GE Hitachi Nuclear Energy

NEDO-34169

Revision B

July 2025

US Protective Marking: Non-Proprietary Information
UK Protective Marking: Not Protectively Marked

BWRX-300 UK Generic Design Assessment (GDA) Chapter 7 – Instrumentation and Control

US Protective Marking: Non-Proprietary Information
UK Protective Marking: Not Protectively Marked

INFORMATION NOTICE

This document does not contain proprietary information and carries the notations “US Protective Marking: Non-Proprietary Information” and “UK Protective Marking: Not Protectively Marked.”

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT
Please Read Carefully

The design, engineering, and other information contained in this document is furnished for the purpose of obtaining the applicable Nuclear Regulatory Authority review and determination of acceptability for use for the BWRX-300 design and licensing basis information contained herein. The only undertakings of GEH with respect to information in this document are contained in the contracts between GEH and its customers or participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone for any purpose other than that for which it is intended is not authorized; and with respect to any unauthorized use, no representation or warranty is provided, nor any assumption of liability is to be inferred as to the completeness, accuracy, or usefulness of the information contained in this document. Furnishing this document does not convey any license, express or implied, to use any patented invention or any proprietary information of GEH, its customers or other third parties disclosed herein or any right to publish the document without prior written permission of GEH, its customers or other third parties.

UK SENSITIVE NUCLEAR INFORMATION, UK EXPORT CONTROL AND US EXPORT CONTROL INFORMATION

This document does not contain any UK Sensitive Nuclear Information (SNI) subject to protection from public disclosure as described in the Nuclear Industries Security Regulations (NISR) 2003, does not contain UK Export Controlled Information (ECI), and does not contain US Export Controlled Information (ECI) subject to the export control laws and regulations of the United States, including 10 CFR Part 810.

EXECUTIVE SUMMARY

The purpose of this Preliminary Safety Report chapter is to present the Instrumentation and Control for the GE-Hitachi BWRX-300 Small Modular Reactor (SMR).

The GE-Hitachi BWRX-300 systems support the plant safety strategy described in Chapter 15.

The BWRX-300 SMR utilises an integrated digital-based Instrumentation and Control design. The Instrumentation and Control architecture is arranged to support a plant level Defence-in-Depth (D-in-D) framework. The BWRX-300 D-in-D framework is supported by a safety analysis framework that provides a consistent analytical basis for the Defence Lines (DLs). The BWRX-300 D-in-D framework links to a classification scheme based on the importance of the individual DLs. The BWRX-300 Instrumentation and Control architecture and associated systems and components are designed in accordance with the relevant international standards and via proven engineering design practices and processes, which represent state-of-the-art methods. The Quality Assurance program is described in Chapter 17.

The BWRX-300 passive safety features present a simpler and more flexible design with large safety margins. These safety improvements also reduce plant complexity and lead to design optimisations that can lower overall cost. The passive safety design requires fewer automatic actuation functions that also eliminate automatic control capabilities and eliminates required operator actions for Design Basis Accidents for 72-hours. The design does not require active monitoring of critical plant safety functions to support near-term operator actions or emergency planning decisions for design basis events. The simplicity of the BWRX-300 design has limited requirements for safety support systems for the highest classified Instrumentation and Control equipment performing safety functions to mitigate design basis events. The short times required for the actuation of safety category Instrumentation and Control functions allow for optimisation of the BWRX-300 support systems and structures.

The scope of this chapter covers Instrumentation and Control systems. It describes the approach to function categorising and system classification. It identifies applicable Instrumentation and Control codes and standards. It describes the Instrumentation and Control networks and their overall architecture. It describes Instrumentation and Control systems and allocated functions for each system Safety Class, including general description, platform hardware and software, system architecture, system design bases and associated safety functions, design principles, qualification, reliability, robustness, security, diversity and defence-in-depth, control rooms and operator interface, compliance alignment, interfaces with other systems, examination, maintenance, inspection, and testing, performance & safety evaluation, application of As Low as Reasonably Practicable principles in design development.

This chapter describes the system Development Processes (Production Excellence), including a High-level overview and detailed descriptions of the Design Phase up to Baseline 1. It also provides a V-model lifecycle detailing all phases of work.

It describes the main control room, secondary control room and emergency response facilities, operator interfaces and accident monitoring.

Claims and arguments relevant to Generic Design Assessment step 2 objectives and scope are summarised in APPENDIX A, along with an As Low as Reasonably Practicable position. APPENDIX B provides a Forward Action Plan (FAP), which includes future work commitments and recommendations for future work where ‘gaps’ to Generic Design Assessment expectations have been identified, to date no FAP findings have been raised. APPENDIX C lists the interfacing systems. APPENDIX D outlines potential Independent Confidence Building Measures.

ACRONYMS AND ABBREVIATIONS

Acronym	Explanation
2oo2	Two Out of Two
2oo3	Two Out of Three
2oo4	Two Out of Four
3D	Three-Dimensional
3D-CTP	Three-Dimensional Core Thermal Power
AC	Alternating Current
ALARP	As Low As Reasonably Practicable
AOF	Allocation of Functions
AOO	Anticipated Operational Occurrence
APR	Automatic Power Regulator
APRM	Average Power Range Monitor
APS	Anticipatory Protection System
ARI	Alternate Rod Insertion
ATLM	Automatic Thermal Limit Monitor
BOP	Balance of Plant
BWR	Boiling Water Reactor
CAE	Claims Arguments Evidence
CB	Control Building
CCF	Common Cause Failure
CCS	Containment Cooling System
CRD	Control Rod Drive
CRDA	Control Rod Drop Accident
COTS	Commercial Off the Shelf
CTPFM	Core Thermal Power/Flow Monitor
CUW	Reactor Water Cleanup System
CWE	Chilled Water Equipment System
D-in-D	Defence-in-Depth
DBA	Design Basis Accident
DC	Direct Current
DCIS	Distributed Control and Information System
DEC	Design Extension Condition
DL	Defence Line
DL1	Defence Line 1
DL2	Defence Line 2
DL3	Defence Line 3

Acronym	Explanation
DL4a	Defence Line 4a
DL4b	Defence Line 4b
DL5	Defence Line 5
DPS	Diverse Protection System
EIMT	Examination, Inspection, Maintenance, and Testing
EMC	Electromagnetic Compatibility
ERF	Emergency Response Facilities
FAP	Forward Action Plan
FMCRD	Fine Motion Control Rod Drive
FSA	Functional Safety Assessment
FW	Feedwater
FWCIV	Feedwater Containment Isolation Valve
FWRIV	Feedwater Reactor Isolation Valve
GDA	Generic Design Assessment
GEH	GE Hitachi Nuclear Energy
GT	Gamma Thermometer
HCU	Hydraulic Control Unit
HDL	Hardware Description Language
HFE	Human Factors Engineering
HSI	Human-System Interface
HVS	Heating, Ventilation, and Cooling System
I&C	Instrumentation and Control
I/O	Input/Output
IAEA	International Atomic Energy Agency
IC	Isolation Condenser
ICBM	Independent Confidence Building Measure
ICS	Isolation Condenser System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
LfE	Learning from Experience
LPRM	Local Power Range Monitor
MCR	Main Control Room
MRBM	Multi-Channel Rod Block Monitor
MSCIV	Main Steam Containment Isolation Valve
MSL	Main Steam Line

Acronym	Explanation
MSRIV	Main Steam Reactor Isolation Valve
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
PAF	Plant Automation Function
PDH	Plant Data Highway
PIE	Postulated Initiating Event
PRNM	Power Range Neutron Monitoring System
PSR	Preliminary Safety Report
QA	Quality Assurance
RB	Reactor Building
RC&IS	Rod Control and Information System
RGP	Relevant Good Practice
RIO	Remote Input/Output
RIV	Reactor Isolation Valve
RLC	Reactor Level Control
RPC	Reactor Pressure Control
RPV	Reactor Pressure Vessel
RWE	Rod Withdrawal Error
RWM	Rod Worth Minimizer
SAMG	Severe Accident Management Guideline
SC	Safety Class
SC1	Safety Class 1
SC2	Safety Class 2
SC3	Safety Class 3
SCDS	Safety Case Development Strategy
SCRRI	Selected Control Rod Run-In
SDC	Shutdown Cooling System
SSCs	Structures, Systems, and Components
SSG	Specific Safety Guide
SSR	Specific Safety Requirements
SCN	Non-Safety Class
SCR	Secondary Control Room
SMR	Small Modular Reactor
SPDS	Safety Parameter Display System
TBV	Turbine Bypass Valve
TCV	Turbine Control Valve

Acronym	Explanation
TMR	Triple Modular Redundant
TS	Technical Specifications
TSM	Technical Specification Monitor
UDH	Unit Data Highway
UK	United Kingdom
UPS	Uninterruptible Power Supply
VDU	Visual Display Unit
WRNM	Wide Range Neutron Monitor

DEFINITIONS

Term	Definition
R10	Emergency Power Backup DC and UPS Electrical System
R20	Standby Power System
R30	Preferred Power System
C10	Primary Protection System
C20	Diverse Protection System
C22	FMCRD Motor Control System
C30	Anticipatory Protection System
C31	Reactor Control System
C32	Reactor Auxiliaries Control System
C33	Equipment Cooling and Environmental Control System
C34	Electrical Power Supply Control System
C35	Reactivity Monitoring System
C36	Plant Data Acquisition, Data Communications, and Normal Operator Interface System
C37	Control and Monitoring System for DL4b Functions
C38	Turbine Generator Control System
C39	Normal Heat Sink and Condensate/FW Control System
C40	Investment Protection System
C41	Plant Performance Monitoring
C43	Water Chemistry
C44	Effluent Cleanup Control System
C45	Network Communications and Operator Interface System
Safety Category	A classification (Safety Category 1, 2, 3, or Non-Safety Category) applied to functions to reflect their role in ensuring plant safety
Safety Class	A classification (SC1, SC2, SC3, or SCN) applied to SSCs to reflect their role in ensuring plant safety.

SYMBOLS

Symbol	Definition
N/A	N/A

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

REVISION SUMMARY

Revision #	Section Modified	Revision Summary
A	All	Initial Issuance
B	Table 7-1, Table 7-9, 7.3.1.3.1, 7.3.2.3.1, 7.3.3.3.1	Update for end of GDA Step 2 consolidation

7 INSTRUMENTATION AND CONTROLS

Introduction

This chapter outlines the claims, arguments, and evidence appropriate to a 2-step Generic Design Assessment (GDA), e.g., methods, strategies, and architecture. It underpins the high-level claim that the GEH BWRX-300 Instrumentation and Control (I&C) systems are designed to meet the safety, functional, and performance design principles and relevant good practice to reduce risks to As Low As Reasonably Practicable (ALARP).

The scope of this chapter covers I&C systems. It describes the approach to function categorising and system classification. It identifies applicable I&C codes and standards. It describes the I&C networks and their overall architecture. It describes I&C systems and allocated functions for each system Safety Class (Safety Class 1 (SC1), Safety Class 2 (SC2), Safety Class 3 (SC3) or Non-Safety Class (SCN)).

This chapter describes the system Development Processes (Production Excellence), including a High-level overview and detailed descriptions of the Design Phase up to Baseline 1. It also provides a V-model lifecycle detailing all phases of work.

It describes the main control room, secondary control room and Emergency Response Facilities (ERF), operator interfaces and accident monitoring.

This chapter organises the information to systematically present the design bases of the I&C systems in the necessary context to support an understanding of the individual I&C system designs and safety category functions and their interconnection into a Distributed Control and Information System (DCIS).

- Section 7.1 presents information on the relationship of the I&C systems to plant level requirements.
- Section 7.2 presents information on the architecture of the I&C system of systems.
- Section 7.3 presents information on the individual I&C systems, including the display of accident monitoring information.
- Section 7.4 presents the development processes for the digital I&C systems.
- Section 7.5 describes the I&C functionality in the Main Control Room (MCR).
- Section 7.6 describes the I&C functionality in the Secondary Control Room (SCR).
- Section 7.7 describes the I&C functionality in the emergency response facilities.
- Section 7.8 describes the Hazards analyses for the BWRX-300 I&C systems.
- Section 7.9 addresses smart devices.

Claims and arguments relevant to GDA step 2 objectives and scope are summarised in APPENDIX A, along with an ALARP position. APPENDIX B provides a Forward Action Plan (FAP), which includes future work commitments and recommendations for future work where ‘gaps’ to GDA expectations have been identified, to date no FAP findings have been raised. APPENDIX C lists the interfacing systems. APPENDIX D outlines potential Independent Confidence Building Measures (ICBMs).

Interfaces with other chapters

The interfaces with other Chapters of the Preliminary Safety Report (PSR) are shown below:

- Chapter 2 “Site Characteristics” (Reference 7-7)

- Chapter 3 “Safety Objectives and Design Rules for Structures, Systems and Components” (Reference 7-8)
- Chapter 4 “Reactor” (Reference 7-9)
- Chapter 5 “Nuclear Boiler System and Associated Systems” (Reference 7-10)
- Chapter 6 “Engineered Safety Features” (Reference 7-11)
- Chapter 7 “Instrumentation and Control” (this chapter)
- Chapter 8 “Electrical Power” (Reference 7-12)
- Chapter 9A “Auxiliary Systems” (Reference 7-13)
- Chapter 9B “Civil Engineering Works and Structures” (Reference 7-14)
- Chapter 10 “Steam and Power Conversion Systems” (Reference 7-15)
- Chapter 11 “Management of Radioactive Waste” (Reference 7-16)
- Chapter 12 “Radiation Protection” (Reference 7-17)
- Chapter 15 “Safety Analysis” (Reference 7-18)
- Chapter 18 “Human Factor Engineering” (Reference 7-19)
- Chapter 19 “Emergency Preparedness and Response” (Reference 7-20)
- Chapter 25 “Cyber Security” (Reference 7-21)

7.1 Instrumentation and Control Introduction and Overview

The BWRX-300 systems are designed to support the plant safety strategy described in Chapter 15. The BWRX-300 Small Modular Reactor utilises an integrated digital-based I&C design. The I&C architecture is arranged to support a plant level D-in-D framework. The BWRX-300 D-in-D framework is supported by a safety analysis framework that provides a consistent analytical basis for the DLs. The BWRX-300 D-in-D framework links to a classification scheme based on the importance of the individual DLs. The BWRX-300 I&C architecture and associated systems and components are designed in accordance with the relevant international standards and via proven engineering design practices and processes, which represent state-of-the-art methods. The Quality Assurance (QA) program is described in Chapter 17.

The BWRX-300 passive safety features present a simpler and more flexible design with large safety margins. These safety improvements also reduce plant complexity and lead to design optimisations that can lower overall cost. The passive safety design requires fewer automatic actuation functions that also eliminate automatic control capabilities and eliminates required operator actions for Design Basis Accidents (DBAs) for 72-hours. The design does not require active monitoring of critical plant safety functions to support near-term operator actions or emergency planning decisions for design basis events. The simplicity of the BWRX-300 design has limited requirements for safety support systems for the highest classified I&C equipment performing safety functions to mitigate design basis events. The short times required for the actuation of safety category I&C functions allow for optimisation of the BWRX-300 support systems and structures.

7.1.1 Relationship Between Instrumentation and Control Functions and Plant level Defence Lines

The I&C functions are allocated to the various defence lines.

Defence Line 1

Defence Line 1 (DL1) includes the quality measures taken to minimise potential for failures and initiating events to occur in the first place and to minimise potential for failures to occur in subsequent lines of defence. These quality measures cover the design, construction, operation, and maintenance of the plant. DL1 also includes the use of appropriate conservatism in design and analyses. Accident monitoring instrumentation supports functions in more than one DL and receives DL1 treatment by application of applicable industry standards for accident monitoring indication, as shown in Table 7-1.

Defence Line 2

Defence Line 2 (DL2) contains Safety Category 3 plant functions (e.g., anticipatory reactor trips) designed to detect and mitigate Postulated Initiating Events (PIEs) in the Anticipated Operational Occurrences (AOOs) frequency range category and prevent plant conditions from escalating to accident conditions. Safety Category 3 functions that normally operate to actively control reactor parameters are also part of DL2 (e.g., reactor level and pressure control and control rod positioning).

Defence Line 3

Defence Line 3 (DL3) contains Safety Category 1 functions that act to mitigate PIEs consisting of AOOs or DBAs by preventing core damage. These Safety Category 1 functions provide a level of assurance for maintaining integrity of the physical barriers that prevent radiological release and place the plant in a safe state. DL3 also includes Safety Category 1 functions that maintain the plant in a safe condition following mitigation of PIEs until normal operations are resumed. Safety Category 1 functions typically include reactor scram and actuation of engineered safety features. Safety Category 1 functions are needed when Safety Category 3 functions are not effective at intercepting a PIE or when a PIE is beyond the capabilities of

Safety Category 3 functions. Accordingly, DL3 provides D-in-D in that it provides an additional layer of mitigation for AOO PIEs. Primary Safety Category 1 functions include actuations of reactor scram, Reactor Pressure Vessel (RPV) and containment isolations, and Isolation Condenser System (ICS) initiation to mitigate the consequences of AOOs or DBAs.

Safety Category 1 functions are credited to mitigate PIEs independent of Safety Category 2 and 3 functions and are therefore required to be independent from Safety Category 2 and 3 functions to the extent needed to meet plant safety goals. Exceptions related to the I&C systems are cases where probabilistic safety analyses indicate safety is improved by the sharing of components (e.g., Local Power Range Monitors (LPRMs) for Safety Category 1 hydraulic scram and Safety Category 3 rod block functions).

Defence Line 4

Defence Line 4 comprises two subsets, designated as Defence Line 4a (DL4a) and Defence Line 4b (DL4b). DL4a includes Safety Category 2 functions required to place and maintain the plant in a safe state in case of PIEs and event sequences with failure of the Safety Category 1 functions (e.g., Design Extension Conditions (DEC) without core damage). DL4a provides D-in-D in that it provides an additional layer of mitigation for DBA PIEs. Safety Category 2 functions detect and mitigate DECs. The need for Safety Category 2 functions arises when specific, postulated Common Cause Failures (CCFs) occur in DL3. Safety Category 2 functions actuate for any condition that satisfies the actuation criteria logic. DL4b functions prevent or mitigate severe accidents, which are extremely unlikely because each PIE caused by a single failure can be mitigated independently by functions in at least two DLs (among DL2, DL3, and DL4a), and failures of multiple DLs therefore have to occur. Accordingly, DL4b functions are considered the least important DL functions from a nuclear safety standpoint, despite the high consequence of failure.

Defence Line 4a

Safety Category 2 functions are used as a backup to DL3 Safety Category 1 functions (e.g., CCFs postulated to occur in DL3 coincident with DBA PIEs). Safety Category 2 functions are designed to work in tandem with Safety Category 3 functions to ensure AOOs and DBAs resulting from a single failure are mitigated by two DLs among DL2, DL3, and DL4a. Accordingly, DL4a is not required to be independent and diverse from DL2. Safety Category 2 functions can be used, along with unaffected Safety Category 3 functions, to mitigate a PIE as part of the same event sequence (i.e., to act as a single DL and not as two independent DLs in an DEC analysis). All AOOs and DBAs resulting from a single failure are required to be mitigated by Safety Category 1 functions and separately by Safety Category 3 functions, Safety Category 2 functions, or a combination of Safety Category 2 and 3 functions. Safety Category 2 and 3 functions are not credited to mitigate the same PIEs independently of each other and are therefore not required to be independent from each other.

Defence Line 4b

DL4b contains Safety Category 3 functions that are explicitly provided to prevent or mitigate a severe accident while keeping radioactive releases to acceptable levels. The Safety Category 3 functions intended for mitigating DECs have functional and design requirements derived from the supporting safety analyses.

Defence Line Independence

The DL independence requirements are consistent with the D-in-D strategy (i.e., the crediting of DLs in the fault evaluation and deterministic safety analyses). Although not specifically required by the BWRX-300 Safety Strategy, there is independence between Safety Category 2 and Safety Category 3 functions to a level that does meet this definition of practicable; it is not justifiable or cost-effective to require full independence between Safety Category 2 and Safety Category 3 functions (i.e., the type of independence required for Safety

Category 1 functions). Equipment performing DL4b functions are independent of any equipment postulated to have failed in the event sequence those functions are mitigating. These interface requirements stem from the different safety classifications of the equipment.

Defence Line 5

Defence Line 5 (DL5) includes emergency preparedness measures to cope with potential unacceptable releases in case the first four DLs are not effective. These are off-site measures taken to protect the public in a scenario involving substantial release of radiation. DL5 is supported by accident monitoring instrumentation.

7.1.2 Instrumentation and Control System Classification

The BWRX-300 DCIS is an integrated control and monitoring system for the power plant. The DCIS is arranged in three Safety Classified DCIS segments and a Non-Safety Class segment with appropriate levels of hardware and software quality corresponding to the system functions they control and their DL location, as described in Chapter 3, Section 3.2. The DCIS provides control, monitoring, alarming and recording functions. The various bus segments of the integrated DCIS are designed to operate autonomously.

The Safety Category 1 functions are allocated to DL3 and implemented by SC1 equipment, with the following exceptions:

1. Structures, Systems, and Components (SSCs) only needed after the first 72-hours of the event are classified as SC2.
2. SSCs only needed after the first 7 days of the event are classified as SC3.

The Safety Category 2 functions allocated to DL4a are implemented in at least SC2 equipment, except for SSCs that are only needed after the first 7 days of the event, which are classified as SC3. Safety Category 2 functions complete the safety objective by means of independent and diverse logic and I&C control of actuated devices (solenoids) if the Safety Category 1 function is not completed due to an SC1 I&C system failure.

The Safety Category 3 functions are allocated to DL2 and implemented in at least SC3 equipment. The Safety Category 3 functions need to be performed independently from diverse Safety Category 1 functions providing protection for the same event.

The Safety Category 3 functions allocated to DL4b are implemented in at least SC3 equipment unless other requirements are justified.

Accident monitoring is a DL1 provision and Safety Category 3 is assigned to functions that support monitoring and display of Plant Accident Monitoring Type B, C, D, E, and F accident monitoring variables. There are no Type A accident monitoring variables as the BWRX-300 does not require manual actions to mitigate design basis events and automatic controls perform mitigation functions.

The Safety Category 1 DCIS functions are allocated to the SC1 systems which require minimal support equipment (e.g., no active systems such as Heating, Ventilation, and Cooling System (HVS) or cooling water for at least 72-hours). Safety Category 1 DCIS functions are implemented on SC1 I&C system hardware and software platforms located in three separate divisional fire barrier rooms in the Reactor Building (RB). The Safety Category 2 and Safety Category 3 actuation functions are implemented in different systems. The Safety Category 2 DCIS functions are implemented with SC2 equipment. The majority of the SC2 equipment is located in its own fire barrier room in the Control Building (CB) with the remainder located in compartmentalised fire barrier rooms in the RB. The Safety Category 3 functions are implemented with SC3 equipment. The SC3 equipment is located in two separate fire barrier rooms in the CB.

SSCs that are not required to be SC1, SC2, or SC3 are classified as SCN. SCN controller equipment failures cannot initiate plant transients. The non-safety category functions can be implemented on vendor packages located in a separate fire barrier room in the CB. Vendor supplied SCN equipment is integrated into the SC3 DCIS network through SC3 gateways, as necessary.

The system designations of Primary Protection System as SC1, Diverse Protection System (DPS) as SC2, Nuclear Controllers as SC3, and Balance of Plant (BOP) Controllers as SCN represent an initial decomposition of the overall I&C systems based on safety classification.

Further refinement of the system decomposition, based on functional grouping within a Safety Class (SC) and equipment selection, is performed as the I&C architecture design process progresses. This process is described in Subsection 7.4.2.2.

7.1.3 Industry Standards Applicable to Instrumentation and Control Systems

The BWRX-300 plant is designed to applicable International Atomic Energy Agency (IAEA), and International Electrotechnical Commission (IEC) guidance, because they are proven engineering design practices and processes that represent Relevant Good Practice. The use of these standards supports harmonised licensing internationally. These standards are tailored for nuclear sector requirements and needs. They represent a complete set of standards that are integrated and organised in a logical framework.

The IAEA guidance primarily consists of the following Specific Safety Requirements (SSRs) and Specific Safety Guides (SSGs):

- IAEA SSR 2/1 - “Safety of Nuclear Power Plants: Design, Safety Standards Series,” (Reference 7-1).
- IAEA SSG-61 - “Format and Content of the Safety Analysis Report for Nuclear Power Plants, Safety Standards Series,” (Reference 7-2).
- IAEA SSG-30 - “Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Safety Standards Series,” (Reference 7-3).
- IAEA SSG-39 - “Design of Instrumentation and Control Systems for Nuclear Power Plants, Safety Standards Series,” (Reference 7-4).

The BWRX-300 I&C systems comply with the IEC 61513 “Nuclear power plants – Instrumentation and control important to safety – General requirements for systems,” (Reference 7-5). The BWRX-300 uses Section 7 of IEC 61226 “Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Categorization of functions and classification of systems,” (Reference 7-6) to identify applicable I&C equipment standards. A summary of the key system and equipment standards applied to the I&C systems based on IEC 61226 (Reference 7-6) is shown in Table 7-1.

Each IEC digital I&C standard is complete with respect to associated V-model (i.e., system, hardware, software development V-models). These standards address process, documentation, and technical requirements that align with the BWRX-300 SCs. They use graded requirements based on the importance of safety and system functionality. The standards are up to date and are proven to support industry needs.

Section 7.3 provides a summary of the alignment for each I&C system to the key industry I&C standard IEC 61513 (Reference 7-5). Section 7.4 provides a summary of the alignment for the I&C system development process to the key industry I&C standard IEC 61513 (Reference 7-5).

7.1.4 Interfacing Systems

The interfacing systems relevant to this I&C Chapter 7 are shown in APPENDIX C.

7.1.5 Claims, Arguments and Evidence

The approach with respect to claims, arguments, and evidence, appropriate to this PSR is presented in APPENDIX A.

7.2 Instrumentation and Control System of Systems

The following sections cover the:

- Distributed Control and Information System.
- Unit Data Highway (UDH) Network.
- Network Managed Switches.
- Plant Data Highway (PDH) Network.

7.2.1 Common System Architecture (SC1, SC2 and SC3)

The following common system architecture applies to all defence lines and I&C systems (SC1, SC2 and SC3):

The DCIS includes the means to check sensor calibration. The DCIS sensor interfaces meet the range and accuracy requirements of the plant functional design. This supports operations ability to monitor plant processes. The DCIS provides the appropriate sensor interface for each sensor specified by the plant functional design.

Equipment that processes application data is separate from DCIS equipment that processes communications data. This supports deterministic operations.

The DCIS diagnostics verifies the integrity of the system software. The DCIS provides the specified equipment status monitoring interface specified by the plant functional design. This support system operates as defined by the system designer. The DCIS analogue inputs are monitored for sensor health by system diagnostics. This alerts the operators to take the required actions due to an unreliable instrument.

The Primary Protection System, Diverse Protection System and Anticipatory Protection System (APS) implement design features that minimise the chance of an inadvertent actuation. This supports unit availability goals.

DCIS monitoring of Post Accident Monitoring variables provides indication to the MCR and SCR. This provides real time plant condition information to all parties during a design basis event.

Isolation devices used to establish a safety boundary are classified as the same SC as the highest SC being isolated. This provides a minimum equipment qualification for SC1 I&C system isolation equipment.

Cyber security equipment and processes do not adversely affect DCIS system performance. This supports deterministic operations.

Communications between lower SC I&C equipment and SC1 I&C equipment is isolated, one-way communications during normal operation. For example, the LPRM gain calibrations depend on communication from SC3 to SC1, but the controller is INOP when this pathway is enabled. This minimises the chances of lower SC I&C equipment from interfering with SC1 I&C system.

The BWRX-300 does not use interlocks to prevent over pressurisation of low-pressure systems, interlocks to prevent over pressurisation of the Reactor Coolant System during low temperature conditions, interlocks to isolate SC systems from SCN systems, and interlocks to preclude inadvertent interconnections between redundant or diverse safety systems for the purposes of testing or maintenance.

No interlocks are required because the BWRX-300 design minimises piping systems, major system components (e.g., pumps and valves), and subsystems connected to the Reactor Coolant Pressure Boundary and connected systems are designed to full reactor coolant pressure, as described in Chapter 5, Section 5.4.

7.2.2 Distributed Control and Information System

The various DCIS systems are implemented on different hardware and software platforms appropriate to the safety classification of the functions they are performing, as indicated by the following colors in Figure 7-1:

- Red - Safety Category 1 DL3 functions and SC1 equipment.
- Green - Safety Category 2 DL4A functions and SC2 equipment.
- Blue - Safety Category 3 DL2 functions and SC3 equipment.
- Gold - Safety Category 3 DL4b functions.
- Black - Non-Safety Category functions and SCN equipment.
- Orange - Plant Data Highway (Enterprise Network).

The BWRX-300 I&C is implemented in an integrated DCIS. The DCIS is divided into separate I&C systems that each accomplish a subset of I&C functions based on DLs.

The DCIS systems, listed below, are developed, and integrated into an architecture that implements the BWRX-300 D-in-D strategy, as described in Section 7.4.2.

The DCIS systems are broadly divided into four SCs (SC1, SC2, SC3 and SCN). Each SC is built to specific quality and reliability requirements. DL functions are assigned to SCs.

The DCIS systems are comprised of the following:

SC1 SSCs support DL3 functions in the following systems:

- C10 - Primary Protection System

SC2 SSCs support DL4a functions in the following systems:

- C20 - Diverse Protection System
- C22 - Fine Motion Control Rod Drive (FMCRD) Motor Control System

SC3 SSCs support DL2 and DL4b functions in the following systems:

- C30 - Anticipatory Protection System
- C31 - Reactor Control System
- C32 - Reactor Auxiliaries Control System
- C33 - Equipment Cooling and Environmental Control System
- C34 - Electrical Power Supply Control System
- C35 - Reactivity Monitoring Systems
- C36 - Plant Data Acquisition, Data Communications, and Normal Operator Interface System
- C37 - Control and Monitoring System for DL4b Functions
- C38 - Turbine-Generator Control System
- C39 - Normal Heatsink and Condensate/Feedwater (FW) Control System

SCN SSCs do not support any DL functions, the following systems are SCN:

- C40 - Investment Protection System
- C41 - Plant Performance Monitoring

- C43 - Water Chemistry
- C44 - Effluent Cleanup Control System
- C45 - Network Communications and Operator Interface System

7.2.3 Network Managed Switches

The DCIS systems for SC3 and SCN are networked using a managed network switch scheme arranged in a spanning tree configuration. This allows the drops to operate independently and prevent faults in one system from adversely affecting other systems. The BWRX-300 I&C drops share data to support common services like alarming, Visual Display Units (VDUs), recording, and sending data offsite. This is to maintain distribution of data between drops on the DCIS.

The blue lines in Figure 7-1 indicate that the redundant SC3 networks appear as busses; in fact, they are a rapid spanning tree network of managed Ethernet switches as shown on Figure 7-3

Each managed network switch provides standard Ethernet switch capability but also provides additional cyber security advantages because they have security features. These include identification of authorised equipment addresses (locking out unauthorised equipment even if it is connected to the network), the capability to ignore or not uplink (to other segments), the capability to control which nodes are allowed to communicate and the capability to alarm abnormal network traffic.

Each switch is programmed to allow intercommunication only between defined nodes and to refuse communication to or from a node whose identification has not been previously defined (i.e., a “stranger” plugging into the network). Only when a switch determines that an information data packet is destined for a node on another switch (and that communication is allowed) is the information put on an uplink to another switch.

The network switches learn and maintain their own forwarding tables containing a list of the nodes and hosts on their respective network segment. When a network switch receives a data communication packet, it forwards only that data packet to the segment to which the receiving host is connected. These protocols prevent data traffic between devices on the network from affecting devices on other segments of the network.

The uplink ports on the switches are connected radially and in a data communication ring because multiple interconnections increase reliability. Specifically, the switches use a “rapid spanning tree protocol” to automatically enable and disable ports so there is only one path from the nodes of one switch to another. Should a path become disabled, the switches automatically reconfigure to establish another path through the remaining switches and fibre optic cable paths. Reconfiguration requires no operator input and is usually accomplished in much less than a second.

As described in the previous section, each switch “node” (workstation, display, and controller) is connected to redundant switches of the segment. These connections support normal plant operation. Each switch has redundant power feeds and can work from either power source. The switches and connected controllers support extensive component and data self-diagnostics, and failures are indicated. Finally, the switches are connected to a cyber security monitoring system that provides alarms for intrusion detection (or more likely, intrusion attempts) even if the switches and the network remain unaffected. Additionally, each switch monitors, controls, rejects, and reports unexpected and excessive (“data storm”) traffic on its respective network segment.

The SC3 nuclear and BOP segments of the DCIS work together as a single network, but independently of one another if failures occur. The networks are redundant and segmented to support the I&C systems with high reliability. The loss of one switch per segment has no effect

on plant operation or data. Such failures are indicated and are repairable online. In the highly unlikely event of both switches of a SC3 nuclear or BOP segment fail simultaneously, that particular segment is lost; however, the remaining segments are unaffected and individual nodes connected to the failed switches can continue to function. The remaining switches then automatically reconfigure their uplink ports such that the remaining segments automatically find available data paths between each other.

No switch or network failure can adversely affect Safety Category 1 functions because the SC1 equipment is isolated from these networks by unidirectional boundary devices.

The BWRX-300 I&C networks are highly fault tolerant such that no single network failure can adversely affect plant operation.

