Form10/00

HITACHI

UK ABWR

Document ID	:	GA91-9101-0101-14000
Document Number	:	3E-GD-A0063
Revision Number	:	C

UK ABWR Generic Design Assessment

Generic PCSR Chapter 14: Control and Instrumentation

Hitachi-GE Nuclear Energy, Ltd.

DISCLAIMERS

Proprietary Information

This document contains proprietary information of Hitachi-GE Nuclear Energy, Ltd. (Hitachi-GE), its suppliers and subcontractors. This document and the information it contains shall not, in whole or in part, be used for any purpose other than for the Generic Design Assessment (GDA) of Hitachi-GE's UK ABWR. This notice shall be included on any complete or partial reproduction of this document or the information it contains.

Copyright

Table of Contents

Executive Summary

This chapter describes the safety case for the UK ABWR Control and Instrumentation (C&I). It lists the high level Safety Functional Claims that are made on these systems, together with the Safety Property Claims that enable compliance with the Nuclear Safety and Environmental Design Principles (NSEDPs) to be demonstrated. It also provides the C&I input to all other systems engineering chapters in the PCSR (Chapters 12, 13, 15, 16, 17, 18, 19, 21 and 31).

The information provided includes: system design, functionality in normal operation and during faults, safety categorisation and classification, important support systems, safety case assumptions, Limits and Conditions for Operation, resistance to hazards, and compliance with the ALARP principle.

The overall PCSR justification that the UK ABWR is safe and satisfies the ALARP principle is underpinned by hazards assessments, design basis analysis, probabilistic safety analysis, beyond design basis analysis and human factors analysis (described in PCSR Chapters 6, 7 and 24 to 27), which demonstrate that the design of the C&I systems are fault tolerant. These analysis chapters specify the high level Safety Functional Claims but do not specify requirements for design parameters on individual C&I Systems. Instead they apply analysis conditions and assumptions that are based on, and fully consistent with, the design information and safety claims for the C&I systems that are presented in this chapter, in order to substantiate those claims.

Risk reduction measures have been introduced (with reference to the J-ABWR reference design) in response to safety assessments undertaken in GDA, these include the provision of additional diversity between the key Safety Class 1, 2 and 3 parts of the C&I systems and also the introduction of a Hardwired Backup System. Other specific issues that have been considered in ALARP assessments include the benefits of strengthening automation in many of the manual hardwired backup functions.

This chapter demonstrates that the risks associated with the design and operation of the C&I systems for the UK ABWR are ALARP. It is acknowledged that further work will be required post GDA phase to develop the design and fully incorporate site specific aspects. This work will be the responsibility of any future licensee.

14.1 Introduction

This chapter provides an overview of the safety justification for the UK ABWR Control and Instrumentation (C&I) systems. It also provides a high level description of the overall structure of the C&I safety case based on a document map (Appendix C of this chapter) showing where detailed evidence is described in a set of supporting technical reports. This consists of a set of Basis of Safety Cases (BSCs) documents and their supporting Topic Reports (TRs).
As with other chapters of this PCSR, ABWR indicates a general design, J-ABWR indicates the reference Japanese design and the UK ABWR is the design of the generic UK facility.

14.1.1 Background

The C&I systems proposed for the UK ABWR represent an evolutionary development from the C&I systems successfully operating on BWRs and ABWRs throughout the world. They also benefit from the application of international codes and standards from C&I systems that have operated very successfully for more than 5 decades on the broader family of light water reactors.

Over the past 5 decades C&I systems have evolved from all analogue electronics in the 1960s and early 1970s to the current generation of technology by taking advantage of modern very large scale integrated circuits such as microprocessors and related technologies such as Field Programmable Gate Arrays (FPGA) to enhance both the safety and functional performance of C&I systems (See Figure 14.1-1). However, as described later in this chapter, the UK ABWR C&I systems retain some simple hardwired electronic technology to enhance the important concept of independence used in the safety analysis and for cyber security reasons.

This chapter takes as its starting point the J-ABWR C&I systems installed at Kashiwazaki-Kariwa Units 6 and 7. It is recognised that there were some gaps between the reference J-ABWR design standards for C&I systems and current UK relevant good practice for such systems. This is not surprising as C&I design standards have evolved since the original J-ABWR C&I systems were designed. This document demonstrates that Hitachi-GE has made sufficient improvements to close these gaps and that both the overall architecture of the C&I systems and its component parts are fully aligned with UK relevant good practice. Additionally section 14.13 of this chapter provides a summary demonstration that the design of the UK ABWR C&I systems reduces the risks to safety from failures of these systems to a level that is As Low As Reasonably Practicable (ALARP).

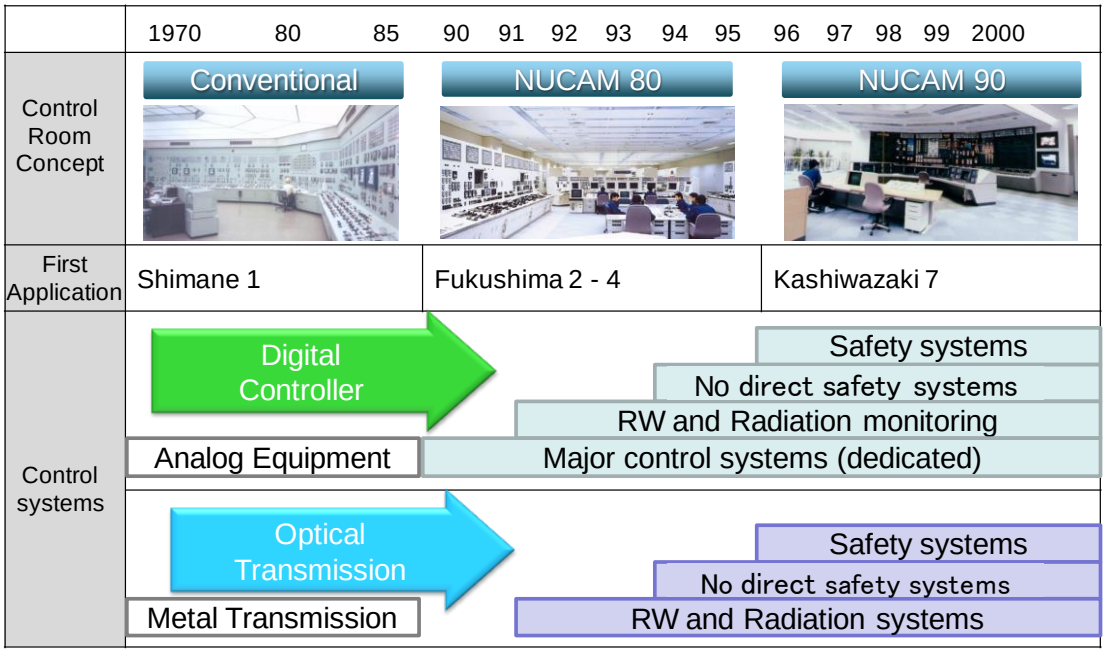


Figure 14.1-1: The evolution of the C&I and associated HMI

14.2 Purpose and Scope

14.2.1 Purpose and scope

The purpose of this document is to provide the following:

- An overview of the safety case for the UK ABWR C&I systems.
- A comprehensive list of all of the Safety Functional Claims (SFCs) and Safety Property Claims (SPCs).
- A route map to where the more detailed Claims, Arguments and Evidence can be found by reference to the Level 2 documents described in the document map given in Appendix C (of this chapter). Please note the Level 3 documents are referenced in the Level 2 documents.
- A comprehensive set of references to Level 2 documents and other chapters in the PCSR.

This Chapter applies to all C&I equipment from the sensors to the devices which actuate and control the mechanical equipment. As shown in Figure. 14.2-1, it covers the:

(1) Sensors,
(2) Actuators,
(3) Control equipment, and
(4) Operator interface (described in Generic PCSR Chapter 21 : Human-Machine Interface)

Although items such as control valves and pumps do not form part of the C&I scope for specification and provision, their effect on the functionality of the C&I systems is considered within the assessment of the design and analysis of the C&I systems during GDA as shown in Table 14.2-1.

The PCSR covers the aspects of human factors and computer security; however, human factor aspects of the HMI are covered in Chapters 21 and 27: Human Factors of the PCSR and the BSCs on Overall HMI [Ref-3]; the security details are covered in the Conceptual Security Arrangements document [Ref-4].

The scope of what is assigned to C&I and what is included in, primarily, the reactor systems and mechanical engineering topics (see Generic PCSR Chapters 12: Reactor Coolant Systems, Reactivity Control Systems and Associated Systems, 13: Engineered Safety Features and 15: Electrical Power Supplies, 16: Auxiliary Systems, and 17: Steam and Power Conversion Systems) is shown in Figure 14.2-1. This shows an example of the Reactor Pressure Vessel (RPV) instrument lines for flow, pressure, level and temperature measurements. Taking the example of the flow measure, the design of the flow restrictor element is within the scope of the RPV system whereas everything downstream of the instrument master valve in Figure 14.2-1 is within the scope of this chapter. Similarly, on the output side if we take the example of a pump (e.g. one of the high pressure core flooder pumps, see Generic PCSR Chapter 13) the circuits that initiate the closure of the circuit breaker to start the pump are within the scope of C&I but the pump and the circuit breaker (not shown) are not. In this example, the pump is within the scope of the mechanical system (Generic PCSR Chapter 13) and the circuit breaker is within the topic of electrical engineering in Generic PCSR Chapter 15.

Although Figure 14.2-1 shows an RPV instrument example, the input and output interface principles described are applicable for all C&I interfaces with other topics.

