS (operating voltage degraded).
  - Division 1 (2, 3, 4) ATWS SLC system injection logic tripped.
  - Division 1 (2, 3, 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 SLC system and FWCS are hardwired (not 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 Inhibit of ADS

For ATWS mitigation, the Automatic Depressurization System (ADS), which is part of the Nuclear Boiler System, is inhibited automatically. Automatic initiation of ADS is inhibited based on the following signals.

- A coincident low RPV water level (L2) signal and Average Power Range Monitor (APRM) ATWS permissive signal (that is, APRM signal above a specified setpoint) from the NMS.
- A coincident high RPV pressure and APRM ATWS permissive signal persisting for 60 seconds.

There are MCR switches for the manual inhibit of 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 and power levels remaining elevated;
- SCRRI/SRI command and power levels remaining elevated; and
- Manual DPS scram signal.

Additionally, the DPS generates a signal to the Rod Control and Information System (RC&IS) to initiate electrical insertion (that is,FMCRD Run-In) of all operable control rods on signals initiating ARI described above.

This ARI and FMCRD Run-In logic reside in the DPS, which is totally separate and independent from the Q-DCIS with both 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 Logic for SRI and Scram and SCRRI/SRI ATWS Mitigation Logic

On either RPS scram command (two-out-of-four logic), or SCRRI/SRI command (two-out-of-three logic) and power levels remaining elevated, DPS will perform the following:

- Initiate a delayed diverse scram (and ARI as indicated previously)
- Initiate a delayed FWRB if the elevated power levels persist

On conditions requiring SCRRI (which is also processed as two-out-of-three logic) and power levels remaining elevated, DPS processes an SRI signal to hydraulically scram selected control rods.

A manual ATWS (ARI/SLC/FWRB) signal initiates the SLC system, initiates ARI, and initiates FWCS runback of feedwater flow. The manual initiation signal is safety-related and is sent to the nonsafety-related portions of the ATWS mitigation logic via qualified isolation devices.

7.8.1.2 Diverse Instrumentation and Control

In addition to the ATWS mitigation functions described previously, other diverse instrumentation and control functions are included in the DPS.

The DPS has a set of diverse reactor protection and diverse ESF logics, which are implemented using separate and independent hardware and software from that of the RPS and SSLC/ESF.

The DPS transmits the feedwater runback signal from the ATWS mitigation logic to the feedwater control system. The DPS also 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 are selected for inclusion in the DPS scope, which provide acceptable diverse protection results. This set of diverse protection logics for reactor scram, combined with the ATWS mitigation features and other diverse backup scram protection and diverse ESF functions, provides the necessary diverse protections to meet the required design position called out in SRM on SECY 93-087 and BTP HICB-19 (referenced in NUREG 0800 (SRP) Section 7). The following scram signals are selected for inclusion in the DPS:

- High RPV Pressure;
- High RPV Water Level (L8);
- Low RPV Water Level (L3);
- High Drywell Pressure;
- High Suppression Pool Temperature; and
- Closure of the MSIVs.

This diverse set of scram logics resides in independent and separate hardware and software equipment from the RPS. The process variables sensors that provide input to this diverse set of logics use different sets of sensors from that used in the RPS. The diverse logic equipment is nonsafety-related with triplicate redundant channels processing coincidence logic from four (4) 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 actuators applied at the return side of the 120 VAC circuit for the HCU scram pilot valve solenoids, whereas 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 triplicate redundant processors and sent via 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 manually scram from either hard-wired switches or the DPS VDU.

7.8.1.2.2 Diverse Engineered Safety Features (ESF) Functions

The ESBWR has several ESF functions including core cooling provided by the GDCS and SLC system and the ADS function using SRV and DPVs. It also has the pressure relief and core cooling function 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 (L1). 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 GDCS, SLC system, ICS and ADS (SRVs and DPVs). The DPS also provides the ability to generate a diverse manual ECCS actuation from the DPS VDU.

This set of nonsafety-related diverse ESF logics resides in separate and independent hardware and software equipment 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 triplicate 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 triplicate 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 a diverse ECCS actuation. The logic for the DPV's is slightly different and is described subsequently. Figure 7.8-4 shows the DPS triplicate 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 each of all 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 7.3.1.1 and 7.3.4, 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 triple

redundant logic path to initiate the DPV squib valve opening. This satisfies the single failure criteria 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. The GDCS squib valves (short term injection) 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 which 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 there is a dual logic path, not triple. However, the SLC system squib valves are actuated by two independent safety-related divisions each, with one valve per loop also being actuated by the DPS. This configuration allows the flow path of both SLC system loops to be available via activation from the DPS and from any safety related division (refer to Subsection 7.4.1.2 for a description of the SLC system logic and squib initiator power assignments).

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 will also provide 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 also “energize to actuate.”

- Closure of the MSIVs on detection of high steam flow, low RPV pressure, or low RPV water level (L2). The isolation function will be 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 RWCU/SDC isolation valves on high differential flow.
- Isolation of the Feedwater System on a feedwater line break inside containment (sensed by differential pressure between feedwater lines coincident with high drywell pressure) by tripping the main feedwater pump adjustable speed drive motor circuit breakers and closing the feedwater containment isolation valves.

The following additional functions are performed by the DPS:

- Similar to the logic in the SSLC/ESF, the DPS will initiate the ICS on low RPV water level (L2) or MSIV closure to provide core cooling.
- The DPS will runback the feedwater pumps on high RPV water level (L8). If level continues to increase, the DPS will trip the feedwater pumps (L9).

The diverse protection logics for ESF function initiation, combined with the ATWS mitigation feature, other diverse backup scram protection and selected diverse RPS logics, provide the diverse protection necessary to satisfy the design position called out in BTP HICB-19.

7.8.1.3 Diverse Manual Controls and Displays

All safety-related systems have displays and controls located in the main control room that provide for 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 which are independent from those of the safety-related protection and SSLC/ESF functions, and 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 respectively.

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
- ICS operation

In addition to the controls provided by the primary safety-related systems, the RSS also 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 inclusion of the DPS, techniques that are employed to ensure safety-related system reliability by minimizing both random and common mode failure probabilities are outlined below:

- The total amount of hardware is minimized.
- Microprocessors with a simple operating system are used.
- The highest quality components are used to gain reliability.
- Self-diagnostics are implemented.
- The man-machine interface is implemented such that the equipment is structured into small units, with enough diagnostics so that a user can repair equipment by replacing modules and 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, which perform setpoint comparison, voting, and interlock logic.
  - Code for calibration, signal I/O, online-diagnostics, and graphical displays is 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 are used to aid in verification and validation (V&V).

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 dicscussed in Appendix B.

7.8.2.2 System 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;
- Input and Output signal processing; and
- Self-test.

The development of common software modules for many of these functions has the following advantages in producing reliable programs:

- Promotes standardization and code reusability;
- Minimizes program design errors; and
- Minimizes timing differences among channels.

The V&V program, which is discussed in Appendix 7B, reduces the probability of common mode failure to a very low level because 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, as follows:

7.8.2.2.1 System level defenses against common mode failure

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 unless a permanent fault is detected, thereby causing the channel to alarm and trip (for the RPS and MSIV isolation functions).
- Continuous cross-checking of redundant sensor inputs.

- Continuous surveillance of trip functions on-line with divisional bypass capability for the RPS and MSIV isolation functions.
- Continuous self-test with alarm outputs in all system devices.

Functional defenses

- Automatic error detection permits early safe shutdown or bypass before common mode effects occur. Instantaneous, simultaneous, and undetected failure on a common mode error is unlikely.
- Separation and independence requirements protect against global effects (EMI, thermal, etc.)

Software defenses against common mode failure

The functional program logic in the RPS and SSLC/ESF controllers also provides protection against common mode failures, as follows:

- Redundant sensors have data messages with unique identifications in each division.
- Modules that are identical are simple functions such as setpoint comparison and two-out-of-four voting that can be readily verified.
- Multiplexing and other data transmission functions use standard protocols that are verified to industry standards and are also qualified to safety-related standards.