7.2.4 Plant Data Highway Network

Figure 7-1 shows the PDH. The communications on the SC3 nuclear and BOP segment UDHs are rigorously controlled and monitored. The managed switches control the information sent to the PDH. The managed switches are the PDH. The PDH is used for important but non-essential and non-control services like printers, plotters, long-term data storage (the current requirement is to keep plant data for at least two years). Information is sent outside the plant network through the unidirectional boundary devices at a nominal data rate of once per second through the unidirectional boundary device to the server. Various lower cyber security levels of users are connected to the server, including the on-site or off-site ERF's and utility business or engineering networks that may have their own cyber security restrictions. Only the server can respond to requests for information from outside the plant network, and the only information it has is the data sent to it through the unidirectional boundary devices. No plant DCIS component receives or is able to respond to a data request from outside the plant network. No component outside the plant network can "reach" the PDH. The managed switches do not allow any such communication to reach the PDH, SC3, or SCN UDHs. The PDH is characterised as nondeterministic and is not designed to be deterministic; instead, the PDH is designed to function as a communication channel that is reliable and responsive for displaying process information.

Access to plant cyber essential assets is appropriately protected from external or business networks by unidirectional boundary devices.

7.2.5 Unit Data Highway Network

The SC3 systems are networked together by the UDH. These systems share data with each other and with the operator workstations, historian, and the alarm function. The SC3 drops are connected together to share data with each other and the historian, alarm system and other functions.

The DL3 gateways, BOP gateway, SC3 and SCN data and control commands data is exchanged on the UDH. The network, network components, and network connections are redundant. This provides for a robust DCIS that continues to perform assigned functions with the failure of any one piece of equipment.

SC3 systems connect to the UDH as shown in Figure 7-1 using the general switch arrangement shown in Figure 7-2. This provides robust network arrangement where the failure of one component or one fibre connection does not interrupt operation.

7.3 Distributed Control and Information Architecture, Systems, Functions and Fundamental Design Properties

7.3.1 Protection System Defence Line 3/Safety Class 1

The SC1 I&C system performs the DL3 functions as detailed in Subsection 7.3.1.2. These functions detect and mitigate DBA PIEs and event sequences comprising AOO PIEs and failure of DL2 functions.

7.3.1.1 System Architecture

7.3.1.1.1 Safety Class 1 Instrumentation and Control System

The SC1 I&C system is comprised of three independent divisions. Three divisions allow for two independent trip signals when one is out of service. Each division provides independent interfaces to divisionally dedicated process variable sensors. This maintains divisional independence for sensing functions. The SC1 I&C system cabinets are in the RB in separate divisions and separate rooms. The RB rooms are seismic 1B qualified and environmentally controlled. The SC1 I&C hardware platform include two independent division outputs that can energise and de-energise outputs to solenoids associated with DL3 functions. These outputs are the interfaces from the I&C system to the mechanical components. The SC1 I&C system provides at least two isolated one-way outputs to C36 gateways. The C36 gateway data is provided for monitoring, alarming and trending. The SC1 I&C system provides isolated one-way outputs to dedicated SC3 displays in the MCR and SCR. This provides for the direct display of accident monitoring parameters. The SC1 I&C system provides an isolated one-way output to each division voting logic. The SC1 system performs DL3 functions without inputs from lower classified systems. Non-Safety Category 1 functions performed by the SC1 system do not interfere with Safety Category 1 functions.

The SC1 I&C system sets the associated outputs to trip when a diagnostic failure is detected except for ICS isolation outputs which fail as-is. The SC1 I&C system automatic DL3 functions are completed independently of operator input. This provides passive safety design. The SC1 I&C system latches all DL3 functions until manually reset by operators. This prevents unstable plant conditions caused by partial component positioning during a momentary actuation.

The SC1 I&C system utilises redundant communications for all internal and external communications paths. This prevents a single component failure from causing a failure of communications.

During a restart, the SC1 I&C system sets all outputs to a value specified by the component system functional design. This prevents uncertainty in component position during a divisional energisation.

The SC1 I&C system is powered by dedicated R10 divisional power. R10 is the dedicated SC1 power providing 72-hour battery backup. See Chapter 8 for more information.

Sensors for Type B and Type C, and other parameters required to be monitored after a seismic event (Type D, E, and F), accident monitoring variables interface with the SC1 I&C system. Type B and Type C accident sensor interfaces meet the same installation and power requirements to remain operable after a Design Basis Event.

The SC1 I&C system does not consider a bypassed division in voter logic. Bypassed equipment cannot be relied on when voting logic determines if an actuation is required. See Figure 7-7: DL3 Fail Safe Actuation Logic. The SC1 system voting logic for DL3 functions initiates a trip state when two inputs are in the trip condition. This implements Two Out of Three (2oo3) voting logic except when one division or channel is in bypass: then it operates in a Two Out of Two (2oo2) voting logic. See Figure 7-7: DL3 Fail Safe Actuation Logic.

If power to two divisions the of SC1 signal acquisition, trip determination, or actuation devices is lost, sensor failure and sensor communication is lost or voting communication is lost the reactor scrams, and the ICS is automatically initiated to remove decay heat.

The setpoints for the SC1 I&C actuation logic are determined with the setpoint methodology defined in IEC 61888, “Nuclear power plants – Instrumentation important to safety – Determination and maintenance of trip setpoints,” (Reference 7-34) using the final analytical limits from the plant safety analyses and the measurement uncertainties associated with SC1 I&C equipment (e.g., sensors and processing units).

The SC1 I&C system equipment is used to implement Safety Category 1 functions. The SC1 DCIS system is the C10 Primary Protection System.

7.3.1.2 System Design Bases and Associated Safety Functions

7.3.1.2.1 C10, Primary Protection System

The C10, Primary Protection System is a SC1 system. The system is specifically designed to perform DL3 system functions and meet the requirements of a SC1 system.

C10 cabinets are located in the RB. The RB room design includes the environmental and seismic requirements for SC1.

C10 has the ability to place an entire division into trip or the ability to insert a trip(s) for any sensor. It enables the system to remain single failure tolerant for safety actuation of the DL3 functions with one division or sensor channel inoperable.

Each division of C10 has a maintenance display in the MCR. It provides operations with the capability to perform maintenance on each division.

C10 is made up of three independent divisions. Each division is connected to dedicated sensors separate from the other two divisions. Each division of C10 includes sensor interfaces and logic used to generate sensor trips when a parameter exceeds the setpoint or a sensor fails. These sensor trips are applied separately to logic that performs the 2oo3 coincidence voting. The voting logic outputs are applied to load drivers. This maintains independence of each division for evaluation of plant conditions and the ability to make DL3 functions the result of coincidence logic. See Figure 7-7: DL3 Fail Safe Actuation Logic.

Fail-safe Solenoid Configuration

Load driver controls power to the solenoids. There are fail-safe and fail as-is load driver configurations, the following describes the fail-safe configuration:

- See Figure 7-4: Fail-Safe Component Interface and See Figure 7-7: DL3 Fail Safe Actuation Logic.
- SC1 power is applied to the solenoid circuit.
- Manual switches (located in the MCR and SCR) interrupt power to the solenoids in the fail-safe component interface circuit.
- The C10 load driver turns off, based on the input from the voting logic. If C10 loses power, the load driver turns off and the solenoid is de-energised.
- SC1 fail-safe solenoid control includes isolated interfaces that can be controlled by C20 and C30.
- The C20 DPS performs DL4a functions by opening a contact in the power path to the solenoid. If C20 loses power, the associated contact remains closed, and the solenoid remains energised.

- The C30 APS performs DL2 functions by opening a contact in the power path to the solenoid. If C30 loses power, the associated contact remains closed, and the solenoid remains energised.
- No failure in C20, C30 or the hand switch logic can prevent C10 from performing the DL3 function.
- The fail-safe logic is repeated in each of two divisions. Both divisions have to de-energise their solenoids for the associated function to occur. Most DL3 functions involve multiple SC1 components so multiple solenoids may be de-energised for a single DL3 function.
- The fail-safe operation ensures any single failure does not result in a spurious action or the loss of a DL3 function.

Fail as-is Solenoid Configuration

Each load driver controls power to one solenoid. There are fail-safe and fail as-is load driver configurations, the following describes the fail as-is configuration:

- See Figure 7-5: Fail As-Is Component Interface and Figure 7-8: DL3 Fail As-Is Actuation Logic.
- SC1 Power is applied to the solenoid circuit only during actuation.
- Fail as-is is only used for the ICS Isolation function.
- The manual switches have three positions. Open/Auto/Close. In Auto position, the power is applied to the load driver. If the C10 logic actuates to close the valve, then the load driver energises the close solenoid.
- Each division controls one close solenoid valve. Two close solenoids need to be energised to close the valve.
- C10 provides for a fail as-is function that functions with a single division failure.
- Fail as-is manual isolation is only from the SCR.

Manual Actuation Switches

Manual actuation switches are located in the MCR and the SCR. These switches allow the operators to manually perform the automatic functions. The reset function for the DL3 I&C functions is provided in the MCR. The manual switches provide the ability for the operator to actuate C10 actuations. This is not a Safety Category 1 function.

Isolated One-way Outputs

Each division provides sensor, trip, and diagnostic information to C36 through their isolated one-way redundant outputs to C36 gateway as shown in Figure 7-6: DL3/SC1 Functions and Signals. C36 provides monitoring, alarming and recording of C10 parameters.

Division Bypass

C10 includes the capability to bypass one division of sensors at a time or no divisions. The bypass switch has four positions:

- Division 1
- Division 2
- Division 3
- Normal

The bypass switch is a mechanical switch that can only be placed in position to bypass one division at a time. C10 provides operators with the means to bypass a division with a failure, or while under test.

Communications

Internal Communications

Each division communicates sensor trip data and bypass status to the voting logic. Any failed sensor for fail-safe logic or loss of communications results in the voting logic seeing these failed or lost signals as trip inputs to the voting.

External communications

The communication portion of each C10 division provides redundant isolated outputs to the C36 gateways. The three divisional optical fibre message streams are sent to two SC3 gateways and then to the UDH network. The gateways are redundant such that if one fails, all three divisions of C10 signals are still available for alarming, recording, and monitoring in the lesser DLs. This communications path is separate from and independent of the communications from the C10 divisional trip logic responsible for 2oo3 voting and actuation of the C10 divisional load drivers.

No Safety Category 1 function is dependent on whether the optical fibre gateways are connected or disconnected as the gateways are via a one-way pathway (e.g. data diode) such that status or operation of the gateways has no effect on any DL3 functions.

C10 prevents any communication failure from causing or preventing a DL3 Safety function.

The design basis of the SC1 I&C system is to mitigate the effects of a PIE (i.e., AOO or DBA and most DECs) assuming no credit for Safety Category 2 or Safety Category 3 functions (e.g., CCF).

The design bases of Safety Category 1 functions are to act when Safety Category 3 functions are not effective at intercepting a transient or when an event is beyond the capabilities of the Safety Category 3 functions. If Safety Category 1 functions completely fail, Safety Category 2 functions are designed to prevent core damage. As such, for common physical parameters measured by the DLs, the Safety Category 3 function setpoint needs to be designed to act first, because the SC3 design bases are to mitigate/prevent SC1 from needing to respond. Safety Category 1 and 2 functions have common analytical limits to simplify transient and accident analyses and application of the formal setpoint methodology. The use of a common analytical basis has no adverse effect on plant operations or safety.

Safety Category 1 functions operating alone ensure no AOO or DBA causes a radiation release greater than the regulatory requirements. Safety Category 1 functions operate independently of Safety Category 3 functions using diverse equipment to perform required Safety Category 1 functions. The supporting safety analyses are described in Chapter 15.

The main functions of the SC1 I&C logic are the initiation of the Safety Category 1 functions for reactor scram, reactor and containment isolation, and ICS initiation functions. The SC1 I&C system design includes provision of instrumentation to monitor plant variables and the system over the respective ranges for operational states and PIE to ensure that adequate information can be obtained on plant status.

SC1 I&C system is designed to be available during all modes of plant operation. Specific safety functions actions are mode dependent, as determined by the Fault Evaluation process described in Chapter 15 and specified by the Mode shown for each function in Table 7-2.

No Safety Category 1 I&C function for control room habitability has been identified at this stage of the design progression. More information on the Control Room Habitability System is found in Chapter 6, Section 6.6.1, and Chapter 9A, Section 9A.5.2.3.

The following DL3 functions are categorised as Safety Category 1 and are implemented in the SC1 I&C equipment:

1. Hydraulic Scram Function
2. Power Range Neutron Monitoring System (PRNM) Function
3. RPV Containment, and System Isolation Functions
4. ICS Isolation Function (x3 Isolation Condensers (ICs) Trains A, B, and C)
5. Isolation Condenser System Initiation Function (Train A, B and C)

The following non-DL3 functions are also implemented in the SC1 I&C equipment:

6. Manual I&C switches
7. Accident Monitoring

These are also shown on Figure 7-6: DL3/SC1 Functions and Signals

These are explained in more detail below:

Hydraulic Scram Function

SC1 I&C initiates a trip when a measured parameter exceeds a predefined setpoint. Initiates a hydraulic scram with a 2oo3 voting logic using the same parameter. The trip logic is used to scram the reactor by hydraulically inserting the control rod blades. Hydraulic Control Units (HCUs) are pressurised accumulators used to forcibly drive the control rod blade into the core. Scram initiation is enabled by de-energising two scram solenoid valves to vent air holding the HCU scram valve closed against a spring force. When the HCU scram valve is opened, two control rod blades are inserted into the core except for one HCU that inserts a single control rod blade. The Safety Category 1 hydraulic scram functions and initiation signals are listed in Table 7-2.

The HCUs are arranged in four spatial groups (three with 7 HCUs and one with 8 HCUs). Twenty-nine HCUs are used to drive the 57 control blades. The SC1 hydraulic scram uses two divisional load drivers to de-energise the HCU scram solenoid valves.

Simultaneous with the initiation of the Safety Category 1 hydraulic scram, a scram follow signal is sent to SC2 equipment to have each FMCRD motor drive its ball nut upward to a position just below the fully inserted and latched hollow piston that is coupled to the control rod blade. This signal is sent whenever a hydraulic scram is demanded by SC1 I&C regardless of whether the hydraulic scram actuation has been successful.

More information on the Control Rod Drive (CRD) System is found in Chapter 4, Section 4.6.

Power Range Neutron Monitoring Function

C10 includes the hardware used to process LPRMs. C10 calculates the average power range power and the simulated thermal power signal to provide for reactor trip. Average power based on neutron flux is the primary means of determining if the reactor is experiencing a reactivity addition AOO.

The LPRM data is provided through the isolated C36 gateway to the C35. C35 calculates calibration factors for the LPRMs. The design includes the capability to perform semi-automatic gain factor updates by transferring data from C35 to each division of C10 while the division is bypassed. Implementation of this capability is pending cyber assessment. Updating LPRM gains based on calculated core thermal power using a heat balance reduces the uncertainty associated with power level and protection.

The PRNM also provides signals for accident monitoring, to the Three-Dimensional (3D) Core Thermal Power Distribution Monitor, and to the SC3 control rod blocking systems. These

additional functions are not required to support any Safety Category 1 function; however, SC1 I&C is used to acquire the sensor inputs.

More information on core monitoring is found in Chapter 4.

RPV, Containment, and System Isolation Function

The SC1 I&C system performs the Safety Category 1 functions for RPV and containment isolation by closing the Main Steam Reactor Isolation Valves (MSRIVs), Main Steam Containment Isolation Valves (MSCIVs), Feedwater Reactor Isolation Valves (FWRIVs), and Feedwater Containment Isolation Valves (FWCIVs) and other valves listed in Chapter 6 to limit line break effects both inside and outside containment. The isolation functions and initiation signals are listed in Table 7-2. The different isolation signals are initiated when 2oo3 divisions agree on an isolation demand.

More information on the different isolation valves is found in Chapter 5 and Chapter 6.

Isolation Condenser Isolation System Function (Three Trains)

The SC1 I&C system performs the Safety Category 1 function to initiate ICS, which is comprised of three ICs.

The three BWRX-300 ICs are each a simple loop including the vessel steam supply, piping to the radiators (i.e., heat exchangers) submerged in the ICS pools and a line to return the condensed steam to the vessel.

Each IC steam supply line and condensate return line are equipped with two series normally open isolation valves mounted directly to the reactor vessel.

This Safety Category 1 function is implemented in three trains of ICS Isolation.

The ICS functions are listed in Table 7-2.

More information on the ICS is found in Chapter 6.

Isolation Condenser System Initiation Function (Three Trains)

This Safety Category 1 function is implemented on an SC1 platform. All three trains are controlled by C10.

The ICS is initiated by opening the normally closed condensate return valves. The SC1 I&C logic activates each IC separately using 2oo3 voting logic.

When initiated by high reactor pressure, a different initiation setpoint is used for each IC. An IC is initiated by opening a normally closed condensate return valve per IC. When the 2oo3 voting logic is satisfied, a pair of load drivers de-energise the solenoids that are being used to hold the fail-open valve closed.

The ICS initiation signals are listed in Table 7-2.

Manual Instrumentation and Control Switches Initiation

Switches are provided in both control rooms to enable manual actuation of the automatic functions performed by C10 although it is part of the system that delivers the DL3 function the manual actuation is not claimed as a DL3 function. For fail-safe functions, two switches are provided. One division 1 switch and one division 2 switch. Both switches have to be operated to cause the actuation. The design ensures that once initiated, the function goes to completion by requiring a reset to clear the demand. The manual switches are software free and control contacts wired in series with the SC1 solenoid circuit. The manual control interface is independent of the automatic control functions. See Figure 7-4: Fail-Safe Component Interface. Fail as-is manual control for the ICS isolation, which is only possible from the SCR, is different. The switches are three position switches (Close/Auto/Open). There are three

solenoids for each ICS isolation valve. See Figure 7-5: Fail As-Is Component Interface. Automatic DL3 functions have the means for manual actuation.

Accident Monitoring

BWRX-300 Accident Monitoring of Type B and Type C variables is a Safety Category 3 function; however, this function is performed by C10. Many of the parameters monitored by C10 to perform its automatic Safety Category 1 functions are used for accident monitoring. The plant architecture specification specifies the population of Type B and C accident monitoring parameters along with select Type D, Type E and Type F for availability after seismic event. Note there are no Type A variables in the BWRX-300 design.

Accident Monitoring of select post-accident variables are required to be monitored during and after a seismic event. C10 is designed to perform their DL3 functions after a seismic event and R10 electrical system is designed to provide power after a seismic event.

Parameters not monitored by C10 for automatic DL3 functions are monitored by dedicated Input/Output (I/O) modules that are electrically isolated from the portions of the system that perform the Safety Category 1 functions. This isolation ensures that the Safety Category 3 accident monitoring inputs cannot adversely affect performance of the automatic Safety Category 1 functions while providing a seismically qualified means of obtaining accident monitoring information required to be available after a seismic event.

To prevent C10 from being affected by the SC3 displays, each division of the primary C10 platform provides redundant one-way data communication pathways to the C10 accident monitoring display platform. The one-way communication outputs for accident monitoring are different than the outputs provided to transmit data to the SC3 network. This provides post-accident monitoring for values that are required to be available after a seismic event.

Redundant pairs of displays are installed in the MCR and SCR. The hardware is redundantly powered from R10 with electrical isolation that prevents the propagation of faults from lower to higher safety class components. Each redundant VDU can display the complete set of accident monitoring data from the three divisions. The VDUs only support monitoring functions, but the platform may enable navigation between different views and screens to comply with Human Factors Engineering (HFE) requirements. This prevents C10 from being affected by the SC3 displays and provides a robust display providing the operators with the data necessary to deal with plant conditions after an AOO.

7.3.1.3 Fundamental Design Properties in the System Design

The SC1 I&C system design includes DL1 properties that represent the quality measures implemented to minimise the potential for failures to occur using conservatism in design and analyses. These DL1 properties of qualification, reliability, robustness, security, diversity, and D-in-D features are discussed in the following five subsections.

Subsection 7.3.1.1 System Architecture describes the architectural design properties that support the SC1 system reliability.

A software-free interface is used in the SC1 I&C system to provide hardwired manual scram, and ICS Initiation and isolation capabilities.

7.3.1.3.1 Equipment Qualification

The SC1 I&C equipment is designed to operate in the environment that would be expected during both normal operations and anticipated off-normal conditions. The SC1 I&C equipment is qualified to perform its intended functions. Qualification addresses both hardware and software aspects of the SC1 I&C system. The SC1 I&C design and manufacturing processes are of sufficient quality to ensure the I&C system can reliably perform their credited protection functions. The SC1 I&C system equipment is designed, developed, fabricated, and tested to quality standards commensurate with the safety significance of the functions to be performed.

The SC1 I&C qualification measures confirm that the I&C system and equipment are capable of reliably performing the design basis functions for which they are credited over the range of environmental conditions postulated for the area in which they are located.

The SC1 I&C hardware platform used to perform its functions is developed in accordance with IEC 60987, “Nuclear power plants – Instrumentation and control important to safety – Hardware requirements,” (Reference 7-35) and meets IEC 61513 (Reference 7-5) requirements and the equipment standards defined in Section 7 in IEC 61226 2020 (Reference 7-6) for the SC1 I&C system.

SC1 software used to perform Safety Category 1 functions is developed in accordance with Category A requirements of IEC 60880, “Nuclear power plants - Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions,” (Reference 7-25) and IEC 62566:2012, “Nuclear Power Plants – Instrumentation and control important to safety – Development of Hardware Description Language (HDL)-programmed integrated circuits for systems performing category A functions,” (Reference 7-59). Noting that Safety Category 1 functions and Safety Category A functions are equivalent terminology.

SC1 hardware used to perform Safety Category 1 functions is qualified for environmental conditions in accordance with IEC 60780, “Nuclear Facilities – Electrical Equipment Important to Safety – Qualification,” (Reference 7-29) and seismic interaction in accordance with IEC 60980-344, “Nuclear facilities – Equipment important to safety – Seismic qualification,” (Reference 7-30).

The SC1 I&C equipment is qualified for electromagnetic compatibility in accordance with IEC 61000-4, “Electromagnetic Compatibility Package,” (References 7-27, 7-36 through 7-52) and IEC 61000-6-2, “Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity standard for industrial environments,” (Reference 7-28).

7.3.1.3.2 Reliability

The SC1 I&C system has the required reliability to perform its intended functions. It has an initial quantitative reliability target of less than 1E-4 probability of failure on demand. These reliability targets are achievable based on GEH experience with similar Nuclear Power Plant protection systems. The reliability of the SC1 I&C system is demonstrated as part of the final design.

The reliability analysis of the SC1 I&C system uses qualitative and quantitative performance measures or criteria, as appropriate, to demonstrate reliability goals. The reliability assessment is used to optimise goals such as minimising out-of-service time for repair and reducing the frequency of surveillance testing.

The SC1 I&C system uses digital technology and different Safety Category 1 I&C functions may be combined on a common platform. It uses three divisions with 2oo3 voting logic for trips and initiations. Spurious actuations due to single hardware failures are prevented. This meets the application of the single failure criterion for Safety Category 1 functions.

The three-division redundancy scheme is acceptable based on high reliability of the SC1 system, administrative controls that limit the time allowed for removal from service for maintenance bypass, and the availability of SC2 DPS as a backstop to ensure that the overall plant safety goals are satisfied.

Online Maintenance

The SC1 I&C Design allows one division’s sensor(s) to be bypassed. There is one Bypass Unit in each division. Each Bypass Unit sends a fibre optic signal to the division of sensors Bypass Switch and monitors for the presence of a return signal. The presence of a return signal indicates that the associated division of sensors should be bypassed. Each Bypass Unit

sends a signal, to all three Output Voter Units, to indicate whether the associated division of sensors should be bypassed. When a division of sensors is bypassed the same division's Output Voter Unit remains operational, but the bypassed division of sensors are no longer counted in the 2oo3 vote. The voting logic effectively becomes 2oo2, and the Output Voter Unit remains operational. The ability to bypass a single division allows for online tests, faults, and maintenance while still maintaining C10's ability to perform all C10 safety functions.

For the BWRX-300 design, no manual online testing of SC1 equipment is required because on-line testing and self-diagnostics features continuously check the system during operation. The need for online maintenance is expected to be infrequent because of the high reliability requirements for the SC1 system. The time allowance for online maintenance is controlled by plant Technical Specifications (TS). During this period, the SC2 DPS provides an additional layer of protection for any additional problems affecting the SC1 system during the maintenance activity.

The use of measuring and test equipment that can impair SC1 I&C equipment requires deliberate manual intervention via hardware interlock features at the system interfaces.

Each division of LPRMs can be bypassed to allow the updated sensor calibrated values to be periodically input to the logic as required by plant TS. Average Power Range Monitor (APRM) signals are periodically calibrated to current core thermal power. The LPRM averaging logic that is used to calculate the APRM value monitors the number of bypassed LPRMs going into the average. If the number drops below a predefined amount, the average is declared invalid, and the downstream logic assumes an APRM trip for that division.

Correct functioning of the SC1 digital I&C platforms are continuously monitored by self- testing features rather than by manual surveillance testing. Critical faults detected by the self- testing features trip the outputs of the division and other faults are alarmed. The SC1 system is designed to support required surveillance testing without affecting plant operation. It provides for signal and division bypass to support maintenance and testing. Bypass conditions are alarmed in the MCR. The SC1 I&C is designed to support periodic testing of the entire division of instrumentation logic, from sensing device to actuating device. See Subsection 7.3.1.2.1.

The SC1 I&C platforms and diagnostics and their communication to the SC3 nuclear segment are designed to support online and automatic surveillance testing that meets TS requirements. Testing and performance assessment requirements are developed using the guidance of IEC 60671, “Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing,” (Reference 7-53) and IEC 62385, “Nuclear power plants – Instrumentation and control important to safety – Methods for assessing the performance of safety system instrument channels,” (Reference 7-54). Redundant divisions are monitored for deviations by an automated function that is performed continuously in the Technical Specifications Monitor (TSM) described in Subsection 7.3.3.2.7. Deviations greater than a specified value are alarmed.

Hydraulic Scram Function

For each pair of HCU scram solenoids, one scram solenoid uses a load driver from Division 1 and the other load driver from Division 2. Division 1 and Division 2 load drivers open on a 2oo3 vote from the three divisions communicated via optical fibre. Both scram solenoids in the HCU are de-energised to initiate a scram. The HCU scram design allows surveillance testing of each division through to the solenoid without causing a scram in normal operation. Testing provisions that are permanently connected to safety systems are classified the same as the safety system. The arrangement of the scram solenoid control and power is shown as Figure 7-4.

Although Figure 7-4 indicates a single load driver in division 1 and in division 2, in fact there are multiple load drivers assigned to the scram solenoids in HCUs located in four separate

rooms in the RB. In addition, the reactor can also be shut down with the complete failure of the Safety Category 1 hydraulic scram function with the diverse backup of Safety Category 2 functions. The cables from the load drivers to the four HCU rooms are in individual grounded conduits to preclude the possibility of a hot short keeping the scram solenoids incorrectly energised. Specifically, the circuit shown in Figure 7-4 is replicated four times per division 1 and division 2 based on the assignment to HCU scram solenoids.

Reactor Pressure Vessel, Containment, and System Isolation Function

The reactor and containment isolation valves are closed by de-energising two isolation valve solenoids mounted on the valve actuators. One of the isolation solenoids uses a load driver and uninterruptible power from Division 1 and the other solenoid is powered from Division 2. Division 1 and Division 2 load drivers open on a 2oo3 vote from the three divisions communicated via optical fibre. Both isolation solenoids per isolation valve are de-energised to initiate a valve closure. This valve design allows surveillance testing of each division through to the solenoid without causing an isolation in normal operation. The arrangement of the isolation solenoid control and power is shown as Figure 7-5.

Isolation Condenser System Function

The ICS actuation circuits have two normally energised solenoids on the IC open or close valves that keep it normally closed. One of the valve solenoids is in division 1 and the other valve solenoid is in division 2. Each solenoid has a normally closed load driver that opens on a 2oo3 vote from the three divisions communicated via optical fibre. Both solenoids per actuation valve are de-energised to initiate a valve opening, this allows surveillance testing of each division through to the solenoid without causing ICS initiation in normal operation.

Isolation Condenser Isolation System Function

Each IC isolation valve is designed with three divisional solenoids, and 2oo3 solenoids must change state for the valve to open or close. Reliable isolation and prevention of inadvertent isolation is achieved by the assignment of the SC1 I&C divisions to solenoid valves that control each IC isolation valve and the mechanical arrangement of the solenoid valves to ensure that a single failure does not result in the unwanted isolation of an IC or prevent a required isolation of an IC. Manual actuation of the IC isolation function can be performed on a train-by-train basis. This manual isolation is implemented via SC1 equipment, because no lower classified equipment can have the ability to isolate an IC train (which would potentially prevent SC1 actuation of that train).

Power

The SC1 I&C system uses dual power supplies and dual power feeds per chassis to increase system reliability and availability.

7.3.1.3.3 Robustness

Robustness of the SC1 I&C design is the degree to which it can function correctly in the presence of invalid inputs or stressful environmental conditions (see Subsection 7.3.1.3.1). The robust SC1 I&C design reflects the use of design methods and adherence to engineering best practices to ensure its functions are achieved for all operational states and accident conditions. The SC1 I&C design requirements address the full range of operating environments associated with normal operation, transient, and accident conditions, as well as foreseeable internal and external hazards.

Separation and Independence

The SC1 I&C system has the required separation and independence to perform its intended functions.

The SC1 I&C equipment is in three separate divisional fire barrier rooms in the RB.

The SC1 I&C system uses sensors and actuators independent of the SC2 DPS.

The SC1 I&C system provides trip communication between divisions for voting using optical fibre. A unidirectional boundary device provides for isolated optical communications to SC3 systems through the SC3 gateways to prevent communication from lower safety class systems from affecting the SC1 I&C system. The SC1 communication protocols meet the data communication requirements for Category A functions in IEC 61500, “Nuclear power plants – Instrumentation and control systems important to safety – Data communication in systems performing category A functions,” (Reference 7-31). The isolation devices are classified as SC1.

The logic used to rapidly scram the reactor by hydraulically inserting the control rod blades is separate and independent of the normal FMCRD positioning controls using the Rod Control and Information System (RC&IS).

Each LPRM string has four LPRMs (which are miniature fission chambers) equally spaced vertically along the approximate 3.7-metre height of the core. The LPRM string is located between the corners of the fuel channels of the adjacent four fuel bundles. The locations are determined such that the 3D core thermal power distribution monitoring program can use mirror and rotational symmetry to virtually rotate and reflect the LPRM readings for unmonitored locations with similar surrounding fuel to gain complete core coverage.

Each LPRM is individually powered and signal conditioned by its associated division and then averaged to generate APRM and Simulated Thermal Power values, which are compared to setpoints to determine if a scram is required.

The SC1 I&C physical separation and signal isolation devices meet the requirements of IEC 60709, “Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Separation,” (Reference 7-22).

Redundancy

The SC1 I&C system is designed with three divisions with 2oo3 voting logic for trips, isolations, and initiations. This redundancy ensures that the protection functions can be actuated even with an assumed single failure. It is only physically possible to bypass one division of sensors or one division of logic at a time, which retains the capability to provide required safety actuations. When a bypass is used, the 2oo3 logic behaves as the equivalent of 2oo2 to trip, isolate, or initiate. Bypass conditions are alarmed in the MCR. The three-fold redundancy scheme is acceptable based on high reliability of the SC1 equipment performing Safety Category 1 functions, administrative controls limit the time allowed for removal from service for maintenance bypass, and the availability of Safety Category 2 functions as diverse D-in-D to ensure that the overall plant safety goals are satisfied.

Fail Safe

The SC1 I&C system has the required fail-safe design features to perform its intended functions. Deliberate operator action is required to return the SC1 I&C system to normal after actuation.

A critical self-diagnostic hardware or software failure initiates a divisional trip for fail-safe logic circuits. Diagnostic failures may be classified as critical (such as the watchdog timer or loss of communication) and cause a trip in that division. Other diagnostics are non-critical (e.g., one of the redundant power supplies fails) and cause an alarm in that division.

Scram, PRNM, and Reactor and Containment Isolation Functions

The SC1 hydraulic scram and Reactor and Containment isolation functions use only fail-safe logic (including loss of sensor and communications data). The SC1 hydraulic scram logic is also equipped with individual manual scram switches in division 1 and division 2, as are the fail as-is IC isolation functions. These switches interrupt the power to the scram solenoids

independently of the SC1 hydraulic scram logic and do not use any software. The switches are included in the MCR and SCR, and both switches are required to be operated to cause a scram. A loss of uninterruptible power or logic power causes a SC1 hydraulic scram, and RPV and containment isolation but does not close the IC Reactor Isolation Valves (RIVs).

The Safety Category 1 PRNM logic provides flux related trip signals to SC1 hydraulic scram. It also provides signals to the SC3 DCIS for use to determine if a rod block is required (see Section 7.3.3) and to computer functions that determine the 3D power distribution of the core.

The LPRM averaging logic that is used to calculate the APRM value monitors the number of available LPRMs going into the average to ensure it is representative. If the number drops below a predefined amount, the average is declared invalid, and the downstream logic assumes an APRM trip for that division.

Isolation Condenser System Initiate/Actuate Function

The SC1 ICS actuation logic initiates the three ICs separately (using 2oo3 voting logic) for both reliability reasons and to allow different initiation setpoints for each IC. A loss of power initiates all three trains of the ICS. The condensate return valves are open/close only and are operated by Safety Category 1 functional logic. The logic is similar to the Safety Category 1 hydraulic scram function logic.