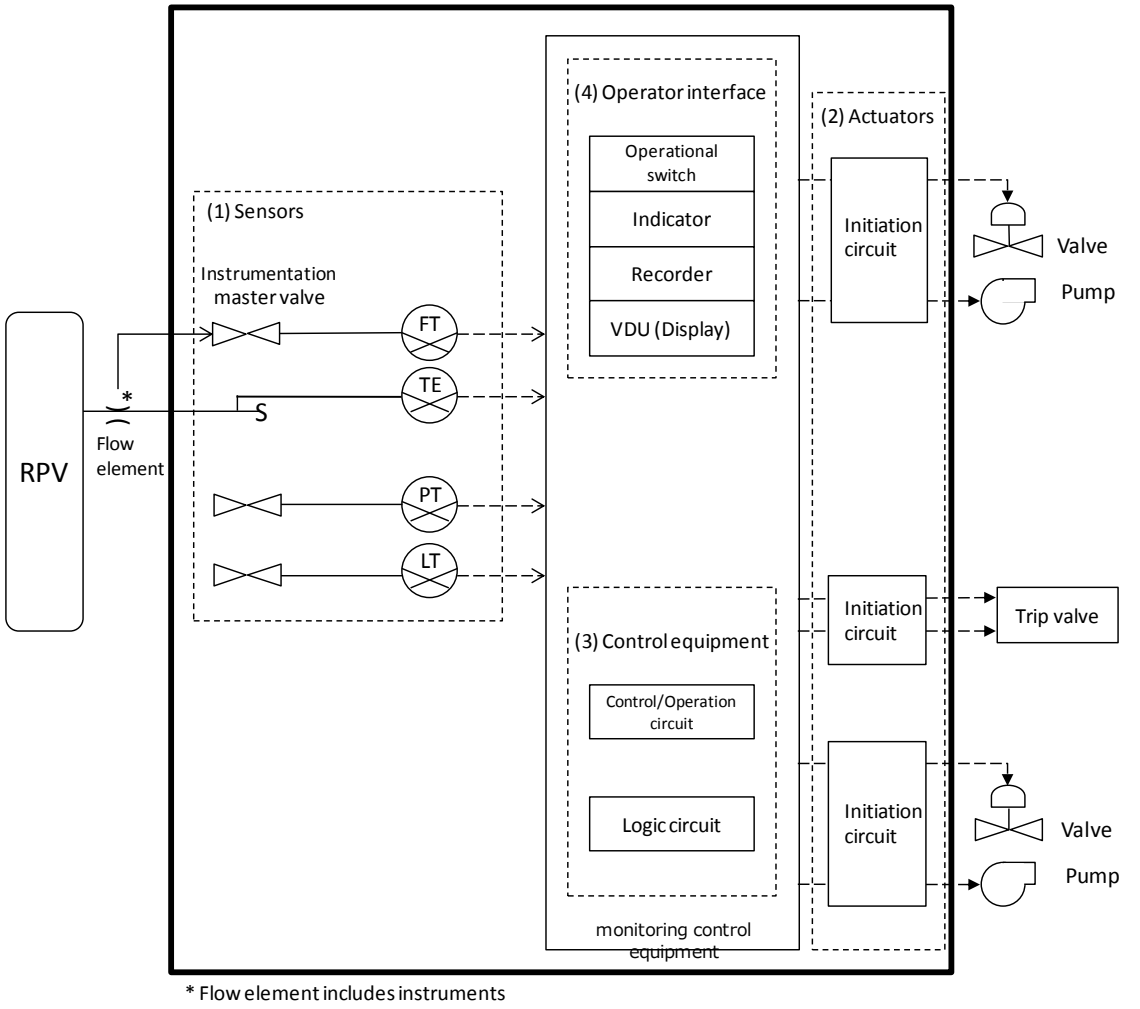


Figure 14.2-1: Example of Scope of C&I system

14.2.2 GDA Scope

The scope of this document covers the depth of the safety analysis supporting the design of the C&I systems. Table 14.2-1 provides a summary of the depth of safety analysis within the scope of GDA for each system.

Table 14.2-1 GDA Depth of Scope for UK ABWR C&I Systems

	SSLC System	Hardwired Backup System	Safety Auxiliary Control System	Plant Control System	Severe Accident C&I System	Reactor/Turbine Auxiliary Control System		Plant Computer System	Others System
						Reactor	Turbine		
Cat-Class	A-1	A-2	B-2	Class 3	B-2 or B-3	Class 3	Class 3	Class 3	A-C/1-3
Sensor	II	II	II	II	II	II	III	-	II
Actuator	II	II	II	II	II	II	III	-	II
Control equipment	I (vCOSS®)	I	I (vCOSS®)	I (HIACS)	I	II (HIACS)	II (HIACS)	II	II
Operator Interface	IV	IV	IV	IV	IV	IV	IV	IV	IV

The interpretation for the entry of Roman numerals I, II, III and IV in the table is as follows:

- Item I: The C&I design is included during the GDA process. Support documents such as SDD (System Design Description), IED (Instrument Electrical Diagram), and IBD (Interlock Block Diagram), involves C&I design are also be presented.
- Item II: The C&I design principles are included during the GDA process. Support documents associated with the C&I design are also presented. It is noted that the final selection of most sensors and actuators will be undertaken post GDA phase and, hence, only selection principals and key properties is included in GDA.
- Item III: Shall be implemented post GDA phase.
- Item IV: The principles are included in the C&I PCSR; the details are defined in Generic PCSR Chapter 21 : Human-Machine Interface.

Please note in Table 14.2-1 all Control Systems are directly classified and do not have a safety functional category. There are a number of embedded C&I systems important to safety that are not included explicitly in Table 14.2-1, these will not be included in GDA (as stated for embedded C&I systems in Table 14.2-1) although the approach to demonstration of their suitability for use has been defined as part of GDA; e.g. as part of the demonstration of use of SMART devices, the completed case will be in the post GDA phase of the project.

A good example of the use of embedded C&I is the Emergency Diesel Generators (EDGs). The Safety System and Logic Control (SSLC) sends start signals to the EDGs but each EDG will have embedded C&I that will perform roles such as engine management and excitation of the generator. This embedded C&I technology is integral to the supplier of the equipment, such as the EDG, and this information will not be known until the site specific phase of the project. What is described in this chapter are the principles that will be applied to the design of embedded C&I covering production excellence and the viability of applying independent confidence building at a later stage of the project. Production excellence and independent confidence building applies specifically to embedded C&I that employs programmable technology. For embedded C&I technology that is hard-wired, identical techniques will be applied to that of the Hard-Wired Backup System (HWBS)

described later in this chapter. The systems in which embedded C&I can be found and the design for which is out of scope of GDA are as follows:

- Fuel route, for example lifting equipment such as the Reactor Building Crane, Fuel Handling Machine (Generic PCSR Chapter 19: Fuel Storage and Handling), etc.,
- Mechanical Engineering Systems such as Heating Ventilation and Air Conditioning Systems, Diesel Generators (Generic PCSR Chapter 16), etc.,
- Electrical Engineering, Protection Relays, Uninterruptible Power Supply Systems (Generic PCSR Chapter 15), etc.,
- Radiation Protection, Access Control, Local Radiation Monitoring (Generic PCSR Chapter 20: Radiation Protection), etc.,
- Internal Hazards, Door Alarms, Fire Detection, (Generic PCSR Chapter 7: Internal Hazards), etc., and
- Radwaste, Treatment and Management (Generic PCSR Chapter 18: Radioactive Waste Management).

For environmental and security aspects of the UK ABWR design, links to GEP, and CSA documentation are referred to in Generic PCSR Chapter 1: Introduction (GA91-9101-0101-01000 (XE-GD-0214)). For GEP, where specific references is required, for example in Radioactive Waste Management,
Radiation Protection and Decommissioning, these are included in the specific sections within the Generic PCSR. Cyber security for Computer Based Systems Important to Safety (CBSIS) and the broader topic of the security of C&I in general are not within the scope of this chapter.

14.2.2.1 Documentation Structure

The generic document structure for the whole of the UK ABWR C&I safety case is shown in Appendix C. The highest level for C&I is this chapter which is the Level 1 document, Level 2 consists of the Basis of Safety Cases (BSCs) and their supporting Topic Reports (TRs) and Level 3 consists of the engineering design documents for the C&I systems.

The approach adopted is that the Level 1 (Generic PCSR Chapter 14 of PCSR for C&I), gives an overview summary of the whole safety case. This overview also links to other chapters of the PCSR, of particular importance are the links to the fault analysis chapters, 24: Design Basis Analysis, 25: Probabilistic Safety Assessment and 26: Beyond Design Basis and Severe Accident Analysis, as all of the safety functional claims are derived from those three chapters through the specification of the High Level Safety Functions (HLSF) shown in Generic PCSR Chapter 5: General Design Aspects. The categorisation of safety functions and safety classification of SSC in this chapter conform with the methodology described in Generic PCSR Chapter 5, section 5.6. Additionally, the general requirements for Equipment Qualification, Examination Maintenance Inspection and Testing (EMIT) and codes and standards that come from this safety categorisation and classification are also described in Generic PCSR Chapter 5, sections 5.7 and 5.9, respectively. Further details can be found in the EMIT section of the corresponding Basis of Safety Cases document for each C&I system referred from this chapter. Similarly Generic PCSR Chapter 19 on fuel storage and handling is also an important source of safety functional claims. Through the safety functional claims there are also very strong links to Human Factors (HF, Generic PCSR Chapter 27), Human-Machine Interface (HMI, Generic PCSR Chapter 21) and mechanical systems (Generic PCSR Chapters 12, 13, 15, 16 and 17).

C&I also has safety functional claims from, and provides information to, topics such as radwaste, radiation protection, decommissioning, structural integrity, spent fuel interim storage, reactor core, operations, emergency arrangements and commissioning. Design to either withstand or be protected

from a wide range of hazards is an important source of safety property claims and therefore links to Generic PCSR Chapter 6: External Hazards and Chapter 7: Internal Hazards are of high importance. Finally section 13 of this chapter provides the summary justification that safety risks from the UK ABWR C&I systems are ALARP and this information links directly to Generic PCSR Chapter 28: ALARP Evaluation. The general principles for the identification of Assumptions, Limits and Conditions for Operation (LCOs), are described in Generic PCSR Chapter 4: Safety Management throughout Plant Lifecycle, section 4.12. General requirements for decommissioning of the systems, structures and components within this chapter scope are described in Generic PCSR Chapter 31: Decommissioning. The related claims are summarised in Generic PCSR Chapter 31, section 31.2 Safety Claims.

For generic links to GEP, and CSA documentation, please refer to Generic PCSR Chapter 1. For GEP, where specific references are required, e.g. in Radioactive Waste Management, Radiation Protection, Decommissioning, these are included in the specific sections within the relevant chapter.

Level 1 for each topic is covered by a single document, for UK ABWR C&I systems it is this chapter. There are many more Level 2 documents, as these documents provide the Claims and Arguments (BSCs) and the Evidence (TRs). Dependent on the topic, Level 2 can consist of between 10 and 30 or more documents. Depending on the complexity and safety importance of the system these system BSCs are supported by one or more TRs. Appendix C shows the main C&I Level 1 and 2 documents. Appendix C also shows the structure of an overall architecture BSCs supported by system specific BSCs.

The BSCs include:
(1) Overall C&I Architecture [Ref-5],
(2) Safety System Logic and Control System (SSLC) [Ref-6],
(3) Hardwired Backup System (HWBS) [Ref-7],
(4) Safety Auxiliary Control System (SACS) [Ref-8],
(5) Plant Control System (PCntlS) [Ref-9],
(6) Severe Accident C&I System (SA C&I) [Ref-10],
(7) Reactor / Turbine Auxiliary Control System (ACS) [Ref-11], and
(8) Plant Computer System (PCS) [Ref-12].

Topic reports support the PCSR and BSCs and include ones on key processes such as the Justification of SMART devices [Ref-13], performance of Independent Confidence Building Measures, e.g. for νCOSS® (Class 1) platform [Ref-14], and also ones giving detailed technical information on the platforms such as νCOSS® [Ref-15], and HIACS for Class 3 Platform [Ref-16].

There is a third tier of documents that sits below the BSCs and TRs that are the output of the engineering processes which provides the evidence supporting the claims and arguments presented for the C&I. These documents include the output from the C&I development processes and include:

(1) System Design Description,
(2) Instrument Electrical Diagram,
(3) Interlock Block Diagram,
(4) Instrument List, and
(5) Setpoints List.

References to the appropriate documents for each system are given in the BSCs documents or TR documents where appropriate.

The structure of this chapter is as follows:

- Section 14.2 is on the Purpose and Scope, this section provides a comprehensive overview of what systems are in the scope of this chapter for C&I and therefore what is in the scope of GDA. It also describes what is within the scope the C&I topic using inputs (sensors), processing (main C&I cubicles and technology) and outputs (actuators) to define the boundaries of the topic.
- Section 14.3 provides an overview of the important safety principles covering the design of the UK ABWR C&I systems on matters such as codes and standards, safety functional categorisation and safety system classification and equipment qualification.
- Section 14.4 describes the claims structure, in particular the role of Safety Functional Claims (SFCs) and Safety Property Claims (SPCs). SFCs are largely actions performed by a system to meet a high level safety function HLSF. A complete list of all HLSFs is shown in Chapter 5, section 5.6.
- Section 14.5 covers the overall architecture of the C&I systems for the UK ABWR. Due to the complexity of C&I systems establishing architectural claims is of considerable importance and is the starting point for the claims on the individual systems.
- Section 14.6 provides an overview of the role and safety justification of each specific C&I system.
- Section 14.7 covers the important topic of sensors, pre-processing, actuators and prioritisation.
- Section 14.8 provides an overview of the fuel route C&I, applied technologies for Other C&I system and embedded C&I.
- Section 14.9 covers the support systems such as electrical power and heating, ventilation and air conditioning systems without which the C&I systems cannot operate.
- Section 14.10 covers formal management systems and design methods for complex systems and includes areas such as Quality Assurance, Requirements Capture, Safety Lifecycle, etc. within the context of an overall management system structure.
- Section 14.11 covers safety justification of the quality and integrity of Hitachi-GE's design process for the development of C&I systems containing either microprocessors and software or devices such as FPGAs and hardware description languages (HDL).
- Section 14.12 provides a high level overview of the methodology for capturing of assumptions and the Limiting Conditions for Operations (LCOs) as a precursor during the site specific part of the project to develop detailed Technical Specifications.
- Section 14.13 details the ALARP summary justification.
- Section 14.14 gives Conclusions
- Section 14.15 details the References.