7.8.2.3 Safety-Related System Defense Against Adverse Interaction With The DPS

The DPS is designed as a highly reliable nonsafety-related system that meets the ESBWR probabilistic risk assessment requirements to minimize failures on demand, and to minimize inadvertent operation. The DPS components are designed to ensure the reliability goals and system design requirements are met. The DPS sensors and actuation devices which interface directly with safety-related 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 also designed to avoid adverse interaction with the protection systems with which DPS interfaces. Since the DPS logic does not communicate with the RPS logic, credible DPS failure modes do not prevent the RPS from performing a reactor trip and 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.

7.8.3 Specific Regulatory Requirements Conformance

For diverse instrumentation and controls, Table 7.1-1 identifies the associated codes and standards applied in accordance with the SRP. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the requirements conformance for each.

7.8.3.1 10 CFR Parts 50 and 52

10 CFR .55a(a)(1), "Quality Standards."

Conformance: The diverse instrumentation and controls are in conformance with this requirement.

10 CFR50.55a (h) “Protection and Safety Systems,” compliance with IEEE Std. 603

Conformance: For the diverse instrumentation and controls, the applicable requirements are from IEEE Std. 603: Item 5.6, ‘Independence’. The transmission of signals between the divisional equipment of protection systems (that is, RPS and ESF systems) or between divisional equipment of ATWS/SLC is performed via fiber optic cables. 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 instrumentation and controls has electrical surge withstand capability and can withstand the electromagnetic interference, radio frequency, and electrostatic discharge conditions that exist where the diverse instrumentation and controls equipment is located in the plant.

The diverse instrumentation and controls equipment can withstand the room ambient temperature, humidity conditions, radiation levels, and seismic accelerations at the mounting locations that will exist at the plant locations in which the diverse instrumentation and controls equipment is located at the times for which the diverse instrumentation and controls equipment is required to be operational or not to fail in a negative manner

10 CFR 50.62, “Requirements for reduction of risk from ATWS events for light-water cooled nuclear power plants.”

Conformance: The ATWS mitigation functions as 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 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 subection.

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

Conformance: The level of detail provided for this diverse I&C functions within the Tier 1 and Tier 2 documents conforms to this requirement.

7.8.3.2 General Design Criteria

In accordance with Table 7.1-1 and with the SRP for Section 7.8 the following GDC are addressed for the diverse instrumentation and controls:

Criteria: GDC, 1, 13, 19, and 24.

Conformance: The diverse instrumentation and controls are in conformance with the GDC identified above.

The design of the diverse instrumentation and controls also 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 Commission Papers (SECY) and Staff Requirements Memoranda (SRM)

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 instrumentation and control 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, conform with the above SRM requirements.

7.8.3.4 Regulatory Guides

In accordance with Table 7.1-1 and with the SRP for Section 7.8 the following Regulatory Guides are addressed as guidelines to Section 7.8, which includes the DPS and ATWS safety-related functions:

- RG 1.22 – (Safety Guide 22) Periodic Testing of Protection System Actuation Functions
- RG 1.29 - Seismic Design Classification
- RG 1.62 - Manual Initiation of Protection Actions
- RG 1.75 - Physical Independence of Electric Systems

- RG 1.105 - Instrument Setpoints for Safety Systems
- RG 1.118 - Periodic Testing of Electric Power and Protection Systems
- RG 1.152 – Criteria for Digital Computers in Safety Systems of Nuclear Power Plants
- RG 1.153 – Criteria Power Instrumentation and Control Portions of Safety Systems
- RG 1.168 - Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.170 - Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants
- RG 1.171 - Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants
- RG 1.172 - Software Requirements Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants
- RG 1.173 - Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants
- 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

7.8.3.5 Branch Technical Position (BTPs)

In accordance with Table 7.1-1 and with the SRP for Section 7.8 the following BTPs are considered applicable and addressed as guidelines to Section 7.8, which includes the DPS and ATWS mitigation functions:

- BTP HICB-8 - Guidance on Application of RG 1.22
- BTP HICB-11 - Application and Qualification of Isolation Devices
- BTP HICB-12 - Establishing and Maintaining Instrument Setpoints
- BTP HICB-14 - Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- BTP HICB-16 - Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
- BTP HICB-17 - Self-Test and Surveillance Test for Digital Computer-Based Instrumentation and Control Systems

- BTP HICB-18 - Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
- BTP HICB-19 - Evaluation of Defense in Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems
  - Licensing Topical Report NEDO-33251, "ESBWR I&C Defense-In-Depth and Diversity Report," details the echelons of defense used in the ESBWR 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 is performed to ensure the radiation limits derived 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