Isolation Condenser Isolation System Function

The ICS isolations do not use a fail-safe design. Instead, the IC steam supply and IC condensate return isolation valves are designed to fail-as-is to minimise the potential for inadvertent isolation (i.e., the valves require active power to change position). Additional design features are provided to ensure that the ICS provides the required safety functions. The SC1 I&C logic actively energises the IC isolation valve solenoids to isolate an IC and each IC is isolated independently and only upon indication of a line break for that IC.

The IC isolation logic works by each division acquiring the isolation parameters. Bypass conditions are alarmed in the MCR. The signals are compared to their setpoints and vote to trip (per division) if the sensed signal exceeds the setpoint. The three divisions communicate their trip decisions, and each division determines if at least two divisions have tripped to initiate an isolation. Unlike fail-safe logic, which treats an invalid input or loss of communication as a vote to trip, fail-as-is logic ignores invalid inputs such that the logic always requires two valid trip votes prior to actuation. If at least two divisions have tripped, an isolation is initiated. If logic or valve solenoid power is lost or the logic fails self-diagnostic monitoring, the isolation valves remain at their last position. From this point the fail-as-is logic differs from the fail-safe logic used for SC1 I&C actuation features.

The divisional logic outputs change state (open or close the isolation valves) only with active power. Logic and sensor diagnostics are alarmed but do not initiate isolation. A loss of power to the division or to the solenoids does not initiate isolation. The isolation is active and latching to fail-as-is. Three solenoids are provided on each isolation valve and energising any 2oo3 solenoids cause the valve to change position and latch. The three solenoids provide single failure tolerance (e.g., loss of one division of power) because the fail-as-is design requires power from at least two divisions. Reliable isolation, when required, is achieved by requiring 2oo3 solenoids and 2oo3 divisional logics to initiate an isolation. The 2oo3 logic minimises the potential for inadvertent isolation for random I&C component failures.

7.3.1.3.4 Security

The SC1 I&C system has features that adequately addresses access control to limit cyber security vulnerabilities and ensure the system can perform its intended functions. The SC1 I&C design incorporates access control features to support establishment of a secure operational environment. The SC1 I&C software is produced in a secure development environment that prevents the insertion of undocumented codes. The SC1 I&C system is

installed and maintained in accordance with the station administrative procedures and control of access programs.

The SC1 I&C network is isolated from the rest of the BWRX-300 DCIS. The three SC1 DCIS divisions operate completely independently from the SC2 and SC3 DCIS. Information only flows through unidirectional boundary devices from SC1 I&C to the SC3 networks when the system is in operation. Two-way data flow can be used with appropriate access control features to support LPRM calibration. The SC3 nuclear segment includes the SC3 gateways that receive isolated SC1 signals through a unidirectional boundary device and provide them to the SC3 nuclear segment.

The SC3 gateways are discussed in Section 7.3.3. Measured parameters, setpoints, logic and trip status, and diagnostic information are continuously sent through these gateways to the SC3 nuclear segment TSM, which can perform online surveillance testing, alarm on discrepancies, and additionally alarm on loss of these expected communications.

Refer to Chapter 25 for more detail.

7.3.1.3.5 Diversity and Defence-in-Depth

The SC1 I&C system provides the main line of protection for AOOs and DBAs. The SC3 nuclear segment provides anticipatory trip functions to support the D-in-D concepts. Safety Category 3 functions are designed to prevent or mitigate AOOs before either Safety Category 1 or Safety Category 2 is required. The design basis of the Safety Category 2 functions provides D-in-D for the complete failure of the Safety Category 1 function (i.e., CCF). Safety Category 2 functions independently provide comparable Safety Category 1 functions using diverse platforms from those used in SC1 equipment. See Figure 7-14.

Hydraulic Scram Function (Manual Initiation)

The hydraulic scram is equipped with individual manual scram switches in division 1 and division 2 (as shown on Figure 7-4). These switches use a software free method to interrupt the power to the scram solenoids independently of the automatic actuation logic and using no software. The switches are included in both the MCR and SCR and both switches are required to be operated to cause a scram.

Isolation Condenser System Function (Manual Initiation)

The SC1 ICS initiation logic is equipped with individual switches in division 1 and division 2 to open the ICS condensate return line valves. These switches use a software free method to close the valves. The switches are included in both the MCR and SCR and both switches are required to be operated to cause an ICS initiation.

Reactor and Containment Isolation Functions (Manual Initiation)

The SC1 I&C reactor, containment, and system isolation functions can be performed using manual hardwired switches in Division 1 and Division 2 to close the MSRIV, MSCIV, FWRIV, and FWCIV. These switches use a software free method to close the valves. The switches are included in the MCR and SCR and both switches are required to be operated to close these valves.

Isolation Condenser Isolation Function (Manual Initiation)

SC1 manual switches provide a manual means of isolating each ICS Isolation Valve train and a manual means of re-opening the ICS RIVs. These manual switches are only present in the SCR.

7.3.1.4 Operator Interface and Accident Monitoring

Data from the SC1 I&C system is available on appropriate displays and these displays are subject to an HFE evaluation to maximise operator responsiveness. Redundant VDUs are

located in both the MCR and SCR. The displays also include an alarm system to provide operator awareness and to prompt to the displays containing further information relating to the alarm. SC1 I&C system bypass conditions are alarmed in the MCR. The displays are menu-driven, and it is possible to switch between related displays without going through the main menu.

A reactor scram, ICS initiation, and reactor and containment isolation, can be manually initiated by switches in the MCR and SCR. Manual actuation of the IC isolation function can be performed on a train-by-train basis using the manual switches in the SCR.

Signals monitored by the SC1 I&C system provide necessary information to achieve or verify correct plant response to transients and accidents. The necessary signals are determined through HFE analysis and applicable regulatory requirements and are referred to as accident monitoring signals.

The signals monitored by the SC1 I&C system are recorded, alarmed, and displayed to the operator on an appropriate display (e.g., range check problems or alarm setpoints exceeded). The SC1 I&C signals and the various SC1 I&C components are alarmed for self-diagnostics.

The monitored parameters required to be available for 72-hours are supported by the SC1 Uninterruptible Power Supply (UPS) and batteries with no off-site power available.

Data from the SC1 I&C system is also transmitted through a unidirectional boundary device to SC3 DCIS and separately to SC3 equipment qualified for Safety Category 3 accident monitoring functions, where the signals are recorded, alarmed, and displayed. The associated monitoring also includes signals needed to monitor divisional support equipment like the UPS and battery chargers, as well as the SC1 equipment room temperatures. The operator can view the information for the SC1 I&C system on the associated VDUs even if the SC3 DCIS is not operational.

The SC1 I&C system acquires and displays the accident monitoring information required to be displayed for 72hrs and/or after a seismic event which consists of Type B and C, select D, and select F accident monitoring variables.

The BWRX-300 plant level safety diversity and D-in-D design has a direct bearing on the design of the accident monitoring instrumentation. The BWRX-300 passive reactor design automatically actuates Safety Category 1 functions that rely solely on natural passive mechanisms based on fundamental physical and thermodynamic principles to mitigate a design basis event (i.e., AOOs or postulated accidents). The BWRX-300 does not require manual actions to mitigate design basis events. Automatic controls perform mitigation functions. As such, no Type A accident monitoring instruments are required. The simplicity of the BWRX-300 safety features to mitigate design basis events and safely shut the plant down, when coupled with the BWRX-300 D-in-D framework, ensures the capability to mitigate the effects of AOOs and DBAs even with a coincident loss of a complete DL.

The simplicity, diversity, and D-in-D framework change the role of the Type B and C accident monitoring instruments for the BWRX-300 accident management strategy. For the BWRX-300, these instruments are only used for immediate verification that DL safety category functions have actuated. They are not needed for subsequent operator actions to realign or control more complicated engineered safety features after the initial actuation phase. The multiple DLs and their capability to accommodate the loss of a complete DL eliminate the need for more immediate operator actions to respond to equipment failures for successful accident management. The specific accident monitoring variables that the operator should monitor to ensure safety during an accident and the subsequent long-term stable shutdown phase are determined through the normal BWRX-300 design process using the HFE process. The Type B and C accident monitoring information is displayed in both the MCR located in the CB

and the SCR located in the RB. The accident monitoring information acquired by the SC1 I&C system is sent through qualified isolation devices to the SC3 DCIS network.

A preliminary list of the Type B and C accident monitoring variable is provided in Table 7-3.

The Human System Interface (HSI) for SC1 protection system is described in Sections 7.5 and 7.6 for the MCR and SCR, respectively.

7.3.1.5 Compliance Alignment

Table 7-6shows how the SC1 I&C system aligns to the key industry I&C standards IEC 61513 (Reference 7-5).

7.3.1.6 Interfaces with Other Systems

- CRD System - Chapter 4
- Core Monitoring - Chapter 4
- Isolation Valves - Chapters 5 and 6
- ICS - Chapter 6

7.3.1.7 Performance and Safety Evaluation

The system designed bases, and associated safety functions are described in Subsection 7.3.1.2, System Design Bases and Associated Safety Functions.

7.3.1.8 Application of ALARP Principles in Design Development

The SC1 I&C system design development is compliant with the ALARP principle through the application of appropriate codes and standards, Operational Experience (OPEX), and optioneering, where relevant. The I&C system development process is detailed in Section 7.4.

7.3.2 Diverse Protection System – Defence Line 4a/Safety Class 2

The SC2 system acquires the plant information from the sensors specified for systems performing Safety Category 2 functions. The specific list of parameters to be measured, the physical locations of the sensors, and environmental qualification envelope for the equipment are specified as part of the detailed design process. The plant information acquired is displayed on the SC3 integrated plant displays developed through the HFE process.

7.3.2.1 System Architecture

7.3.2.1.1 Safety Class 2 Systems

The SC2 I&C systems perform the DL4a I&C functions. The DL4a I&C functions for reactor trip, ICS initiation and most isolations are fail as-is, this excludes any mechanical actuators which are all fail-safe. This detects and mitigates DECs, including event sequences associated with certain DBA PIEs and failure of DL3 functions.

SC2 I&C system equipment is used to implement Safety Category 2 functions. The SC2 DCIS systems are C20 and C22. The following are I&C architecture requirements for C20 and C22.

As stated in Section 7.2.1 common system architecture applies to all defence lines and I&C systems. Further detail on these systems and their allocated functions are given in Subsection 7.3.2.2.

7.3.2.2 System Design Bases and Associated Safety Functions

The design bases for Safety Category 2 functions assume the complete failure of Safety Category 1 functions (i.e., CCF). Safety Category 2 functions are implemented in SC2 equipment that is independent and diverse from the SC1 equipment. The SC2 equipment design for systems implementing Safety Category 2 functions include provisions for instrumentation to monitor plant variables and systems over the respective ranges for

operational states and PIEs in order to ensure adequate information can be obtained on plant status. The supporting safety analyses are described in Chapter 15.

SC2 equipment is designed to be in service during all modes of plant operation. Specific safety functions are mode dependent, as determined by the Fault Evaluation process in Chapter 15 and the initiating signals are enabled based on the Reactor Mode Switch position shown for each function in Table 7-4.

7.3.2.2.1 C20, Diverse Protection System

The C20 DPS maintains safety functions if SC1/DL3 systems fail. The C20 controllers are in the CB with power from R20; this provides appropriate seismic and environmental conditions for SC2 equipment and maintains operation with a loss of one power input.

C20 DPS architecture is N+1 redundancy; this prevents a single component failure from disabling a DL4a function. The C20 actuation outputs fail as-is (energised to actuate); see Figure 7-4: Fail-Safe Component Interface; this prevents inadvertent actuation due to C20 loss of power.

The C20 system includes 4 Remote Input/Outputs (RIOs). One for each FMCRD motor controller room. The C20 RIOs are utilised to interface with the FMCRD Motor Controllers and Alternate Rod Insertion (ARI) valves.

Sensor trips are applied separately to logic that performs the 2oo3 coincidence voting.

SC3 systems may use isolated SC2 sensor signals from splitters. The splitters are shown below in Figure 7-9: Defence Line 4a/Safety Class 2 Functions and Signals and Figure 7-10: Defence Line 4a Analogue Signal Splitters.

C20 provides one-way isolated outputs to C36 for operator display of diagnostic and sensor data, alarms, and historian recording; this allows operators to evaluate C20 status in the control room.

Reactor Mode Switch

The Reactor Mode Switch provides the operators with the means to configure the SC2 and SC3 I&C systems operating mode of the plant. Functions are enabled and disabled based on plant operating mode. The Reactor Mode Switch is part of C20 and classified as SC2, consistent with the highest safety category of the functions it serves.

It is a four-position switch with the following positions:

- RUN
- STARTUP
- SHUTDOWN
- REFUEL

The switch is manually positioned by the operator as the reactor is transitioned from cold (refueling outage) to rated power. Isolated one-way outputs are provided to the following:

- DL4a-C20, Diverse Protection System (3 redundant channels)
- DL2-C30, Anticipatory Protection System (3 redundant channels)
- DL2-C31, Reactor Control System (3 redundant channels)

Electrical isolation is provided between safety classes.

Diverse Protection System

The DPS provides the logic for the Safety Category 2 functions. The C20 DPS is implemented on a Triple Modular Redundant (TMR) digital platform which is diverse from the SC1 equipment. Multiple redundant instruments belonging to the process system gather input data from the monitored environment. Each instrument feeds its data to three separate processing paths, ensuring that any single point of failure does not compromise the overall system integrity. These paths operate in parallel, each performing identical computations and processing tasks independently. The data processed by each path is then subjected to a 2oo3 voting logic. This voting mechanism compares the outputs from the three paths and determines the correct result based on majority agreement, ensuring that any discrepancies due to a fault in one path do not affect the outcome. The voted output is then transmitted to the output actuators or systems, which carry out the necessary actions based on the processed data.

The DPS functions include (excluding ARI Pilot Valve actuation which is a none DL function implemented on a DL4a system):

A. Hydraulic scram independent of Safety Category 1 functions
B. RPV, containment and system isolations independent of Safety Category 1 functions
C. ICS initiation independent of Safety Category 1 functions
D. FMCRD Motor Run-in
E. ARI pilot valve actuation
F. FW and Condensate Pumps Trip

The scram follows and ARI signals are initiated whenever a hydraulic scram function is demanded regardless of whether it has been successful.

The DPS functions and initiation signals are listed in Table 7-4.

The setpoints for SC2 DPS actuation logic are determined with the setpoint methodology defined in IEC 61888 (Reference 7-34) using the final analytical limits from the plant safety analyses and the measurement uncertainties associated with the DPS equipment (e.g., sensors and processing units). Safety Category 2 functions are designed to prevent core damage for PIE assuming the complete failure of a Safety Category 1 function. As such, common physical parameters measured by Safety Category 1 and Safety Category 2 functions have common analytical limits to simplify transient and accident analyses, as well as the application of the formal setpoint methodology. The use of a common analytical basis has no adverse effect on plant operations or safety.

There are four SC2 C20 RIOs. The C20 RIOs have two functions. The first is to multiply the scram demand signals from the SC3, manual scram actuation, and SC1 systems, as well as Safety Category 2 motor run-in demand signals from the SC2 DPS to each of the 57 FMCRD motor controllers. The second is to multiply any rod block demand signal to each of the 57 FMCRD motor controllers. The Multi-channel Rod Block Monitor (MRBM) rod block, short reactor period blocks, and Automatic Thermal Limit Monitor (ATLM) blocks stop the rods from being able to withdraw and the motor run-in has priority. The circuit design ensures control rod insertion is always available. The motor run-in is automatically initiated upon receipt of a valid hydraulic scram demand from any of the interfacing systems.

The C20 DPS sends the motor run-in and motor power block signals to the C20 RIOs. The motor run-in is automatically initiated whenever the APS, DPS, or Safety Category 1 hydraulic scram function initiates a hydraulic scram.

The first two (SC1 hydraulic scram and SC3 anticipatory) hydraulic scram initiation signals are shared with SC2 equipment to generate an FMCRD motor run-in. Simultaneous with the

initiation of the Safety Category 1 and Safety Category 3 anticipatory hydraulic scram functions, the motor run-in function drives each FMCRD motor upward, stopping just short of re-engaging the control rod blade. This, in addition to the SC1 internal control rod blade full in rod latches, prevents the control rod blade from dropping out of the reactor post scram. This also ensures that any rod scram failure (due to a failed HCU component, for instance) is inserted into the reactor within minutes of the scram signal. The Safety Category 2 DPS motor run-in is mechanically independent of the scrams initiated by Safety Category 1 and Safety Category 3 functions and serves as the backup to the complete failure of the hydraulic scram in case of complete failure of the mechanical/hydraulic portions of the CRD system. This function is performed by the C20 DPS sending signals to the C20 RIOs to indicate that a hydraulic scram has been initiated from any source.

A motor power withdraw block signal comes from the blocking systems in C35, which stops the rods from being able to withdraw. The circuit design ensures that control rod insertion is always available.

7.3.2.2.2 C22, Fine Motion Control Rod Drive Motor Control

The Fine Motion Control Rod Drive Motor Control System consists of FMCRD motor controllers (one per control rod). The SC2 interfaces are from the C20 DPS and the C20 RIOs. SC3 interfaces are from C31. See the architectural relationships in Figure 7-11: Overall Rod Control System. This maintains proper separation of DLs.

The BWRX-300 needs to control each control rod individually; therefore, each control rod requires its own FMCRD Motor Controller. The FMCRD Motor Controllers are organised into four groups, and these groups are located in separate rooms within the RB. This minimises single component failure from removing more than 25% of shutdown margin.

Each FMCRD Controller provides the power output to the FMCRD and receives rod position data from the FMCRD. Rod Position data from the FMCRD is provided to C31 RC&IS.

The FMCRD Controller receives Rod Position Demand Signals from C31 RC&IS; this controls reactor power.

FMCRD Motor Controllers energises a brake output to the FMCRD. The brake is energised to release and allow FMCRD rotation. The brake output is turned off when there is no rod motion command or when a safe stop command is received from the FMCRD motor controller C20 RIOs. This provides needed outputs to the FMCRD for accurate rod positioning.

The FMCRD motor receives the following signals from the C20 RIOs:

- Rod Safe Stop
- Motor Run-in Signal
- Rod Withdrawal Block

The FMCRD Motor Controllers are powered from R20 dedicated FMCRD UPSs.

Each FMCRD is required to be controlled individually. Each control rod position has to be known and communicated to all necessary systems.

There are four C20 RIOs. One for each group of FMCRD Controllers. The C20 RIOs are located in four different rooms within the RB.

The C20 RIOs receive the following signals from the C20 DPS:

- Rod Block Signals
- Motor Run-in Signal
- Rod Safe Stop

- ARI Valve command

Two of the C20 RIOs provide outputs to energise the ARI valves. The ARI valves fail as-is on a loss of power.

The C20 RIOs provide input signals to the FMCRD motor controllers.

The C20 RIOs are powered from R20 and are located in the RB in proximity to FMCRD Motor Controllers. The C20 RIOs are required to ensure only the correct signals are communicated to each FMCRD Motor Controllers. The C20 DPS performs the validity checks and prioritisation logic on input signals.

The C20 DPS receives the following signals used to generate control signals to the FMCRD Motor Controllers:

- Hydraulic scram demand and bypass signal from each division of C10.
- Hydraulic scram demand and bypass signal from C30.
- Manual Scram
- Rod withdrawal block and bypass signals from C35 Rod Worth Minimizer (RWM)/ATLM/MRBM Channel A & B.
- Safe Stop Signal from C31
- Channel Short Reactor Period Rod Block signal from Wide Range Neutron Monitor (WRNM) System.

The motor run-in after any scram demand signal is a category 2 function implemented on an SC2 platform. Other functions are processed by C20 to minimise control complexity.

There are 57 FMCRDs in the BWRX-300 and each one has an individual motor and an individual motor controller. The motor controllers are classified as SC2 equipment and interface with the DPS (C20) and FMCRD Position Control (C31). Each motor controller uses software to supply the appropriate commands to the FMCRD motors using individual position controllers (i.e., position demand and position feedback).

Control rod position indication is provided to RC&IS. Normally the FMCRDs are individually (or in gangs) positioned by the RC&IS to control reactor power in response to either operator or automation system insert and withdraw commands. The FMCRD motor controller software is required for the motor run-in, but the DPS actuated hydraulic scram is independent from this function and does not rely on this software.

Fine Motion Control Rod Drive Motor Uninterruptible Power Supply (R20)

These UPSs are dedicated to the FMCRD motor controllers and motors and are not part of the SC1 or SC2/SC3 normal DCIS UPS. The FMCRD motors and controllers have four dedicated UPS that can supply the FMCRD motors in the absence of off-site power or the absence of standby diesel generator power.

See Chapter 8 for additional detail.

7.3.2.3 Fundamental Design Properties in the System Design

The SC2 system includes DL1 properties that represent the quality measures implemented to minimise potential for failures to occur using conservatism in design and analyses. These DL1 properties of qualification, reliability, robustness, security, diversity, and D-in-D features are discussed in the following five subsections.

7.3.2.3.1 Equipment Qualification

The SC2 equipment is designed to operate in the environment that would be expected during both normal operations and anticipated off-normal conditions. The SC2 equipment is qualified to perform its intended functions. Qualification addresses both hardware and software aspects of the SC2 equipment. The design and manufacturing processes are of sufficient quality to ensure I&C systems can reliably perform their credited protection functions. The SC2 equipment is designed, developed, fabricated, and tested to quality standards commensurate with the safety significance of the functions to be performed. The SC2 equipment qualification measures confirm the I&C systems and equipment are capable of reliably performing the design basis functions for which they are credited over the range of environmental conditions postulated for the area in which they are located. The SC2 hardware platforms meet IEC 61513 (Reference 7-5) requirements and the SC2 equipment standards defined in Section 7 of IEC 61226 (Reference 7-6) requirements. SC2 software used in the DPS and FMCRD motor controllers is developed in accordance with the Category B requirements in IEC 62138, “Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions,” (Reference 7-26) and IEC 62566-2, “Nuclear power plants – Instrumentation and control system important to safety – Development of HDL-programmed integrated circuits – Part 2: HDL-programmed integrated circuits for system performing category B or C functions,” (Reference 7-60). Noting that Safety Category 2 and 3 functions and Safety Category B and C functions are equivalent terminology.

SC2 hardware is developed in accordance with IEC 60987 (Reference 7-35). SC2 hardware is qualified for environmental conditions in accordance with IEC 60780-323 (Reference 7-29) and seismic interaction in accordance with IEC 60980-344 (Reference 7-30).

The SC2 equipment is qualified for electromagnetic compatibility in accordance with IEC 61000-4 Series (References 7-27, 7-36 through 7-52) and IEC 61000-6-2 (Reference 7-28).

7.3.2.3.2 Reliability

The SC2 equipment has the required reliability to perform its intended functions. It has an initial quantitative reliability target of less than 1E-3, probability of failure on demand. The reliability analysis of the SC2 equipment demonstrates it meets its reliability goals using qualitative and quantitative performance measures or criteria, as appropriate. The reliability assessment is used to optimise goals such as minimising out-of-service time for repair and reducing the frequency of surveillance.

Online Maintenance

The DPS provides self-diagnostics to SC3 DCIS for equipment status monitoring through qualified isolation features classified as SC2. FMCRD motor controller self-diagnostics and rod separation signals are also used by RC&IS. The SC2 DPS is designed to support required surveillance testing without affecting plant operation. It provides the capability for signal and channel bypass to support maintenance and testing. Bypass conditions are alarmed in the MCR. The SC2 design provides for periodic testing of the entire channel of instrumentation logic, from sensing device to actuating device. Testing and performance assessment requirements for DPS are developed using the guidance of IEC 60671 (Reference 7-53) and IEC 62385 (Reference 7-54). The use of measuring and test equipment that can impair a Safety Category 2 function requires deliberate manual intervention via hardware interlock features at the system interfaces. Testing provisions permanently connected to safety systems are classified the same as the safety system.

Power

The C20 System is redundantly and uninterruptedly powered by the SC2/SC3 electrical system load groups. The FMCRD motor controllers are normally powered from the SC2/SC3 electrical system and have dedicated SC2 UPS. See Chapter 8 for further information.

7.3.2.3.3 Robustness

Robustness of SC2 equipment is the degree to which it can function correctly in the presence of invalid inputs or stressful environmental conditions (See Subsection 7.3.2.3.1 Equipment Qualification). The robust SC2 DPS design reflects the use of design methods and adherence to engineering best practices to ensure that the protection functions are achieved for the specified conditions.

The SC2 systems have the required separation and independence to perform their intended functions as a diverse backup to SC1 equipment.

The majority of the SC2 equipment performing Safety Category 2 functions is located in a separate fire barrier room in the CB with the remainder located in compartmentalised fire barrier rooms in the RB. It is separated from SC1 equipment performing Safety Category 1 functions that is located in three separate divisional fire barrier rooms in the RB. The SC2 equipment is powered by separate power supplies than the SC1 equipment. The four C20 RIOs are located in the RB near the cabinets housing the FMCRD motor controllers.

Safety Category 2 functions do not share any sensors with Safety Category 1 functions. SC2 equipment is independent from SC3 equipment to an extent that is practicable in that shared sensors are not credited with mitigation for the same PIE. Select signals shared between SC2 and SC3 equipment, as identified in Figure 7-9, are used by both SC2 and SC3 TMR controllers allocated to each parameter performing Safety Category 2 and Safety Category 3 functions.

The splitters for redundant signals are located in separate cabinets. The shared signals are analogue signals. Signal sharing is accomplished using non-software, analogue splitters that are powered with redundant uninterruptable power supplies. The splitter technology supplies isolated outputs that allow short circuits or common mode voltages up to 300 volts (Alternating Current (AC) or Direct Current (DC)) applied to one output without affecting the other output. The splitter design is shown in Figure 7-10. The splitter design ensures a splitter output is unable to adversely affect the other outputs. The splitters are assigned a Safety Class commensurate with the highest Safety Category function the splitter supports.

The three channels of the SC2 DPS from the separate SC2 splitters are used by the 2oo3 voting logic for trips and initiations.

The SC2 physical separation and signal isolation devices meet the requirements of IEC 60709 (Reference 7-22).

The FMCRD motor controllers receive normal control signals from RC&IS; however, the motor controller SC2 software instructs the controller to ignore the SC3 RC&IS network commands and run the rods in when instructed by the C20 System.

The control rods and motors are located inside containment in the RB. The FMCRD motor controllers are organised into four groups located in four separate rooms in the RB outside containment.

The SC2 FMCRD UPS provides the necessary independent power to the control rods and monitoring. The FMCRD motors and controllers have four dedicated UPS that can supply the FMCRD motors in the absence of off-site power or the absence of standby diesel generator power. The FMCRD UPS can operate from and be charged by those sources. The power sources are also independent of the normal SC2 UPS that power the SC2. The C20 RIOs,

FMCRD motor controllers, and the UPS to power them are arranged in four independent and separately located groups.

Where software is used, SC2 equipment diagnostics include watchdog timers, sensor range checks, power supply monitoring, communications, and the SC2 controlled contact in the actuator circuit monitoring. The DPS is monitored digitally through unidirectional isolated signals. The digital monitoring for self-diagnostics cannot adversely affect Safety Category 2 functions. The digital monitoring checks for inconsistencies between redundant signals, performs sensor range checks, and monitors actuator, communication, and power supply status. The C20 DPS logic is designed to ensure that an actuation device failure can only affect one FMCRD. Motor run-in is initiated when a manual scram is initiated from either control room. The motor run-in actuation devices are sealed in for at least four minutes once energised to ensure the motors have time to drive the rods full in.

The SC2 DPS has the required fail-as-is design features to perform its intended functions and avoid spurious actuations. The fail-as-is, energise to actuate, design is used to prevent lesser classified DPS from creating unnecessary challenges to plant safety (e.g., spurious actuations for expected failures) requiring action by Safety Category 1 functions.

Deliberate operator action is required to return the Safety Category 2 functions to normal after actuation.

SC2 equipment operating by itself (or in combination with Safety Category 3 functions unaffected by the PIE) and assuming a complete failure of a Safety Category 1 function, ensures that no AOO or DBA causes a radiation release greater than regulatory requirements. No SC1 equipment can prevent a scram, reactor isolation, containment solation, or ICS initiation from SC2 equipment or vice versa.

The SC2 equipment performing Safety Category 2 functions provides diversity to support the BWRX-300 D-in-D strategy.

DPS initiates hydraulic scrams, isolations, and ICS using the same solenoids as Safety Category 1 functions but using actuation devices instead of load drivers. Independence between these safety category functions is discussed below.

For diversity, the SC2 equipment is able to independently shutdown the plant using the FMCRD motors. The SC2 C20 System accepts isolated hydraulic scram demand signals from the Primary Protection System Safety Category 1 hydraulic scram, manual scram, and the APS Safety Category 3 anticipatory hydraulic scram functions to also initiate reactor shutdown using the FMCRD motors. The motor run-in inserts rods even if the hydraulic scram does not work. A motor run-in can be initiated from independent scram signals from DL3, DL4a, or DL2.

7.3.2.3.4 Security

The SC2 equipment performing Safety Category 2 functions adequately address access control to limit cyber security vulnerabilities and ensure the system can perform its intended functions.

The SC2 DPS and FMCRD designs incorporate features to support establishment of a secure operational environment. SC2 equipment diagnostics and internal data are available to the SC3 networks and controllers via one-way data communications. The SC2 DPS and FMCRD software is produced in a secure development environment that prevents the insertion of undocumented codes and precludes their use. The SC2 digital equipment is installed and maintained in accordance with the station administrative procedures and control of access programs.

See Chapter 25 for more detail.

7.3.2.3.5 Diversity and Defence-in-Depth

The SC2 systems provide diverse protection functions to place and maintain the plant in a safe state in the event of PIE concurrent with failure of Safety Category 1 functions to support the D-in-D strategy.

The design bases of the SC2 systems provide diversity and D-in-D for the complete failure of a Safety Category 1 function (i.e., CCF). Safety Category 2 functions independently provide safety functions comparable to the Safety Category 1 functions using diverse platforms from the SC1 equipment. The SC2 sensors are selected to be as diverse as practical from SC1 sensors. The C20 DPS provides diversity and D-in-D by sending the manual scram, SC1 hydraulic scram and SC3 anticipatory hydraulic scram signals to the C20 RIOs to command the C22 FMCRD Motor Controllers to drive in rods by the FMCRDs.

The SC2 C20 system is diverse from the SC1 C10 system as an additional level of protection for potential systematic faults caused by design and implementation defects within redundant divisions of the SC1 I&C system. The SC2 C20 system is implemented on a diverse platform from that of SC1 C10 with the instrumentation as diverse and independent as practicable. The SC2 components method of actuation in the actuation circuit is diverse from the method of actuation implemented by Safety Category 1 hydraulic scram function. The SC2 actuation relays shown in Figure 7-4 and Figure 7-5 are configured as “energise to actuate” whereas SC1 I&C load drivers are configured as “de-energise to actuate” which provides functional diversity in these actuation circuits.

The FMCRD motor mitigates mechanical failure (hydraulic scram) due to CCF. The FMCRD UPS provide additional D-in-D if normal power is lost. See Chapter 8 for additional detail.

7.3.2.4 Operator Interface and Accident Monitoring

Data obtained by the SC2 equipment is sent to the SC3 DCIS for display, recording, monitoring, and alarming. SC2 system bypass conditions are alarmed in the MCR.

The operator interface is described in Sections 7.5 and 7.6 for the MCR and SCR, respectively. SC2 sensors signals shared with SC3 equipment provide measurements that are independent, and diverse to the extent practicable from SC1 sensors for selected parameters.

7.3.2.5 Compliance Alignment

Table 7-7 shows how the SC2 systems align to meet the key industry I&C standards IEC 61513 (Reference 7-5).

7.3.2.6 Interfaces with Other Systems

- FMCRD – Chapter 4
- FMCRD Motor UPS – Chapter 8

7.3.2.7 Performance and Safety Evaluation

The system design bases, and associated safety functions are described in Subsection 7.3.2.2

7.3.2.8 Application of ALARP Principles in Design Development

The SC2 I&C system design development is compliant with the ALARP principle through the application of appropriate codes and standards, OPEX, and optioneering, where relevant. The I&C system development process is detailed in Section 7.4.

7.3.3 Nuclear Controllers including Anticipatory Protection System – Defence Line 2/Safety Class 3/Nuclear Segment

7.3.3.1 Systems Architecture

7.3.3.1.1 Safety Class 3 Systems

SC3 I&C system equipment is used to implement Safety Category 3 functions. The SC3 DCIS systems are C30 through C39, listed below.

- C30, Anticipatory Protection System
- C31, Reactor Control System
- C32, Reactor Auxiliaries Control System
- C33, Equipment Cooling and Environmental Control System
- C34, Safety Class Electrical Power Supply Control System
- C35, Reactivity Monitoring System
- C36, Plant Data Acquisition, Data Communications, and Normal Operator Interface System
- C37, Control and Monitoring System for DL4b Functions
- C38, Turbine Generator Control System
- C39, Normal Heat Sink and Condensate/FW Control System

Further detail on these systems and their allocated functions are given in Subsection 7.3.3.2 System Design Basis and Associated Functions.

As stated in Section 7.2.1 common system architecture applies to all defence lines and I&C systems. The functional architecture for the SC3 controllers is shown in Figure 7-12. The following are I&C architecture requirements for C30 through C39.