There are three appendices. Appendix A provides a comprehensive table of the Safety Functional Claims (SFCs), while Appendix B provides the equivalent for Safety Property Claims (SPCs). Finally Appendix C provides the document map showing the structure of the Levels 1 and 2 documents for all of the UK ABWR C&I systems.

14.3 Safety Principles and Development Practice

This section identifies the safety principles and company policies applicable to C&I systems. It also identifies, at high level, the regulatory principles and expectations.

14.3.1 High Level Safety Principles

This section provides a Statement of Company Policies, safety principles and safety criteria that are applicable to the development of the UK ABWR and its C&I systems. These policies and principles were used in the development of the existing ABWRs and have been modified to consider UK expectations of good practice.

(1) Safety principles for Nuclear facilities.
(2) Safety principles for Nuclear Power Plants.
(3) Nuclear safety and quality policy of Hitachi-GE.
(4) ABWR Historical Approach for Safety Principles.
(5) C&I Approach for Safety Principles.
(6) C&I Platform Defence in Depth and Diversity Approach for Safety Functions.

(1), (2) are described in this section.
(3) is described in Generic PCSR Chapter 4, section 4.3.1: Hitachi-GE's Safety and Quality Policy.
(4) is described in Generic PCSR Chapter 28, section 28.3: Development of the Standard ABWR.
(5) is described in Basis of Safety Cases on Control and Instrumentation Architecture [Ref-5].
(6) is described in Basis of Safety Cases on Control and Instrumentation Architecture [Ref-5], and further information of the diverse platforms is described in: Basis of Safety Cases on Safety System Logic and Control System [Ref-6], Basis of Safety Cases on Hardwired Backup System [Ref-7] and Basis of Safety Cases on Plant Control System [Ref-9].

14.3.1.1 Safety principle for Nuclear facilities

A Nuclear facility has potential risks arising from the presence of radiation and radioactive substances and aims to ensure safety by mitigation of those risks using various countermeasures. Safety principles for nuclear facilities include:

(1) Unification of management responsibility,
(2) Adoption of defence in depth, and
(3) Adoption of proven technical principles

These safety principles are described in Section 2 and 3 of NS-R-1 [Ref-17].

14.3.1.2 Safety Principle for Nuclear Power Plants

Nuclear Power Plant design shall include measures to prevent abnormal transients or accidents, and provide countermeasures divided into several levels to mitigate consequences should the preventive measures be ineffective. The contents of countermeasures in the Japanese Approach which is based on section 4 and 5 of NS-R-1 [Ref-17] are listed in Table 14.3-1. These countermeasures are applicable to the UK ABWR and described further in section 14.3.2 of this chapter.

Table 14.3-1: Ensuring safety of Nuclear Power Plants

Ensuring safety	Method
(1) Structure confining Fission Products	Multi-Layer Structure - Pellet - Cladding tube - Reactor Pressure Vessel - Pressure Containment Vessel - Reactor Building
(2) Safety System for Emergency (Defence in Depth)	(a) Protection System (PS) application - Margin of safety design - Prevent accidents due to incorrect operation (b) Mitigation System (MS) application - Early detection of abnormal events - Reactor Shutdown Function - Emergency Core Cooling Function - Isolation of Containment Vessel
(3) Robustness against Natural hazard	- Earthquake specific countermeasure - Flooding specific countermeasure - Extreme wind specific countermeasure

14.3.1.3 Nuclear Safety and Quality Policy of Hitachi-GE

Details of the nuclear safety and quality policy of Hitachi-GE are given in Generic PCSR Chapter4, section 4.3.1: Hitachi-GE's Safety and Quality Policy.

Hitachi-GE understands that it is of the upmost importance that its C&I work processes are identified and clarified, the processes and results are monitored, and records are maintained and reviewed. Hitachi-GE is committed to ensuring full transparency of its work and implementing continual improvement in its work processes. The Hitachi-GE management and work process for C&I development are set out in sections 14.10 and 14.11 of this chapter.

14.3.1.4 ABWR Historical Approach for Nuclear Power Plant Safety Principles

ABWR safety features are based on the Defence in Depth (DiD) concept wherein multiple layers of protection are provided with each layer designed to provide the safety function independently of the other layers. The ABWR uses well-designed Safety Systems to achieve a sufficiently low core damage frequency, as required by Japanese practice. The details are described in Generic PCSR Chapter 28, section 28.3: Development of the Standard ABWR.

UK ABWR applies advanced light water technology classified as Generation III or III+, and has been in commercial operation for several years as shown on Figure 14.3-1.

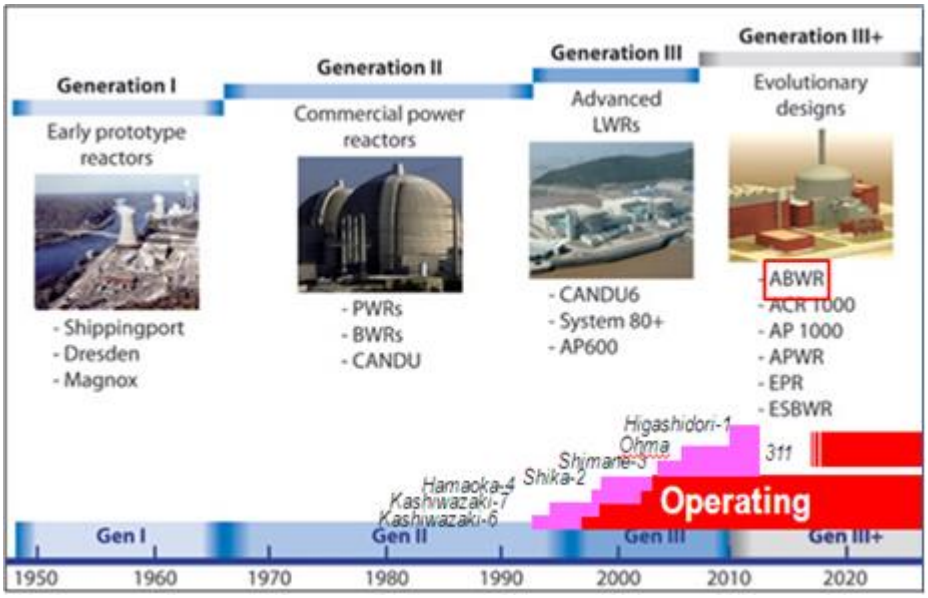


Figure 14.3-1: Definition of Reactor generation and ABWR status

The BWR (Boiling Water Reactor) design has passed through a series of evolutionary changes and has achieved significant design and technological advances to arrive at the current generation of the UK ABWR. The major key features of the UK ABWR design evolution are described in Generic PCSR Chapter 9: General Description of the Unit, section 9.3.1: Basic Plant Design Characteristics.

14.3.1.5 C&I Approach for Nuclear Power Plant Safety Principles

The C&I systems of UK ABWR adopt multiple technologies, e.g. microprocessors, FPGAs and hardwired / analogue and make use of fault detection and fault tolerance techniques. The digital systems have also adopted 3 updates in line with the most recent J-ABWR to improve reliability and plant operability:

(1) Integrated Digital Control System
Integrated Digital Control System contributes to improve reliability and ease of maintenance. Digital technology is also applied to the Class 1 safety functions in the J-ABWR although an alternative (FPGA) technology will be deployed in the UK ABWR.

(2) Wide Display Panel Facilitates Sharing of Information
(a) The overall plant status is supplied as shared information.
(b) Alarms are displayed using hierarchies for improved identification.

(3) Expanded Automation Reduces Load on Operator
Automatic operations, including control rod operation, reduces the operator burden allowing greater focus on overall plant monitoring.

14.3.1.6 C&I Platform Defence in Depth and Diversity Approach for Safety Function

When adopting complex electronic devices as part of the defence in depth principle, the role of diversity is very important particularly in providing defence against Common Cause Failure (CCF) to ensure an effective defence in depth strategy.

There are a number of approaches to achieving and assuring diversity; for example by forcing diversity of people, technology, development practices and supplies; these are discussed in NUREG/CR-6303 [Ref-20]. These approaches will be adopted for the UK ABWR and are described in detail in the BSCs on C&I Architecture [Ref-5].

For reactor protection systems, several diversity strategies are discussed in NUREG/CR-7007 [Ref-19], these include:

(1) Different technology,
(2) Different approaches within the same technology, and
(3) Different architectures within the same technology.

The UK ABWR C&I design has adopted the following approaches:

(1) Provide diversity from the complex technologies, by using hardwired logic, i.e. simplified technology such as relay logic and analogue circuits, to provide defence in depth. This is implemented between the hardwired logic platform for the A-2 HWBS and B-2/3 SA C&I which is diverse from the complex technology platforms for the main safety system and plant control system (FPGA and micro-processor respectively).
(2) Provide diversity between the complex technologies: the control systems based on micro-processor technology and the main safety system based on FPGA. This is implemented between the FPGA platform (Hitachi technology known as νCOSS®) for the A-1 SSLC and B-2 SACS, and micro-processor based (Hitachi technology known as HIACS) for Class 3 PCntlS, ACS and PCS.

This arrangement is shown schematically against the IAEA (International Atomic Energy Agency) defence levels in Table 14.3-2; the table shows that even if one system fails, the plant safety is secured because it is covered by other systems.

The main claims for diversity are between the SSLC, HWBS and the PCntlS (three-way diversity). There is no requirement for the SACS to be diverse from the HWBS as no claims are made on the need for such diversity. However in the design both are diverse as the SACS is based on the same technology as the SSLC and therefore is diverse from the HWBS. The SSLC is the design basis safety measure (for more information on design basis analysis see Generic PCSR Chapter 24 of this PCSR) and as some of the fault sequences that can lead to a severe accident involve a CCF of the SSLC there is a requirement for the SSLC to be diverse from the SA C&I.

For HWBS and SA C&I, both are based on simple and very robust hardwired technology and there is no formal claim on diversity requirements. The PCntlS and SA C&I are required to be diverse as a CCF of the PCntlS and that of the SSLC could lead to a beyond design basis or SA event and therefore there is a need for diversity with the HWBS and the SA C&I.