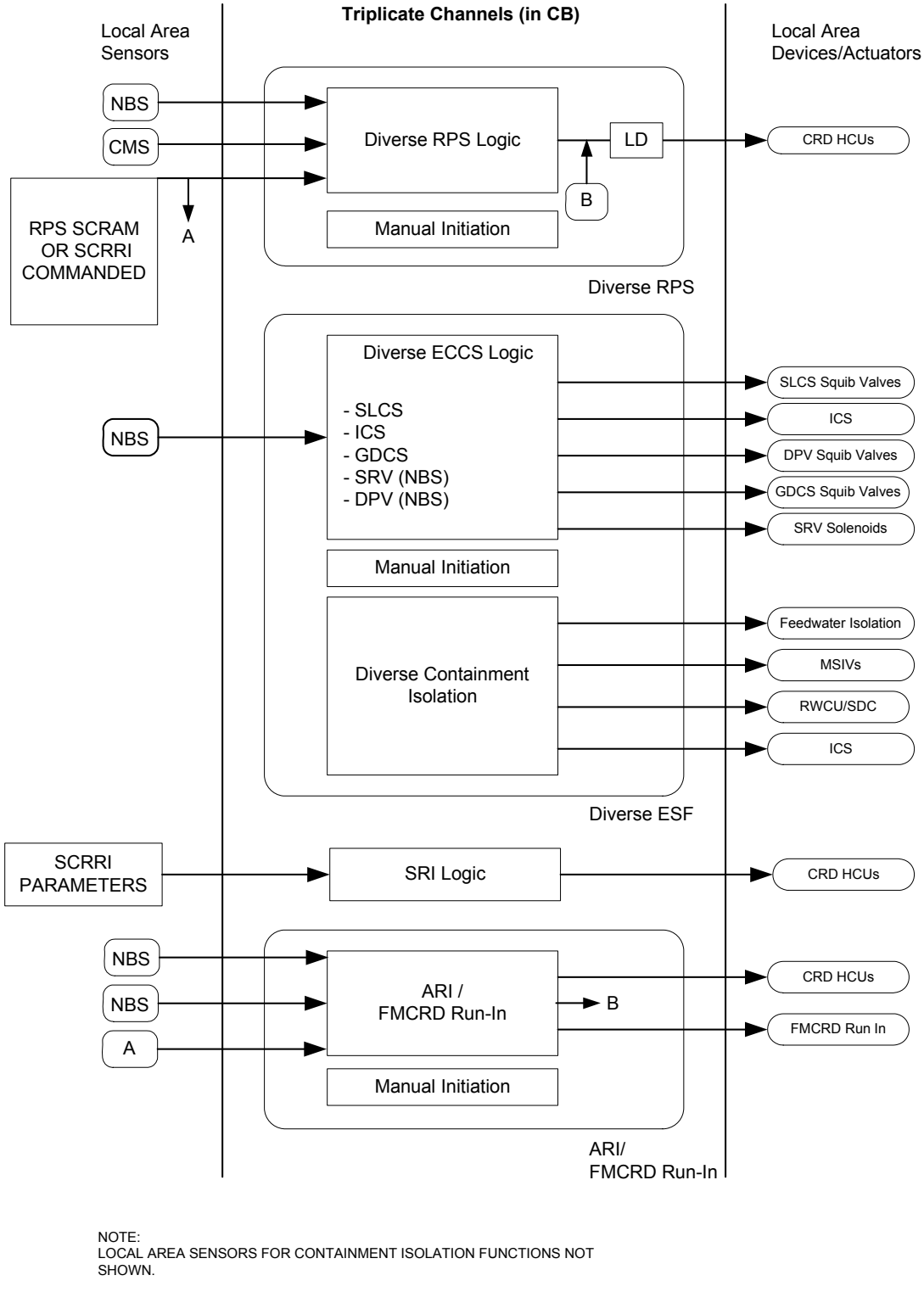
7.8.4 COL Information

None

7.8.5 References

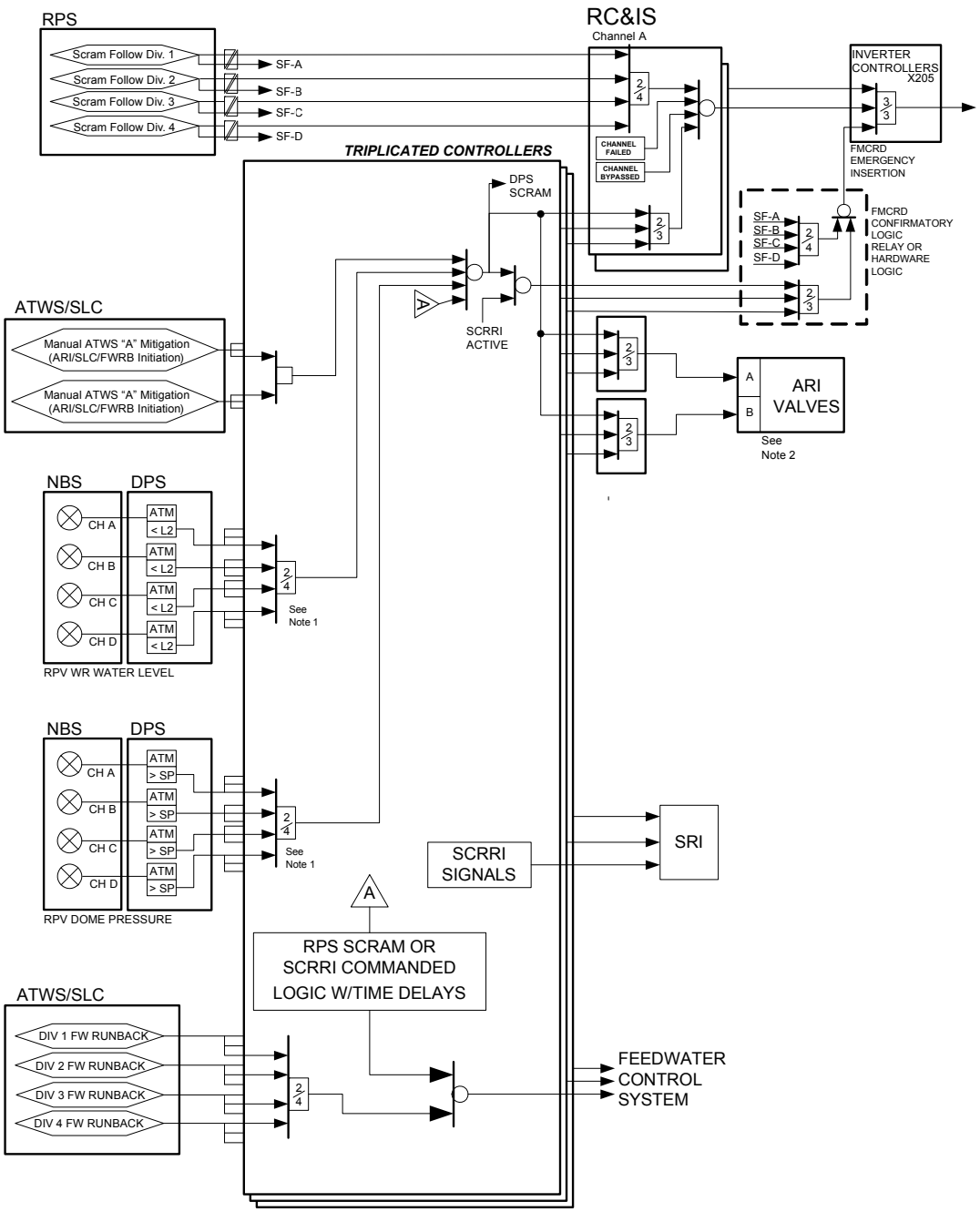
7.8-1 GE Nuclear Energy, ESBWR I&C Defense-In-Depth and Diversity Report, NEDO-33251, Class I (Non-proprietary), Revision 0, July 2006.

7.8-2 NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection systems, December 1994



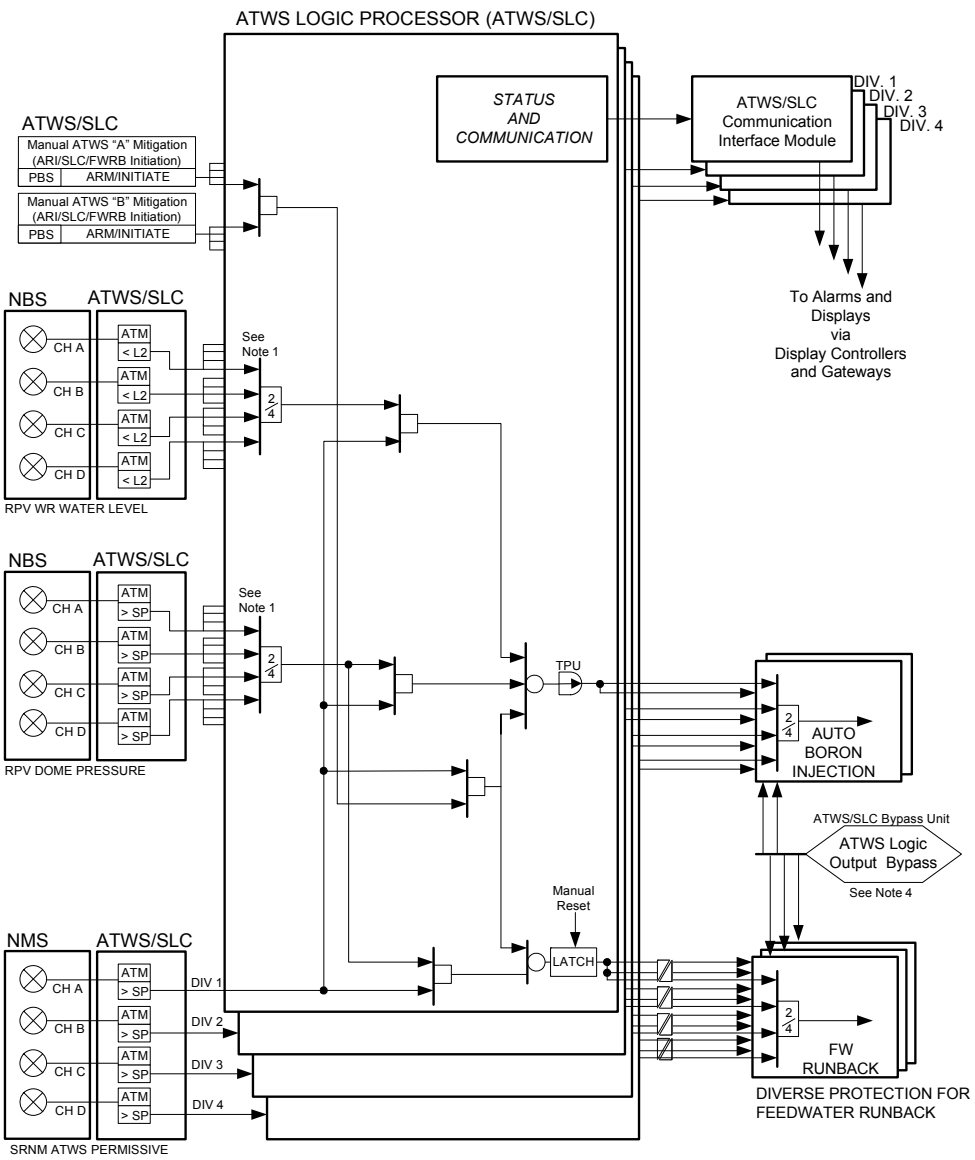
NOTE:
LOCAL AREA SENSORS FOR CONTAINMENT ISOLATION FUNCTIONS NOT SHOWN.