- The controller cabinets are in the CB.
- RIOs are used to obtain and multiplex inputs from local field devices and may be in proximity to the controlled and monitored equipment as determined by the design team.
- The systems are implemented on the SC3 DCIS with its controllers located in the CB.
- The systems are implemented on TMR controllers which utilise 2oo3 voting. The systems are fail as-is, this provides reliable operation without causing spurious actuation.
- Interfaces with the Plant Automation Function (PAF) to support the automation of the plant functions.
- SC3 systems connect to the UDH. See Figure 7-1: BWRX-300 Distributed Control and Information System Network Architecture.
- The systems are powered from battery backed R30 UPSs located in the CB.
- SC3 systems may use isolated SC2 sensor signals from splitters. In these cases, there may also be additional SC3 sensors used to measure the same process variable as determined by the system design team to the extent practicable.

7.3.3.2 System Design Bases and Associated Safety Functions

The design bases of the Safety Category 3 functions are to prevent or mitigate AOOs before either Safety Category 1 or Safety Category 2 functions are required. Safety Category 3 action precludes the need for other DL intervention. Safety Category 3 functions are implemented in SC3 equipment. These SC3 hardware and software are diverse from SC1 equipment performing Safety Category 1 functions. The SC3 system design includes provision of instrumentation to monitor plant variables and systems over the respective ranges for operational states and during a PIE in order to ensure that plant status information can be obtained. The supporting safety analyses are described in Chapter 15.

SC3 equipment is designed to be in service during all modes of plant operation. Specific safety functions are mode dependent, as determined by the Fault Evaluation process in Chapter 15 and specified by the Mode Switch position shown for each function in Table 7-5.

7.3.3.2.1 C30, Anticipatory Protection System

The APS does not perform any active safety category functions during normal plant conditions. The APS is continuously monitoring plant conditions to detect an off-normal condition during normal operation.

The APS performs the DL2 anticipatory protection functions identified by the fault list to prevent the need for DL3 protective actions. The APS automatically initiates a rapid reactor shutdown (scram) by inserting control rods on various off-normal conditions.

The C30 APS is designed to perform the major safety function of DL2 which is mitigating transients and providing investment protection for expected transients by tripping the plant in advance of any required DL3 or DL4a response. The APS is not a control system but instead uses logic similar to the C10 system and C20 system in that parameters are measured, compared to a setpoint, and voted then actuation is initiated.

The APS performs DL2 functions that can control SC1 field equipment. For these functions, one-way signals are transmitted to control contacts wired in series with the SC1 C10 controlled load drivers. See Figure 7-4: Fail-Safe Component Interface.

There is no failure of APS that can adversely affect the Safety Category 1 or Safety Category 2 functions. An APS malfunction cannot stop a SC1 hydraulic scram, nor can a SC1 hydraulic scram stop a Safety Category 3 APS scram function.

The APS scram initiation signals are listed in Table 7-5. Simultaneous with the initiation of the APS hydraulic scram demand, a scram follow signal is generated such that each FMCRD motor drives its ball nut upward to a position just below the fully inserted and latched hollow piston that is coupled to the control rod blade. This signal is sent whenever a hydraulic scram is demanded by APS regardless of whether the hydraulic scram actuation has been successful.

As well as the APS scram functions, the APS also provides Safety Category 3 non-scram functions, including:

A. Turbine Trip on Low Main Condenser Vacuum

B. Turbine Bypass Valves (TBVs) Closure on Low Main Condenser Vacuum

C. TBVs Fast Open on Fast Closure of Turbine Control Valves (TCVs)/Turbine Stop Valve Demand

D. MSRIV/MSCIV Isolation on Low Main Condenser Vacuum

E. Standby Diesel Generator Start on Low Electrical Bus Voltage

F. FW and Condensate Pumps Trip on High RPV Level

G. FW Isolation on High-High RPV Level

H. ICS Pressure Control on High Reactor Pressure

I. Indications and Alarms

7.3.3.2.2 C31, Reactor Control System

The C31 Reactor Control System implements DL2 functions related to the Plant Automation function, the Reactor Level Control function, the Feedwater Temperature Control function, the Reactor Pressure Control function, and the FMCRD Position Control function. Each of these functions are implemented on separate controllers.

C31 supports functional segmentation requirements defined in the fault evaluation.

The following functions are on different segments:

- The FW Heating control is separate from the Reactor Pressure Control (RPC) and Reactor Level Control (RLC).
- The ATLM, MRBM, RPC and RLC are separate from the rod control digital functions.
- The RPC is separate from RLC and Shutdown Cooling System (SDC) manual initiation.
- The RLC is separate from RPC.
- The DL4a RW isolation function is separate from RPC.
- The DL2 and DL4a ICS initiation is separate from RLC and RPC.

Plant Automation Function

The PAF provides automatic power control as part of a larger automation scheme that includes sending commands to SC3 and SCN controllers via the UDH.

The PAF does not issue any commands for off normal operations.

The PAF allows coordination of plant system functions during normal operations.

The SC3 and SCN control systems need to be put into automatic mode individually, by the operator, for PAF automation to be functional; without this operator permissive, any commands originating from PAF are ignored. This provides auto control to reduce operator burden during reactor startup, heatup, shutdown, and cooldown.

The operators can either perform all the actions necessary to execute these functions, or they can use PAF. The following plant control functions interface with PAF for the indicated actions:

- Reactor Level Control – Maintain level during heatup and cooldown.
- Feedwater Temperature Control – Maintain Feedwater at the programmed temperature or at a temperature set by the operator.
- Reactor Pressure Control – Ramp pressure setpoint up during startup/modulate TCV/Turbine Bypass System/modulate pressure setpoint down during cooldown.
- FMCRD Position Control – change control rod position demand to withdraw or insert control rods as necessary to modulate reactor power.
- Turbine Generator Control System – Warmup/roll/synchronise/load turbine for startup.

Reactor Level Control

The RLC operates level control valves in the shutdown cooling system and the reactor water cleanup system during cold and heatup operations.

RLC controls reactor level at reactor power greater than 10-15% by adjusting the frequency of the Adjustable Speed Drives supplying power to the feedwater pump motors. At reactor powers lower than 10% the system controls a low flow control valve supplied with either a condensate pump or feedwater pump operating at fixed speeds, depending upon reactor pressure.

As described in DPS Subsection 7.3.2.2.1, select signals are acquired from analogue splitters with one signal available to the DL4a equipment and the other to DL2 equipment.

In addition to signals received from analogue splitters, a fourth analogue signal is provided to wide and narrow range reactor water level. This accommodates failure of analogue splitters.

Feedwater Temperature Control

The C31 system modulates the steam flow control valve into FW Heater #6 to control FW temperature, and monitors FW temperature downstream of FW Heater #6.

Reactor Pressure Control

The C31 system controls reactor pressure by modulating the TBV when the main generator is off-line, and by modulating the TCV when the main generator is online.

The RPC system controls reactor pressure from a cold vessel through pressurisation and heatup to power operation.

During transients the RPC controls reactor pressure by sending a flow demand signal to the turbine generator that determines TCV position.

Fine Motion Control Rod Drive Position Control (Rod Control and Information System)

The RC&IS provides the functional control logic used to generate rod position demand signals. These rod position demand signals are transmitted to C22. The RC&IS ensures control rods are correctly positioned within the reactor core to achieve the desired power level and blocks control rod motion based on received rod block signals from C35 and is programmed with predetermined rod withdrawal sequences.

The FMCRD supports Selected Control Rod Run-In (SCRRI) function by requesting the selected control rod(s) to the target positions defined in the applicable SCRRI profile in the active sequence at fast insertion speed regardless the rods INSERTION permissive.

The C31 RC&IS ensures control rods are correctly positioned within the reactor core and has an automatic mode of operation where the control rods are positioned automatically to achieve or maintain a specific reactor power level. It receives reactor power commands from the PAF when in the automatic mode, a semi-automatic mode of operation where the operator enters the target reactor power, and a manual mode of operation where the operator can select and position a single control rod.

~~7.1.1.1.1~~7.3.3.2.3 C32, Reactor Auxiliaries Control

The C32 Reactor Auxiliary Control System implements DL2 functions related to the CRD, SDC, IC/Spent Fuel Pond Cleanup & Cooling and the Reactor Water Cleanup System (CUW).

Control Rod Drive Controllers

The CRD Controller controls the CRD pumps and PCVs to provide for flow control of the FMCRD purging water, charging of the HCU accumulators, and supplying a pressurized source of water to auxiliary loads such as the SDC pump, Process Radiation and Environmental Monitoring System and the Nuclear Boiler System reactor water level reference leg instrument lines.

The CRD Controller continuously performs self-diagnostics and generates an alarm to inform operators of an issue.

The CRD Controller controls the CRD pumps and PCVs to provide makeup water into the RPV, when necessary (Safety Category 3 function)

Isolation Condenser System/Spent Fuel Pond Cleanup and Cooling Function

The isolation condenser and fuel pool cooling, and cleanup function provides monitoring and control for the ICS pool redundant heat exchangers and pumps and their associated valves. This system provides monitoring and control for the Fuel Pool Cooling and Cleanup System. The controller interfaces with redundant pumps and heat exchangers and filter demineralisers. Two pumps are controlled with one in operation and one in standby, if the operating pump trips the logic automatically starts the standby pump.

Shutdown Cooling Function

The shutdown cooling function provides separate controllers for monitoring and control for the SDC system to remove decay heat from the reactor.

The SDC controllers provide monitoring and control of SDC equipment. It interfaces with the PAF to support the automation of the plant functions or can be manually operated. The SDC controllers receive signals from RLC (C31) during plant heatup.

Reactor Water Cleanup System Control

The CUW controller monitors the temperature, pressure, and flow within the CUW and controls the SC3 valves for overboarding the reactor, reducing thermal stratification, cleanup flow to the condenser, and interfaces with the PAF to support the automation of the plant functions.

~~7.3.3.2.3~~7.3.3.2.4 C33, Equipment Cooling and Environmental Control System

The C33 Equipment Cooling and Environmental Control System implements DL2 functions related to the Containment Cooling System (CCS), Plant Cooling Water System /Chilled Water Equipment System (CWE), Instrument Air/Pneumatic System, RB/CB Heating Ventilation and Airconditioning (HVAC), NBM/Containment Inerting Control System (CICS).

During normal operations, the CCS Controller continuously monitors the temperature and pressure to control the TCV from the CWE. The controller monitors the flow sensors in the drain lines as well. The controller also initiates the lead Air Handling Unit (AHU) train while the other train is on Standby.

During off-normal operations, The CCS Controller continuously monitors the temperature elements, pressure transmitter, flow sensors and Pressure Differential Transmitter (PDT) for the AHU during off-normal conditions.

~~7.3.3.2.4~~7.3.3.2.5 C34, Electrical Power Supply Control System

The C34 Electrical Power Supply Control System implements DL2 monitoring and alarming functions related to the R20 Electrical System Control, R30 Electrical System Control, SC3 I&C EDS, R20 Protective Relaying, R30 Protective Relaying.

~~7.3.3.2.5~~7.3.3.2.6 C35, Reactivity Monitoring Systems

The C35 Reactivity Monitoring Systems implement DL2 functions related to the ATLM, MRBM, Core Thermal Power/Flow Monitor (CTPFM), Three-Dimensional Core Thermal Power (3D-CTP) Distribution Monitor, RWM Monitor, WRNM, and Gamma Thermometers (GTs).

Automatic Thermal Limit Monitor

The ATLM is designed to enforce normal operating limit restrictions on fuel thermal limit values and operating limits when core thermal power is above predefined threshold power levels. The limits are enforced by continuously monitoring control rod positions, calculated core flow, and reactor power conditions to detect potential core thermal limit or Soft Duty Guideline violations

in any of the fuel bundles within the reactor core. Should a violation be detected, the C35 ATLM System removes the control rod movement permissive signals to the C31's FMCRD Position Control System (RC&IS) and sends a triplicated hardwired discrete signal to the C22's FMCRD Prioritisation Control Logic and Interface.

Multi-Channel Rod Block Monitor

During normal operations, with the reactor mode switch in the RUN position and the core thermal power above the MRBM thermal limits enforcement enable setpoint, MRBM thermal limits enforcement is enabled automatically and functions continuously. Once the MRBM thermal limits enforcement is enabled, the MRBM provides control rod withdrawal permissives to the C31 FMCRD Position Control System, identifies the control rod(s) selected for withdrawal and the LPRM neutron flux data around the selected rod(s), and monitors the associated local flux data. If the ratio of the withdrawing average to the initial average flux exceeds a defined setpoint (calculated based on user configurations), then the MRBM initiates control rod withdrawal blocks to the C22 FMCRD Motor Control System.

During off-normal operations, with the reactor mode switch in the RUN position and the core thermal power above the MRBM thermal limits enforcement enable setpoint (i.e., the MRBM thermal limits enforcement is active), the MRBM removes rod withdrawal permissives to the C31 FMCRD Position Control System and issues control rod withdrawal block signals to the C22 FMCRD Motor Control System during abnormal conditions such as digital failures of the FMCRD Position Control System, loss/failure of communications, loss of power, or failure of self-diagnostics.

Core Thermal Power/Flow Monitor

The CTPFM processing units continuously calculate reactor thermal power and core flow. One CTPFM can be bypassed at a time, as one CTPFM required for rod withdrawal.

Three-Dimensional Core Thermal Power Distribution Monitor

During normal operation, the primary function of the 3D-CTP is to compute detailed on-line reactor/fuel thermal performance parameters in order to confirm that the reactor is operating in conformance to the required/licensed fuel design limits. The system determines periodically and on demand the core power distribution, core thermal limits including the maximum fraction of limiting critical power ratio – a flux/flow correlation, the maximum linear heat generation rate (equivalent to W/cm2 through the fuel clad) and Soft Duty Guidelines (used to mitigate pellet clad interaction of each node). Fuel, LPRM, and control rod exposures are also determined. Additionally, the 3D-CTP predicts future core performance parameters that are used to support reactor maneuver and future cycle operation.

Rod Worth Minimizer

During startup operations and at low reactor powers in the BWRX-300, a large negative void reactivity feedback has not formed. In this condition, unrestrained control rod patterns can result in high individual control rod reactivity worth capable of violating fuel thermal design limits in a Control Rod Drop Accident (CRDA) and Rod Withdrawal Error (RWE). To mitigate the consequences of the CRDA and RWE, the BWRX-300 control rod insertion and withdrawal is constrained to predefined sequences which, if followed, ensures that the individual reactivity worth of each control rod remains low enough to prevent exceeding thermal limits of the fuel during the postulated CRDA or RWE. Compliance with the predefined rod insertion and withdrawal sequences also ensures core stability and minimises thermal stresses on fuel rods during power ascension (i.e., while raising reactor power).

The RWM enforces compliance with the predefined control rod insertion and withdrawal sequences which ensures that thermal limits of the fuel are not exceeded in the event of a postulated CRDA or RWE. Its purpose is to ensure that control rod movements comply with insertion and withdrawal sequence rules. As a subsystem in the DL2 Reactivity Monitoring

System, the RWM prevents the operator or equipment from establishing high worth control rod patterns which possibly require DL3 or DL4a actions to mitigate transients beginning from those initial conditions. The RWM monitors control rod positions and constrains control rod positions by providing control rod movement blocks. The RWM also provides indications and alarms related to current control rod positions and compliance of the current control rod patterns with the predefined control rod insertion and withdrawal sequences.

Wide Range Neutron Monitoring System

The WRNM provides protective action by sending a shorter reactor period reactor trip signal to the APS. The scram logic operates if any unbypassed WRNM initiates a trip. The anticipatory trip is faster than the DPS because there is a direct connection between the WRNM and the APS.

The WRNM System controllers continuously monitor neutron flux, from WRNM preamplifiers, then act to prevent high reactor periods during startup. WRNM instruments generate a signal that is used to determine reactor power and periods and are used by C35 to generate rod withdrawal block for a short period and a C30 hydraulic SCRAM for a shorter period. One channel can be bypassed at a time.

WRNM rod block signals are hard-wired to C20. WRNM SCRAM signals are hardwired to C30.

Gamma Thermometers

A GT is an in-core device that converts local gamma flux to an electrical signal. The GT signals are acquired and converted to data that represent reactor power and collected by the C35 System. The GT data is sent to C36 for display.

~~7.3.3.2.6~~7.3.3.2.7 C36, Plant Data Acquisition, Data Communications, and normal Operator Interface System

The C36 Plant Data Acquisition, Data Communications, and normal Operator Interface System implements DL2 functions related to Plant Data Acquisition, Data Communications, and normal Operator Interface Systems implement DL2 functions related to the DL3 Gateways, Network Functions (via switches), Operator Interface, Safety Parameter Display System (SPDS), TSM, Plant Alarm Function, and SC3 I&C RIOs, Plant Historian and Monitoring.

~~7.3.3.2.7~~7.3.3.2.8 C37, Control and Monitoring System for DL4b Functions

The C37 Control and Monitoring System facilitates support of the following DL4b Functions:

- RPV Venting Control
- Containment Venting Control
- Boron Injection Control
- 7-Day Coping (Indication Functions)

The C37 system includes the logic and I/O to perform the control and monitoring functions provided as further protection to prevent or mitigate a severe accident performed by an I&C system.

~~7.3.3.2.8~~7.3.3.2.9 C38, Turbine-Generator Control System

The C38 Turbine-Generator Control System implements DL2 functions related to the Turbine Generator Protection, Turbine Auxiliary Control, Turbine Speed Control, Generator/Exciter Auxiliary Controllers, and Moisture Separator Reheater.

~~*7.3.3.2.9*~~*7.3.3.2.10 C39, Normal Heatsink and Condensate/ FW Control System*

The C39 Normal Heatsink and Condensate/FW Control System implements DL2 the functions: Condensate/FW Control, FW Heater Drains/Extraction Steam Control, Circulating Water Cooling as determined by the site design, Condensate Polishing System Control, Condenser Control, Condensate Storage & Transfer Control, Circulating Water Control, and Intake Structure.

7.3.3.3 Fundamental Design Properties in the System Design

The SC3 system includes DL1 properties that represent the quality measures implemented to minimise potential for failures and initiating events to occur in the first place, using conservatism in design and analyses. These DL1 properties of qualification, reliability, robustness, security, diversity, and other D-in-D features are discussed in the following five subsections.

7.3.3.3.1 Equipment Qualification

The SC3 equipment is designed to operate in the environment in which the equipment is required to function during both normal operations and anticipated off-normal conditions, and the equipment is qualified to perform its intended functions and meets IEC 61513 (Reference 7-5) requirements and the equipment standards defined in Section 7 in IEC 61226 (Reference 7-6) requirements for Class 3 systems. The SC3 nuclear segment software is developed to meet IEC 62138 (Reference 7-26) and IEC 62566-2 (Reference 7-60), Category C requirements. Equipment qualification addresses both hardware and software aspects of the SC3 nuclear segment. The SC3 nuclear segment design and manufacturing processes are of sufficient quality to ensure I&C systems can reliably perform their credited protection functions. The SC3 nuclear segment equipment is designed, developed, fabricated, and tested to quality standards commensurate with the safety significance of the functions to be performed. The SC3 nuclear segment equipment qualification measures demonstrate that the I&C systems and equipment are capable of reliably performing the design bases functions for which they are credited over the range of environmental conditions postulated for the area in which they are located.

The SC3 equipment is qualified for seismic interaction in accordance with IEC/Institute of Electrical and Electronics Engineers (IEEE) 60980-344 (Reference 7-30) if located near SSCs required for mitigation of seismic-related events. The SC3 equipment is qualified for electromagnetic compatibility in accordance with IEC 61000-4 Series (References 7-27, 7-36 through 7-52) and IEC 61000-6-2 (Reference 7-28).

7.3.3.3.2 Reliability

The SC3 nuclear segment has the required reliability to perform its intended functions. The main SC3 hardware platform uses TMR controllers for the major plant control systems. It has an initial quantitative reliability target of less than 1E-2 probability of failure on demand for standby functions. The reliability analysis of the SC3 nuclear segment demonstrates it meets its reliability goals using qualitative and quantitative performance measures or criteria, as appropriate.

The SC3 nuclear segment process controllers are designed with TMR controllers to prevent random I&C component failures from causing plant transients. The TMR controller outputs are dual ported to the plant SC3 nuclear segment network. Where a mechanical system has safety functions and is redundant two controllers are furnished so the redundant components may be operated separately, and the system is not affected by a single failure.

For the functions with TMR controllers, single controller failures (and certain double failures) have no adverse effect on system or plant operation, and failed controller parts may be replaced online. The controllers perform Safety Category 3 functions and are implemented in SC3 equipment designed with a specific requirement that there be no failures more often than

once per 100 years. The intent is that no random controller failure initiates an AOO. The reliability of the controller depends on final design and the formal analyses to determine failure rates are performed as part of the detailed plant design.

SC3 nuclear segment rod block functions are implemented on redundant processors for reliability. Normally both redundancies are online, and their data continuously compared. Any one redundancy can be bypassed at a time but, if bypassed, it takes the plant out of automation mode.

Design reliability assurance program and reliability, availability, and maintainability plan documents are used to quantify the required failure rates of the DCIS to assure plant safety and plant availability goals. Testing and performance assessment requirements for APS are developed using the guidance of IEC 60671 (Reference 7-53) and IEC 62385 (Reference 7-54).

Extensive hardware and software diagnostics are provided for the TMR controllers to provide for operator monitoring and alarms.

The Safety Category 3 functions for ATLM, MRBM, WRNM, SPDS, Technical Specification Monitor, Core Thermal Power/Flow Monitor, 3D Core Thermal Power Distribution Monitor, Plant Alarm System, and Plant Historians and Monitoring are powered by the SC3 electrical system which provides redundant UPS and power feeds.

7.3.3.3.3 Robustness

Robustness of the SC3 nuclear segment is the degree to which it can function correctly in the presence of invalid inputs or stressful environmental conditions. The robust SC3 nuclear segment design reflects the use of design methods and adherence to engineering best practices to ensure that its functions are achieved for the specified conditions.

The SC3 nuclear segment has the required separation and independence to perform its intended functions. SC3 equipment is independent from SC1 equipment. Safety Category 3 functions are also independent from Safety Category 2 functions to an extent that is practicable in that shared sensors are not credited with mitigation of the same PIE. Safety Category 2 and Safety Category 3 functions share support equipment. Safety Category 3 functions are designed to ensure that they cannot adversely affect Safety Category 1 or Safety Category 2 functions from fulfilling their protection functions. Safety Category 3 functions share select signals with Safety Category 2 functions sent via qualified isolation devices (as described in Subsection 7.3.2.3.3). Safety Category 3 functions may use signals from SC1 equipment sent via qualified isolation devices (as described in Subsection 7.3.1.3.3) for control purposes. Plant operation is not adversely affected by the loss or inaccuracy of these individual signals.

The SC3 equipment implementing Safety Category 3 functions is located in two separate fire barrier rooms in the CB. The SC1 equipment implementing Safety Category 1 functions is located in three separate divisional fire barrier rooms in the RB. The SC2 equipment implementing Safety Category 2 functions is located in a separate fire barrier room in the CB. There is no communication from SC3 equipment to online SC1 equipment and only rod block or motor run-in initiation (dry contact) communication to the SC2 C20 System. There is no direct connection between SC1 equipment and the SC3 Automatic Power Regulator (APR). The APR does use LPRM signals from SC1 equipment for power feedback, but it also uses GT signals and the core thermal power computers for similar feedback. These signals are continuously compared, and any discrepancy takes the plant out of automation mode to prevent any power signal from misleading the control system. Other than the APRM signals, Safety Category 1 functions and the SC3 APR controller have no sensors or actuators in common. There are no Safety Category 3 commands or communications sent to SC1

equipment. The Safety Category 3 physical separation and signal isolation devices meet the requirements of IEC 60709 (Reference 7-22).

The SC3 nuclear segment has the required fail-as-is design features to perform its intended functions and avoid spurious actuation. The fail-as-is, energise to actuate, design is used to prevent lesser classified systems (e.g., APS) from creating unnecessary challenges to plant safety (e.g., spurious actuations for expected failures) requiring action by Safety Category 1 functions. Where software is used for SC3 equipment diagnostics, the SC3 equipment includes watchdog timers, sensor range checks, and monitoring of power supplies, communications, and actuators. Each output is produced separately by a 2oo3 discrete, or median select analogue vote from each of the three controllers. The scheme is used to provide reliable trips and avoid inadvertent trips.

The Safety Category 3 blocking system functions (i.e., ATLM, MRBM, and WRNM) are redundant and are used to supervise the control systems and plant conditions. Either of the redundant blocking pair can block rod motion. One of the redundant pair can be bypassed for maintenance activities. The remaining component of the blocking pair can still block rod motion. If both blocking pairs are not available, semi-automatic and manual control rod motion is halted until at least one is available. The blocking pairs alarm and block if they lose communication with the SC3 gateways or RC&IS, cannot receive an update from the core 3D Core Thermal Power Distribution Monitoring program, or if their internal data do not agree. As described, the system is fail-safe to block when both blocking pairs are not available, on a loss of communication between systems, or on a loss of input data.

Signals from the redundant WRNM controllers are used to initiate a rod withdrawal block for a short reactor period and initiate a Safety Category 3 anticipatory hydraulic scram for a shorter reactor period. The scram is only available when the Reactor Mode Switch is not in RUN (typically below 15% thermal power as measured by the APRMs). The WRNM detectors are distributed radially in the core at fixed heights with at least two detectors in each quadrant with two additional detectors (ten total) at the boundaries of two adjacent quadrants such that each quadrant has a backup in the event of a single WRNM failure. If no WRNM detector is available in any core quadrant, rod motion is prohibited except in manual mode. If no WRNM detector is available in any core quadrant during refueling activities, then fuel movement is halted.

The APS or a reactor control system TMR controller may use three isolated signals from the SC2 splitters, and a fourth SC3 signal to measure the same process variable parameter. Typically, these parameters include containment pressure, reactor level, reactor pressure, and condenser vacuum. Each APS controller and reactor control system validates the analogue signal with a range and consistency check, compares each of the four signals to a common setpoint, and then indicates the analogue value and trip status. For example, the reactor level and pressure controller analogue validation algorithms use the three splitter signals from SC2 equipment, and the fourth signal dedicated to Safety Category 3 functions to make a fault tolerant control signal that functions even if the splitter signals are lost:

- If four signals are valid, use average of two median signals.
- If three signals are valid, use median signal.
- If two signals are valid, use average of two signals.
- If only one signal is valid, use signal.

For trip signals derived from analogue inputs the Safety Category 3 validation algorithms functions:

- If four signals are valid, use Two Out of Four (2oo4) logic.
- If three signals are valid, use 2oo3 logic.

- If two signals are valid, use 2oo2 logic.
- If only one signal is valid, do not trip.

The scheme is used to provide reliable trips and avoid inadvertent trips.

7.3.3.3.4 Security

The SC3 nuclear segment adequately addresses security to limit cyber security vulnerabilities and ensure the system can perform its intended functions.

The SC3 nuclear segment design incorporates features to support establishment of a secure operational environment. It is installed and maintained in accordance with the station administrative procedures and control of access programs.

The BWRX-300 network switches interconnect the SC3 DCIS segments. The network switches have security features described in Section 7.2.3. The communications on the nuclear Unit Data Highways are rigorously controlled and monitored and information sent off-site is through unidirectional boundary devices, as described in Section 7.2.4.

See Chapter 25 for further information.

7.3.3.3.5 Diversity and Defence-in-Depth

The SC3 nuclear segment provides anticipatory trip functions to support the D-in-D strategy. An example of anticipatory trips is an APS scram on loss of off-site power which is initiated before the Safety Category 1 and Safety Category 2 functions scram the plant on reactor low level on loss of the feed pumps or a high flux resulting from a reactor isolation on loss of vacuum. Another example is the APS scram on a turbine trip or load rejection before the Safety Category 1 and Safety Category 2 functions scram the plant on reactor high flux or pressure; this also mitigates the adverse thermal limit response because the reactor is scrammed before the pressurisation wave affects the reactor.

The Safety Category 3 functions are implemented in SC3 hardware and software that are diverse from SC1 equipment. The SC3 APS actuation relays shown in Figure 7-4 are configured as energise to actuate and the SC1 I&C load drivers are configured as de-energise to actuate, which provides functional diversity in these actuation circuits.

Diversity measures are incorporated within the SC3 nuclear segment design as an additional level of protection for potential systematic faults caused by design and implementation defects when equipment is credited to as backup in the safety analyses.

The use of a fourth SC3 signal provides immunity against loss of control signals due to the postulated CCF of the SC2 signal splitters.

The SC3 nuclear segment provides diversity to support the D-in-D strategy. The SC3 hardware and software performing Safety Category 3 functions are diverse from SC1 equipment performing Safety Category 1 functions. The turbine overspeed protection control logic uses two diverse and independent systems to provide sufficient reliability to eliminate the risk of turbine missile generation and to avoid the need for a mechanical overspeed trip. These turbine overspeed protection systems use TMR control architecture to eliminate random hardware vulnerabilities that could result in spurious turbine trips.

Independence

The SC3 I&C systems can initiate hydraulic scrams, automatically and manually initiate isolations, and operate the ICS. No SC3 I&C equipment can prevent a scram, isolation, or ICS initiation actuated from SC1 or SC2 systems. Similarly, Safety Category 1 and Safety Category 2 functions cannot adversely affect Safety Category 3 functions. If Safety Category 3 functions do not send out their anticipatory trip commands, plant safety is ensured by Safety Category 1 and Safety Category 2 functions.

Although the SC2 equipment, the SC3 nuclear and BOP segments, and the SCN BOP controllers are powered by UPS with battery backups, the power supply is redundant, and a single failure does not affect either DL or segment. The UPS and the battery chargers can be powered by off-site power or either of the standby diesel generators. Double breakers or fuses are used to separate the different SC equipment and to separate the SC3 nuclear and BOP segments such that a fault does not propagate. No power feeds to equipment performing Safety Category 2 or Safety Category 3 functions are shared with SC1 equipment performing Safety Category 1 functions.

The SC3 software and logic is independent of the SC2 software and logic.

7.3.3.4 Operator Interface and Accident Monitoring

The SC3 data are available on their appropriate displays. The layout and content of the displays are designed as part of the HFE program of activities integrated into the BWRX-300 design. The SC3 DCIS has its own displays in both the MCR and SCR and locally in the SC3 equipment rooms. The SC3 displays also include an alarm system to provide operator awareness and to prompt to the displays containing further information relating to the alarm. SC3 system bypass conditions are alarmed in the MCR.

Signals monitored by the SC3 systems provide necessary information to achieve or verify correct plant response to transients and accidents. The necessary signals are determined through HFE analysis and applicable regulatory requirements and are referred to as accident monitoring signals.

The SC3 signals are alarmed to prompt the operator to an appropriate display (e.g., range check problems or alarm setpoints exceeded). The SC3 signals and the various SC3 components are alarmed for self-diagnostics.

The SC3 system acquires accident monitoring information associated with Type B and C accident monitoring variables from SC1 I&C through isolated interfaces. It also acquires accident monitoring information associated with Type D, E, and F accident monitoring variables from SC3 and SCN equipment. The aggregated SC3 displays of accident monitoring information are provided to the MCR located in the CB and the SCR located in the RB.

The Type D, E, and F are defined in IEC 63147 “Criteria for accident monitoring instrumentation for nuclear power generating stations,” (Reference 7-23). Type D variables provide information to accident management personnel to verify safety system status and that indicate the performance of safety systems, required auxiliary support features, and other systems necessary to achieve and maintain a safe shutdown condition. Type E variables provide information to accident management personnel to monitor radioactive releases identified pathways and environmental conditions used to determine the effects of releases in the plant environs and radioactivity levels in the control rooms and selected plant areas where access may be required for plant recovery. Type F variables provide information that indicates fuel damage and the effects of fuel damage to support accident management response to severe accidents. A preliminary list of the Type D, E, and F accident monitoring variables is provided in Table 7-3.

The SC3 and SCN DCIS rooms, which include SC3 I&C equipment and associated electrical support equipment are located in the CB. The MCR is used by plant operators unless conditions require relocation to the SCR. The CB provides the necessary seismic ruggedness and habitability capabilities to support the expected post-accident conditions with a SC3 level of quality and reliability for required protection functions.

The operator interface HSI for the SC3 nuclear segment is in Sections 7.5 and 7.6 for the MCR and SCR, respectively.

7.3.3.5 Compliance Alignment

Table 7-8 shows how the SC3 systems align to meets the regulatory guidance in the key industry I&C standards IEC 61513 (Reference 7-5).

7.3.3.6 Interfaces with Other Systems

- Chapter 4.7 Core Monitoring.

7.3.3.7 Performance and Safety Evaluation

The system design bases, and associated safety functions are described in Subsection 7.3.3.2.

7.3.3.8 Application of ALARP Principles in Design Development

The SC3 I&C system design development is compliant with the ALARP principle through the application of appropriate codes and standards, OPEX, and optioneering, where relevant. The I&C system development process is detailed in Section 7.4.

7.3.4 Balance of Plant Controllers – Non-Safety Class/Balance of Plant Segment

This section addresses the SCN BOP controllers that feed the SCN BOP segment, which contains the control and monitoring systems associated with power generation and support systems.

7.3.4.1 Systems Architecture

The Non-Safety Class I&C Systems are assigned to perform Safety Category None functions that are not assigned to SC1, SC2, or SC3 I&C systems. These SCN systems include equipment needed for control, diagnostics, network support, and cyber security for systems that cannot generate an AOO.

The SCN I&C Systems that perform Safety Category None functions are implemented on platforms that are independent from the SC1 platforms.

The functional architecture for the SCN BOP controllers is shown in Figure 7-13. The functions shown using TMR controllers are dual ported to the plant SCN BOP segment network. The other functions are implemented as “packaged systems” (typically embedded controllers) provided by an equipment vendor. Depending on final DCIS design and processor loading, functions may be combined onto common or shared controllers. Similarly, the use of TMR may be changed as the design progresses based on assessment of controller failure effects on the plant.