Table 14.3-2: Objective and Essential means for Defence in Depth

DiD Level	Objective	Essential means	UK ABWR*
Level 1	Prevention of abnormal operation and failures by design.	Conservative design, construction, maintenances and operation in accordance with appropriate safety margins, engineering practices and quality levels.	ACS (Class 3) [HIACS] and PCntlS (Class 3) [HIACS]
Level 2	Prevention and control of abnormal operation and detection of failures.	Control, indication, alarm systems or other systems and operating procedures to prevent or minimise damage from failures.	ACS (Class 3) [HIACS], PCntlS (Class 3) [HIACS] and SSLC (A-1) [νCOSS®]
Level 3	Control of faults within the design basis.	Engineering safety features, multiple barriers and accident or fault control procedures.	SSLC (A-1) [νCOSS®], SACS (B-2) [νCOSS®] and HWBS (A-2) [Hardwired]
Level 4	Control of beyond design basis accidents and severe plant conditions in which the design basis may be exceeded, including the prevention of fault progression and mitigation of the consequences of severe accidents.	Additional measures and procedures to prevent or mitigate fault progression and for accident management.	HWBS (A-2) [Hardwired] SA C&I system (B-2/3) [Hardwired and/or embedded C&I] and SSLC (A-1) [νCOSS®], SACS (B-2) [νCOSS®]
Level 5	Mitigation of radiological consequences of significant release of radioactive substances.	Emergency control and on- and off-site emergency response.	SA C&I system (B-2/3) [Hardwired and/or embedded C&I]

* The table is created assuming the control system and the safety systems are not the initiator of the fault sequence. If the failure of one of these systems is the event initiator then that system is not available to provide defence in depth; however, it is observed that if one system is the initiator then with the exception of level 5 there is always a system still available to provide defence in depth at each level. Starting at level 1 it would multiple failures of independent C&I systems to lead to a severe accident condition.

14.3.2 Design Policy for C&I Systems Important To Safety

The design policy for the J-ABWR base line design follows Japan Safety Design and Japan Electric Association Guides (JEAG). The Japan Safety Design is the guidance made by Japanese government, Prime Minister's Secretariat Nuclear Safety Commission, in order to enhance objectivity and rationality for licensing safety review. The head document for this is 'Regulatory Guide for Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities, Mar. 2001' [Ref-22] further details are given below. The JEAGs are the guidelines produced by the private sector in order to explain, complement and supplement the Japan Safety Design.

The UK ABWR development follows a similar approach as past practice using Japan Safety Design and JEAG. However, it includes the latest IAEA guidance, (e.g. SSG-39 [Ref-23]) and additionally follows the guidance within SAP and TAG, as well as the requirements of IEC standards. It also takes cognisance of ONR guidance including the Safety Assessment Principles (SAPs) and the Technical Assessment Guides (TAGs), e.g. T/AST/003, Sep. 2011 and NS-TAST-GD-046, Apr. 2013 recognising the SAPs and TAGs are ONR's guidance to its inspectors. See Figure.14.3-2. It is noted that in both cases the start point is the documents of the IAEA Safety Standard series.

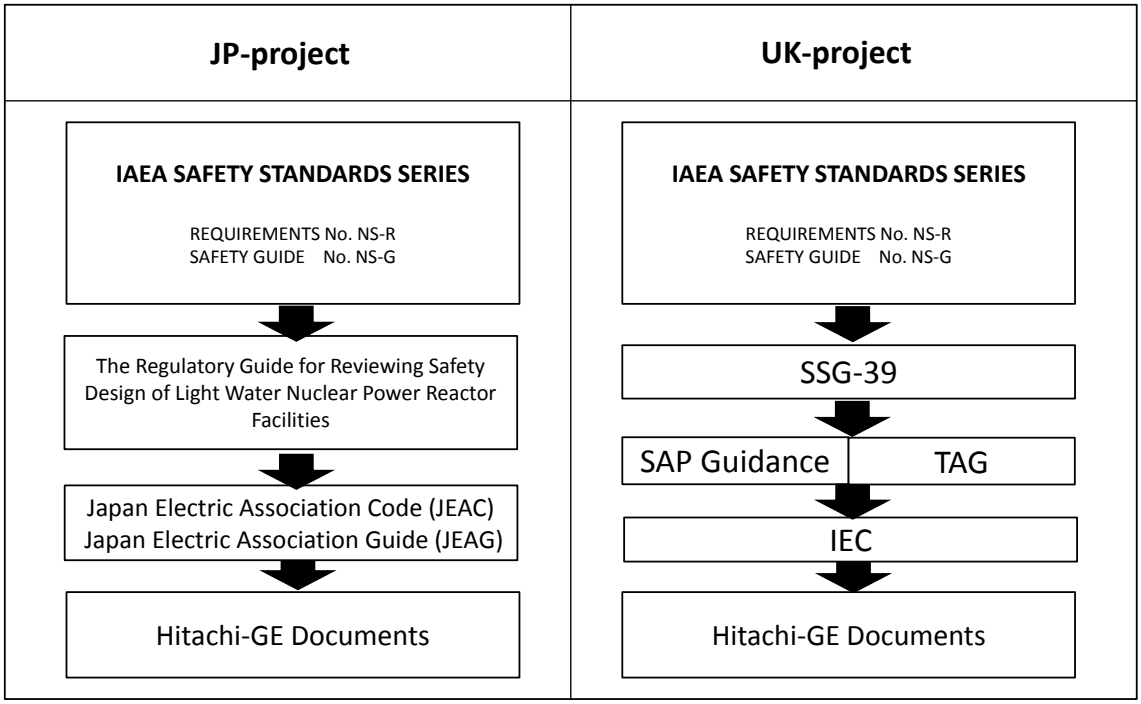


Figure 14.3-2: Design guidelines

Table 14.3-3 gives examples of extracts from the Regulatory Guide for Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities, Mar. 2001 [Ref-22]. Table 14.3-4 provides an example of a comparison of Regulatory Guide for Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities and the JEAC, JEAG, SSG-39, and the SAPs.

Table 14.3-3: Example of Regulatory Guide for Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities

1	Defence in Depth (Guide #9)
	Classify structures, systems and components with a safety function into the following two categories based on the "Review guide for Classification of Importance of Safety Functions for Light Water Nuclear Power Reactor Facilities" (hereinafter referred to as the "Importance Classification Guide"):
2	Redundancy of the safety protection system (Guide #34)
	The safety protection system shall be designed to have redundancy so as not to lose its safety protection function even when a single failure occurs to any of the components or channels (e.g. divisions of the SSLC) that constitute the system or when a single item is removed from use (e.g. for maintenance).
3	Independence of the safety protection system (Guide #35)
	The safety protection system shall be designed to allow the channels that constitute the system to be separated physically and electrically from each other so as to prevent failure propagation and its safety protection functions from being lost during normal operation, maintenance, repair, testing and abnormal condition, thus ensuring independence among the channels as much as practically possible.
4	Functions of the safety protection system during a transient (Guide #36)
	The safety protection system shall be designed to be able to detect abnormal condition during an accident condition, then automatically starting the appropriate systems including the reactor shutdown, emergency core cooling and isolation of containment.
5	Functions necessary at an accident of the safety protection system (Guide #37)
	The safety protection system is designed to detect abnormal condition at an accident, subsequently starting the operation of the reactor emergency shutdown system automatically. It is also be designed to allow automatic actuation of engineered safety facilities, such as closure of the main steam isolation valves, operation of the emergency core cooling system and operation of the safeguard standby gas treatment system.
6	Functions of the safety protection system at a failure (Guide #38)
	Electric power or instrumentation air will be used for the drive power of safety protection system. Valves used in this system are designed to be fail-safe or to actuate to maintain the current condition (fail-as-is) no sooner than a failure occurs. The design of the valves ensures that even in the case of fail-as-is condition, protective operation is actuated by another circuit provided redundantly.

7	Separation of the safety protection system and the instrumentation and control system from each other (Guide #39)
	The safety protection system and the instrumentation and control system are designed to be separated from each other, separating their power sources, detectors, cable routes and the instrumentation piping that pass through the reactor containment, as a rule.
8	Possibility for the safety protection system to be tested (Guide #40)
	The reactor emergency shutdown operation circuit is constituted in four channels. Each channel, receiving signals input from a detector divided into four sections respectively for one measurement variable, constitutes a 2-out-of-4 trip logic circuit. The reactor emergency shutdown operation circuit is designed to allow itself to be tested even during operation of the reactor.
9	Control room (Guide #41)
	The main control room (MCR) shall be designed to permit monitoring the operating condition of the reactor, the major related facilities, the major parameters, and to permit quick manual operation to secure safety when such manual operation is necessary.
10	Other guides include
	The UK ABWR, the design policy has been demonstrated (in GDA) to satisfy SAP guidance.

Table 14.3-4: Comparison summary for Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities

No.	Regulatory Guide for Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities, Mar 2001		JEAC*	JEAG*	IAEA (SSG-39)	SAP
1	Considerations for design against fires	#5	4626	4103,4607		ESS.10
2	Considerations for design against environmental conditions	#6		4621,4623	8.87 to 8.90	EAD.2, ESS.10, ERC.2
3	Considerations for design regarding operation by operators	#8		4617	7.18 to 7.26, 8.47 to 8.50	ESS.8,14
4	Considerations for design concerning reliability	#9	4604,4605 4620	4611	6.6 to 6.10, 7.7,7.96	EKP.1, EDR.2,4 ERL.1, ESS.2, 10
5	Considerations for design concerning testability	#10	4604,4620	4609,4611	6.161 to 6.167	EMT.7
6	Independence and testability of reactor shutdown system	#14				ESS.10
7	Reactivity control system	#15			6.161 to 6.167 6.24 to 6.31	ERC.2
8	Shutdown margin of reactor by control rods	#16				ESS.1,10 ERC.2
9	Shutdown capability of reactor shutdown system	#17			6.24 to 6.31	ESS.1,10
10	Emergency core cooling system	#25				ESS.12
11	Considerations on design against blackout	#27	4603		7.62	ESS.12,16
12	Redundancy of the safety protection system	#34	4604,4605 4620	4611	6.14 to 6.23, 7.30	EDR.1,2,3,4 ESS.24
13	Independence of the safety protection system	#35	4604,4620	4611	6.24 to 6.31, 7.30	EDR.2,3 ESS.18,20
14	Functions of the safety protection system during a transient	#36	4604,4620	4611	7.16,7.17	ESS.4,6,7,8
15	Functions necessary at an accident of the safety protection system	#37	4604,4620	4611	7.16 to 7.20, 8.1,8.2	ESS.1,4,6,7,8
16	Functions of the safety protection system at a failure	#38	4604,4620	4611	6.66 to 6.78, 7.46 to 7.49	EKP.2, EDR.1 ESS.12,17,21
17	Separation of the safety protection system and the instrumentation and control system from each other	#39	4604,4620	4611	6.32 to 6.39, 6.46 to 6.58, 7.50	EDR.1, ESS.12,20

No.	Regulatory Guide for Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities, Mar 2001		JEAC	JEAG	IAEA (SSG-39)	SAP
18	Possibility for the safety protection system to be tested	#40	4604,4620	4609,4611	6.161 to 6.167	EQU.1, EMT.1,2,6,7 ESS.23
19	Control room	#41	4624	4617	8.1,8.2	ESS.3, 13, ESR.1, EHF1-10
20	Reactor shutdown from outside the control room	#42			8.13 to 8.18	ESS.3, ESR.1, EHF1-10
21	Consideration in design on control room habitability	#43			8.12	ESS.3, EHF1-10
22	On site emergency station	#44	4603,4615	4102,4627	8.13 to 8.18	ESS.3, ESR.1, EES8
23	Considerations in design on communications equipment	#45	4603		8.36 to 8.46	ESR.7
24	Instrumentation and control system	#47		4611	3.1 to 3.6	EKP.2, EDR.1 ESS.3,7,13, ESR.3,9
25	Electrical system	#48		4612	7.60 to 7.62	ESS.6,12,16, ESR.6
26	Fuel storage and handling systems	#49	4616			ESR.26
27	Monitoring fuel handling places	#51		4606		ESR.8
28	Surrounding radiological protection	#56	4615	4606		EKP.3,ECV.6
29	Radiation monitoring	#59		4606		EKP.3, ESR.8, ECV.6,7

* Full references for the JEAC and JEAG documents are given in Table 14.3-6.