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. Non safety 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)

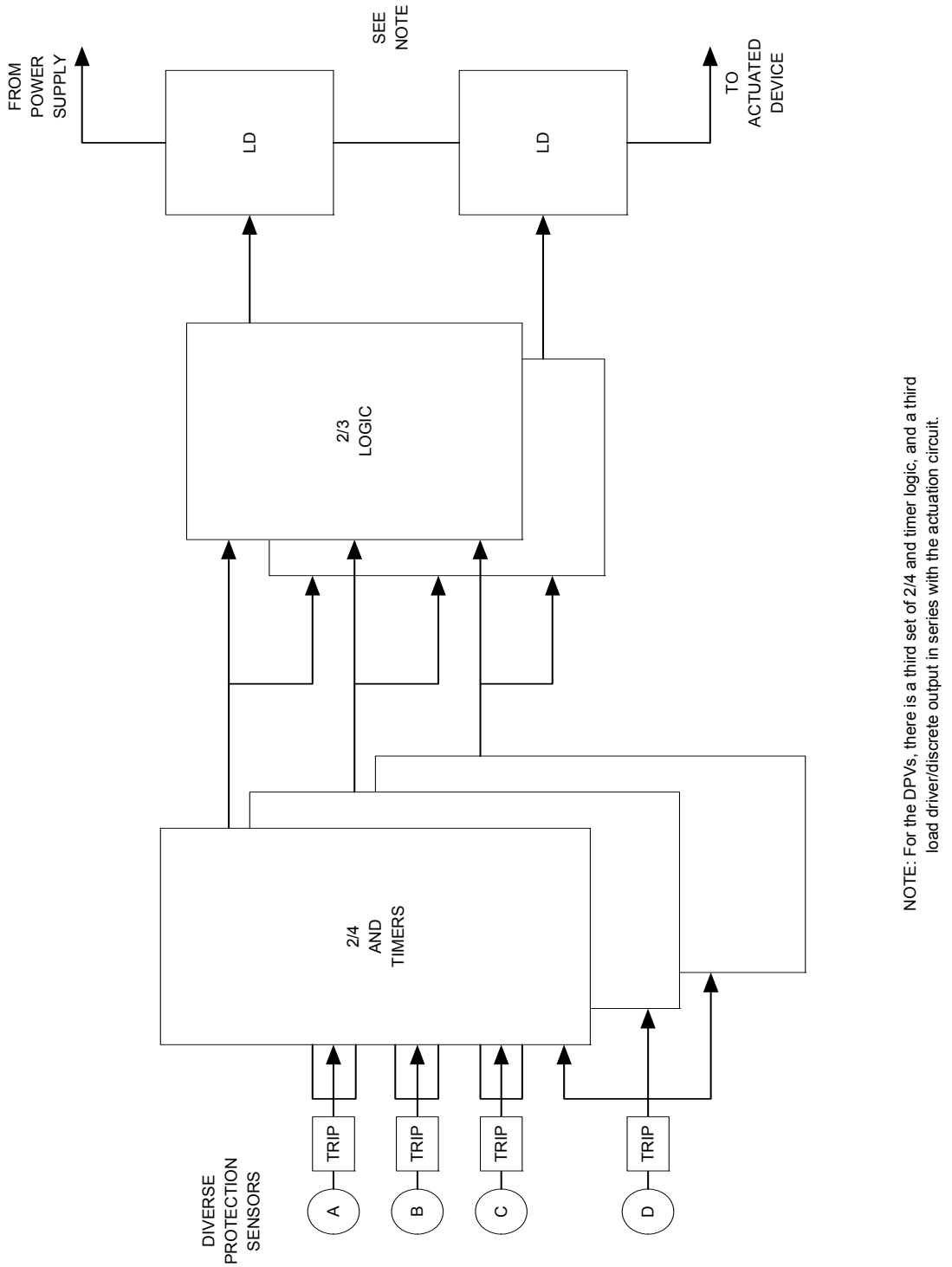


Figure 7.8-4. Diverse ESF TMR Logic

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. THIS SECTION DELETED

7B. SOFTWARE QUALITY PROGRAM FOR SOFTWARE DESIGN AND DEVELOPMENT

This section summarizes the managerial, design and development and software quality assurance requirements for Digital Computer-based Instrumentation and Control (I&C) software for the ESBWR project.

The ESBWR computer-based safety-related control system designs conform to RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (see Reference 7B-2). Conformance with RG 1.152 is twofold: one comprises the functional and design requirements of computers used in safety systems of nuclear power plants, and the other comprises security of various hardware, controls and data networks with safety-related systems, as described in DCD/Tier 2, paragraph 7.1.6.4. Cyber security program is described in NEDO-33295, "ESBWR – Cyber Security Program Plan" Licensing Topical Report (LTR). The software process plans will refer to the cyber security program plan for development, operation and maintenance of safety-related software that, as stated above, conforms to RG 1.152. RG 1.152 endorses IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (see Reference 7B-9), for the functional and design requirements of computers used in safety systems of nuclear power plants. IEEE Std 7-4.3.2 does not provide guidance regarding security measures for computer-based system equipment and software systems. However, RG 1.152 provides specific guidance concerning computer-based (cyber) safety system security to supplement the lack of guidance in IEEE Std. 7-4.3.2. The functional and design requirements of the safety-related systems conform to IEEE Std. 7-4.3.2, and these requirements comprise the hardware and software designs.

Branch Technical Position HICB-14 (BTP 7-14) (see Reference 7B-1) outlines the many activities to be considered when constructing a design development and quality assurance program for the computer-based I&C product, herein referred to as a software-based product. BTP 7-14 documents these activities as eleven software development groups. The overall guidance from BTP 7-14 is that the software planning documents should encompass all of the topics. In this appendix, the eleven software development groups are documented in two overall software (SW) plans. According to BTP 7-14, a separate document need not be developed for each of the software development topics, provided that the required information is included in one of the SW plans. The SW plans are in a hierarchy under the ESBWR Man-Machine Interface System and Human Factors Engineering (MMIS/HFE) Implementation Plan (see Reference 7B-24).

The ESBWR SW plans address the software quality assurance requirements specified in selected RGs and industry standard guidance documents . In certain cases, deviation has been taken from the detailed requirements described in the guidance documents, in which case the process outlined in this appendix is followed. This appendix summarizes the SW development activities to be implemented for ESBWR safety-related software-based products. The ESBWR SW plans are:

- "ESBWR I&C Software Management Plan" Licensing Topical Report (LTR)
- "ESBWR I&C Software Quality Assurance Plan" LTR (See Section 7B-7)

Documentation of the conformance to BTP 7-14, Regulatory Guides, IEEE Standards and other applicable guidance documents will be included in the SW plans delivery scheduled per Reference 7B-27, "ESBWR Software Plans Revision Submittal Schedule".

Inspections, tests, analyses, and acceptance criteria (ITAAC) associated with the SW plans are identified in ESBWR DCD Tier 1 document.