Control signals needed between controllers for their functions are point-to-point wire or optical fibre. The signals needed by a controller for its functions are radially connected to the controller and do not use plant networks.

The SCN systems are listed below.

- C40, Investment Performance
- C41, Platform Performance Monitoring
- C43, Water Chemistry
- C44, Effluent Cleanup Control System
- C45, Network Communications and Operator Interface

The majority of the SCN I&C systems are powered from battery backed R30 UPSs and are located in CB.

The SCN I&C systems use RIOs installed at various locations around the plant to obtain and multiplex inputs from local field devices.

The SCN I&C systems connect to the UDH via C45.

7.3.4.2 System Design Bases and Associated Safety Functions

The design basis of the SCN BOP controllers is to provide for the control and monitoring of the SCN power generation and support equipment. The SCN I&C system design includes provision of instrumentation to monitor plant variables and systems over the respective ranges for operational states to ensure that adequate information can be obtained on plant status.

This equipment is not credited for protection functions although they may be available for beyond design basis and severe accident scenarios.

The main SCN I&C system are:

- C40, Investment Protection
- C41, Plant Performance Monitoring
- C43, Water Chemistry
- C44, Effluent Cleanup Control
- C45, Network Communications and Operator Interface

7.3.4.2.1 C40, Investment Protection

The C40 Investment Protection Systems implement interfaces to the Cathodic Protection and Monitoring packaged system (R61), Freeze Protection packaged system (R61), and Fire Protection Packaged system (U43).

7.3.4.2.2 C41, Plant Performance Monitoring

The C41 Plant Performance Monitoring system provides interfaces to the Advanced Condition Monitoring (ACM) packaged system including RIO cabinets, and the Thermal Performance Monitor (TPM) packaged system.

7.3.4.2.3 C43, Water Chemistry

The C43 Water Chemistry System controls and monitors the FW hydrogen injection function and operates the noble metal injection system.

7.3.4.2.4 C44, Effluent Cleanup Control

The C44 Effluent Cleanup Control System implements SCN functions related to the Liquid, Gas, and Solid Radwaste Control Functions, Equipment and Floor Drains System Controller, and Potable Water/Sewage Control.

7.3.4.2.5 C45, Network Communications and Operator Interface

The C45 Network Communications and Operator Interface system bridges the communications between the SCN packaged systems and the UDH. It interfaces with the area radiation monitoring, environmental monitoring equipment and seismic monitoring.

7.3.4.3 Fundamental Design Properties in the System Design

The SCN system properties are based in the quality measures implemented to minimise the potential for failures and initiating events to occur. The SCN systems are conservatively designed and analysed. These properties of qualification, reliability, robustness, security, diversity, and other D-in-D features are discussed in the following five subsections.

7.3.4.3.1 Equipment Qualification

The SCN BOP controllers are designed to operate in the environment that is to be expected during normal operations. The SCN BOP controller design and manufacturing processes are of sufficient quality to ensure that I&C systems can reliably perform their design bases functions. The SCN BOP controller equipment is designed, developed, fabricated, and tested to quality standards commensurate with the safety significance of the functions to be performed. The SCN BOP controller equipment qualification measures confirm that the I&C systems and equipment are capable of reliably performing the design functions for which they are credited over the range of environmental conditions postulated for the area in which they are located.

The SCN BOP controller equipment is assessed as a potential hazard if located near safety classified equipment and, if necessary, qualified for electromagnetic compatibility in accordance with IEC 61000-4 (References 7-27, 7-36 through 7-52) and IEC 61000-6-2 (Reference 7-28) for emissions only.

7.3.4.3.2 Reliability

The SCN BOP controllers have the required reliability to perform their intended functions. The reliability analysis of the SC3 BOP Segment demonstrates it meets its reliability goals using qualitative and quantitative performance measures or criteria, as appropriate. Separately, the SCN BOP controllers have the required reliability to perform their intended functions.

SCN BOP controllers are implemented with redundancy as appropriate to ensure that single controller failures have no adverse effect on system or plant operation. The controllers have a specific reliability requirement goal that there be no failures more often than once per 100 years. The intent is that no random controller failure initiates an AOO. Controller reliability will be formally analysed to determine failure rates, as part of the detailed plant design.

Extensive hardware and software diagnostics are provided for the TMR controllers to provide operator monitoring and alarms. Failed TMR controller parts may be replaced online.

The main SCN BOP controller platform’s control and monitor design support both local and remote data acquisition, the latter with optical fibre or wire. The intent is that the failure of a SCN controller does not initiate an AOO.

7.3.4.3.3 Robustness

Robustness of the SCN controllers is the degree to which it can function correctly in the presence of invalid inputs or stressful environmental conditions. The robust SCN BOP controller design reflects the use of design methods and adherence to engineering best practices to ensure that its functions are achieved for the specified conditions.

The SCN BOP controllers have no direct connections (i.e., commands or communication) with the SC1 systems.

The SCN BOP controller equipment is in different rooms than the SC3 nuclear segment rooms and physically separated from SC1 and SC2 equipment rooms. The SCN BOP controller physical separation and signal isolation devices meet the requirements of IEC 60709 (Reference 7-22). Vendor supplied SCN hardware is connected through an SC3 gateway.

7.3.4.3.4 Security

The SCN BOP controller design incorporates features to support establishment of a secure operational environment. This equipment is installed and maintained in accordance with the station administrative procedures and control of access programs.

The BWRX-300 network switches that interconnect the SC3 BOP segment have security features, as described in Section 7.2.3. The communications on the SC3 BOP Unit Data Highways are rigorously controlled and monitored and information sent off-site is through

unidirectional boundary devices, as described in Section 7.2.4. The vendor packaged SCN BOP controllers are interfaced to the SC3 BOP Segment through SC3 gateways to provide communication protocol conversion and eliminate cyber security vulnerabilities.

See Chapter 25 for further information.

7.3.4.3.5 Diversity and Defence-in-Depth

The SCN BOP Segment I&C platform equipment has no specific diversity requirements as it performs no credited protection functions.

7.3.4.4 Operator Interface

The operator interface HSI for the SC3 BOP Segment is described in Section 7.5 for the MCR.

7.3.4.5 Compliance Alignment

Table 7-8 shows how SCN BOP Segment align to meet the regulatory guidance in the key industry I&C standards IEC 61513 (Reference 7-5).

7.3.4.6 Interfaces with Other Systems

Rest to be confirmed during the detailed design.

Gamma Thermometers – Chapter 4.

7.3.4.7 Performance and Safety Evaluation

The system design bases, and associated safety functions are described in Subsection 7.3.4.2.

7.3.4.8 Application of ALARP Principles in Design Development

The SCN I&C system design development is compliant with the ALARP principle through the application of appropriate codes and standards, OPEX, and optioneering, where relevant. The I&C system development process is detailed in Section 7.4.

7.4 Digital Instrumentation and Control System Development Process (Production Excellence)

The BWRX-300 I&C systems design is the result of a past and continuing top – down systematic design process. This process makes risk-informed decisions about the scope and level of design detail required at various stages of the BWRX-300 design process. The BWRX-300 I&C design process is derived from IEC 61513 (Reference 7-5).

The BWRX-300 I&C design process is informed by first-hand experience and lessons learned from already licensed and delivered Boiling Water Reactor (BWR) I&C designs and proposed new plant I&C designs (e.g., United States, Finland, Taiwan, and United Kingdom).

7.4.1 Design Control

The BWRX-300 I&C design process is used to ensure that the design and its associated design documentation meet applicable technical requirements, regulatory requirements, codes and standards, and contractual requirements. It is an iterative and recursive design process to allow sequencing and development of requirements. The design phases are defined by the maturity of each of the requirement levels, and deliverables are defined for each phase.

1. **Baseline 0 Design Phase**: The Baseline 0 Design Phase focuses on an abbreviated concept design cycle to more closely examine the design and technology selections suited for demonstration on the desired timeline. This phase focuses on rapid study and design of requirements, systems, and component design alternatives to support timely regulatory submittals, and refinement of the selections into an optimised safety and licensing package. Based on these studies, top-level design requirements are established for the standard plant design based on stakeholder and product requirements, including expected regulatory requirements for desired markets. I&C system requirements are defined and allocated based on high-level conceptual mechanical systems design, and high-level planning documents are prepared. An initial plant level architecture document is prepared.
2. **Baseline 1 Design Phase**: The Baseline 1 Design Phase focuses on developing the specific design definition of primary SSC. This includes detailed system and, where appropriate, component analysis, specifications, and drawing development, and detailed manufacturing and fabrication analyses for long lead procurement activities. Technical reviews are conducted to confirm the adequacy of design requirements and objectives. System interfaces are established and integrated models, baseline safety analyses, and probabilistic safety analyses to support construct permit application submittals to regulators are developed. System design descriptions are developed for primary systems based on known requirements allocated from identified plant level requirements, interfacing systems, and the overall plant operational concept. At the plant level, the I&C system of systems architecture is developed, and diverse hardware- and software-based implementing control and monitoring platforms are provisionally selected. Various plant level architecture and design documents and diagrams are prepared defining the relationships associated with topics including I&C control and monitoring functions from the reactor and power plant process systems, I&C functions to I&C systems or groups, I&C systems to I&C equipment or platforms, and interconnectivity “from-to” cable and wiring route tables between major I&C equipment or platform cabinets as well as their physical characteristics (e.g., space, weight, electric power demand, heat generation load, and location in the buildings, floors, and rooms).
3. **Baseline 2 Design Phase**: The Baseline 2 Design Phase focuses on the effort to complete the standard plant design and prepare for construction planning, detailed component design, and support for equipment procurement/fabrication required at this

stage of design. Key system and component design documents and calculations of record is to be issued to support licensing and construction, and equipment specifications are finalised for procurement. Design verification is performed to support submittal of the operating licence application.

4. **Baseline 3 Design Phase**: The Baseline 3 Design Phase focuses on finalisation of all remaining system and component design in preparation for construction activities. The remaining equipment specifications are finalised and executed for procurement, and all remaining system and component design documents and calculations of record are issued. This phase includes the detailed efforts necessary to apply the standard plant design to a specific project (e.g., satisfaction of local codes and engineering requirements for stamping of drawings and documents, plant/customer-specific equipment identification for turnover to customer operating systems, and finalisation of commodity purchases and construction details). Updates may be needed to component specifications and datasheets based on feedback from selected vendors, and these are evaluated for application to the standard plant design.

The remaining equipment specifications are finalised and executed for procurements, and remaining system and component design documents and calculations of record are issued.

7.4.2 Defence-in-Depth and Architecture Design

A structured, formal approach to defining the overall I&C architecture is a prerequisite for successful licensing of a new nuclear plant design. The development process output includes a definition of each I&C system in terms of its assigned functions, its safety classification, and its relationships to other systems. The design of the I&C architecture provides a top-level definition of the I&C systems of the BWRX-300 and the communication between BWRX-300 systems. The design process and supporting tools ensure a consistent interface between these systems.

The BWRX-300 I&C architecture design process is shown in Figure 7-15.

7.4.2.1 Baseline 0 Phase and Activities

The requirements which define the necessary functions to control, operate or monitor are specified. An I&C functional requirement is defined in such a way that it:

- Gives a complete representation of a functional objective.
- Can be categorised according to its degree of importance to safety.

Inputs to the I&C Functional Requirements include:

- Process and electrical system design descriptions
- Transient and accident analyses
- Human factors analyses

Requirements that define the necessary independence and diversity for I&C systems are specified. An I&C architectural requirement is defined in such a way that it specifies a safety classification and level of redundancy for each I&C system.

Inputs to the Architectural Requirements include:

- Transient and accident analyses
- Severe accident analyses
- D-in-D concept for the plant
- Applicable regulations, guidance, and endorsed standards

- Human factors analyses

These are the constraints placed on the BWRX-300 I&C architecture from external influences. Examples of external influences include:

- Plant building and room layouts
- Process system interfaces
- Support system designs
- Environmental conditions
- Sources of internal and external hazards
- Concept for online maintenance
- Human factors constraints
- Cyber security constraints

Requirements are defined and allocated based on high-level conceptual mechanical systems design, and high-level planning documents are prepared. An initial plant level architecture document is prepared.

7.4.2.2 Baseline 1 Phase and Activities

The Allocation of Functions (AOF) activity involves the definition of a set of criteria to govern the process of allocating I&C functions to I&C systems and the act of allocating the I&C functions following the criteria. This can be done initially at the level of control and monitoring functions, but eventually needs to be done for each I&C function. I&C sub-functions are created during this process.

The definition of architecture activity is the top-level definition of I&C systems in terms of the functional scope of each I&C system. At a minimum, the definition of an I&C system comprises its safety classification, its design bases functions, and its position in the lines of defence. This work can also include top-level assignment of I&C systems to physical locations in the plant.

Both the AOF and definition of architecture are iterative, both to each other and as the BWRX-300 plant design progresses.

The definition of interfaces activity represents the organisation and documentation of the interfaces created by the architecture definition and function allocation processes. The key elements to document are:

1. Basis (need) for the interface.
2. Top-level nature of the interface (e.g., hardware, data communication, point-to-point, and switched network).
3. Primary requirements on the interface (e.g., independence, diversity, and failure modes).

Interfaces also include support systems for the I&C system.

HSIs are integrated in the architecture and design structure for each system control and monitoring areas including the MCR, SCR, local control panels, and any emergency control location. The design of the I&C architecture implements the principles for plant operation established in the BWRX-300 plant design including:

1. Requirements between automatic signals and manually initiated control signals.
2. Requirements between the different HSI systems during normal, accident, and post-accident operation.

3. Requirements between normal and backup HSI systems (including any switchover rules). The human factors engineering program is described in Chapter 18.

7.4.3 Instrumentation and Control System Life Cycle

The I&C System Life Cycle applied to each I&C system follows the overall lifecycle of IEC 61513 (Reference 7-5) and the system engineering “V” model to show top-down design and bottoms up integration for Verification and Validation testing, as shown in Figure 7-16.

This plan includes the project timeline in X axis and vertical level project progression with verification and validation arrows included. Configuration management requirements for the project are defined in Configuration Management Plan for the project.

The Requirements Management Plan for the project provides direction for managing requirements appearing in project documents developed during execution of the design process.

Each plant level I&C architecture lifecycle phase within the lifecycle contains activities and output documentation aimed at fulfilling the purpose of the phase. The phases are not strictly sequential in their execution; rather, they are iterative. For example, decisions and discoveries made in a ‘subsequent’ phase can necessitate a return to ‘previous’ phases to modify requirements, design decisions, or output documentation. In certain cases, portions of different phases can be executed in parallel. In general, a ‘subsequent’ phase can be started prior to completion of the ‘previous’ phase.

The software related activities in I&C System Life Cycle are shown in Figure 7-17 from IEC 60880 Figure 2 (Reference 7-25).

7.4.4 Cyber Security Life Cycle

The BWRX-300 Cyber Security Program Plan is designed to meet relevant industry standards and best practices for the design, operation, and protection of the BWRX-300 I&C systems. The BWRX-300 Cyber Security Program Plan applies advanced security principles throughout the product development and deployment lifecycle of the BWRX- 300 I&C systems.

The objective of the program plan is to achieve a high assurance that unauthorised access to the protection, control, and adjustment systems of the BWRX-300 is prevented. The program is based on three key principles:

1. Regulatory compliance.
2. Integration of cyber security controls into the BWRX-300 I&C systems development process.
3. Integration of cyber security features into the BWRX-300 I&C systems.

The BWRX-300 Cyber Security Program Plan recognises that protecting cyber essential assets is an ongoing program throughout the I&C system development and operations stages. It is designed to:

- Implement security controls to protect the necessary digital assets from cyber-attacks.
- Apply and maintain D-in-D protective strategies to ensure the capability to detect, respond to, and recover from cyber-attacks.
- Mitigate the adverse effects of cyber-attacks.
- Ensure functions of protected assets are not adversely affected due to cyber-attacks.

The cyber security life cycle is shown in Figure 7-18. See Chapter 25 for more information.

7.4.5 Compliance Alignment

This section describes how the BWRX-300 I&C development life cycle aligns to meets the key industry I&C standard IEC 61513 (Reference 7-5) as shown in Table 7-9.

7.5 Instrumentation and Control in the Main Control Room

The MCR is in the CB. The MCR is the primary location for plant monitoring and control during normal, abnormal, and emergency conditions. The MCR includes controls, indications and alarms that enable operators to perform the defined set of functions during normal operation modes and PIE conditions.

The MCR equipment is designed in accordance with the HFE processes describe in Chapter 18.

7.5.1 Main Control Room Use

The MCR is designed with HSIs to support the following tasks:

1. Assessing the overall status and performance of the plant in any condition and providing necessary information to support operator actions.
2. Monitoring and controlling fundamental safety functions.
3. Monitoring the status and trends of key plant parameters (such as reactor power and rates of power change).
4. Operating the plant safety during all operational states, automatically or manually when the MCR is available.
5. Taking measures to maintain the plant in a safe state or to bring it back into a safe state after design basis events and DECs.
6. Maintaining the plant within the specified limits and conditions for the parameters associated with plant systems and equipment.
7. Monitoring for failure of critical instrumentation and equipment.
8. Confirming safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended.
9. Determining the need and the time for manual initiation or intervention of specified safety actions.
10. Implementing Emergency Operating Procedures (EOPs), emergency mitigating equipment guidelines, and Severe Accident Management Guidelines (SAMGs).

The MCR is designed to be optimal for nominal shift complement of the control room operator role-holders. The MCR at concept stage is sized and designed to accommodate the expected maximum number of people on a continuous basis. This maximum number will be based on the MCR nominal staffing plus six other people. The basis for six additional people is to allow sufficient space for the supervisory role and five others (e.g., trainees, observers). The capability for six additional people also provides the necessary facilities to support plant conditions and evolutions that require more than the normal operations complement, for example during pre-operational and startup testing. The size and layout of the MCR are expected to be adjusted as the design progresses as a result of the staffing analysis being conducted as part of the HFE program of activities, as described in Chapter 18. The required MCR personnel have workstations designed to support their specific control, information, communication, and work coordination needs. Each MCR workstation also contains space for a role trainee. The MCR is designed in accordance with current international best practice codes and standards for control room design, integrating results from HFE analyses and specified HFE design requirements as described in Chapter 18.

7.5.2 Main Control Room Layout

Figure 7-19 represents the concept for the MCR. This concept is expected to evolve with the program of safety analyses and HFE activities being performed as an integral part of the

BWRX-300 design. The analyses are used to develop an MCR design that optimally supports required personnel roles for all plant conditions.

Key to the MCR layout design is that tasks take place in a position that does not result in blocking views of the Group-View Display. The arrangement of the workstations in the MCR also facilitates communication between all MCR personnel, including direct conversation and visual contact. MCR design also fosters the oversight and command and control responsibilities of the required supervisory roles. The layout of workstations provides sufficient clearance for foot traffic and maintenance between consoles. The layout of workstations provides enough space for the proper storage, placement, and use of tools and procedures in the MCR. The workstations are generally designed for seated operations; however, it is expected that the HFE analysis activities described in Chapter 18 will identify the correct configuration and height required to ensure optimal visibility of individual and shared workspaces within the MCR.

The MCR Group-View display is an array of large VDUs displaying a consolidated overview of information about plant systems. The purpose of the Group-View Display is to support cohesive situational awareness and crew coordination through shared monitoring of key parameters and alarm information relating to overall plant status, including Emergency Operating Procedure entry conditions.

The Group-View display VDUs are located and designed to support optimal line-of-sight and viewing angles by the necessary subset of MCR users. Group-View Display and their content are designed and sized to support monitoring and readability of on-screen component labels and indications to the required MCR users. Group-View display content can be managed at the supervisory workstation via mouse and keyboard interface, including access to closed circuit televisions. Group-View Display VDUs do not have plant control functions, as these are designed for monitoring purposes only. Group-View Display alarms from SC1, SC2, SC3, and SCN systems are also included on the Group-View display VDUs. Additional information about alarms will be accessible at the workstation. The Group-View display connected to the DCIS are also available at the workstation VDUs. The purpose of the Group-View display is to be a supplemental, not a sole source, of information.

The MCR operator workstation is made up of three sections: two SC3 workstation sections and one critical action panel workstation section. The MCR operator workstations contain the controls and indications needed to perform the assigned MCR tasks. VDU displays are designed using the HFE processes described in Chapter 18 and provide easy and simple navigation to available parameters and controls.

The Critical Action Panel includes redundant SC3 workstations that display data associated with Type B and C Accident Monitoring parameters as well as other data obtained by C10. The workstations enable data trending and alarming but provide no control capabilities. Data are sent one-way from the three SC1 divisions to the redundant SC3 workstations. The Critical Action Panel also includes hardwired switches that enable operators to manually initiate functions that are automatically performed in DL3 and DL4a. The manual switches do not rely on control system logic and their functionality is not assigned to DL3 or DL4a.

The SC3 workstations will contain the necessary VDUs to support monitoring, control, and alarm management of all other plant functions. These VDUs are controlled by an appropriate number of wired keyboards and mouse interfaces.

SC3 workstation VDUs are capable of displaying any provided plant and system information, as supported by the I&C architecture. These VDUs only allow for control of SC3 and Non-Safety categorised functions and does not allow more than one operator to control the same equipment at the same time.

MCR SC3 workstation VDUs are sized and positioned in compliance with specified HFE design requirements for viewing angles for frequently used indications and alarms, to support readability, and to preserve line-of-sight to Group-View Display. The arrangement of the SC3 workstations in the MCR facilitates verbal communication.

The MCR SC3 workstations also contain a VDU (each with a mouse and keyboard input device) dedicated for business Local Area Network (LAN) and one of the SC3 workstations contain a VDU (with a mouse and keyboard input device) for the fire protection system. The SC3 workstation also contains space for communications equipment, procedure laydown, and administrative tasks.

The MCR supervisory role workstation is implemented with SC3 equipment and designed with a work area large enough to accommodate three seated people. The MCR supervisory workstation is located behind the SC3 workstation; it is suitably positioned to maintain a clear line-of-sight to the SC3 workstations and support verbal communication with the other workstations in the room. The supervisory workstation is also positioned to maintain a clear line-of-sight to the Group-View Display. The MCR supervisory workstation contains at least two VDUs with indications (no control) to monitor operations as they are being performed. The MCR supervisory workstation VDUs are controlled by a wired keyboard and mouse interface. The MCR supervisory workstation also contains two VDUs dedicated to the business LAN, as well as space for communications equipment, procedure and drawing laydown, and administrative tasks.

The MCR also contains an emergency communications workspace. The intent of the workspace is to allow designated personnel as required during events to communicate externally to the MCR, in such a way as to not disrupt the personnel focused on monitoring and controlling the plant in response to the event. The emergency communications workspace is located and designed with suitable provisions to minimise disturbance to the operating crew. The emergency communications workstation contains at least one VDU with indications (i.e., no control) from all Safety Class and Non-Safety Class systems for monitoring plant conditions. The emergency communications workstation also contains at least two VDUs to access the business LAN. The emergency communications workstation VDUs are controlled by a wired keyboard and mouse interface. VDUs are sized and positioned in compliance with specified HFE design requirements. The emergency communications workspace also contains space for all required communications equipment and administrative tasks.

7.6 Instrumentation and Control in the Secondary Control Room

In the current concept design, the SCR is in the RB. The routes from the MCR to the SCR are described in Chapter 6. The SCR includes the required HSI that enable operators to perform the defined set of functions required for responding to the identified plant events and conditions for which the MCR cannot be used.

The SCR is designed in accordance with current international best practice codes and standards for control room design, integrating results from HFE analyses and specified HFE design requirements as described in Chapter 18.

7.6.1 Control Transfer Function

Access to the SCR is under strict administrative controls and indicated by alarms in the MCR to ensure unauthorised access is detected. The SCR includes HSI inventory required to maintain the plant in a safe state for scenarios requiring MCR evacuation. Suitable provisions are provided inside the SCR for transferring control to the SCR whenever the MCR is abandoned, as well as to transfer control back to the MCR. Any design features, if needed to affect I&C control transfer, are located in a suitable location determined through HFE analysis, either in the SCR or accessible via the qualified access path.

Design features that prevent or mitigate spurious actuations due to fire are described in Chapter 9.

7.6.2 Secondary Control Room Use

The SCR is utilised to perform the functions required to keep the plant in a safe state when the MCR is unavailable. The required functions are derived as a result of safety and HFE analyses.

The SCR includes suitable facilities for habitability and well as workspace for tasks to support required usage. The SCR contains a suitable supply of food and water. The SCR also contains adequate space and provisions for sleeping as required by the postulated scenarios in which it is used.

The SCR is designed to accommodate the expected staffing based on BWRX-300 HFE staffing analysis for the expected usage conditions. A suitable number of workstations are provided to support the specific task, communication, and work coordination needs for expected personnel.

7.6.3 Secondary Control Room Layout

The layout of the workstations and HSI in the SCR provides the personnel with adequate information to assess the plant state and perform actions to maintain the plant in a safe state, if required for the expected usage scenarios.

To reduce the likelihood of human errors and time needed to resume monitoring and control tasks within the SCR, the layout and HSI of the SCR are design to be consistent with the MCR to the extent possible, with differences driven by different purpose and user task needs.

The SCR operator workstation can accommodate two people. The workstation contains the required HSI to perform the functions expected to be performed in the SCR.

The SCR SC3 workstation section contains two VDUs to support monitoring, control, and alarm management. The SC3 workstation VDUs can display any provided plant and system information, as supported by the I&C architecture, but will only allow for control of SC3 and Non-Safety categorised functions. SC3 VDUs allow for flexible use and are not divisionally separated or dedicated. These VDUs are controlled by a wired keyboard and mouse.

SCR SC3 workstation VDUs are sized and positioned in compliance with specified HFE design requirements for viewing angles for frequently used HSI components. The SCR SC3

workstation suitably positioned to support effective verbal communication with the other workstations in the room. The SCR SC3 workstation also contains space for communications equipment, procedure laydown, and administrative tasks.

The SCR supervisory workstation is suitably positioned to maintain a clear line-of-sight to the SC3 workstation and support effective verbal communication throughout the room. The supervisory workstation contains two non-safety classified VDUs to provide SPDS indications (i.e., no control) to monitor plant conditions, and a VDU or tablet is provided for business LAN connection. The SCR supervisory workstation also contains space for communications equipment, procedure and drawing laydown, and administrative tasks.

VDUs are controlled by a wired keyboard and mouse interface except, where applicable or dictated by safety requirements.

The SCR has an emergency communications workspace located and designed with suitable provisions to minimise disturbance to the operating crew. The emergency communications workstation contains VDUs or Wi-Fi-enabled tablets for connection to business LAN with at least one VDU with displaying SPDS indications (i.e., no control) to monitor and report externally on plant conditions. The emergency communications workspace also contains space for communications equipment, procedures, and drawings in support of performing administrative tasks.

7.7 Instrumentation and Control in the Emergency Response Facilities

The BWRX-300 MCR is the primary location for plant monitoring and control during normal, abnormal, and most emergency conditions. The I&C capabilities in the MCR are described in Section 7.5. The SCR is utilised to perform the functions required to keep the plant in a safe state when the MCR is unavailable. The I&C capabilities in the SCR are described in Section 7.6.

The Emergency Preparedness and Response capabilities and associated facilities are described in Chapter 13, Section 13.3.

The plant information necessary to support overall emergency response from the MCR, SCR, Emergency Offsite Centre, Site Management Centre, and ERFs is provided either directly via the Unit Data Highway or the Plant Data Highway unidirectional boundary device interface shown in Figure 7-1, depending on cyber security requirements and I&C requirements required for each location.

The MCR emergency communications workspace contains space for communications equipment and administrative tasks. The plant communication systems are described in Chapter 9.

7.8 Hazard Analysis for Instrumentation and Control Systems

Hazards for the BWRX-300 I&C systems are addressed in five ways.

First, specific system requirements are developed based on plant safety analysis (i.e., plant-level hazards), as described in Chapter 15. These are the Safety Category 1, 2 and 3 actuation functions.

Second, specific hardware and software technology hazards for the digital I&C equipment (i.e., digital technology hazards) are addressed by system level failure modes and effect analyses performed using the methods described in IEC 60812, “Failure modes and effects analysis (FMEA and FMECA),” (Reference 7-24).

Third, a rigorous development process, as described in Section 7.4, is used to minimise human errors during system development and operation (i.e., systematic hazards).

Fourth, the I&C equipment is designed to provide protection against external and internal hazards, as described in Chapter 3, Sections 3.3 through 3.7.

Fifth, the I&C equipment is qualified, as described in Chapters 3, Sections 3.10 and 3.11, and Section 7.3.

7.9 Smart Devices

Smart devices/digital technology equipment is only used in SC3 and SCN applications.

Table 7-1: I&C System and Equipment Standards

Safety Class	Description	Systems	Equipment
SC1, SC2 and SC3	I&C equipment supporting Safety Category 1, 2 and 3 functions	IEC 61513 (Reference 7-5) IEC 60709 (Reference 7-22) IEC 63147 (Reference 7-23) IEC 60812 (Reference 7-24)	IEC 61000-4, “Electromagnetic Compatibility Package,” (Reference 7-27) IEC 61000-6-2 (Reference 7-28)
SC1	I&C Equipment supporting Safety Category 1 functions	IEC 60880 (Reference 7-25) IEC 60987 (Reference 7-35) IEC 62566:2012 (Reference 7-59)	IEC 60780-323 (Reference 7-29) IEC 60980-344 (Reference 7-30) IEC 61500 (Reference 7-31)
SC2	I&C Equipment supporting Safety Category 2 functions	IEC 60987 (Reference 7-35) IEC 62138 (Reference 7-26) IEC 62566-2:2020 (Reference 7-60)	IEC 60780-323 (environmental) (Reference 7-29)
SC3	I&C Equipment supporting Safety Category 3 functions	IEC 62138 (Category C software) (Reference 7-26) IEC 62566-2:2020 (Reference 7-60)	IEC 60980-344 (seismic) – Note 1 (Reference 7-30) IEC 62671, “Nuclear power Plants – Instrumentation and Control Important to Safety - Selection and use of industrial digital devices of limited functionality,” (Reference 7-32) IEC 61508 – Note 2, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Parts 1 to 7, Commented Version,” (Reference 7-33)

Notes

1: If required for mitigation of seismic-related event

2: Only used for pre-developed software for SC3.

Table 7-2: Safety Category 1 Control Functions & Associated SC1 Initiation Signals

Initiating Signal	Monitored Parameters	Reactor Mode
Function - Hydraulic Scram		
HIGH RPV pressure [HP1]	Reactor Pressure	RUN or STARTUP
LOW RPV pressure [LP1]	Reactor Pressure	RUN
LOW RPV level [L3]	Reactor Water Level	RUN or STARTUP
HIGH simulated thermal power	Simulated Thermal Power	RUN
HIGH containment pressure	Containment Pressure	RUN or STARTUP
HIGH neutron flux (STARTUP setpoint)	Neutron Flux	STARTUP
Indication of a line break (Main Steam Line (MSL), ICS Line, or FW)	Main Steam Line Flow FW Line Pressure Reactor Dome Pressure Steam Supply Flow Train A/B/C Condensate Return Flow Trains A/B/C	RUN, STARTUP
Function - Isolation Condenser Actuation		
HIGH RPV pressure [HP2] (ICS Train A actuation)	Reactor Pressure	RUN, STARTUP, or SHUTDOWN
HIGH RPV pressure [HP3] (ICS Train B actuation)	Reactor Pressure	RUN, STARTUP, or SHUTDOWN
HIGH RPV pressure [HP4] (ICS Train C actuation)	Reactor Pressure	RUN, STARTUP, or SHUTDOWN
LOW RPV water level [L2]	Reactor Water Level	RUN, STARTUP, or SHUTDOWN
HIGH containment pressure	Containment Pressure	RUN, STARTUP, or SHUTDOWN
Line break indication (MSL, ICS, FW)	Main Steam Line Flow FW Line Pressure Reactor Dome Pressure Steam Supply Flow Train A/B/C Condensate Return Flow Trains A/B/C	RUN, STARTUP, or SHUTDOWN
Function - RPV and Containment Isolation		
LOW RPV level [L2]	Containment Pressure	RUN, STARTUP, or SHUTDOWN
HIGH containment pressure	Reactor Water Level	RUN, STARTUP, or SHUTDOWN
Function - MSRIV and MSCIV Isolation		
LOW RPV pressure [LP1]	Reactor Pressure	RUN
LOW RPV level [L2]	Reactor Water Level	RUN, STARTUP, or SHUTDOWN

Initiating Signal	Monitored Parameters	Reactor Mode
Indication of a MSL break	Main Steam Line Flow	RUN, STARTUP, or SHUTDOWN
Indication of a FW line break	FW Line Pressure Reactor Dome Pressure	RUN, STARTUP, or SHUTDOWN
Indication of a ICS line break	Steam Supply Flow Train A/B/C Condensate Return Flow Trains A/B/C	RUN, STARTUP, or SHUTDOWN
Function - FWRIV and FWCIV Isolation		
HIGH RPV Level [L9]	Reactor Water Level	RUN, STARTUP, or SHUTDOWN
LOW FW-RPV Differential Pressure	FW Line pressure Reactor Dome Pressure	RUN, STARTUP, or SHUTDOWN
Indication of a FW line break	FW Line pressure Reactor Dome Pressure	RUN, STARTUP, or SHUTDOWN
Indication of a FW Train A/B line break	FW Line pressure Reactor Dome Pressure	RUN, STARTUP, or SHUTDOWN
Function - SDC Isolation		
Indication of a SDC line break	SDC Liquid Temperature SDC Supply Flow SDC Return and Reject Flow	RUN, STARTUP, or SHUTDOWN
Function - CUW Isolation		
Indication of a CUW line break	CUW Liquid Temperature CUW Supply Flow CUW Return and Reject Flow	RUN, STARTUP, or SHUTDOWN
Function - ICS Train Isolation (Train A)		
Indication of an ICS train A line break	Steam Supply Flow Train A Condensate Return Flow Train A	RUN, STARTUP, or SHUTDOWN
Function - ICS Train Isolation (Train B)		
Indication of an ICS train B line break	Steam Supply Flow Train B Condensate Return Flow Train B	RUN, STARTUP, or SHUTDOWN
Function - ICS Train Isolation (Train C)		
Indication of an ICS train C line break	Steam Supply Flow Train C Condensate Return Flow Train C	RUN, STARTUP, or SHUTDOWN

Table 7-3: Candidate Accident Monitoring Variables

Variable	Type	Selection Reason	Remarks
None	A	BWRX-300 has no specific planned manually controlled actions for safety systems to perform their safety function	N/A
Containment Sump Water Level	B, C	BWR legacy knowledge	Designated for monitoring Fundamental Safety Functions during the implementation of EOPs and Severe Accident Management Guidelines and needs to comply with the requirements for safety classifications.
Neutron Flux	B	BWR legacy knowledge	N/A
Reactor Pressure	B, C, D	BWR legacy knowledge	Designated for monitoring FSFs during the implementation of EOPs and SAMGs and needs to comply with the requirements for safety classifications.
RPV Dome Pressure	B	BWR legacy knowledge	Designated for monitoring fundamental safety functions during the implementation of EOPs and SAMGs and shall comply with the requirements for safety classifications
Reactor Isolation Valve Positions	B	BWR legacy knowledge	Designated for monitoring fundamental safety functions during the implementation of EOPs and SAMGs and shall comply with the requirements for safety classifications
RPV Water Level	B	BWR legacy knowledge	Designated for monitoring FSFs during the implementation of EOPs and SAMGs and needs to comply with the requirements for safety classifications.
Containment Area Radiation Level	C, E	BWR legacy knowledge	N/A
Containment Hydrogen Concentration	C, F	BWR legacy knowledge NEDO-33911-A Revision 3, “Licensing Topical Report BWRX-300 Containment Performance”	Provided for severe accident monitoring.
Containment Oxygen Concentration	C, F	BWR legacy knowledge NEDO-33911-A Revision 3	Provided for severe accident monitoring.