14.3.3 Categorisation and Classification

(The references to the IECs standards in this section are in Table 14.3-5.)

Categorisation of functions and classification of systems is introduced in Generic PCSR Chapter 5, section 5.6: Categorisation of Safety Functions and Classification of Structures, Systems and Components (SSCs); this section outlines the C&I interpretation of this.

The categorisation of the UK ABWR functions follow the practice of functional categorisation used in the UK, see Generic PCSR Chapter 5, section 5.6; i.e. following SAP, 2014 Edition, Revision 0, ECS.1 and IEC61226, with 3 safety categories A to C of safety functions. The systems that provide the functions above are classified in accordance with their importance to safety using the safe requirements of 'principal role,' 'significant contribution' and 'other' see SAP ECS.2. The categorisation of the function and the classification of the system are directly linked; i.e. Category A functions are implemented in Class 1 systems as identified in IEC61513 and IEC61226. However,

IEC61226 and ONR guidance allows some relaxation; for example a Class 2 system may be used to deliver a Category A function in the case where 1) it is already delivered by a Class 1 system, i.e. first line provision, and 2) the additional reliability required of the second line provision is not onerous. This approach has been adopted for the UK ABWR Hardwired Backup System which performs Category A functions but is a Class 2 system; a justification of this is provided as part of the Basis of Safety Cases for the Hardwired Backup System [Ref-7].

More detailed information is given in Generic PCSR Chapter 5, section 5.6: Categorisation of Safety Functions and Classification of Structures, Systems and Components (SSCs). The information of Category and Classification is developed in Basis of Safety Cases on Control and Instrumentation Architecture [Ref-5].

14.3.4 Codes and Standards

(The references to the IECs standards in this section are in Table 14.3-5.)

The generic approach to standards for the UK ABWR is presented in Generic PCSR Chapter 5, section 5.8.3: for C&I.

The intention for the UK ABWR is to make use of IEC standards and, where appropriate, to demonstrate that the development processes and practices currently used are, as a minimum, compatible (compliant) with IEC standards. Hence, in the case of function categorisation the intention for the UK ABWR is to comply with the requirements of IEC61226, as set out in section 14.3.3 above. The system class follows from the categorisation of the function (see IEC61513) but with some relaxation possible where the reliability claims are reduced, for example for the Hardwired Backup System.

As indicated above, the existing system development processes and practices are based on Japanese guidance but for the UK ABWR it is shown during GDA to be compliant with IEC61513, supported by IEC61508 as required. The C&I design process for UK ABWR which follows IEC 61513 is shown in C&I Design Process Plan [Ref-42]. For the development of the Class 1 systems for Category A functions the compatibility of the Hitachi-GE processes with IEC60987 for computer hardware and IEC62566 for complex programmable devices has been demonstrated. A similar approach has been adopted for the development processes of the Class 3 systems for Category B and C functions. The main control loops are and will continue to be on the HIACS platforms; hence IEC62138 and IEC60987 are the relevant standards for software and hardware for the demonstration (in GDA) of compliance. IEC61508 is used where there are gaps in the IEC nuclear standards, e.g. requirements associated with probabilistic claims.

The IEC nuclear standards have been taken as the basis of this exercise. Table 14.3-5 identifies the top tier of the IEC nuclear standards for the C&I design. These IECs are the primary standards which are fundamental for system design and implementation. There are a number of related IEC standards which are described in the C&I Architecture BSCs and carried through the C&I system BSCs [Refs-5 to 12].

Table 14.3-5: IEC Nuclear Standards

No.	Document Name
IEC61226, Ed 3.0, Jul. 2009	Nuclear power plants – instrumentation and control systems important for safety – classification of instrumentation and control functions
IEC61513, Ed 2.0, Aug. 2011	Nuclear power plants – instrumentation and control for systems important to safety – general requirements for systems
IEC62138, Ed 1.0, Jun. 2014	Nuclear power plants – instrumentation and control important for safety – software aspects for computer-based systems performing category B or C functions
IEC 60987, Ed 2.1, Feb. 2013	Nuclear power plants – instrumentation and control important to safety – hardware design requirements for computer-based systems
IEC62566, Ed 1.0, Jan. 2012	Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions

These primary standards are linked to lower tier IEC standards described in each C&I system BSCs [Refs-5 to 12]. Compliance has been confirmed by identifying the relevant C&I design specification for each clause of the applicable IEC standards.

Table 14.3-6 provides a cross reference from the JEAG and JEAC used for the development of the reference plant KK-6 & 7 to the IEC standards that are used for the UK-ABWR. The main link between the top tier IEC standards and the JEAG and JEAC are: JEAG 4611and 4612 (Cat & Class), JEAG 4609 (Verification and Validation) and JEAC 4620 (digital technology).

Table 14.3-6: Japanese Guides and Codes related IEC/TC45 Standard

No.	Document Name	Related IEC/TC45 Standard
JEAG 4102-2010	Guide for contingency plan of nuclear power plant	IEC60768, Ed 2.0, Apr. 2009 IEC60951-1, Ed 2.0, Jun. 2009
JEAG 4103-2009	Guide for management of fire protection for nuclear power plants.	
JEAG 4121-2009	Guideline for quality assurance regulations of safety in nuclear power plants (JEAC4111-2009) -Operation stage of the nuclear power plant	IEC60515, Ed 2.0, Feb. 2007 IEC60671, Ed 2.0, May. 2007 IEC61771, Ed 1.0, Dec. 1995
JEAG 4601-2008	Guidelines for Nuclear power plant seismic design technical	IEC60980, Ed 1.0, Jun. 1986
JEAG 4606-2017	Guideline for radiation monitoring of nuclear power plants	IEC60768, Ed 2.0, Apr. 2009 IEC61504, Ed 1.0, May. 2000
JEAG 4607-2010	Guideline for fire protection of nuclear power plants	
JEAG 4609-2008	Guidelines for verification and validation of digital safety protection systems of nuclear power plants.	IEC60880, Ed 2.0, May. 2006
JEAG 4611-2009	Guide for design of instrumentation & control equipment with safety functions	IEC61226, Ed 3.0, Jul. 2009
JEAG 4612-2010	Guidelines for Severity classification of electrical and mechanical device with safety function	IEC61226, Ed 3.0, Jul. 2009
JEAG 4617-2013	Guide for development and design of computerized human-machine interfaces in the main control room of nuclear power plants	IEC60964, Ed 2.0, Feb. 2009 IEC61227, Ed 2.0, Apr. 2008 IEC61772, Ed 2.0, Apr. 2009 IEC61839, Ed 1.0, Jul. 2000 IEC62241, Ed 1.0, Nov. 2004 IEC61771, Ed 1.0, Dec. 1995
JEAG 4621-2007	Guideline for Drift evaluation of safety protection system instrument	IEC62342, Ed 1.0, Aug. 2007
JEAG 4623-2008	Guideline for environmental qualification method of safety related electrical and I&C equipment for nuclear power stations	IEC60780, Ed 2.0, Oct. 1998
JEAG 4627-2010	Guide for design of emergency response centre for nuclear power plants	IEC60960, Ed 1.0, Aug. 1988
JEAC 4111-2009	Quality assurance managements for safety in nuclear power plants	IEC60515, Ed 2.0, Feb. 2007 IEC60671, Ed 2.0, May. 2007 IEC61771, Ed 1.0, Dec. 1995

No.	Document Name	Related IEC/TC45 Standard
JEAC 4601-2008	Nuclear power plant seismic design technology regulations	IEC60980, Ed 1.0, Jun. 1986
JEAC 4603-2010	Code for design of security equipment for nuclear power plants	IEC62443-1-1, Ed 1.0, Jul. 2009
JEAC 4604-2009	Code for design of safety protection systems for nuclear power plants	IEC60671, Ed 2.0, May. 2007 IEC61513, Ed 2.0, Aug. 2011
JEAC 4605-2004	Regulations defining the scope of the related facilities and nuclear power plants engineered safety features	IEC60768, Ed 2.0, Apr. 2009 IEC60951-1, Ed 2.0, Jun. 2009
JEAC 4615-2008	Code for design of radiation shielding for nuclear power plants	
JEAC 4616-2009	Technical regulations for the design of infrastructure of spent fuel interim storage building using dry cask	IEC62235, Ed 1.0, Mar. 2005
JEAC 4620-2008	Code of application of digital computers to safety protection systems of nuclear power plants	IEC60880, Ed 2.0, May 2006 IEC60987, Ed 2.1, Feb. 2013 IEC61500, Ed 2.0, Oct. 2009 IEC61513, Ed 2.0, Aug. 2011 IEC62138, Ed 1.0, Jun. 2014 IEC62340, Ed 1.0, Dec 2007
JEAC 4624-2009	Code for equipment design to reduce operational errors in the main control room of nuclear power plants	IEC60964, Ed 2.0, Feb. 2009 IEC61227, Ed 2.0, Apr. 2008 IEC61772, Ed 2.0, Apr 2009 IEC 61839, Ed 1.0, Jul. 2000 IEC62241, Ed 1.0, Nov. 2004 IEC61771, Ed 1.0, Dec. 1995
JEAC 4626-2010	Code for fire protection of nuclear power plants	

14.3.5 Qualification

The C&I system are qualified for seismic, environment, EMC according to predefined standards (e.g. tier 2 nuclear standards).

The C&I equipment used in the J-ABWR has been qualified in accordance with ISO 9001:2008 [Ref-24], IAEA Safety Requirement No.GS-R-3, environmental management based on ISO 14001:2004 and IEC 61000 series for EMI. Hitachi-GE followed these requirements in addition to the requirement from JEAG and JEAC and test procedures and work instructions.

For the UK ABWR the qualification of the C&I equipment to demonstrate that it is robust to hazards such as seismic, EMI and environment has been performed for GDA to IEC standards including IEC/IEEE 60780-323 (qualification), IEC60980 (seismic) and 61000 series (EMI).

Where possible, the existing proven documented test methods have been demonstrated as being compatible with the standards identified above and will be used to conduct the testing and demonstration of compliance. Items of C&I equipment that is required in extreme environmental conditions, such as equipment inside the containment or which is required in the event of the severe accident, will be reviewed on an individual basis to determine their qualification requirements post GDA.

14.3.6 Justification

The justification of the C&I systems follows the Claims Arguments Evidence (CAE) approach. The Fundamental Safety Functions (that apply to the whole plant) and High Level Safety Functions are included in the PCSR with key arguments. The detailed Safety Function Claims are developed for each C&I system in the BSCs for the respective system. The Safety Property Claims, which include separation, diversity and performance requirements, are developed in the C&I Architecture BSCs and relevant C&I system BSCs. Part of the performance requirements are bounded as described in the Fig. 4.10-1 of Generic PCSR Chapter 4, section 4.10.

The detailed safety cases for the complex systems such as the main safety system (the SSLC) are presented in Basis of Safety Cases documents, these are referenced from the PCSR. These safety cases will be developed as the systems are designed in detail, implemented then commissioned and set to work. The justification includes demonstration that the development processes and developed products meet with good practice and are compliant with modern (IEC) standards; e.g. Production Excellence. The totality of the information (evidence) required to complete the system justification will not be available at the outset. For example, the evidence of Production Excellence and standards compliance will be generated during detailed design and implementation of the systems as part of the site specific phase of the project. Other evidence from commissioning testing and the programme of Independent Confidence Building Measures (ICBM), including the analysis and testing of the product, will only be generated once the final systems are available. Most of this evidence will be generated post GDA phase.