7B.1 "ESBWR I&C SOFTWARE MANAGEMENT PLAN" LTR

The "ESBWR I&C Software Management Plan" LTR contains the following plans:

- Software Development Plan (SDP) (See Section 7B.2)
- Software Integration Plan (SIntP) (See Section 7B.3)
- Software Installation Plan (SIP) (See Section 7B.4)
- Software Training Plan (STrngP) (See Section 7B.5)
- Software Operations and Maintenance Plan (SOMP) (See Section 7B.6)

The SMP describes the management aspect of the design and development activities that produce the software-based products for the ESBWR. The management process follows the guidance provided in IEEE Std. 1058.1, "IEEE Standard for Software Project Management Plans" (see Reference 7B-20). The SMP provides:

- Description of the project organization, which includes the description of responsibilities of each individual for carrying out the project planning activities and the design and development activities for the software-based product for this ESBWR project.
- Description of the organizational structure. The design organization is independent from the Software Quality Assurance (SQA) organization. The ESBWR project organization chart is depicted in the MMIS/HFE Implementation Plan.
- The management activities, which include:
  - Management of the overall software development process;
  - Coordination between ESBWR design organization and interfacing organizations, including suppliers participate in the design and development of the software-based products;
  - Establish plans of resources and staffing, qualifications and training of project personnel;
  - Establish schedules and milestones for project deliverable and work package, including financial resources needed to execute the project. (Note: The financial records are GE proprietary information, thus, the GE policies and procedures used in controlling financial budget is referenced by the LTR, methods and strategies will not be described in the LTR);

- Develop the mechanism to track and report progress;
- Description of the methods, techniques and tools used;
- Software developed by subcontractors;
- Procedures to be used in the software development; including interrelationships between software design activities;
- Security to provide assurance that the integrity of the software-based product is maintained, and to provide methods to be used to prevent contamination of the developed software by viruses;
- System for collection of software metrics and using them to improve processes and software quality; and
- Risk management to identify, assess, control and mitigate project risks.

The Software Management Plan is used to guide, monitor and control the following project management, design and development activities and as such may be updated throughout the course of the project.

7B.2 SOFTWARE DEVELOPMENT PLAN

The Software Development Plan (SDP) defines the technical processes necessary to accomplish the design and development of the ESBWR software-based products. This SDP meets the intent of RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power" (see Reference 7B-8). RG 1.173 endorses IEEE Std. 1074, "Standard for Developing Life Cycle Processes" (see Reference 7B-21), which this SDP uses as a guide. The SDP addresses:

The applicable company policies and procedures, industry codes and standards; and regulatory guidelines to be followed during the design and development of ESBWR software-based products;

The software engineering process, which is composed of the following life-cycle phases:

- The Planning Phase. The planning phase design activities address the following system design requirements and software development plans:
  - Evaluation of technical design inputs, such as system requirements
  - Preparation of Software Management Plan
    - Software Development Plan
    - Software Integration Plan
    - Software Installation Plan
    - Software Operations and Maintenance Plan

- Software Training Plan

- Preparation of Software Quality Assurance Plan (See Section 7B.7)
  - Software Verification and Validation Plan (See Section 7B.8)
  - Software Safety Plan (See Section 7B.9)
  - Software Configuration Management Plan (See Section 7B.10)
- The Requirements Phase. The Requirements Phase design activities address the development of the software-based products design and configuration requirements in accordance with RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (see Reference 7B-7). RG 1.172 endorses IEEE Std 830, "IEEE Recommended Practice for Software Requirements Specifications" (see Reference 7B-14), which provides an acceptable approach for specifying software requirements. The design and review activities are documented in the following documents and drawings, analysis and review reports:
  - Software Requirements Specification (See Table 7B-1)
  - Hardware/software specification
  - User's manual
  - Data communications protocol
  - Software Safety Analysis of the software requirements and
  - Disposition of design and/or documentation non-conformance identified during this phase.
- The Software Design phase. The Software Design phase addresses the design of the software architecture the configuration of software requirements into well-structured components, and the definition of software module functions. IEEE Std. 1016, "IEEE Recommended Practice for Software Design Descriptions" (see Reference 7B-17), which provides an acceptable approach for preparing software design specification. The design and review activities are documented in the following documents, analysis and review reports.
  - Software Architecture Description if applicable (See Table 7B-2)
  - Software Validation Test plan and test procedure
  - Coding style guide
  - Software Design Specification (See Table 7B-3)
  - Software Safety Analysis of the software design

- Disposition of design and/or documentation of non-conformances identified during this phase.

- The Software Implementation Phase. The Software Implementation phase activities address software implementation, which includes, software code review, software integration process and software functional testing of software design. Software functional testing includes software module/unit testing and software integration testing. Software module/unit testing is conducted to ensure software module/unit or group of software modules/units executes as specified in the software design specification. Software module/units testing is conducted in accordance with RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Reference 7B-6), which endorse IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing" (see Reference 7B-15). Software integration testing is conducted to evaluate the performance of the integrated software modules/units. The implementation and review activities are documented in the following documents, analysis and review reports:

  - Software source code listings (See Table 7-4)
  - Software functional test reports
  - Software Safety Analysis of the software coding
  - Disposition of non-conformances identified in this phase's design documentation and test results.

- The Test Phase. Test phase addresses the software validation testing activities. Software validation testing is conducted to demonstrate that integrated software-packages is operational and conforms to the intended functional and performance requirements, and performs no unintended functions. The test and review activities are documented in the following analysis and review reports:

  - Software Validation test procedures
  - Software Validation test reports
  - Description of the validated software/System Build Documents (See Table 7B-5)
  - Software Safety Analysis of the validation test results
  - Disposition of non-conformances identified in this phase's design documentation and test results, and
  - Set of indicators is collected during software validation testing to determine the success or failure of the technical aspects of the development process and the resulting design outputs.
  - The Installation Phase. The Installation phase activities involve procedures and guidelines necessary to physically install the validated (released/production)

software. The installation and review/checkout activities are documented in the following analysis and review reports:

i. Software Installation Procedures

ii. Software Installation and Checkout Report

iii. Installation Configuration Tables (See Table 7B-6)

iv. Operations-Maintenance Manuals (See Table 7B-7)

v. Training Manuals (See Table 7B-8)

– The Operation and Maintenance Phase. The Operation and Maintenance Phase occurs during the functional and operational life of the software-based product. The use, operation, maintenance, calibration, surveillance, and other processes associated with use of the software-based product are provided in the Operation and Maintenance Manual. Maintenance of the software includes performing troubleshooting when abnormal conditions occur and procedures to correct the identified anomalies. Software modification is performed in accordance with an established configuration change control process and V&V, software testing shall be re-performed on the revised software.

– The Retirement Phase. The Retirement phase is initiated when a Software-based product (software and hardware components) is no longer supported or has become obsolete. The equipment operating authority shall assess the effect of replacing or removing the existing system from the operating environment. This scope of assessment shall include the effect on safety and nonsafety system interfaces resulting from removing the system functions. The methods by which a change in the safety system security functions is mitigated (for example, replacement of the security functions, isolation from other safety systems and licensee interactions, or retirement of the safety system interfacing functions) shall be documented. The security procedures shall include cleansing the hardware and data by data cleansing, disk destruction, or complete overwrites.

7B.3 SOFTWARE INTEGRATION PLAN

The Software Integration Plan (SIntP) summarizes the management, implementation, resource characteristics and testing of the integration program. The SIntP provides:

Description of the purpose, organization, and responsibilities:

- Software integration and the hardware/software integration process and test to be conducted to ensure the final software-based product performs as intended.

- Software integration organization, including the authority and responsibilities of the individual responsible for the integration activities, boundaries between the software integration organization and other organizations (that is, Quality Assurance, Configuration Control Management, suppliers), as well as reporting channels.

Description of the measurement and procedures:

- Measurement of the implementation of the integration effort.
- Data collection and analysis associated with the integration of the software and of the hardware/software combination, to determine the adequacy of the integration effort.
- Methods, strategies and controls for software integration and combined hardware/software integration. This includes the design outputs and reports, and documentation describing the software integration tests and the hardware/software integration tests.