Variable	Type	Selection Reason	Remarks
Containment Pressure	C, D	BWR legacy knowledge	Designated for monitoring fundamental safety functions during the implementation of EOPs and SAMGs and shall comply with the requirements for safety classifications
Isolation Condenser Condensate Line Flowrate	C, D	BWR legacy knowledge	N/A
Isolation Condenser Steam Line Flowrate	C, D	BWR legacy knowledge	N/A
Off Gas Activity	C	BWR legacy knowledge	Designated for monitoring FSFs during the implementation of EOPs and SAMGs and needs to comply with the requirements for safety classifications.
Boron Injection System Indications	D	BWR legacy knowledge	Not associated with any events requiring environmental or seismic qualification
Containment Isolation Valve Positions	D	BWR legacy knowledge	Primary accident monitoring information for the containment is provided by reactor pressure, reactor water level, and containment pressure
Containment Temperature	D	BWR legacy knowledge	N/A
Control Rod Position	D	BWR legacy knowledge	The rod position indication is a normal operating system that is not required to be seismically designed. Its function is completed before experiencing a harsh environment. Also, the proper functioning of the Hydraulic Scram and Control Rod Drives can be inferred from other parameters
Electrical Power Status	D	BWR legacy knowledge	N/A
Feedwater Flow	D	BWR legacy knowledge	Not associated with any events requiring environmental or seismic qualification
Isolation Condenser Valve Positions	D	BWR legacy knowledge	N/A
Isolation Condenser System Pool Water Level	D	BWR legacy knowledge	N/A
Area Radiation Level	E	BWR legacy knowledge	N/A
Control Building Air Intake HVS Radiation Level	E	BWR legacy knowledge	N/A
Effluent radioactivity - noble gases	E	BWR legacy knowledge	N/A
Meteorological Data (Wind Speed, Wind Direction, and Atmospheric Stability)	E	BWR legacy knowledge	N/A

Variable	Type	Selection Reason	Remarks
Plant Environment Radiation/Radioactivity Levels	E	BWR legacy knowledge	N/A
Spent Fuel Pool Level	F	IEC 63147	Provided for severe accident monitoring.

Table 7-4: Safety Category 2 Diverse Protection System Functions and Associated SC2 Initiating Signals

Initiating Signal	Reactor Mode Switch Position
Function - Diverse Hydraulic Scram	
HIGH RPV pressure	RUN or STARTUP
LOW RPV pressure [L3]	RUN or STARTUP
LOW RPV level [L3]	RUN or STARTUP
HIGH containment pressure	RUN or STARTUP
HIGH main condenser pressure	STARTUP
Line break indication (MSL, FW, or ICS)	RUN, STARTUP
Function - CRD Motor Run-In	
Any Scram Signal	RUN or STARTUP
Function - Isolation Condenser Actuation	
HIGH containment pressure	RUN, STARTUP, or SHUTDOWN
LOW RPV level [L2]	RUN, STARTUP, or SHUTDOWN
Indication of an IC line break (unaffected ICS trains initiated)	RUN, STARTUP, or SHUTDOWN
Indication of a FW line break	RUN, STARTUP, or SHUTDOWN
Indication of a MSL line break	RUN, STARTUP, or SHUTDOWN
High RPV Pressure	RUN or STARTUP
Function - RPV and Containment Isolation	
HIGH containment pressure	RUN, STARTUP, or SHUTDOWN
LOW RPV level [L2]	RUN, STARTUP, or SHUTDOWN
Function - MSRIV and MSCIV Isolation	
Sustained LOW feedwater flow	RUN, STARTUP, or SHUTDOWN
Indication of a MSL break	RUN, STARTUP, or SHUTDOWN
Indication of a FW line break	RUN, STARTUP, or SHUTDOWN
Indication of a SDC line break	RUN, STARTUP, or SHUTDOWN
Function - FWRIV and FWCIV Isolation	
HIGH RPV level [L9]	RUN
Loss of normal FW flow	RUN, STARTUP, or SHUTDOWN
Function - Feedwater and Condenser Pump Trip	
Detection of FW line Break	RUN, STARTUP, or SHUTDOWN
Function - Feedwater and SDC Isolation	
Indication of SDC line break	RUN, STARTUP, or SHUTDOWN
Detection of FW line Break	RUN, STARTUP, or SHUTDOWN
Function - CUW Isolation	
Indication of a CUW line break	RUN, STARTUP, or SHUTDOWN

Initiating Signal	Reactor Mode Switch Position
Function - Cavity Pool Makeup from ICS Pools	
RPV level reduction	REFUEL

Table 7-5: Safety Category 3 Anticipatory Trip and Block Functions and Associated SC3 Initiating Signals

Initiating Signal	Reactor Mode Switch Position
Function - Reactor Scram	
Turbine Trip Demand	RUN
Closure of an MSIV <90%	RUN
Short reactor period (at low power) from WRNM	STARTUP
LOW bus voltage (from R20 electrical system)	RUN or STARTUP
HIGH main condenser pressure	RUN
High RPV level	RUN or STARTUP
Sustained LOW feedwater flow	RUN
Manual initiation	RUN or STARTUP
Function - Control Rod Withdrawal Block	
ATLM	RUN
MRBM	RUN
Short Reactor Period	STARTUP
Control Rod Separation	RUN, STARTUP, or SHUTDOWN

Table 7-6: Safety Class 1 I&C Compliance Alignment

I&C Topic	IEC 61513 Section
Qualification I&C	5.5.2 and 6.2.2.7
Reliability I&C	5.4.2.2, 5.4.4.3, 5.5.6, 6.2.2.3.4, 6.2.2.3.5, 6.2.2.3.6, 6.2.3.5, and 6.2.4.2.2
Robustness I&C	5.4.2.6, 5.4.4.2, 6.2.2.3.3, 6.2.3.3.3, and 6.2.3.3.4
Security I&C	5.5.3
Defence-In-Depth	5.2.2
Operator Interface	5.4.2.3
I&C Performance Objectives	5.2.2, 5.2.4, and 5.4

Table 7-7: Safety Class 2 Compliance Alignment

I&C Topic	IEC 61513 Section
Qualification I&C	5.5.2 and 6.2.2.7
Reliability I&C	5.4.2.2, 5.4.4.3, 5.5.6, 6.2.2.3.4, 6.2.2.3.5, 6.2.2.3.6, 6.2.3.5, and 6.2.4.2.2
Robustness I&C	5.4.2.6, 5.4.4.2, 6.2.2.3.3, 6.2.3.3.3, and 6.2.3.3.4
Security I&C	5.5.3
Defence-In-Depth	5.2.2
Operator Interface	5.4.2.3
I&C Performance Objectives	5.2.2, 5.2.4, and 5.4

Table 7-8: Safety Class 3 Compliance Alignment

I&C Topic	IEC 61513 Section
Qualification I&C	5.5.2 and 6.2.2.7
Reliability I&C	5.4.2.2, 5.4.4.3, 5.5.6, 6.2.2.3.4, 6.2.2.3.5, 6.2.2.3.6, 6.2.3.5, and 6.2.4.2.2
Robustness I&C	5.4.2.6, 5.4.4.2, 6.2.2.3.3, 6.2.3.3.3, and 6.2.3.3.4
Security I&C	5.5.3
Defence-In-Depth	5.2.2
Operator Interface	5.4.2.3
I&C Performance Objectives	5.2.2, 5.2.4, and 5.4

Table 7-9: Digital I&C System Development Process Compliance Alignment

I&C Topic	IEC 61513 Section (Reference 7-5)
Qualified I&C	5.5.2. - Overall I&C Quality Assurance Plan 6.2.2.7 - Qualification Approach as supplemented by IEC 60880 (Reference 7-25), IEC 62566 (Reference 7-59), IEC 62138 (Reference 7-26), and IEC 62566-2 (Reference 7-60).

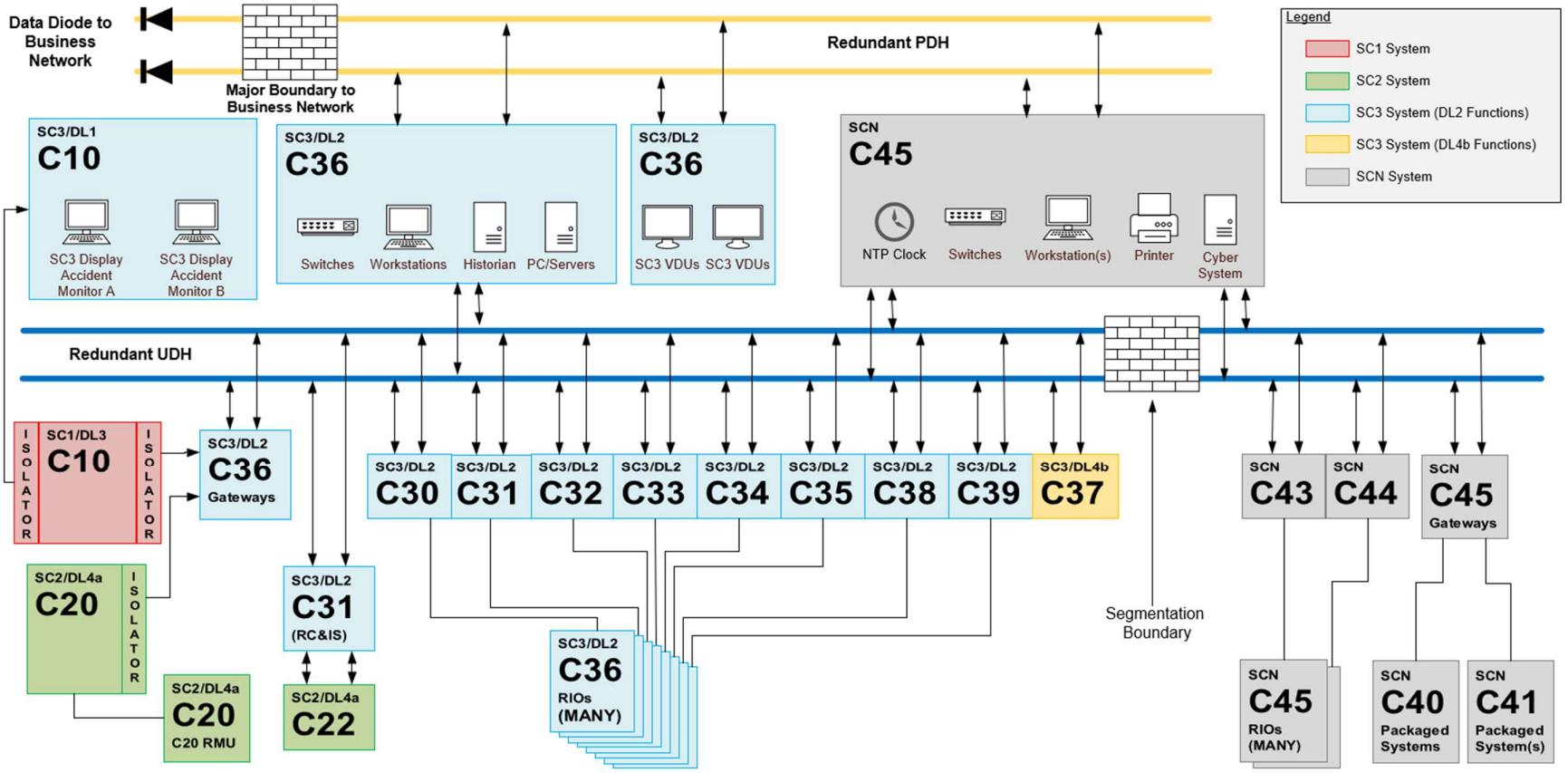

Figure 7-1: BWRX-300 Distributed Control and Information System Network Architecture

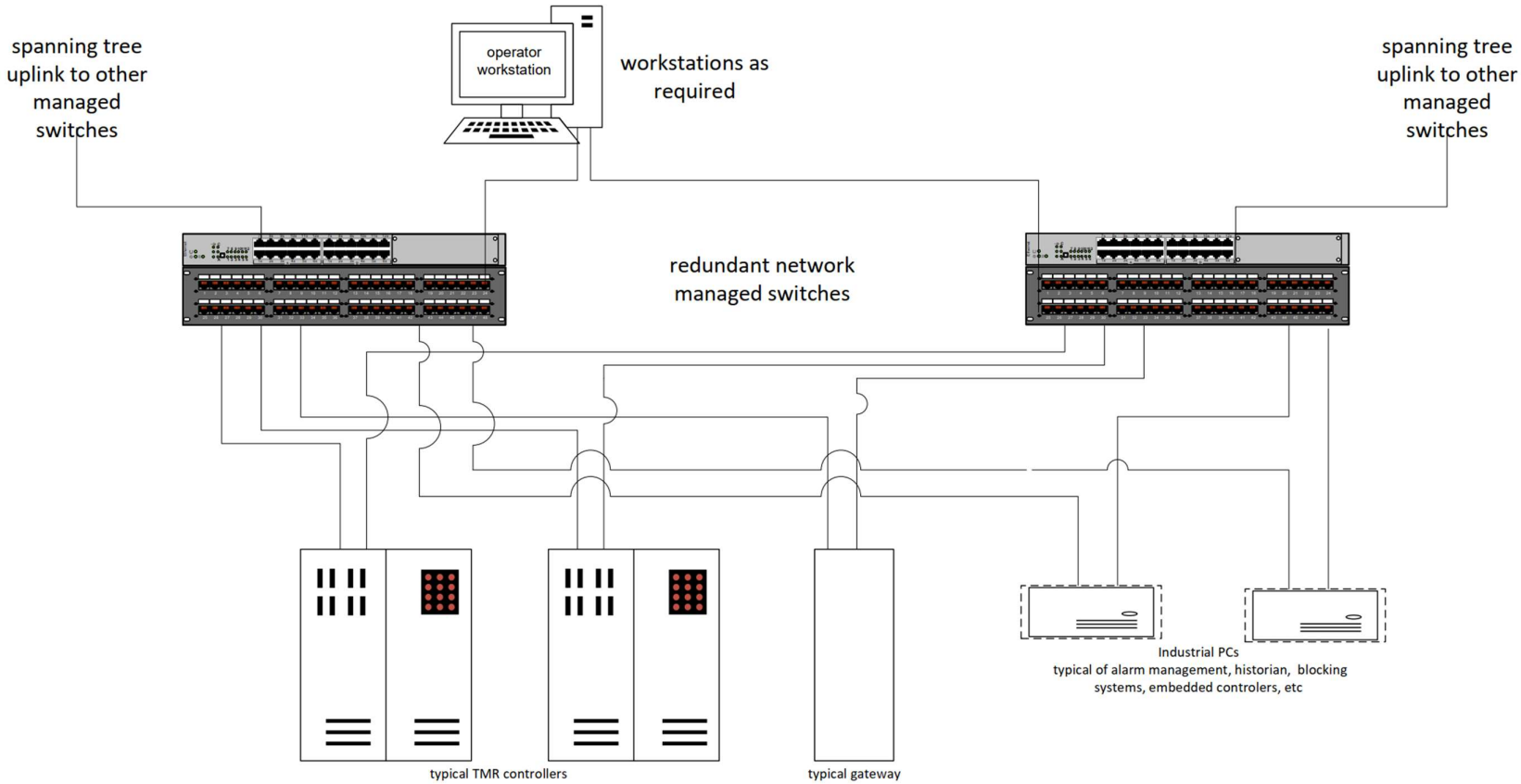

Figure 7-2: Typical I&C Controller and Component Network Connections

Redundant network UDH nuclear and BOP segments and PDH are actually pairs of network managed switches.

Most equipment and all controllers, operator workstations and historians are dual ported, one port to each switch.

Any redundant switch can be lost without affecting plant operation.

Any segment can be lost without affecting the other segments.

Managed switch uplinks (inter-switch communication) normally allow any segment controller, historian or workstation to send/receive data to any other.

Dark black links indicate normal switch communication, the lighter black links represent possible connections should ports fail or be shut down for self diagnostic monitoring reasons.

Yellow links represent cyber security monitoring connections.

Managed switches control which nodes are allowed to communicate and can prevent any unauthorized internal or external communication.

Managed switches have dual power supplies.