Confidence in the capability of the C&I systems to perform their safety role will not be solely dependent on this final evidence. Confidence in the capability of the C&I systems developed during the site specific phase will grow with high quality evidence produced during the detailed design phase and will continue with verification activities and important phases of the project such as factory acceptance tests. This means that there will be a high degree confidence in the ability of the C&I systems to perform their safety role before the final activities of independent confidence building and site commissioning are undertaken.

An important element is having a document structure that will be suitable for the post GDA phase. For C&I, during GDA a document structure has been developed with BSCs for each C&I System supported by a series of Topic Reports and more detailed technology Topic Reports. The document structure for GDA is shown in Appendix C. This document structure has been designed to readily cope with additional and more detailed information that will be produced in the post GDA phase.

The system BSCs are for the:
(1) Control and Instrumentation Architecture [Ref-5],
(2) SSLC including safety system platform and application [Ref-6],
(3) Hardwired Backup System [Ref-7],
(4) Safety Auxiliary Control System [Ref-8],
(5) Plant Control System [Ref-9],
(6) Severe Accident C&I System [Ref-10],
(7) Reactor / Turbine Auxiliary Control System [Ref-11], and
(8) Plant Computer System [Ref-12].

These BSCs are supported by system specific Topic Reports and by equipment and technology Topic Reports (Examples are shown in Appendix C).

Topic Reports are produced where a need is identified to provide a detailed explanation, justification, evidence or references to evidence. References to the appropriate Topic Report are provided in the BSCs documents where appropriate.

14.4 Claim Architecture

This section sets out the claims for the C&I Architecture, systems and equipment. It identifies the sources of the Safety Functional Claims. It also identifies the non-functional Safety Property Claims such as independence, segregation, diversity, reliability and the standards to be met in equipment design, construction and operation.

14.4.1 Safety Functional Claim

The Safety Functional Claims (SFC) are defined based on the Fundamental Safety Functions (FSFs) [Generic PCSR Chapter 5, section 5.6.2: UK ABWR Safety Functions, and section 3.2.1 of Ref-26], these relate to Criticality, Cooling and Containment. The five FSFs are developed to generate the High Level Safety Functions (HLSFs) [Table 5.4-1 and sub-section 3.6 of Ref-26]. The 56 HLSF are relevant to all technical areas and are the starting point for generating Safety Functional Claims (SFCs) for each technical area. The SFCs for the C&I are identified on a system basis and are related to the HLSF by the first two numbers of their identifier that match the HLSF.

14.4.1.1 Claims and Link to High Level Safety Functions

The list of C&I SFC claims in this section and the linkage to corresponding High Level Safety Functions is shown in Appendix A1 and A2. A short description on the application of High Level Safety Functions in the development of the claims, arguments and evidence is provided in Generic PCSR Chapter 1.

14.4.2 Safety Property Claim

The Safety Property Claims (SPCs) are defined based on good engineering practice from standards, UK ABWR Nuclear Safety and Environmental Design Principles (NSEDPs) [Ref-1] and IAEA guides that consequently results in the systems being consistent with the expectations in the SAP, 2014 Edition, Revision 0. The C&I SPCs are described in the Appendix B. The table of SPCs, shown in Appendix B, were derived for the topic covered in this chapter based on the ‘guide word’ approach specified in Hitachi-GE’s Safety Case Development Manual [Ref-37].

14.5 C&I Architecture

This section describes the evolution, and identifies the totality, of the C&I Architecture. This includes the:

- Plant Control System, Reactor / Turbine Auxiliary Control Systems and Plant Computer System (PCntlS, ACS and PCS) for startup and power operation,
- Safety System Logic and Control System (SSLC) which includes the Reactor Protection system (RPS), Emergency Core Cooling system / Engineered Safety Features (ECCS/ESF)), Safety Auxiliary Control System (SACS) and Hardwired Backup System (HWBS) for safety, and
- Severe Accident C&I (SA C&I), for severe accident mitigation.

The C&I architecture considers the classification, categorisation, independence and diversity requirements from IEC61226. Figure 14.5-1 is a single line diagram of the architecture showing schematically the systems and their inputs and outputs / connections to other systems.

The description of the architecture does not include the C&I safety and safety related equipment in the support systems such as the protection relays in the electrical system or the ancillary equipment such as the control system for fuel handling. The electrical system equipment is described and assessed in the Generic PCSR Chapter 15 and high level principles for the architecture design of ancillary equipment, including embedded C&I and fuel, detailed in section 8 of this chapter.

14.5.1 Introduction

The architecture has been divided into a hierarchy with 3 levels as identified in the following table.

Hierarchy level	Main Function
Level 1	The main Human-Machine Interface and overall unit operation, monitoring control / data management functions
Level 2	The control and protection processing equipment including automatic equipment and that interfacing the Level 1 equipment to the sensors and actuators.
Level 3	Local monitoring and control function / sensors and actuators

(1) Level 1

There are major Human-Machine Interfaces in four locations: Main Control Room (MCR), Remote Shutdown Station (RSS), the Backup-Building (B/B) and Radwaste facility. These are applied as the operator interface at the plant level.

The malfunction of these C&I devices does not prevent the safe operation or shutdown of the plant provided by the level 2 and 3 C&I equipment.

(2) Level 2

This level contains the main processing equipment for automatic control and protection of the plant including the Plant Control System, Reactor / Turbine Auxiliary Control systems, SSLC, SACS, HWBS and Plant Computer System. It also includes the equipment providing the interface between the plant

sensors and actuators and the level 1 control, monitoring and recording equipment. The majority of this equipment is implemented using complex electronics, e.g. digital and programmable C&I systems; the major exception being the Hardwired Backup System.

(3) Level 3

This level includes the sensors and actuators and their local processing equipment. This level interfaces with level 2 systems to receive actuation signals and transmit measured values.

14.5.2 Overall C&I Architecture

The C&I architecture is shown in Figure 14.5-1 and indicates schematically each major C&I system and the communication links.

The C&I architecture has the eight major groupings of systems in the baseline design:

(1) Safety System Logic and Control System,
(2) Hardwired Backup System,
(3) Safety Auxiliary Control System,
(4) Plant Control Systems,
(5) Severe Accident C&I System,
(6) Reactor / Turbine Auxiliary Control Systems,
(7) Plant Computer Systems, and
(8) Other System.

These eight groups are identified in Figure 14.5-1. Note, the HMI is shown as a separate block; however, the HMIs are considered as part of the individual systems.

The basic architecture of the C&I systems is designed to limit propagation of failures so far as is reasonably practicable by use of separation, segregation and isolation and provide defence against loss of functions by redundancy. It implements information transmission between systems according to their classification; i.e. Class 2 and 3 C&I systems do not input to Class1 C&I systems. A schematic of the connection of the systems showing the type of connection and the direction of the data flow is shown in Figure 14.5-1. This shows the interconnecting of elements of the architecture.

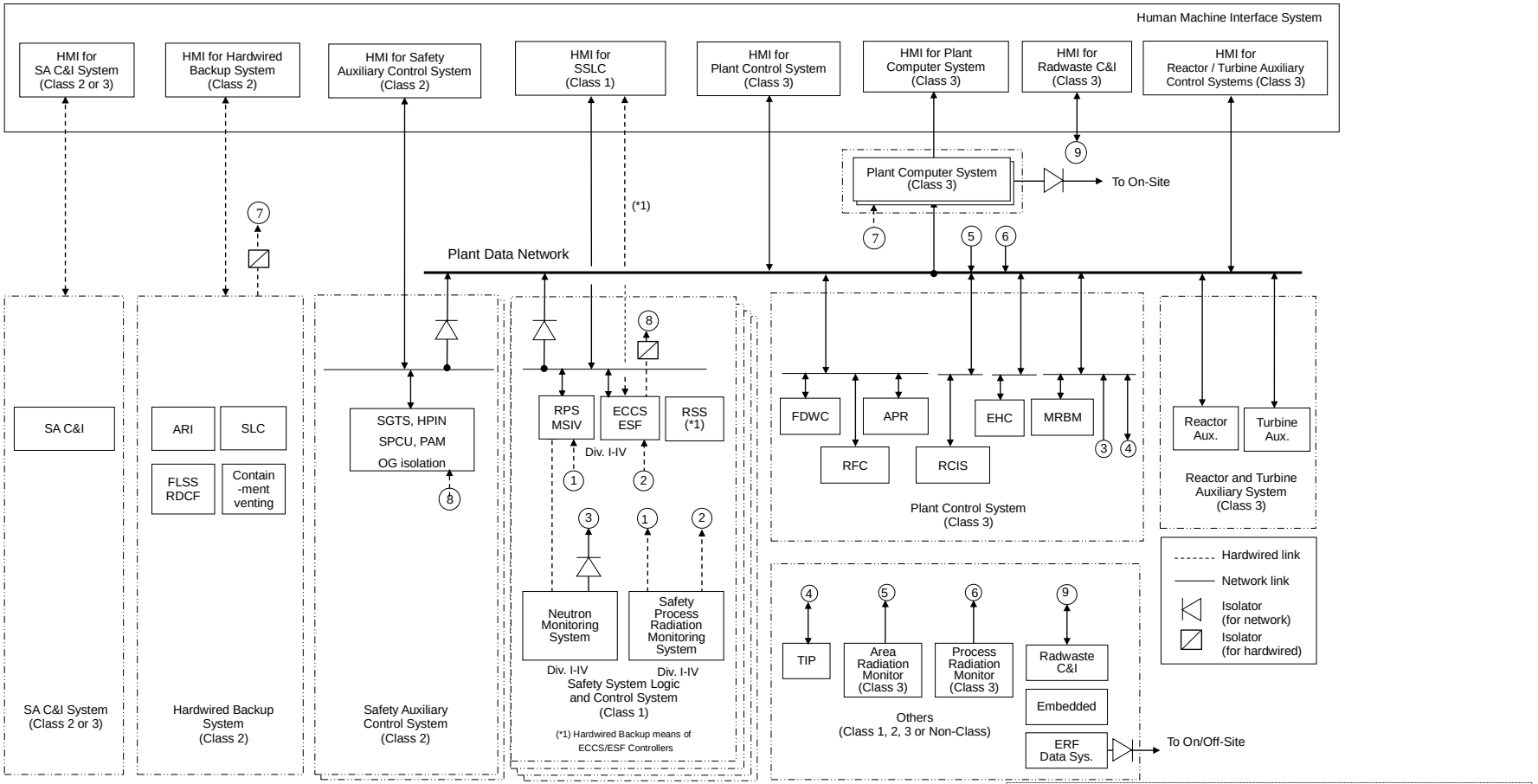


Figure 14.5-1: High level schematic of C&I Architecture

APR: Automatic Power Regulator System, ARI: Alternative Rod Insertion, Aux: Auxiliary
CCF: Common Cause Failure, ECCS: Emergency Core Cooling System,
EHC: Turbine Electro-Hydraulic Control System, ERF:Emergency Response Facility
FDWC: Feedwater Control System
FLSS: Flooding System of Specific Safety Facility, HMI: Human Machine Interface
HWBS: Hardwired Backup System, MRBM: Multi Rod Block Monitor, OG: Off-Gas System
PAM: Post Accident Monitoring System, RCIS: Rod Control and Information System,
RDCF: Reactor Depressurisation Control Facility, RFC: Recirculation Flow Control System
RPS: Reactor Protection System, RSS: Remote Shutdown System, SLC: Standby Liquid Control System
SSLC: Safety System Logic and Control System, TIP: Traversing In-Core probe

14.5.3 Location of Architecture Elements

The section presents the physical location of the systems and the divisions of equipment to show that they meet the requirements for physical separation as part of reliability enhancement, defence against common cause failure, e.g. due to internal hazards, and consideration of radiation protection.