Description of the methods and integration tools appropriate to the safety significance of the software, which is to be created using the tools.

Description of integration test activities. System acceptance testing is conducted to validate that the software-based product has been correctly configured, calibrated and performed as designed. System acceptance testing is conducted in accordance with the system test plan. The description of test activities included in the system test plan includes:

- The test organization, which includes the description of responsibilities of each individual for carrying out each test activity
- Test management, such as, but not limited to, schedule, resources, security, risks and contingency planning, anomaly and problem reporting, and training needs
- Scope of the equipment to be tested
- Definition of the test guidelines for:
    i. Test preparation to assure that the required test activities can be properly carried out within the project schedule. This is accomplished by identification of resources, including applicable tools and environmental conditions required to support the development, execution, and the documentation of the test.
    ii. Test design to specify the test methods and test strategies (acceptance criteria, test techniques and test approaches) to assure completeness of the test coverage.
    iii. Test execution to analyze the test item in order to evaluate each identified feature or combination of features to determine if the feature or combination of features are passed or failed based on the defined acceptance limits.
    iv. Test summary to summarize the results of the designated testing activities and to provide evaluations based on these results.

    – Definition of the required test documentation, such as test plan, test procedures and test cases, and test summary and anomaly reports. Test documentation is prepared to meet the intent of RG 1.170, “Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants” (Reference 7B-5). RG 1.170 endorses IEEE Std. 829, “IEEE Standard for Software Test Documentation” (see Reference 7B-13), which is used as guide to prepare the test documentation.

– Measurement system for error tracking and resolution, and to assess the success or failure of the test effort.

7B.4 SOFTWARE INSTALLATION PLAN

The Software Installation Plan (SIP) summarizes the management, implementation, and resource characteristics of the installation program.

Description of purpose, organization and responsibilities:

- The installation process, the goals of that process, as well as the eviromental conditions within which the software-based product is qualified to operate.
- The installation organization, including the boundaries between the software installation organization and the broader safety system installation organization.
- Responsibilities and authority of the installation organization.

Description of measurement and procedures includes:

- Measurement implementation of the installation effort, including installation data collection and analysis.
- Procedures, methods, and controls for installation activities. This includes checking procedures for proper system and inputs/outputs functionality, installation of correct software version, installation anomalies, testing, etc.

Description of methods and tools includes:

- Methods, techniques and tools to be used to accomplish the installation activities, as well as the qualification of the required tools used to support the installation effort.

7B.5 SOFTWARE TRAINING PLAN

The Software Training Plan (STrngP) describes the management, implementation, and resource characteristics of the STrngP. The STrngP defines:

Description of the organization supporting the software-based product training effort.

- Organizational interfaces and responsibilities, the qualification and responsibilities of individual carrying out each training module and personnel assignments for performing the training. The qualified trainers must be knowledgeable in the operation of software-based product.
- The authority and responsibilities of the individual responsible for the training program. Depending on the contract agreement, the ESBWR project's customer may be responsible for the training program.

Overall objectives, describing the training needs of appropriate plant staff, including operators and I&C engineers and technicians.

The required procedures needed to operate and maintain the software-based product.

The methods, techniques, tools and facility use to accomplish the training function.

Written test or assessment that demonstrates the student's knowledge as it relates to the objectives. This covers test and/or quiz that relates directly to the subject material presented to the student.

Collection of metrics to provide a basis for determining the effectiveness of the training program.

7B.6 SOFTWARE OPERATIONS AND MAINTENANCE PLAN

The Software Operations and Maintenance Plan (SOMP describes the instruction and guideline to operate and maintain the software-based product. IEEE Std. 1219, "IEEE Standard for Software Maintenance" (see Reference 7B-22) provides an acceptance approach to management and execution of the software maintenance activities, which this SOMP uses as a guide.

The O&M Manual exhibits the following characteristics:

- Describes the organization supporting the software-based product operations and maintenance effort. This includes:
  - The authority and responsibilities of the individual responsible for the operations and maintenance of the software-based products;
  - The qualification and responsibilities of individual carrying out each operations and maintenance task;
  - Personnel assignments for performing the operations and maintenance tasks;
  - Security measures to limit access to information, use of critical functions, and changes to critical functions;
  - Organizational interfaces;
  - Training requirements.
- Describe the purpose and functions of the software-based product, including the associated safety classification and operational environment.
- Define the procedures, including the safety and cautions warnings to allow responsible personnel to:
  - Initiate and perform normal system operational activities;
  - Perform required maintenance and perform troubleshooting when abnormal conditions for system operation occur;
  - Develop problem reporting and resolution channel.

- Specifies the methods, techniques and tools use to accomplish the operations and maintenance function, including:
  - Monitoring the software to detect security breaches (for example, intrusions, viruses, worms, Trojan horses, or bomb codes) and develop an incident response and recovery plan for responding to such threats;
  - Risks and potentially impact to the safety functions safety, if mishandled.
- Include the required system documentation such as (but not limited to) elementary diagram, schematic, user's manuals to assist operations and maintenance personnel in operating and maintaining the software-based product.
- Define the procedures on failure detection during operation, correction of faults that have caused those failures, and if applicable, regression testing to be conducted. Proposed changes to design documentation including software is processed in accordance with the change control procedures defined in the SCMP.
- Define procedures to shut down and restore the software-based product to normal operation.
- Provide a list of recommended spare parts.
- Develop a system for collection of metrics and using them to assess the success or failure of the operating and maintenance procedures.

7B.7 ESBWR I&C SOFTWARE QUALITY ASSURANCE PLAN LTR

The ESBWR I&C Software Quality Assurance Plan LTR defines the SQA activities to be performed during the software life cycle phases of the ESBWR software-based product. The SQAP thefollowing plans:

- Software Verification and Validation Plan (SVVP)
- Software Safety Plan (SSP)
- Software Configuration Management Plan (SCMP)

The SQAPestablishes a SQA program to control the software design, development and implementation activities of the software-based products and identify the organization responsible for the SQA program and its organizational boundaries The SQAP conforms to the requirements of 10 CFR 50, Appendix B and is consistent with the requirements specified in IEEE-730 Std., "IEEE Standard for Quality Assurance Plans" (see Reference 7B-11). The SQAP:

- Defines the quality assurance management of the software-based product. This includes:
  - The organizational structure that influences and controls the quality of the software. The SQA organization is financially and administratively independent from the design organization.

  - The organizational boundaries between the software QA organization and other organizations, including suppliers supporting the design and development of the software-based product.
  - The responsibilities and authority of the software quality organization, and identify the specific organizational elements responsible for each task (that is, configuration management, V&V, safety analysis, etc).
  - Tasks to be performed with special emphasis on software quality assurance activities for each software life cycle phase (described in the Software Management Plan)

- Defines the documentation governing the development, verification and validation, use, and maintenance of the software-based product and state how design documentation and design outputs are to be checked for adequacy, and the documentation needed to ensure that the implementation of the software satisfies requirements.
- Defines the standards, practices, conventions and metrics to be applied and how compliance with these requirements is to be monitored, and traceability is maintained through all phases of the software life cycle.
- Defines the reviews and audits to be conducted and accomplished, such as (but not limited to), software requirements review, software design review, managerial reviews, functional audits and in-process audits; and if applicable, defines further actions required and how they are to be implemented and verified.
- Describes the practices and procedures to be followed for reporting, tracking, and resolving problems identified in both software items and the software development and maintenance process.
- Identifies the software tools, techniques, and methodologies that support SQA.
- Defines the methods used to control and secure the software source code and software media.
- Defines the provisions for assuring that software provided by suppliers through purchase meet the established requirements; also for assuring that SQAP covers the proper methods used to assure the suitability of previously-developed software for use with the software-based product.
- Identifies the SQA documentation to be retained, the methods and facilities to be used to assemble, safeguard, and maintain this documentation, and the retention period.