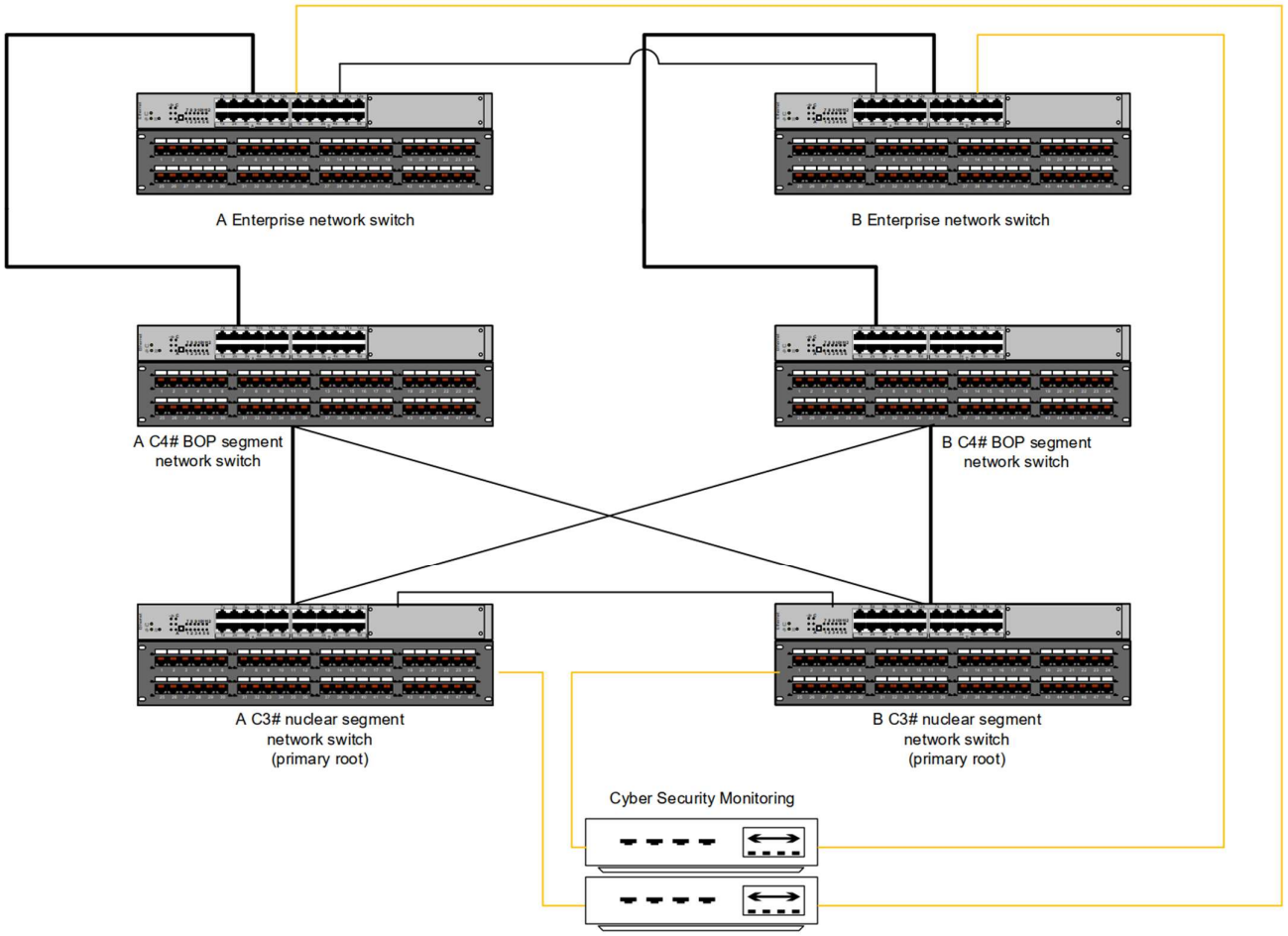

Figure 7-3: Rapid Spanning Tree Network Managed Switches

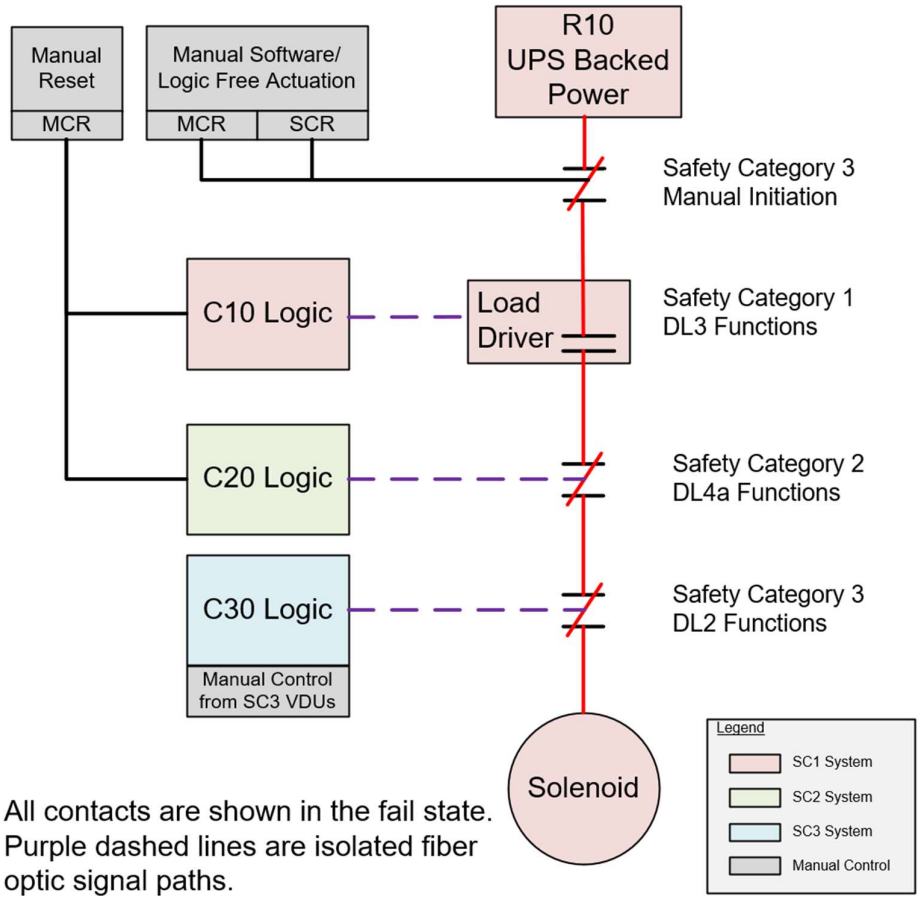

Figure 7-4: Fail-Safe Component Interface

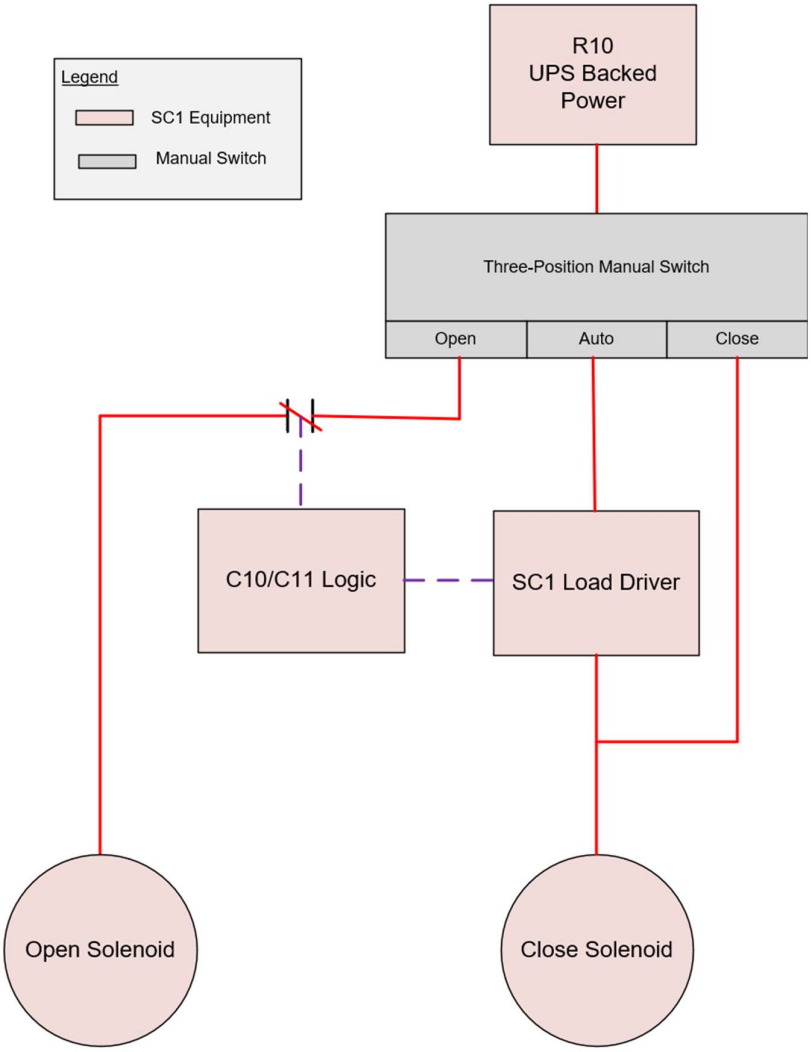

Figure 7-5: Fail As-Is Component Interface

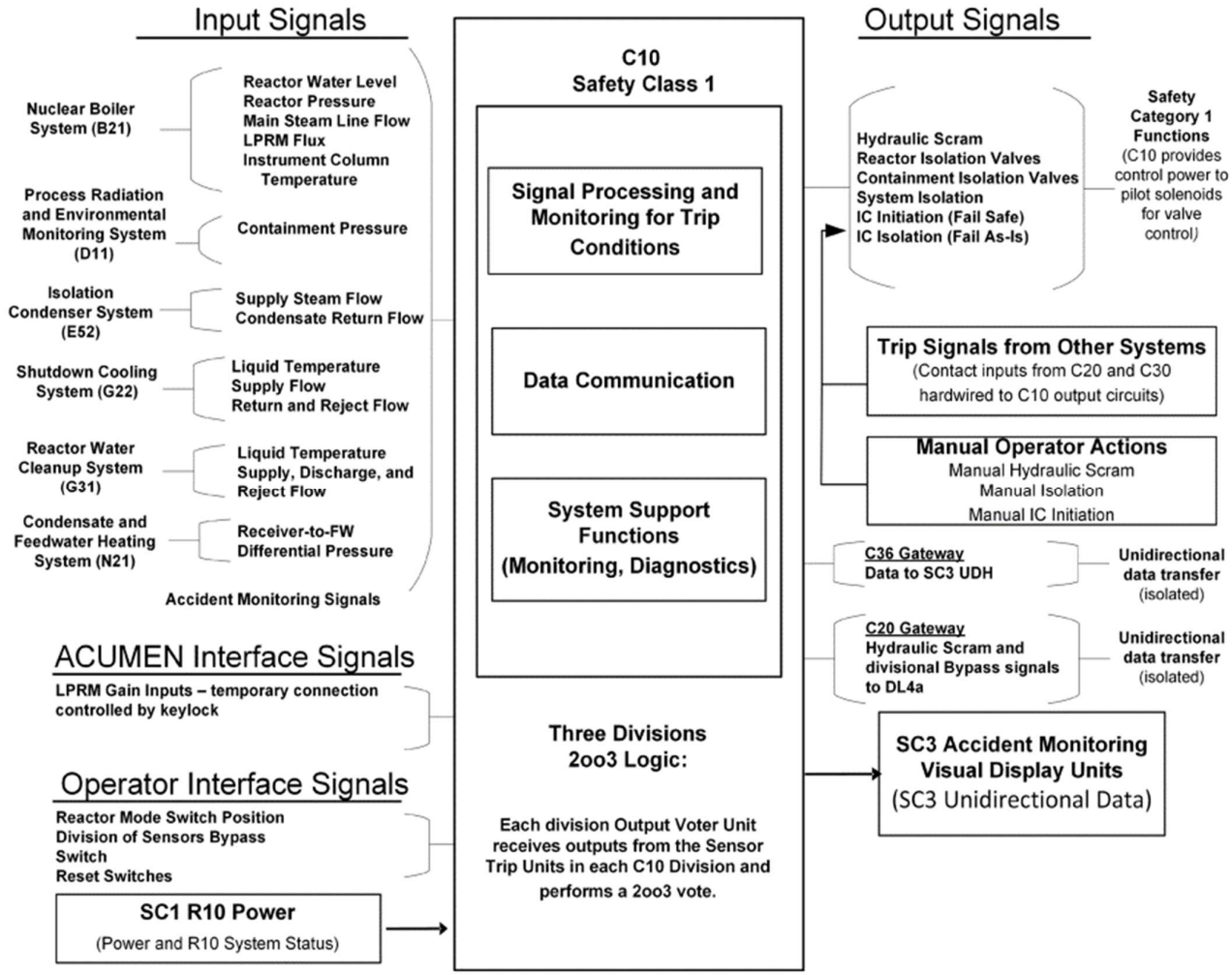

Figure 7-6: DL3/SC1 Functions and Signals

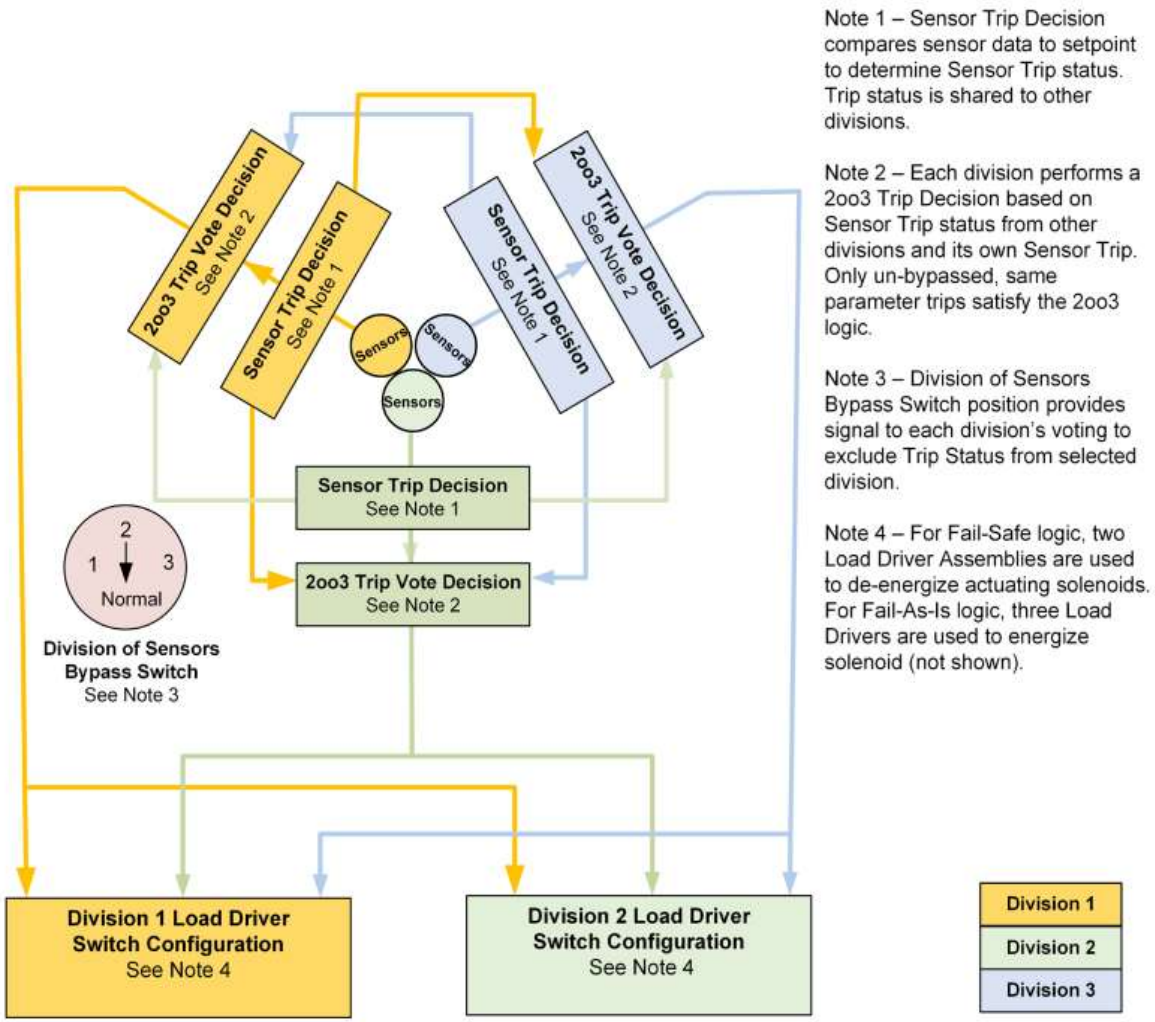

Figure 7-7: DL3 Fail Safe Actuation Logic

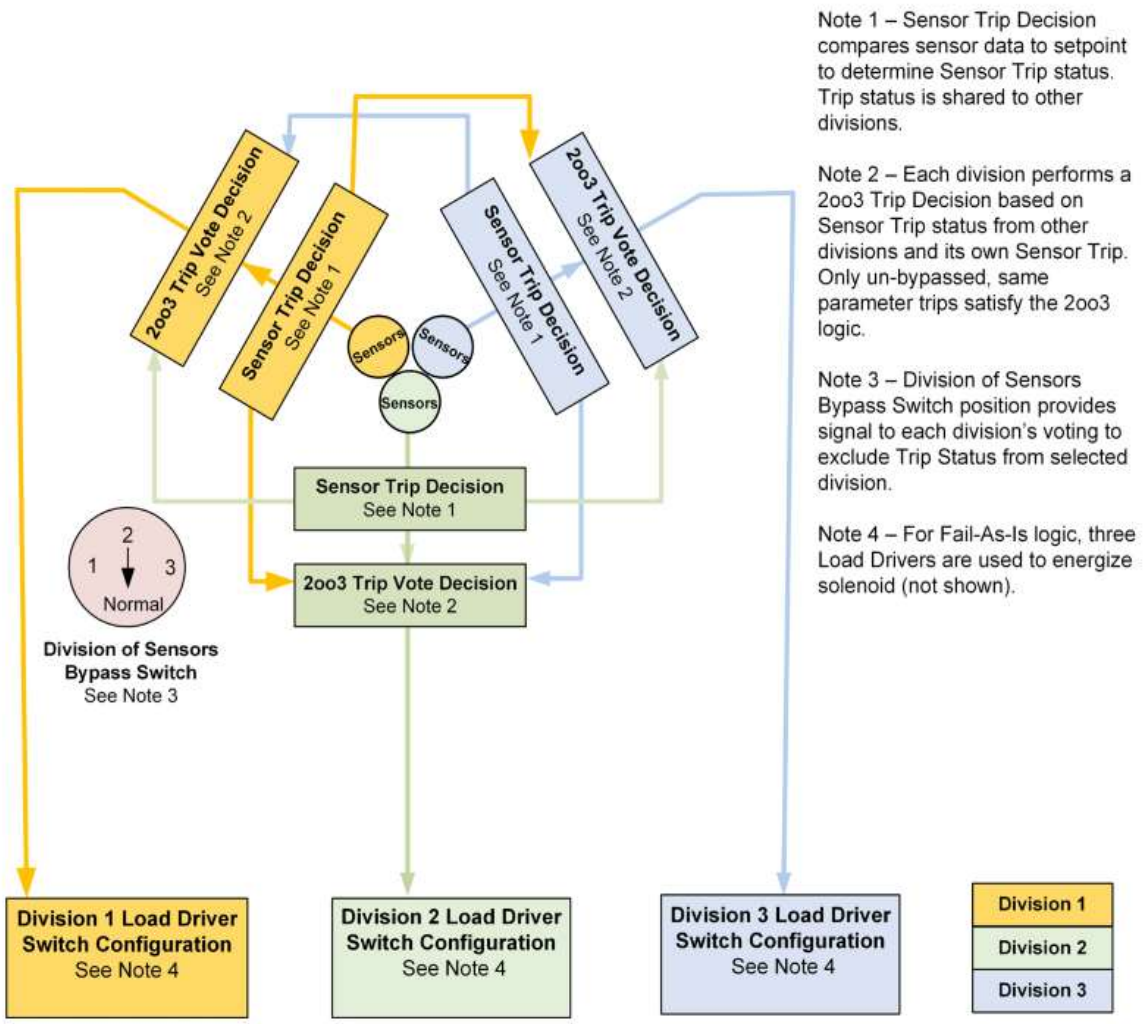

Figure 7-8: DL3 Fail As-Is Actuation Logic

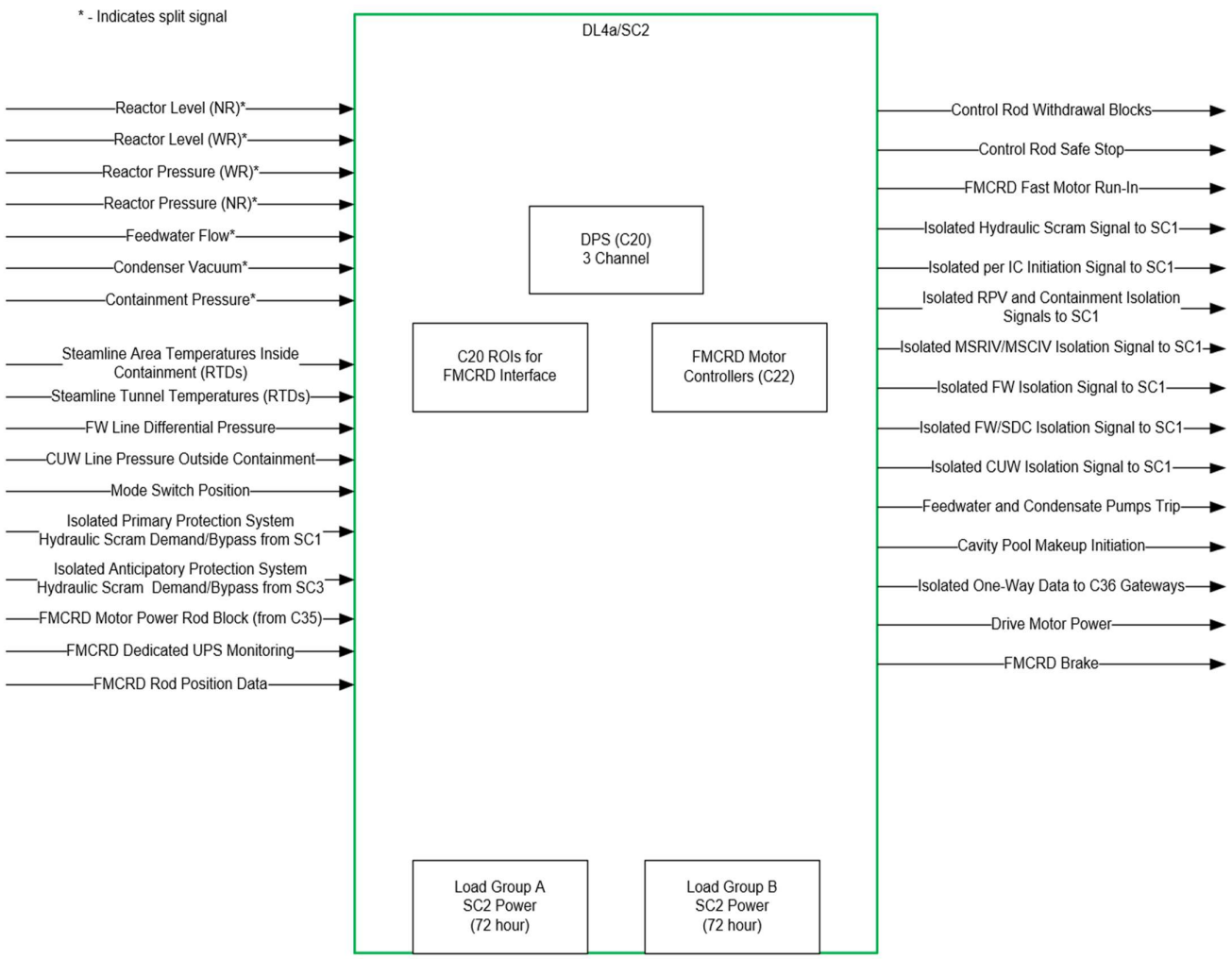

Figure 7-9: Defence Line 4a/Safety Class 2 Functions and Signals

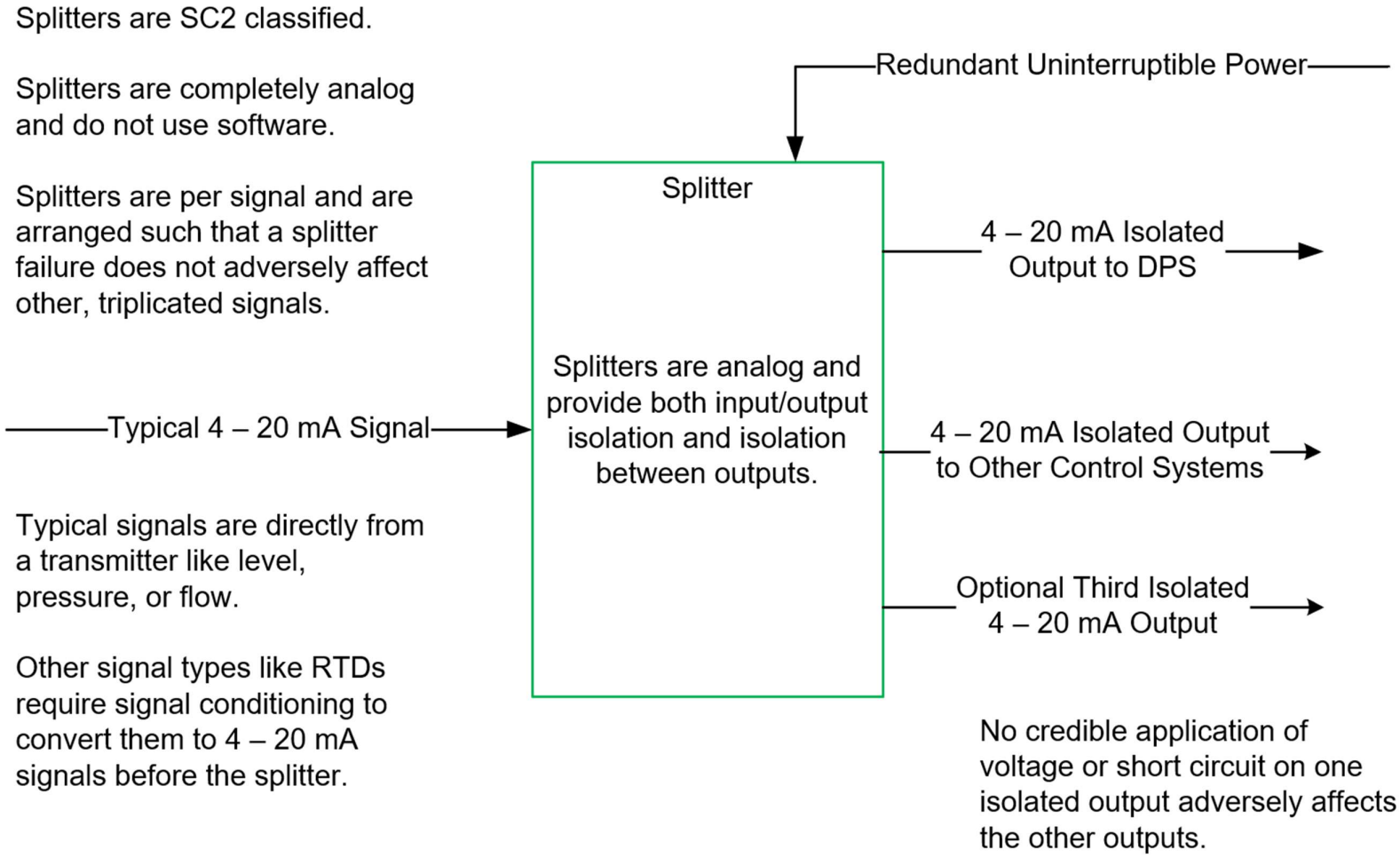

Figure 7-10: Defence Line 4a Analogue Signal Splitters

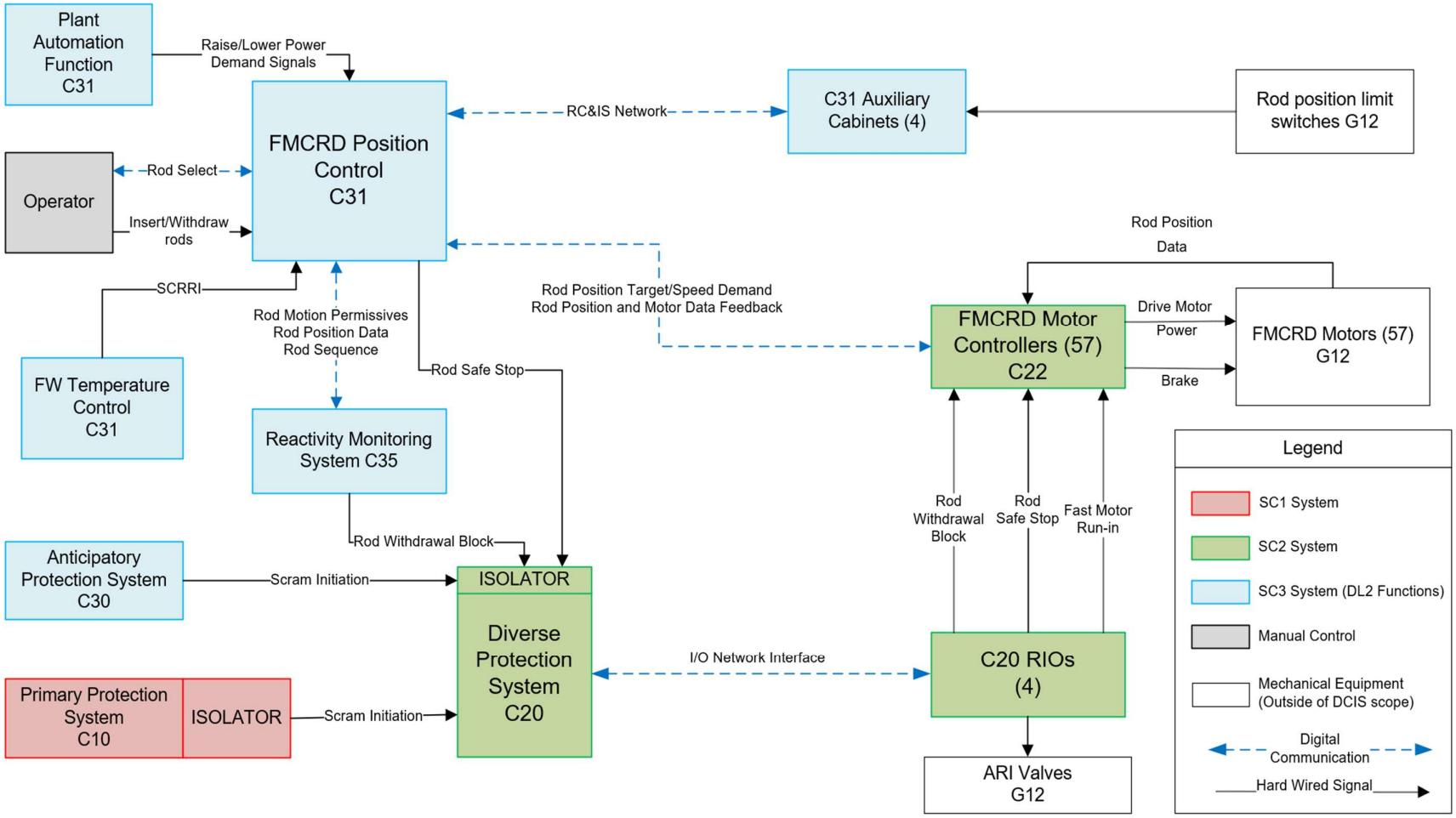

Figure 7-11: Overall Rod Control System

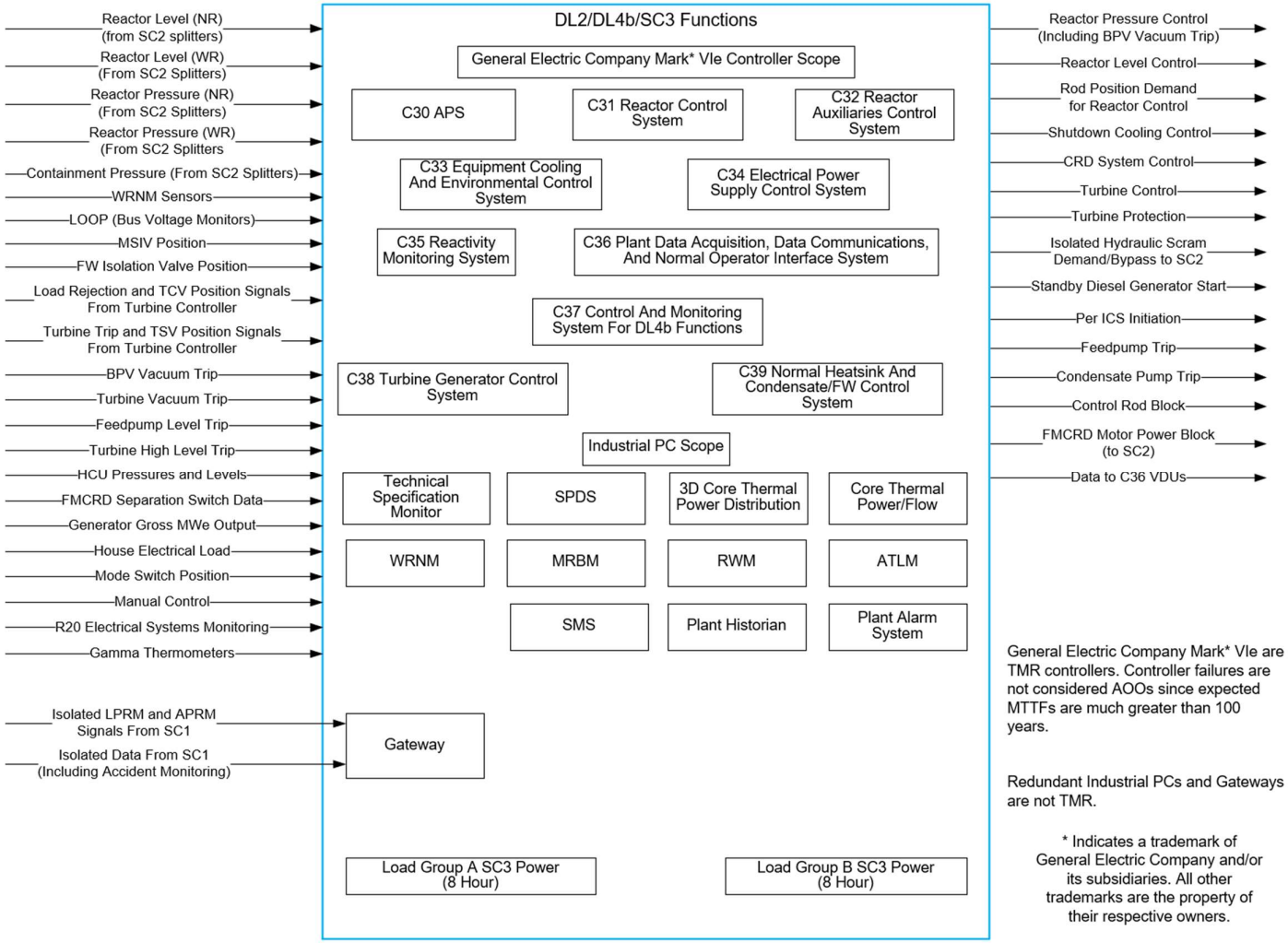

Figure 7-12: Safety Class 3 Nuclear Segment Functional Architecture

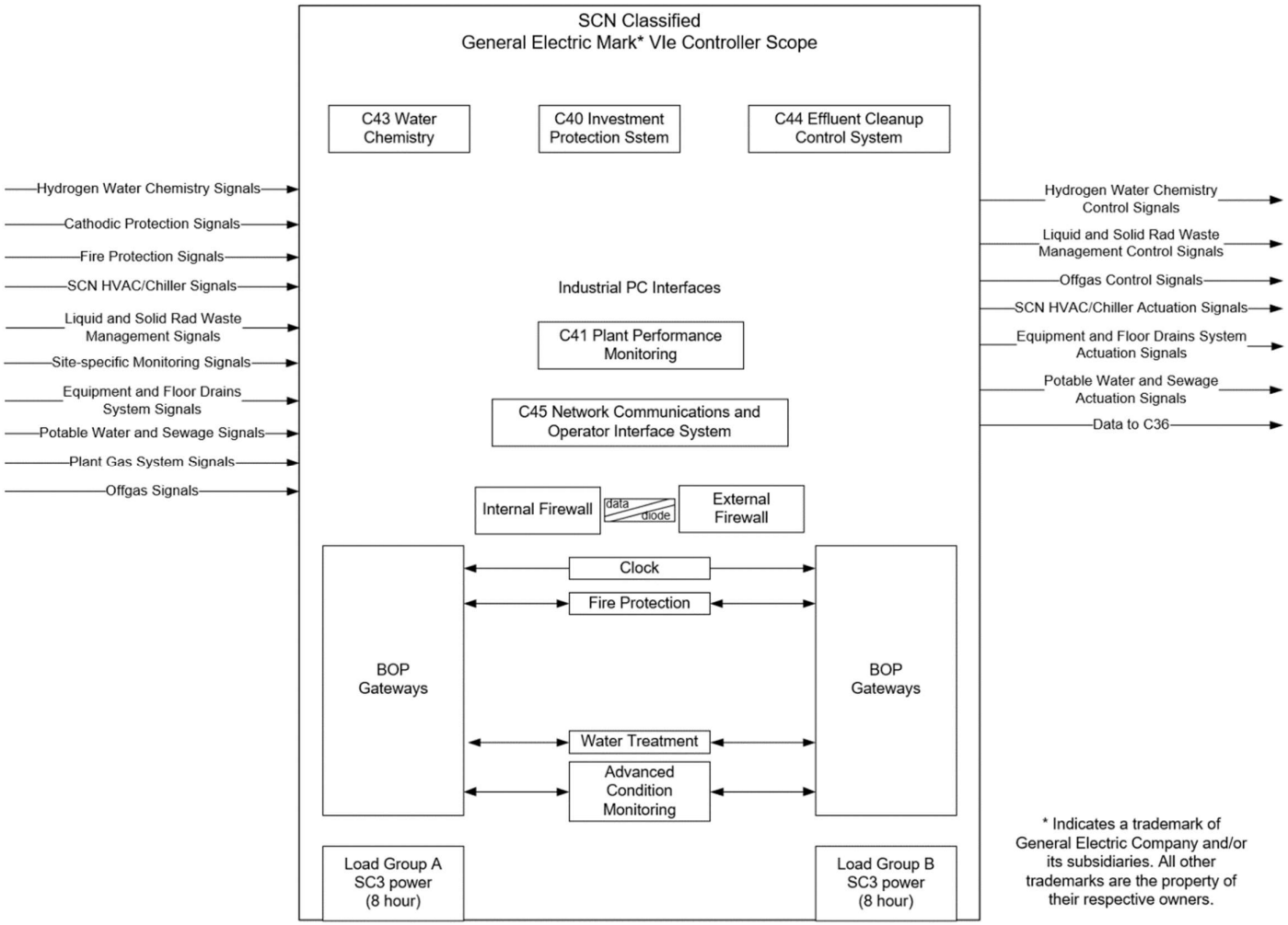

Figure 7-13: Non-Safety Class BOP Functional Architecture

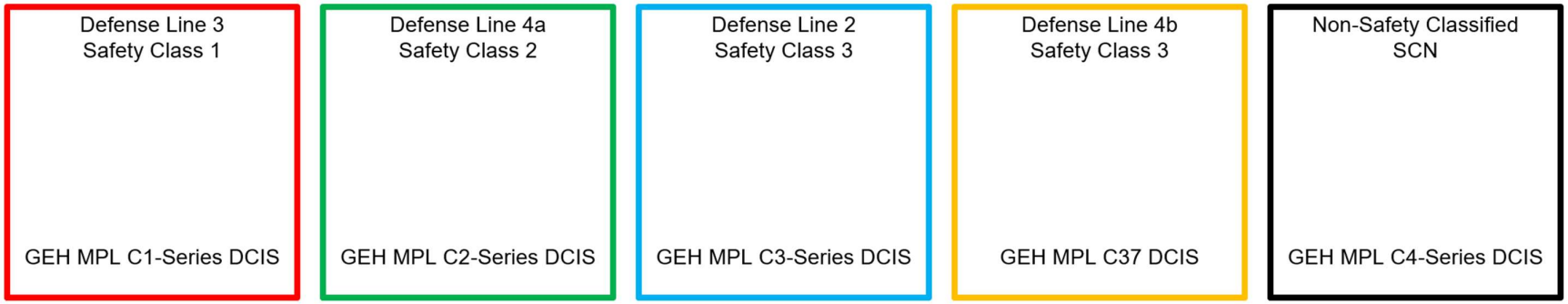

Figure 7-14: System Defence Lines & Classifications

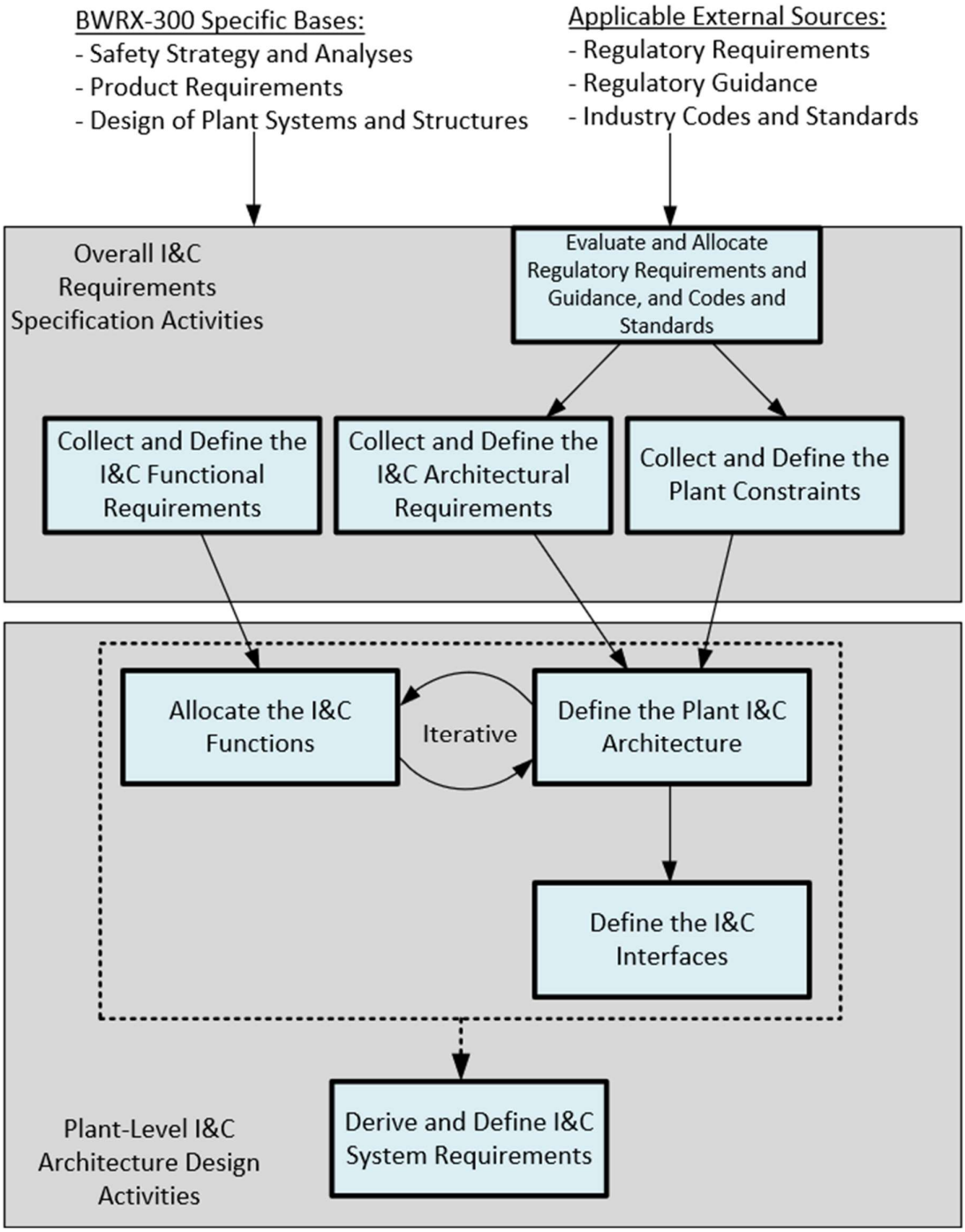

Figure 7-15: I&C Architecture Design Process

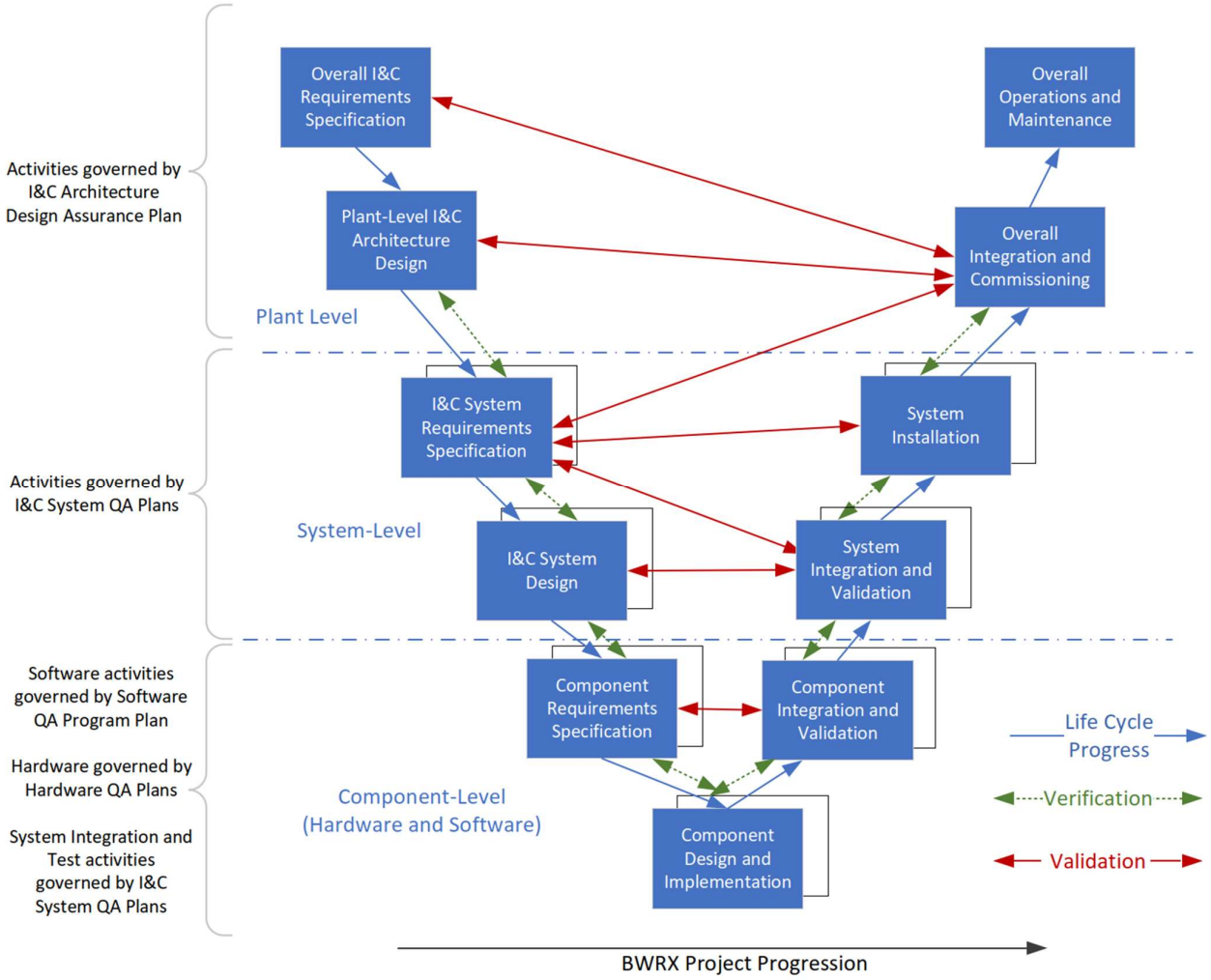

Figure 7-16: Overall BWRX-300 I&C System Life Cycle

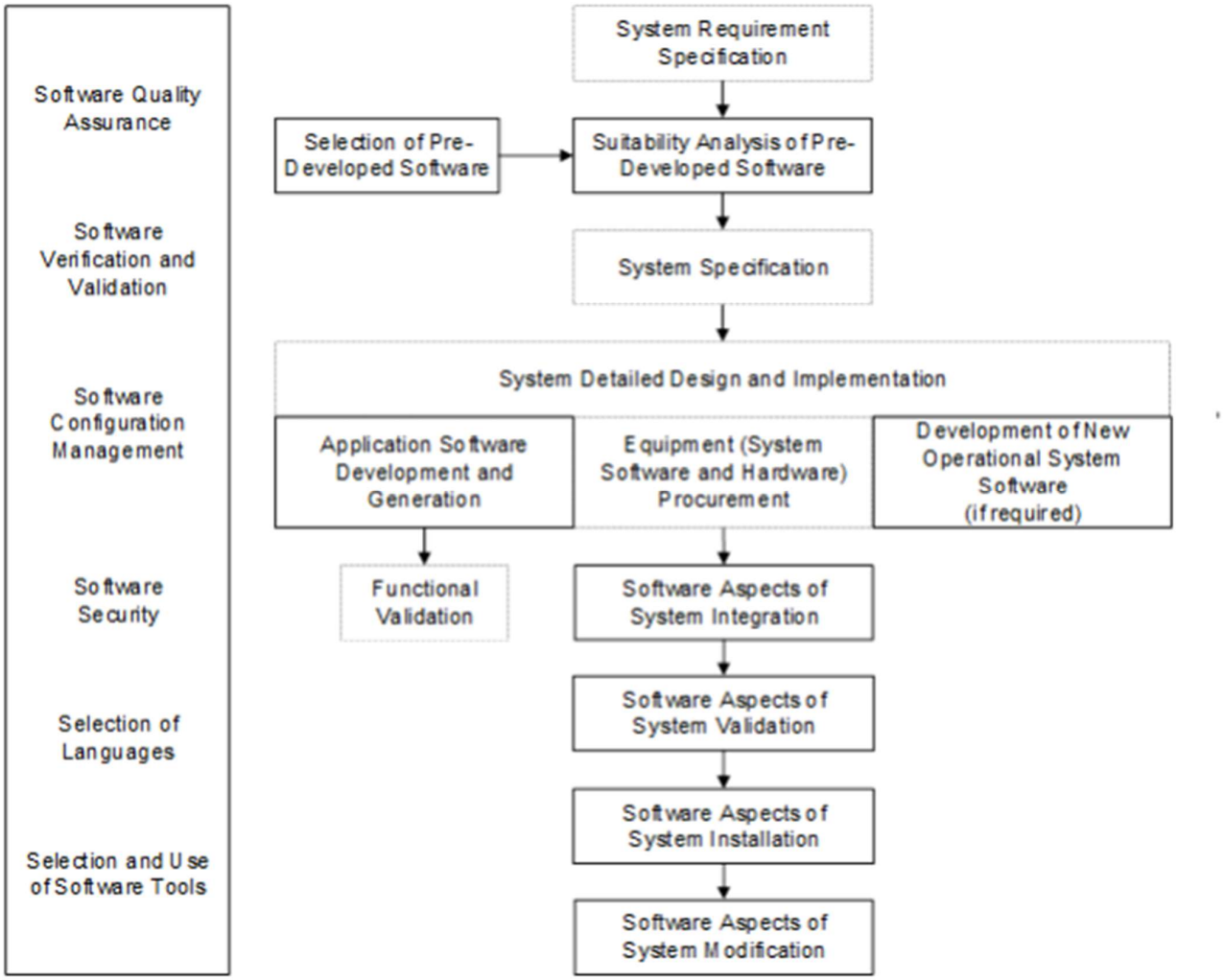

Figure 7-17: Software Related Activities in I&C Life Cycle

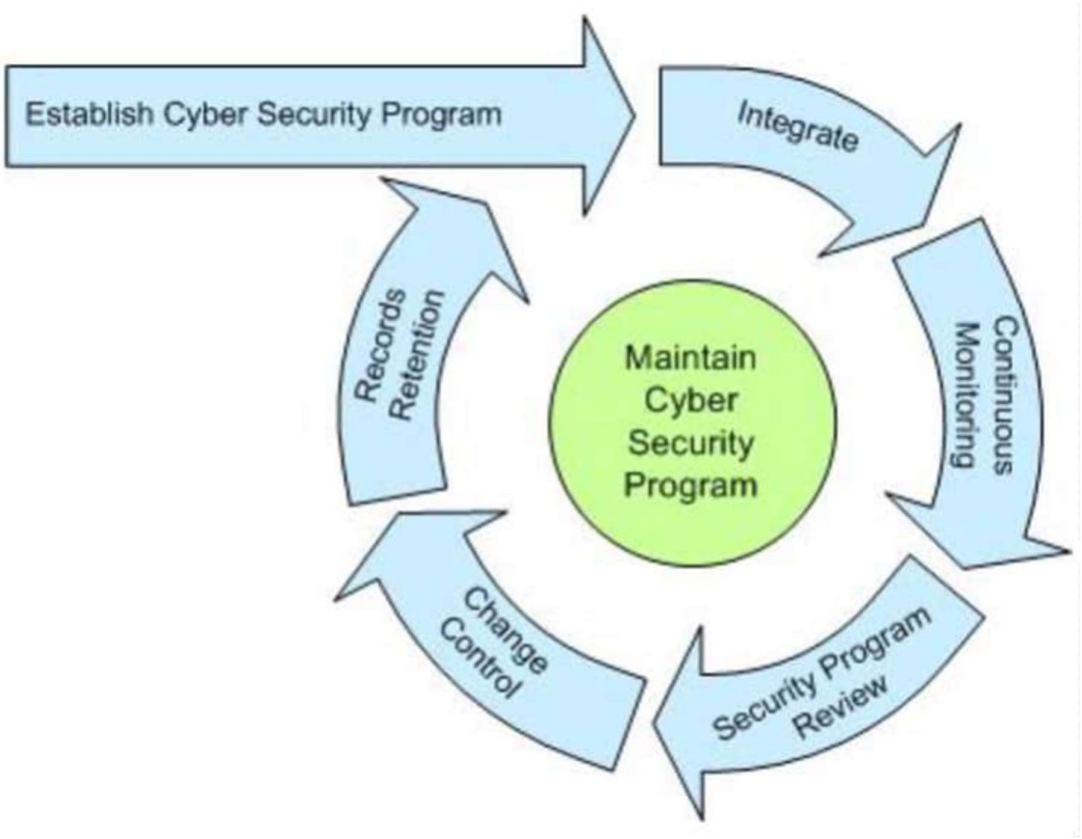

Figure 7-18: Cyber Security Life Cycle

Figure 7-19: Main Control Room and Surrounding Areas (Plan View)

7.10 References

7-1 SSR-2/1, “Safety of Nuclear Power Plants: Design, Safety Standards Series,” International Atomic Energy Agency, 2016.

7-2 SSG-61, “Format and Content of the Safety Analysis Report for Nuclear Power Plants, Safety Standards Series,” International Atomic Energy Agency, 2021.

7-3 SSG-30, “Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Safety Standards Series,” International Atomic Energy Agency, 2014.

7-4 SSG-39, “Design of Instrumentation and Control Systems for Nuclear Power Plants, Safety Standards Series,” International Atomic Energy Agency, 2016.

7-5 IEC 61513, “Nuclear power plants – Instrumentation and control important to safety – General requirements for systems,” International Electrotechnical Commission, 2011.

7-6 IEC 61226, “Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Categorization of functions and classification of systems,” International Electrotechnical Commission, April 2020.

7-7 NEDO-34164, “BWRX-300 UK GDA Ch. 2: Site Characteristics,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-8 NEDO-34165, “BWRX-300 UK GDA Ch. 3: Safety Objectives and Design Rules for SSCs,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-9 NEDO-34166, “BWRX-300 UK GDA Ch. 4: Rector (Fuel and Core),” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-10 NEDO-34167, “BWRX-300 UK GDA Ch. 5: Reactor Coolant System and Associated Systems,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-11 NEDO-34168, “BWRX-300 UK GDA Ch. 6: Engineered Safety Features,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-12 NEDO-34170, “BWRX-300 UK GDA Ch. 8: Electrical Power,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-13 NEDO-34171, “BWRX-300 UK GDA Ch. 9A: Auxiliary Systems,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-14 NEDO-34172, “BWRX-300 UK GDA Ch. 9B: Civil Structures,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-15 NEDO-34173, “BWRX-300 UK GDA Ch. 10: Steam and Power Conversion Systems,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-16 NEDO-34174, “BWRX-300 UK GDA Ch. 11: Management of Radioactive Waste,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-17 NEDO-34175, “BWRX-300 UK GDA Ch. 12: Radiation Protection,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-18 NEDO-34178, “BWRX-300 UK GDA Ch. 15: Safety Analysis (including Fault Studies, PSA, and Hazard Assessment),” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-19 NEDO-34190, “BWRX-300 UK GDA Ch. 18: Human Factor Engineering,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-20 NEDO-34191, “BWRX-300 UK GDA Ch. 19: Emergency Preparedness and Response,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-21 NEDO-34197, “BWRX-300 UK GDA Ch. 25: Security Annex,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

7-22 IEC 60709, “Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Separation,” International Electrotechnical Commission, 2018.

7-23 IEC 63147, “Criteria for accident monitoring instrumentation for nuclear power generating stations,” International Electrotechnical Commission, 2017.

7-24 IEC 60812, “Failure modes and effects analysis (FMEA and FMECA),” International Electrotechnical Commission, 2018.

7-25 IEC 60880, “Nuclear power plants - Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions,” International Electrotechnical Commission, 2006.

7-26 IEC 62138, “Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions,” International Electrotechnical Commission, 2018.

7-27 IEC 61000-4, “Electromagnetic Compatibility Package,” International Electrotechnical Commission.

7-28 IEC 61000-6-2, “Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity standard for industrial environments,” International Electrotechnical Commission, 2016.

7-29 IEC/IEEE 60780-323, “Nuclear Facilities – Electrical Equipment Important to Safety – Qualification,” International Electrotechnical Commission/Institute of Electrical and Electronics Engineers, 2016.

7-30 IEC/IEEE 60980-344, “Nuclear facilities – Equipment important to safety – Seismic qualification,” International Electrotechnical Commission/Institute of Electrical and Electronics Engineers, 2020.

7-31 IEC 61500, “Nuclear power plants – Instrumentation and control systems important to safety – Data communication in systems performing category A functions,” International Electrotechnical Commission, 2018.

7-32 IEC 62671, “Nuclear power Plants – Instrumentation and Control Important to Safety - Selection and use of industrial digital devices of limited functionality,” International Electrotechnical Commission, 2013.

7-33 IEC 61508 CMV, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Parts 1 to 7, Commented Version,” International Electrotechnical Commission, 2010.

7-34 IEC 61888, “Nuclear power plants – Instrumentation important to safety – Determination and maintenance of trip setpoints,” International Electrotechnical Commission, 2002.

7-35 IEC 60987, “Nuclear power plants – Instrumentation and control important to safety – Hardware requirements,” International Electrotechnical Commission, 2021.

7-36 IEC 61000-4-2, “Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – electrostatic discharge immunity test,” International Electrotechnical Commission, 2008.

7-37 IEC 61000-4-3, “Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency electromagnetic field immunity test,” International Electrotechnical Commission, 2020.

7-38 IEC 61000-4-4, “Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test,” International Electrotechnical Commission, 2012.

7-39 IEC 61000-4-5, “Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test,” International Electrotechnical Commission, 2014.

7-40 IEC 61000-4-6, “Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, Induced by radio-frequency fields,” International Electrotechnical Commission, 2013.

7-41 IEC 61000-4-8, “Electromagnetic compatibility (EMC) – Part 4-8: Testing and measurement techniques – Power frequency magnetic field immunity test,” International Electrotechnical Commission, 2009.

7-42 IEC 61000-4-9, “Electromagnetic compatibility (EMC) – Part 4-9: Testing and measurement techniques – Impulse magnetic field immunity test,” International Electrotechnical Commission, 2016.

7-43 IEC 61000-4-11, “Electromagnetic compatibility (EMC) – Part 4-11: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations immunity tests,” International Electrotechnical Commission, 2020.

7-44 IEC 61000-4-12, “Electromagnetic Compatibility (EMC) – Part 4-12: Testing and measurement techniques - Ring wave immunity test,” International Electrotechnical Commission, 2017.

7-45 IEC 61000-4-13, “Electromagnetic compatibility (EMC) – Part 4-13: Testing and measurement techniques - Harmonics and interharmonics including mains signalling at a.c. power port, low frequency immunity tests,” International Electrotechnical Commission, 2002.

7-46 IEC 61000-4-14, “Electromagnetic compatibility (EMC) – Part 4-14: Testing and measurement techniques - Voltage fluctuation immunity test for equipment with input current not exceeding 16 A per phase,” International Electrotechnical Commission, 2009.

7-47 IEC 61000-4-16, “Electromagnetic compatibility (EMC) – Part 4-16: Testing and measurement techniques - Test for immunity to conducted, common mode disturbances in the frequency range 0 Hz to 150 kHz,” International Electrotechnical Commission, 2015.

7-48 IEC 61000-4-18, “Electromagnetic compatibility (EMC) – Part 4-18: Testing and measurement techniques – Damped oscillatory wave immunity test,” International Electrotechnical Commission, 2019.

7-49 IEC 61000-4-19, “Electromagnetic compatibility (EMC) – Part 4-19: Testing and measurement techniques – Test for immunity to conducted, differential mode disturbances and signaling in the frequency range 2 kHz to 150 kHz at a.c. power ports,” International Electrotechnical Commission, 2014.

7-50 IEC 61000-4-28, “Electromagnetic compatibility (EMC) – Part 4-28: Testing and measurement techniques - Variation of power frequency, immunity test for equipment with input current not exceeding 16 A per phase,” International Electrotechnical Commission, 2002.

7-51 IEC 61000-4-31, “Electromagnetic compatibility (EMC) – Part 4-31: Testing and measurement techniques – AC mains ports broadband conducted disturbance immunity test,” International Electrotechnical Commission, 2016.

7-52 IEC 61000-4-34, “Electromagnetic compatibility (EMC) – Part 4-34: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations immunity tests for equipment with mains current more than 16 A per phase,” International Electrotechnical Commission, 2005.

7-53 IEC 60671, “Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing,” International Electrotechnical Commission, 2007.

7-54 IEC 62385, “Nuclear power plants – Instrumentation and control important to safety – Methods for assessing the performance of safety system instrument channels,” International Electrotechnical Commission, 2007.

7-55 ONR SAPs 2014, “Safety Assessment Principles for Nuclear Facilities,” Office for Nuclear Regulation, 2014.

7-56 NEDC-34140P, “BWRX-300 Safety Case Development Strategy,” Rev 1, GE-Hitachi Nuclear Energy, Americas, LLC, June 2024.

7-57 006N3139, “BWRX-300 Design Plan,” GE-Hitachi Nuclear Energy, Americas, LLC, 2023.

7-58 NEDC-34137P, “BWRX-300 Design Evolution,” GE-Hitachi Nuclear Energy, Americas, LLC.

7-59 IEC 62566, “Nuclear Power Plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions,” International Electrotechnical Commission, 2012.

7-60 IEC 62566-2, “Nuclear Power Plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits – Part 2: HDL-programmed integrated circuits performing category B or C functions,” International Electrotechnical Commission, 2020.

APPENDIX A CLAIMS, ARGUMENTS AND EVIDENCE, AND ALARP

Claims, Argument, Evidence

The Office for Nuclear Regulation (ONR) Safety Assessment Principles 2014, "Safety Assessment Principles for Nuclear Facilities," (Reference 7-55) identify ONR's expectation that a safety case should clearly set out the trail from safety claims, through arguments to evidence. The Claims Argument Evidence (CAE) approach can be explained as follows:

1. Claims (assertions) are statements that indicate why a facility is safe.
2. Arguments (reasoning) explain the approaches to satisfying the claims.
3. Evidence (facts) supports and forms the basis (justification) of the arguments.

The Generic Design Assessment (GDA) CAE structure is defined within NEDC-34140P, "BWRX-300 Safety Case Development Strategy," (Reference 7-56) and is a logical breakdown of an overall claim that:

"The BWRX-300 is capable of being constructed, operated and decommissioned in accordance with the standards of environmental, safety, security and safeguard protection required in the United Kingdom (UK)."

This overall claim is broken down into Level 1 claims relating to environment, safety, security and safeguards, which are then broken down again into Level 2 area related sub-claims and then finally into Level 3 (chapter level) sub-claims.

The Level 3 sub-claims that this chapter demonstrates compliance against are identified within the Safety Case Development Strategy (SCDS) (Reference 7-56) and are as follows:

2.1.2: The design of the system/structure has been substantiated to achieve the safety functions in all relevant operating modes.

2.1.3: The system/structure design has been undertaken in accordance with relevant design codes and standards (Relevant Good Practice (RGP)) and design safety principles and taking account of Operating Experience to support reducing risks As Low As Reasonably Practicable (ALARP).

2.1.4: System/structure performance will be validated by suitable testing throughout manufacturing, construction, and commissioning.

2.1.5: Ageing and degradation mechanisms will be identified and assessed in the design. Suitable examination, inspection, maintenance, and testing will be specified to maintain systems/structures fit-for-purpose through-life.

2.1.6: The BWRX will be designed so that it can be decommissioned safely, using current available technologies, and with minimal effect on the environment and people.

2.4.1: RGP has been taken into account across all disciplines.

2.4.2: Operational Experience (OPEX) and Learning from Experience (LfE) has been taken into account across all disciplines.

2.4.3: Optioneering (all reasonably practicable measures have been implemented to reduce risk).

To facilitate compliance demonstration against the above Level 3 sub-claims, this Preliminary Safety Report (PSR) chapter has derived a suite of arguments that comprehensively explain how their applicable Level 3 sub-claims are met (see Table 7-A-1 below).

It is not the intention to generate a comprehensive suite of evidence to support the derived arguments, as this is beyond the scope of GDA Step 2. However, where evidence sources are available, examples are provided.

Risk Reduction As Low As Reasonably Practicable

It is important to note that nuclear safety risks cannot be demonstrated to have been reduced ALARP within the scope of a 2-Step GDA. It is considered that the most that can be realistically achieved is to provide a reasoned justification that the BWRX-300 Small Modular Reactor design aspects will effectively contribute to the development of a future ALARP statement. In this respect, this chapter contributes to the overall future ALARP case by demonstrating that:

- The chapter-specific arguments derived may be supported by existing and future planned evidence sources covering the following topics:
  - RGP has demonstrably been followed. See Subsections 7.3.1.3, 7.3.2.3, 7.3.3.3, and 7.3.4.3 for the fundamental design properties undertaken in the system design.
  - OPEX has been taken into account within the design process. For example, for digital equipment:
    - Large quantities of Commercial-off-the-Shelf (COTS) is used (e.g. obsolescence mitigation).
    - Less space required
    - Lower electrical load required
    - Less heat generation (less HVAC load)
    - Faster response time
  - All reasonably practicable options to reduce risk have been incorporated within the design. The design process will follow PE as detailed in Section 7.4.
- It supports its applicable level 3 sub-claims, defined within the SCDS (Reference 7-56).