(1) Locations
The Level 1 HMIs are in separate locations: Main Control Room, Remote Shutdown System Panel Rooms, Radioactive Waste Building Main Control Room and Backup-Building Control Panel Room. The HMI in the MCR is for all the major C&I and other, e.g. electrical, systems regardless of their Class.

The MCR contains:

- SSLC Class 1 HMI,
- Safety Auxiliary Panel, i.e. SSLC manual HMI,
- Hardwired Backup Panel, i.e. HWBS manual HMI*,
- Plant Control System Class 3 HMI,
- Plant Computer System Class 3 HMI,
- Reactor / Turbine Auxiliary Control System Class 3 HMI, and
- Safety Auxiliary Control System Class 2 HMI.

* If it is available, the HMI is also used for the SA management.

The RSS contains:

- Class 1 segregated Reactor Shutdown Panels each which can be used to achieve cold shutdown from hot shutdown when the MCR become unavailable.

The Backup-Building contains:

- Manual controls and monitoring HMIs for the SA management.

The Radwaste facilities contains:

- HMIs for the radioactive waste facilities.

The details are described in Generic PCSR Chapter 21, and related Basis of Safety Cases [Ref-3, 27, 28, 29, 30].

The Level 2 major electronics are primarily in the control building. The control systems are in their own room separate from the four divisions of the SSLC electronics which are each segregated into divisional panel rooms. Both systems are located separately from the room containing the HWBS equipment. The rooms individually provide protection from hazards including fire i.e. each room is in a separate fire zone to protect from fire.

The Level 3 sensors and actuators are located around the plant with steps taken to maintain the separation of equipment belonging to different systems and also equipment belonging to different divisions of the SSLC. Arrangements of the major plant associated with the SSLC located in the Reactor Building are shown in Figure 14.5-2. One important exception to this separation of location are the sensors from different systems that share connection to the RPV for pressure and water level measurements as illustrated in Figure 14.7-1.

(2) System interconnections

Figure 14.5.1 shows the interconnection of the C&I systems. The four divisions of the Class 1 SSLC C&I are isolated from the other systems and can only transmit to other C&I system. Similarly the Hardwired Backup System transmits information directly to the Plant Computer System. The two systems are also directly connected to their displays in the main control room.

The divisions making up the SSLC are designed with dedicated cable trays, electric lines, instrumentation piping, instrument racks and the link for each division so that interference between the divisions will not occur. The divisions are also designed so that each one is independent and separated physically and isolated electrically as far as possible from the other divisions. The segregation of the four divisions allows for them to be protected individually against hazards such as fire providing defence against common loss of safety functions. Schematic of Reactor Building C&I location is shown in Figure 14.5-2.

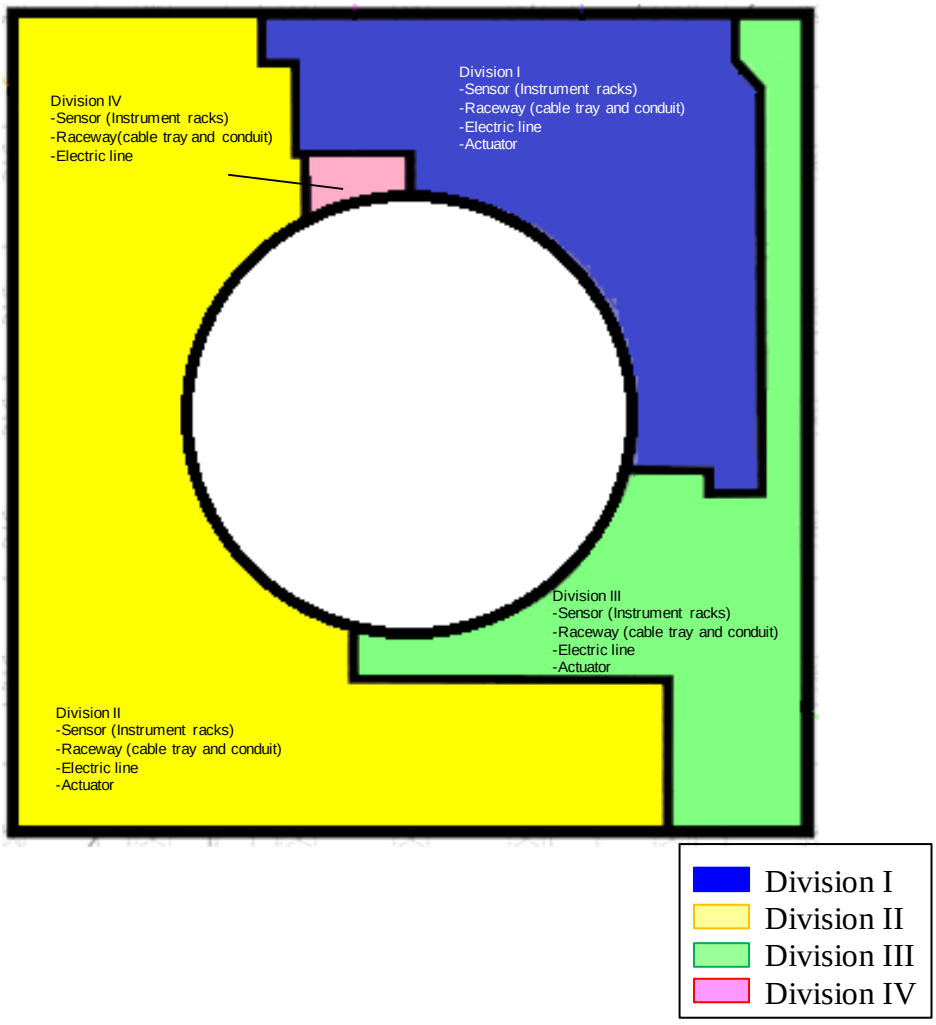


Figure 14.5-2: Schematic of Reactor Building C&I location

(3) Radiation protection

Radiation Protection and decommissioning aspects are considered in the development of the C&I architecture and positioning of the equipment. The priority is to locate the potentially sensitive C&I electronics away from high radiation fields that might adversely affect its performance. The equipment located in high radiation zones is minimised, this (a) reduces the dose to staff during inspection, maintenance, repair and calibration activities; (b) removes potentially sensitive electronics from exposure to high radiation and (c) reduces the volume of equipment that might become activated hence the amount of waste arising in decommissioning. Major exceptions to this policy include in the core neutron flux detectors and the sensing lines for pressure and differential pressure instruments used for measurement pressure, level and flow.

14.6 Control and Instrumentation Systems

The design of the individual C&I systems that make up the C&I Architecture is in accordance with the Hitachi-GE principles and practice for C&I see Sections 14.3 and 14.10 of this chapter. The systems deliver the Safety Functional Claims detailed in section 14.4.1 of this chapter, conform to IEC nuclear standards and satisfy the Safety Property Claims detailed in section 14.4.2 of this chapter.

14.6.1 Introduction

The C&I consists of the following systems (please note the control systems are directly classified) with a target reliability and probability of failure. The target reliability and probability of failure are derived from the numerical targets shown in Generic PCSR Chapter 5, section 5.6.

Plant Status	Systems	Category	Class	Target reliability, Probability of Failure
Normal	Plant Control System (PCntlS)	-	3	$1x10^{-1}$/yr, N/A
	Reactor/Turbine Auxiliary Control System (ACS)	-	3	$1x10^{-1}$/yr, N/A
	Plant Computer System (PCS)	-	3	N/A, N/A [Note 1]
Fault Condition	Safety System Logic and Control System (SSLC) • Reactor Protection System • Emergency Core Cooling System/ Engineered Safety Features	A	1	$1x10^{-4}$/yr, $1x10^{-4}$ pfd
	Safety Auxiliary Control System (SACS)	B	2	$1x10^{-2}$/yr, $1x10^{-2}$ pfd
	Hardwired Backup System (HWBS)	A	2	$1x10^{-2}$/yr, $1x10^{-2}$ pfd
Severe Accident	Severe Accident C&I (SA C&I) (for principle role or the part sharing with HWBS)	B	2	$1x10^{-2}$/yr, N/A [Note 2]
	Severe Accident C&I (SA C&I) (for backup role)	B	3	N/A, N/A [Note 1]

[Note 1] The PCS and SA C&I systems are not required to demonstrate the overall numerical plant safety targets. Therefore, no specific target is set.
[Note 2] The part of SA C&I system shared with the HWBS meets the reliability targets imposed on the HWBS to ensure the SA C&I does not impede the delivery of a HWBS safety function.

The C&I systems monitor and control the plant through operating condition transitions, e.g. change of load, or disturbance which could occur during power operation. The systems also include those required to bring the plant to a safe state in the event the capability of the normal control systems is exceeded and mitigate the consequences of an accident.

The automatic systems interface with Human-Machine Interfaces located in the Main Control Room which provide centralised management and monitoring of the plant, and the operator controls for the main systems.

The following systems are described:

- Section 14.6.2: Safety System Logic and Control including
  (1) Neutron monitoring system
  (2) Safety Process Radiation monitoring system,
- Section 14.6.3: Hardwired Backup System,
- Section 14.6.4: Safety Auxiliary Control System,
- Section 14.6.5: The main Plant Control Systems, including reactor power control system consisting of:
  (1) Recirculation Flow Control System,
  (2) Rod Control and Information System,
  (3) Electro hydraulic Turbine control system,
  (4) Feed water flow control system, and
  (5) Automatic power regulator,
- Section 14.6.6: Severe Accident C&I System,
- Section 14.6.7: Reactor / Turbine Auxiliary Control System, and
- Section 14.6.8: Plant Computer System.

For all systems the following topics are not addressed here but are considered in the system BSCs.

(1) Implementation,
(2) Qualification of platform, equipment and system,
(3) Commissioning,
(4) Operation and Maintenance,
(5) Ageing and Obsolescence, and
(6) Justification of system.

14.6.2 Safety System Logic and Control System

14.6.2.1 Safety System Logic and Control System

(1) Overview

Safety System Logic and Control System (SSLC) which is based on FPGA technology (νCOSS® platform) is provided for the purpose of protecting the reactor in the event of abnormal transients or spurious operation of systems (including C&I) which might possibly impair the reactor safety or in cases where the occurrence of such events is anticipated. In such cases, the SSLC detects these transients or spurious operations and initiates safety-protection operations for the purpose of preventing or suppressing such events. The SSLC contains the following sub-systems:

- Control of reactivity (shutdown the reactor): Reactor Protection System (RPS),
- Fuel Cooling, Long-term heat removal: Engineered Safety Functions (ESF) including Emergency Core Cooling System (ECCS), and
- Confinement/ Containment radioactive materials: Engineered Safety Functions (ESF) including Primary Containment and Isolation System (PCIS) and Main Steam Isolation Valve (MSIV).

The SSLC is supported by the Class 1 essential electrical supplies and HVAC; some functions require support from other services, e.g. hydraulic pressure, pneumatic supply of air or nitrogen and water.

A full description with the Safety Functional and Safety Property Claims for the system is given in the BSCs on SSLC [Ref-6].

(2) System Architecture Interfaces and Layout

The SSLC is the Class 1 main safety system and is the primary means of protecting both frequent and infrequent design basis faults. It has four divisions configured in a 2 out of 4 voting logic scheme to perform Category A functions to initiate a shutdown, isolate the primary containment vessel and actuate the three divisions of mechanical plant for core cooling. An overview of the system architecture is shown in Figure 14.6-1. These functions are required in order to bring the reactor to a controlled state and then a safe shutdown state in response to an event causing a challenge to the protection limits.