7B.8 SOFTWARE VERIFICATION AND VALIDATION PLAN

The Software Verification and Validation Plan (SVVP) defines the verification and validation process to assure the following:

- Design outputs of each life cycle phase are in compliance with the requirements defined in the previous phase;
- Final software product meets the system requirements and applicable standards.

The SVVP meets the intent of RG 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems for Nuclear Power" (See Reference 7B-3). RG 1.168 endorses IEEE Std. 1012, "IEEE Standard for Verification and Validation Plans" (see Reference 7B-16) and IEEE Std. 1028, "IEEE Standard for Software Reviews and Audits" (see Reference 7B-18), which the SVVP uses as guides. The SVVP provides the:

- Description of the organization supporting the software V&V effort. This includes:
  - Software V&V staff qualification and responsibilities of individual carrying out the V&V task and personnel assignments for performing the V&V tasks;
  - The authority and responsibilities of the individual responsible for the V&V activities and approving the V&V tasks conducted;
  - Risk management to identify, assess, control and mitigate V&V risks;
  - Organizational interfaces;
  - Training requirements.
- Description of the degree of independence between the design organization and independent V&V Team.
- Description of how the V&V effort will be managed. This includes
  - Reporting procedures;
  - Management reviews and audits. Management review and audit are conducted to evaluate the effectiveness and accomplishment for the V&V activities;
  - The individual and/or team conducting the V&V;
  - Methods of carrying out the different V&V activities, and validation testing is conducted in accordance with documented test plan and procedure;
  - Completion criteria for the V&V activities. Software development is not complete until the specified verification and validation activities are complete and design documentation is consistent with the developed software;
  - Evaluation of commercial software and commercial development tools for safety-related applications;
  - V&V requirements for non-conformance tracking and closure.
- Schedule, milestone and resources plans needed to support the V&V activities.
- A description of the V&V activities, including

  - Verification and Validation Methods and Test Tool;
  - Acceptance criteria for each activity;
  - Relationships with the product development life cycle tasks;
  - Coordination with Software Configuration Management (SCM) activities.

- Description of all required testing and test documentation requirements, including error reporting and methods for identification, closure, and documentation of design and/or design documentation non-conformances and anomaly resolution procedures. Test documentation is prepared to meet the intent of RG 1.170, "Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants". RG 1.170 endorses IEEE Std. 829, "IEEE Standard for Software Test Documentation", which is used as guide to prepare the test documentation.
- Description of V&V documentation including:
  - Activities performed during the V&V are documented in the V&V task reports. The V&V task report includes description of V&V performed, reference to the V&V inputs and traceability matrix (forward and backward direction). Non-conformances identified during the V&V shall be documented in the anomaly report. The V&V task reports are placed under configuration management control;
  - Use of commercial software and commercial development tools for safety-related applications is a controlled and documented procedure.
- System for collection of metrics and using them to assess the success or failure of the V&V efforts.

7B.9 SOFTWARE SAFETY PLAN

This Software Safety Plan (SSP) establishes the processes and activities intended to be used to ensure the safety of the safety related software for the software-based product and to address the potential software risksIEEE Std. 1228, "IEEE Standard for Software Safety Plans" (see Reference 7B-23) provides an acceptance approach in preparing the SSP. The SSP exhibits the following characteristics:

- Specifies the purpose and scope of the software safety activities.
- Defines the responsibilities and authority of the software safety organization (that is, specify a person or group responsible for software safety tasks). The designated individual has a clear authority for enforcing safety requirements in the software-based products being designed and developed. The software safety organization has the authority to reject the software, including previously developed software and commercial software if the software cannot be shown to be adequately safe.

- Defines the resources required for the software safety organization, including qualification and training requirements.
- Describes the management of software safety activities, including how the safety activities are integrated and coordinated between the design organizations and other organizations (that is, Quality Assurance, Configuration Control Management, suppliers).
- Describes the safety analyses (for example, FMEA) to be performed on the applicable design documents during each software life cycle phasedefined in the SMP, including methods and strategies to be used to minimize safety risks cause by software failures.
- Describe the documentation requirements for software safety analysis, including configuration management of the software safety documents.
- Describe any safety related tests that are not included in the SVVP.
- Describe the methods for error tracking to assess the success or failure of the software safety analysis effort.

7B.10 SOFTWARE CONFIGURATION MANAGEMENT PLAN

The Software Configuration Management Plan (SCMP) defines the specific product or system scope to which it is applicable, the organizational responsibilities for SCM, and methods to be applied to SCM. The SCMP meets the intent of RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (see Reference 7B-4) RG 1.169 endorses IEEE Std. 828, "IEEE Standard for Software Configuration Management Plans" (see Reference 7B-12) and IEEE Std. 1042, "IEEE Guide to Software Configuration Management" (see Reference 7B-19), which the SCMP uses as guides. The SCMP provides:

- Description of the SCM organization, which includes the description of responsibilities of each individual for carrying out each SCM activity, identifies the individual with authority to authorize release of software, data, or revised design documentation.
- A list of documents to be placed under configuration control.
- SCM activities, which include
  - Configuration identification, which requires assignment of unique document identification number, revision status and quality classification and procedures for managing software libraries;
  - Configuration control, which includes:

i. Design control to ensure compliance with all applicable safety and performance requirements;

ii. Design change control to process change initiation, review, approval, implementation, disposition, status reporting, document updating, and distribution;

iii. Design interface control to manage changes to design interface documentation and software design documentation; and

iv. Change notification.

– Configuration review and audits;

– Baseline review to be conducted at completion of each software life cycle phase, and the scope and methods to be used in the baseline reviews to evaluate the configuration status of the implemented design, design documentation, and compliance with the requirements specified in the SMP and the SQAP;

- Configuration management of tools (such as compilers) and software development procedures;
- Control of supplier(s) responsible for software development;
- Evaluating and dedicating commercial off-the-shelf (COTS) software in accordance with EPRI TR-106439, "Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment in Nuclear Safety Application" (see Reference 7B-25) and NUREG/CR-6421 "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications" (see Reference 7B-26).
- Procedures for managing corrective actions to resolve deviations identified in software design and design documentation, including notification to end user of errors discovered in software development tools or other software;
- Methods for design record collection, retrieval and retention; including control and release of software source and object code during and after the project development process;
- Methods for tracking error rates during software development, such as the use of software metrics and actions taken on recommendations to improve operation.

7B.11 REFERENCES

7B-1 NUREG-0800, Standard Review Plan (SRP), Chapter 7, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," Branch Technical Position HICB-14, Rev 4, 6/1997.

7B-2 USNRC, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," RG 1.152. Rev. 2, 1/2006

7B-3 USNRC, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems for Nuclear Power," RG 1.168, Rev 1, 2/2004.

7B-4 USNRC, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," RG 1.169, Rev 0, 9/1997.

7B-5 USNRC, "Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants," RG 1.170, Rev 0, 9/1997.

7B-6 USNRC, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," RG 1.171, Rev 0, 9/1997.

7B-7 USNRC, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," RG 1.172, Rev 0, 9/1997.

7B-8 USNRC, "Development Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," RG 1.173, Rev 0, 9/1997.

7B-9 IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

7B-10 IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," (date from 10 CFR 50.55a(h) 08/02/2006).

7B-11 IEEE Std. 730-2002, "IEEE Standard for Quality Assurance Plans."

7B-12 IEEE Std. 828-1990, "IEEE Standard for Software Configuration Management Plans."

7B-13 IEEE Std. 829-1983, "IEEE Standard for Software Test Documentation."

7B-14 IEEE Std. 830-1993, "IEEE Recommended Practice for Software Requirements Specifications."

7B-15 IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing."

7B-16 IEEE Std. 1012-1998, "IEEE Standard for Verification and Validation Plans."

7B-17 IEEE Std. 1016-1998, "IEEE Recommended Practice for Software Design Descriptions."

7B-18 IEEE Std. 1028-1997, "IEEE Standard for Software Reviews and Audits."