Probabilistic safety aspects of the ALARP argument are addressed within PSR Chapter 15.

Table 7-A-1: Claims, Arguments, Evidence Route Map

L3 No.	Level 3 Chapter Claim	Chapter 7 Arguments	PSR Chapter Subsections Where the Arguments Are Supported
2.1: The functions of structures, systems and components have been derived and substantiated taking into account RGP and OPEX, and processes are in place to maintain these through-life. (Engineering Analysis)			
2.1.2	The design of the system/structure has been substantiated to achieve the safety functions in all relevant operating modes.	Safety functions associated with the relevant Structures, Systems, and Components (SSC) have been substantiated during normal operating conditions (including design codes and standards compliance).	The level of substantiation will be commensurate with the design maturity. The I&C systems design will follow a tailored life-cycle process. Interim verification and validation work will be conducted to confirm the adequacy of design requirements and objectives. The I&C systems will meet the requirements of the relevant design principles (generic and system specific) and therefore of relevant good practice. 7.1 Instrumentation and Control Introduction and Overview. 7.3.1.2 System Design Bases and Associated Safety Functions. 7.3.2.2 System Design Bases and Associated Safety Functions. 7.3.3.2 System Design Bases and Associated Safety Functions. 7.4 Digital Instrumentation and Control System Development Process (Production Excellence). 7.3.1.5 Compliance Alignment. 7.3.2.5 Compliance Alignment. 7.3.3.5 Compliance Alignment. 7.3.3.5 Compliance Alignment. 7.3.4.5 Compliance Alignment.
		A record of safe BWR plant operation and continuous improvement demonstrates a well-founded design.	GEH to advise
		Safety functions associated with the relevant SSC have been substantiated during hazard and fault conditions.	Safety function will be identified in Chapters 3 & 15. 7.8 Hazard Analysis for Instrumentation and Control Systems.
		Any shortfalls in safety function substantiation have been identified and assessed to identify any reasonably practicable means to reduce risk.	This argument is out of the scope of a 2-Step GDA and will be addressed during a site specific stage (when evidence is developed)
2.1.3	The system/structure design has been undertaken in accordance with relevant design codes and standards (RGP) and design safety principles, and taking account of Operating Experience to support reducing risks ALARP.	Design evolutions to SSC have been considered taking into account relevant BWR OPEX, and any reasonably practicable changes to reduce risk have been implemented.	BWRX-300 Design Evolution, GEH reference NEDC-34137P, Revision 0. 7.4 Digital Instrumentation and Control System Development Process (Production Excellence). For digital equipment: • Large quantities of COTS equipment is used • Shorter lead times. • Less space required. • Lower electrical load required. • Less heat generation (less HVAC load). • Faster response time.
		The SSC have been designed in accordance with relevant codes and standards (RGP)	Codes and Standards report (tranche 2 version) plus its associated spreadsheet. This PSR chapter also discusses the codes & standards to which it has been designed. 7.1.3 Industry Standards Applicable to Instrumentation and Control Systems
		The SSC have been designed in accordance with an appropriate suite of design safety principles.	The GEH Safety and Design Principles are documented in the BWRX-300 Safety Strategy, supplemented by the BWRX-300 General Description. These principles are also be presented within PSR Chapter 3. 006N5064, BWRX-300 Safety Strategy, Revision 6. 005N9751, BWRX-300 General Description, Revision F. 7.3.1.3, 7.3.2.3, 7.3.3.3, and 7.3.4.3 for the fundamental design properties undertaken in the system design.

L3 No.	Level 3 Chapter Claim	Chapter 7 Arguments	PSR Chapter Subsections Where the Arguments Are Supported
2.1.4	System/structure performance will be validated by suitable testing throughout manufacturing, construction and commissioning.	SSC pre-commissioning tests (e.g. NDT) validate the relevant performance requirements.	7.4 Digital Instrumentation and Control System Development Process (Production Excellence).
		SSC commissioning tests (e.g. system level pressure and leak tests) validate the relevant performance requirements.	7.4 Digital Instrumentation and Control System Development Process (Production Excellence).
		SSC are manufactured, constructed and commissioned in accordance with QA arrangements appropriate to their safety classification.	PSR Chapter 3 defines this approach. 7.4 Digital Instrumentation and Control System Development Process (Production Excellence).
2.1.5	Ageing and degradation mechanisms will be identified and assessed in the design. Suitable examination, inspection, maintenance and testing will be specified to maintain systems/structures fit-for-purpose through-life.	SSC ageing and degradation mechanisms will be identified during SSC design. These will be assessed to determine how they could potentially lead to SSC failure.	PSR Chapter 3 & 13 defines this approach. 7.4 Digital Instrumentation and Control System Development Process (Production Excellence).
		Appropriate Examination, Maintenance, Inspection and Testing (EMIT) arrangements will be specified taking into account SSC ageing and degradation mechanisms.	PSR Chapter 3 & 13 defines this approach. 7.4 Digital Instrumentation and Control System Development Process (Production Excellence).
		The SSCs that cannot be replaced have been shown to have adequate life.	PSR Chapter 3 & 13 defines this approach. 7.4 Digital Instrumentation and Control System Development Process (Production Excellence).
		Ageing and degradation OPEX will be considered as part of the design stage component/materials selection process in order to mitigate SSC failure risk.	PSR Chapter 3 & 13 defines this approach. 7.4 Digital Instrumentation and Control System Development Process (Production Excellence).
2.1.6	The BWRX will be designed so that it can be decommissioned safely, using current available technologies, and with minimal effect on the environment and people.	SSC decommissioning is considered at the design stage to ensure that safe decommissioning may take place.	BWRX 300 Decommissioning planning (Chapter 21). OPEX demonstrates that decommissioning of reactor facilities is facilitated if considered during the design phase: [1] Materials are selected to minimise the quantities of radioactive waste and assisting decontamination. [2] Plant layout is designed to facilitate access for decommissioning or dismantling activities. [3] Future potential requirements for storage of radioactive waste. Chapter 3 7.4 Digital Instrumentation and Control System Development Process (Production Excellence)
		SSC are designed in order to minimise effects on people and the environment during decommissioning.	PSR Chapter 21 defines this approach. 7.4 Digital Instrumentation and Control System Development Process (Production Excellence).
2.4 Safety risks have been reduced as low as reasonably practicable			
2.4.1	RGP has been taken into account across all disciplines.	Relevant SSC codes and standards (RGP) are identified.	Codes and Standards report (tranche 2 version) plus its associated spreadsheet.
		SSC have been designed in accordance with relevant codes and standards (RGP).	This PSR chapter also discusses the codes & standards to which it has been designed.
		Any shortfalls in codes and standards compliance are identified and assessed to reduce risks ALARP.	Codes and Standards report (tranche 2 version) plus its associated spreadsheet. 7.1.3 Industry Standards Applicable to Instrumentation and Control Systems
2.4.2	OPEX and LfE has been taken into account across all disciplines.	Design improvements to SSC have been identified considering relevant OPEX and LfE.	BWRX-300 Design Evolution, GEH reference NEDC-34137P, Revision 0.
		Any reasonably practicable design changes to reduce risk have been implemented.	7.1 Instrumentation and Control Introduction and Overview.

L3 No.	Level 3 Chapter Claim	Chapter 7 Arguments	PSR Chapter Subsections Where the Arguments Are Supported
2.4.3	Optioneering (all reasonably practicable measures have been implemented to reduce risk).	Design optioneering has been performed in accordance with an approved process.	006N3139, “BWRX-300 Design Plan,” (Reference 7-57) The BWRX-300 Design Plan (006N3139, Rev 5 section 4.7) mentions the GEH OPEX process CP-16-101 (Lessons learned/Operating Experience Program). The design process incorporates applicable OPEX to mitigate nuclear design and construction risk, in accordance with CP-16-101 and the BWRX-300 OPEX/lessons learned programme. Operating experience sources include the Institute of Nuclear Power Operations, Electric Power Research Institute and BWR Owners Group. Construction experience and improved construction methods from previous large projects are also used to improve the quality and efficiency of the construction effort.
		Design optioneering has considered all reasonably practicable measures.	006N3139, BWRX-300 Design Plan (Reference 7-57) NEDC-34137P, “BWRX-300 Design Evolution,” (Reference 7-58)
		Any reasonably practicable design changes to reduce risk have been implemented.	NEDC-34137P, BWRX-300 Design Evolution (Reference 7-58)

APPENDIX B FORWARD ACTION PLAN

The FAP is not required to capture the 'normal business' of Safety, Security, Safeguards and Environmental case development as the design progresses from concept to design for construction and commissioning. FAP items can arise from several sources:

- Assumptions and commitments made in the GDA submissions that will require future verification/implementation, for example, by the future constructor and/or plant operator.
- A gap in the underpinning of the GDA submissions currently under development.
- A potential gap in a future phase of submissions if additional work is not performed or
- A gap identified by the regulators and communicated to the Requesting Party (RP) through a Regulatory Query or Regulatory Observation.

The forward action plan items that have been raised for the I&C topic are detailed below:

Table 7-B-1: Forward Action Plan Items

Action ID	Source	Finding	Forward Actions	Lead Discipline	Delivery Phase

Note: No findings have been raised.

APPENDIX C INTERFACING SYSTEMS

Chapter 2 Site Characteristics

- Meteorological Monitoring System

Chapter 4 Reactor

- Control Rod Drive System

Chapter 5 Nuclear Boiler System and Associated Systems

- Nuclear Boiler System

Chapter 6 Engineered Safety Features

- Isolation Condenser System
- Containment and Associated Systems
- Containment Isolation
- Systems for Protection Against Over Pressure and Under Pressure
- Control Room Habitability

Chapter 7 Instrumentation and Control (This Chapter)

Chapter 8 Electrical Power

- On-site AC Power Systems
- On-site DC Power Systems

Chapter 9A Auxiliary Systems

- Fuel Pool Cooling and Cleanup System
- Plant Cooling Water System
- Reactor Water Cleanup System
- Shutdown Cooling System
- Chilled Water Equipment System
- Isolation Condenser System Pool Cooling and Cleanup System
- Process Sampling Systems
- Plant Pneumatic System
- Containment Inerting System
- Heating, Ventilation, and Cooling System
- Control Building Heating, Ventilation, and Cooling System
- Radwaste Building Heating, Ventilation, and Cooling Systems
- Turbine Building Heating, Ventilation, and Cooling System
- Service Building Heating, Ventilation, and Cooling Systems
- Containment Cooling System
- Fire Protection (Packaged)

- Supporting Systems for Diesel Generators (Storage and Transfer, Cooling Water and Cooling Air, Starting, Lubrications, Combustion Air Intake and Exhaust)
- Equipment and Floor Drain System
- Potable Water System
- Water Treatment (Packed)
- Makeup Water System
- Sanitary Water Systems
- Hydrogen Water Chemistry
- On-Line NobleChem™ Injection
- Plant Communication System

Chapter 9B Civil Engineering Works and Structures

- Foundations (Seismic instrumentation)
- Integrated Reactor Building (Seismic instrumentation)
- Containment Internal Structures (Seismic instrumentation)

Chapter 10 Steam and Power Conversion Systems

- Turbine Generator System
- Condensate Filters and Demineralizers System
- Condensate and Feedwater Heating System
- Main Steam System
- Main Condenser and Auxiliaries System
- Moisture Separator Reheater
- Turbine Auxiliary Systems
- Circulating Water System
- Generator and Exciter

Chapter 11 Management of Radioactive Waste

- Systems for Management of Liquid Radioactive Waste
- System for Management of Gaseous Radioactive Waste
- System for Management of Solid Radioactive Waste
- Process Radiation and Environmental Monitoring System

Chapter 12 Radiation Protection

- Containment Monitoring Subsystem

Chapter 15 Safety Analysis

- Boron Injection System

Chapter 18 Human Factor Engineering

- Operator Interfaces

Chapter 19 Emergency Preparedness and Response

- Safety Parameter Display System

APPENDIX D INDEPENDENT CONFIDENCE BUILDING MEASURES

Within the UK context, I&C systems that contain software or complex hardware require a two-legged justification: Production Excellence (PE) and Independent Confidence-Building Measures (ICBMs). This document addresses PE in Section 7.4. ICBMs are a UK-specific method of providing additional safety justification. PE and ICBMs follow a graded approach to selecting measures to support the safety justification of I&C systems containing software or complex hardware. Possible ICBMs are listed below (See Table 7-D-1), although the list is not exhaustive and does not rule out alternative techniques. The ICBMs will be specified once details of the specific I&C systems are understood. The selected techniques are different from those employed in the PE leg. The adequacy of the chosen measures and the strategy for implementing ICBMs will be detailed at the appropriate stage in the project lifecycle.

Table 7-D-1: Independent Confidence Building Measures

Class 3	Class 2	Class 1
Example of suitable techniques and measures: • Device type tests • Commissioning tests • Examination, Inspection, Maintenance, and Testing (EIMT) records • Data on prior use from reputable sources • Evidence of manufacturer pedigree • Device hardware failure modes and effects analysis Justification may require the following, as appropriate: • Dynamic analysis of source code • Static analysis of source code • Independent desk top review of source code • Statistical testing; Certification by an independent body (supported by evidence) • Independent Functional Safety Assessment (FSA) • Independent tool review	Example of suitable techniques and measures: • Device type tests • Commissioning tests • EIMT records • Data on prior use from reputable sources • Evidence of manufacturer pedigree • Device hardware failure modes and effects analysis • Dynamic analysis of source code • Static analysis of source code • Independent desk top review of source code • Certification by an independent body (supported by evidence). Justification may require the following, as appropriate: • Statistical testing • Independent FSA • Independent tool review	Example of suitable techniques and measures: • Device type tests • Commissioning tests • EIMT records • Data on prior use from reputable sources • Evidence of manufacturer pedigree • Device hardware failure modes and effects analysis • Dynamic analysis of source code • Static analysis of source code • Independent desk top review of source code • Certification by an independent body (supported by evidence) • Statistical testing • Independent FSA • Independent tool review

Note:
The source is NS-TAST-GD-046 ONR Technical Assessment Guide (TAG 046) Computer Based Safety Systems - December 2023.