7B-19 IEEE Std. 1042-1987, "IEEE Guide to Software Configuration Management."

7B-20 IEEE Std 1058.1-1987, "IEEE Standard for Software Project Management Plans."

7B-21 IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes."

7B-22 IEEE Std 1219-1998, "IEEE Standard for Software Maintenance."

7B-23 IEEE Std. 1228-1994, "IEEE Standard for Software Safety Plans."

7B-24 GE Energy Nuclear, "ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan," NEDO-33217, (Non-proprietary), Rev 2 (Draft).

7B-25 Electric Power Research Institute (EPRI), "Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment in Nuclear Safety Application," EPRI TR-106439.

7B-26 NUREG/CR-6421, "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications."

7B-27 Letter to NRC, "ESBWR Software Plans Revision Submittal Schedule", MFN 06-471, 12/8/2006

Table 7B-1

Software Requirements Specification

Characteristics	Requirements
Functionality	The operations that must be performed for each mode of operation be completely specified
Reliability	All requirements for fault tolerance and failure modes be fully specified for each operating mode
Robustness	The behavior of the software in the presence of unexpected, incorrect, anomalous and improper (1) input, (2) hardware behavior, or (3) software behavior be fully specified
Safety	The software functions, operating procedures, input, and output be classified according to their importance to safety
Security	Security threats to the computer system be identified and classified according to severity and likelihood
Timing	Functions that must operate within specific timing constraints be identified, and that timing criteria be specified for each
Completeness	1. All actions required of the computer system be fully described for all operating modes and all possible values of input variables (for example, the complete span of instrument inputs or clock/calendar time) 2. Fully specify All variables in the physical environment that the software must monitor and control
Consistency	The contents of the SRS be consistent with the safety system requirements, the safety system design, and documented descriptions and known properties of the operational environment within which the safety system software will operate
Correctness	The description of actions required of the computer system be free from faults and that no other requirements be stated
Style	The contents of the SRS be understandable
Traceability	Two way trace exist between each requirement in the SRS, and the safety system requirements and design
Unambiguity	Each requirement, and all requirements taken together, have one and only one interpretation
Verifiability	Possible to construct a specific analysis, review, or test to determine whether each requirement has been met

Table 7B-2

Software Architecture Description

Characteristics	Requirements
Reliability	The combined hardware and software architecture be such that individual software element failure will not compromise safety
Safety	The software architecture introduce no new hazards into the safety system
Security	The architecture correctly handle identified security threats, and introduce no new security threats
Timing	That the architectural design describe all timing limitations, the strategy for handling each, the required margins, and the method of measuring those margins
Completeness	All the software requirements be satisfied in the architecture
Consistency	Each software architectural element be compatible with the SRS, the hardware architecture, documented descriptions and known properties of the operational and hardware environment, and other software elements
Style	The contents of the SAD be understandable
Traceability	Two way trace exist between the requirements in the SRS and the elements in the architecture
Verifiability	Possible to construct specific analyses, reviews, and tests to verify that the architecture satisfies the software requirements

Table 7B-3

Software Design Specification

Characteristics	Requirements
Accuracy	All calculations be specified in such a way that the accuracy requirements for the calculations will be satisfied
Reliability	The detailed software design be such that single failures of individual elements will not cause safety system failure
Robustness	The design be such that the software will operate correctly in the presence of unexpected, incorrect, anomalous and improper (1) input, (2) hardware behavior, or (3) software behavior
Safety	The detailed design introduce no new safety hazards into the safety system
Security	Unauthorized changes be prevented, detected, or mitigated as appropriate
Timing	The time delay between stimulus and response be deterministic. BTP HICB 21 provides additional guidance on real time performance
Completeness	The detailed design specify the actions of each software unit for the entire domain of each input variable (for example, the complete span of instrument inputs or clock/calendar time)
Consistency	The detailed design be consistent with the architectural design, and that the detailed design elements be mutually consistent
Correctness	All equations, algorithms, and control logic be evaluated for potential errors
Style	The detailed design documents description should conform to the developer's style guide
Traceability	Two way trace exist between the elements of the detailed design and the elements in the architecture
Verifiability	Possible to construct specific analyses, reviews, and tests to verify that the design satisfies the software architecture

Table 7B-4

Software Source Code Listings

Characteristics	Requirements
Functional	The requirements imposed on the software for that characteristic should be satisfied by the code
Accuracy	The actual source code be written so that the accuracy requirements and accuracy design specifications are met
Robustness	The system be coded in such a way that corrupted data will not cause the safety system to fail
Safety	The code introduce no new hazards into the safety system
Security	The code introduce no new security threats into the safety system software
Timing	The execution time be deterministic
Completeness	The code meet all the specifications of the design and all implementation constraints
Consistency	All variable names, types, locations, and array sizes be defined consistently throughout the software units
Correctness	That the code be correctly implemented
Style	The programming style constraints specified in the design documents be followed
Traceability	A two way trace exist between the elements of the detailed design and the elements in code
Verifiability	Possible to construct specific analyses, reviews, and tests to verify that the code correctly implements the detailed design

Table 7B-5

System Build Documents

Characteristics	Requirements
Robustness	The software build documents specify methods to detect incorrectly built software releases
Safety	The software build activity introduce no new hazards into the safety system
Security	The software build activity introduce no new security threats into the safety system software
Completeness	All build procedures be fully specified
Consistency	The software build documents be consistent with the software specifications, as described in the SRS, software design description, and software code
Correctness	The software build documents identify the correct versions of all required software elements and all required software documents
Style	The software build documents conform to applicable standards imposed by the developer
Traceability	Possible to trace each element of the integrated builds (software subsystem or software system) backward to the code elements contained in the build
Verifiability	Be possible to analyze, review, or test each integrated software build for the product functional requirements

Table 7B-6

Installation Configuration Tables

Characteristics	Requirements
Functionality	The installation tables configure the installed system to have the functionality that is required for the plant
Safety	The installation tables introduce no new hazards into the safety system
Security	The installation tables introduce no new security threats into the installed system, and that the installation tables be protected from unauthorized change
Completeness	The software configuration tables include all information necessary for the correct operation of the system
Consistency	The installation configuration tables be consistent with the software specifications, as described in the SRS, software design description, software code, and software build documents
Correctness	The software configuration tables contain all plant specific data
Traceability	Possible to trace each installed program element backward to the integrated software elements that created that installed program element
Verifiability	Possible to analyze, review, or test each installed software system on initial software installation, all subsequent installations, and periodically during operation

Table 7B-7

Operations-Maintenance Manuals

Characteristics	Requirements
Completeness	That all actions available to the system operator be fully described for all operating modes, including error recovery and backup. Maintenance procedures be fully defined.
Consistency	The operations manual be consistent with the system operations, safety system requirements, the safety system design, the SRSs, the SDS, and documented descriptions and known properties of the operational environment within which the safety system will operate
Style	The operations manual be understandable by the users of the manual. That the maintenance manual be understandable by the users.
Traceability	A forward trace exist between the SRS, the operations plan, and the operations manual, which shows how each requirement is to be carried out by the operators, or carried out automatically by the safety system without operator action, and how the results of each requirement are displayed to the operators. A forward trace exist between the maintenance plan and the maintenance manual, which shows how each requirement is carried out by the maintenance organization
Unambiguity	Instructions to users have only one interpretation by the users

Table 7B-8

Training Manuals

Characteristics	Requirements
Completeness	All actions available to the operator be fully described for all operating modes, including error recovery
Consistency	The training manual be consistent with the safety system requirements, the safety system design, the SRSs, the SDS, and documented descriptions and known properties of the operational environment within which the safety system will operate
Style	The training manual be understandable by the users
Traceability	A forward trace exist between the SRS, the training plan, and the training manual, which shows how each requirement is to be carried out by the users, or carried out automatically by the safety system without user action, and how the results of each requirement are displayed to the users