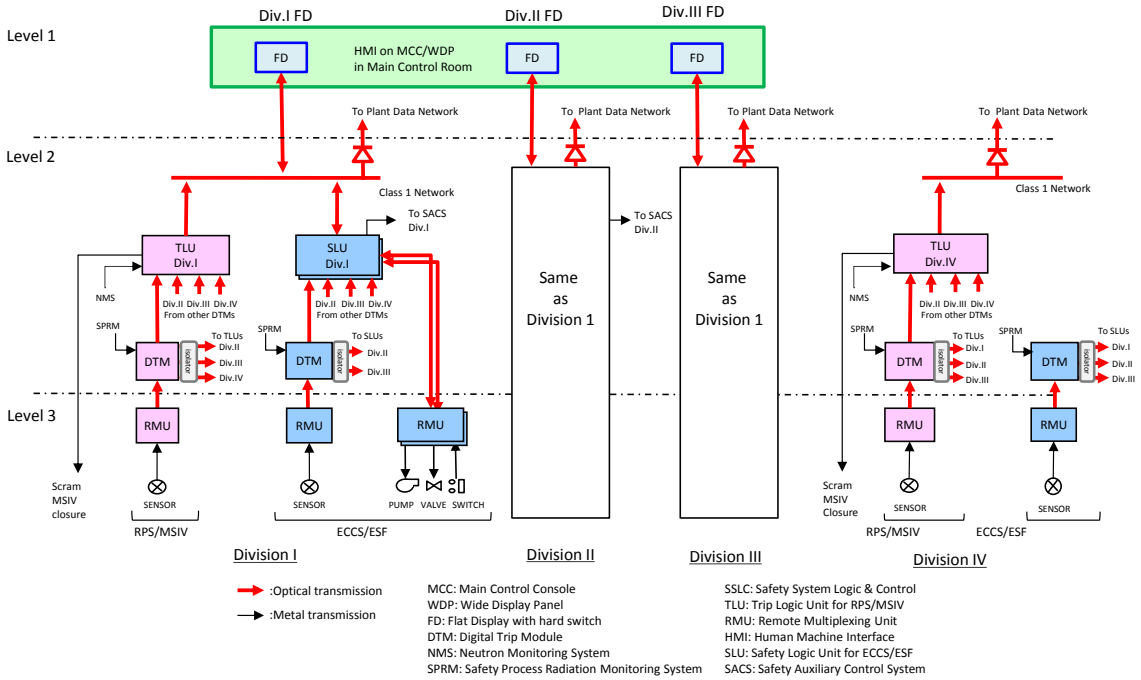


Figure 14.6-1: C&I Architecture of Safety System Logic and Control System (SSLC)

Each division is divided into two sub-systems, the SSLC (RPS / MSIV) and the SSLC (ECCS / ESF). The SSLC (RPS / MSIV) inserts the control rod and closes the main steam isolation valves to shut the reactor down and isolate the Reactor Pressure Vessel. The SSLC (ECCS / ESF) maintains core coverage, provides decay heat removal and related engineered safe guards including containment isolation. The SSLC is built on the νCOSS® platform which is diverse from HIACS, this diversity includes technology, development and communications.

The SSLC (RPS/MSIV) consists of four-divisions that are independent from each other and other C&I systems both electrically and physically. Each division contains its own Sensors, Remote Multiplexing Unit (RMU), Digital Trip Module (DTM), Trip Logic Unit (TLU), Output Logic Unit (OLU) and Load Driver (LD).

The SSLC (ECCS/ESF) consists of four divisions that are independent from each other and other C&I systems both electrically and physically. Each division contains sensors, Remote Multiplexing Unit (RMU), Digital Trip Module (DTM), but only three divisions contain Safety Logic Units (SLUs). The RMU is also used to output the signal from the SLUs to the actuators. The three divisions containing SLU each actuate a single division of the mechanical equipment required to deliver the ECCS and ESF functions.

(a) RPS/MSIV

(i) Overview

The RPS/MSIV detectors are divided into four divisions each with one or more sensor for every variable to be measured. Each of the four divisions uses the inputs signals from the detectors for that division to determine in the DTM if an abnormal plant state has occurred and outputs the state to TLUs of all four divisions. A trip is initiated when the DTM in two or more divisions detects an abnormal plant state, the vote is carried out in the TLU. The signals from each TLU are input into the Load Drivers (LDs) belonging to the corresponding trip channel via the Output Logic Unit (OLU) for that division. The reactor scram is initiated by the solenoid operated scram pilot valves when two or more divisions are tripped. The SCRAM (Emergency Shut Down System for Terminating the Reactor Chain Reaction) valves are actuated on a 2 out of 4 vote de-energise to trip of the solenoid operated scram pilot valves or 2 out of 4 energise to trip of the solenoid operated backup scram valves.

The RPS/MSIV also activates the load drivers for the MSIVs. These are connected to the two solenoid valves associated with each MSIV. The solenoid valves are de-energised on a 2 out of 4 logic vote of the load driver; both solenoid valves are required to open to release the gas pressure and close the MSIV.

Figure 14.6-2 shows the system architecture of SSLC (RPS/MSIV).

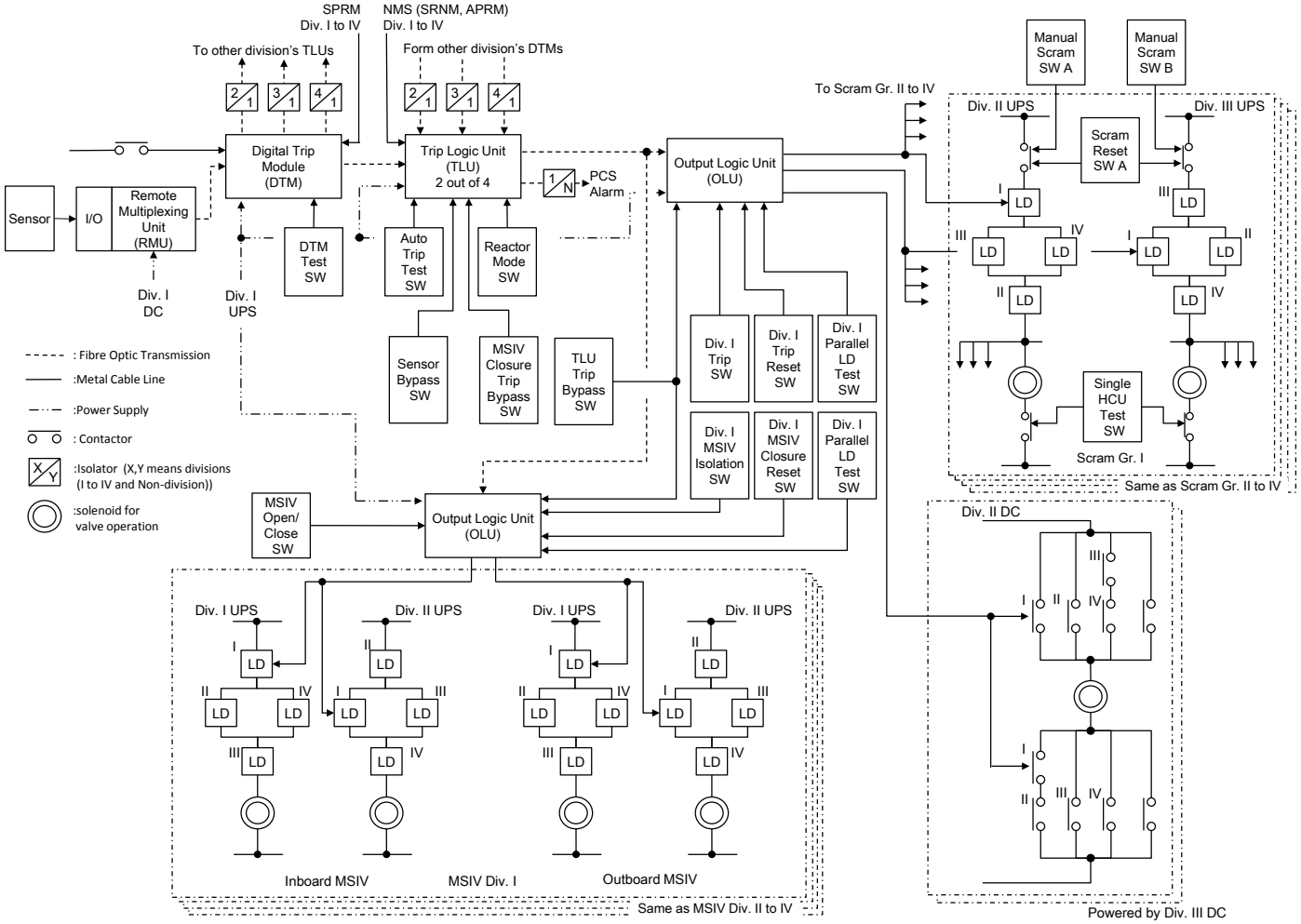


Figure 14.6-2: System Architecture of SSLC (RPS/MSIV)

(ii) Function at failure

The trip division output signals normally energise the load driver at all times during operation, a division trip demand will result if there are failures such as a loss of a trip division's power. The load driver and pilot valve solenoids are normally energised at all times during operation, and a trip demand will result if they are de-energised. Therefore, a trip demand will occur in most cases of failures such as loss of power, broken wires or short circuits in a division. The trip divisions are also designed so that a trip demand will occur in case of failure of the FPGA components. As a result, the circuit of the RPS is designed to fail in the safe direction for most failure conditions.

The failure of one trip division or load driver will not initiate the scram operation, as the scram function requires two load drivers to be de-energised as they have a 2-out-of-4 voting architecture. This prevents spurious RPS initiation caused by a single failure and implements scram by fail-safe operation against most failure conditions.

(iii) Initiation Logic

The initiation logic of the SSLC (RPS/MSIV) functions is set out below.

I. Reactor Scram initiation

SSLC RPS/MSIV automatically initiates reactor scram when the following conditions are detected in at least 2-out-of-4 divisions:

A) Reactor Pressure High,
B) Reactor Water Level Low,
C) Drywell Pressure High,
D) Neutron Flux High (APRM, TPM),
E) Neutron Flux Instrument Inoperative (APRM, SRNM),
F) Reactor Period Short (SRNM),
G) Core Flow Rapid Drop,
H) CRD Injection Pressure Low,
I) Main Steam Isolation Valve (MSIV) Closure,
J) Main Steam Stop Valve (MSV) Closure,
K) Steam Control Valve Rapid Closure,
L) Main Steam Line Radiation High,
M) Suppression Pool Temperature High, and
N) An additional function to protect against "all-rod-insertion".

SSLC RPS/MSIV manually initiates reactor scram by following.

O) Manual scram, and
P) Reactor Mode switch in 'shutdown mode'.

Reactor Mode Switch has 4 modes which cause some scram initiation logic to be bypassed as detailed below:

- "Shutdown"
  If this mode is selected, scram signals are output, and all the control rods are inserted into the core. Scram signals due to closure of the MSIV are bypassed automatically when the reactor pressure is low. Scram signals due to low CRD injection pressure can also be bypassed by using the bypass switch.
- "Refuel"
  Scram signals due to MSIV closure are bypassed automatically when the reactor pressure is low. Scram signals due to low CRD injection pressure can also be bypassed by using the bypass switch.

- "Start-up"
  In this mode, Scram signals due to MSIV closure are bypassed automatically when the reactor pressure is low.
- "Run"
  In this mode, scram signals due to Reactor Period Short or Neutron Flux Instrument Inoperative (SRNM) are bypassed.

II. MSIV closure initiation

SSLC RPS/MSIV automatically initiates MSIV closure when the following conditions are detected in at least 2-out-of-4 divisions:

A) Reactor Water Level Low,
B) Main Steam Line Pressure Low,
C) Main Steam Line Flow High,
D) Condenser Vacuum Low,
E) Main Steam Line Radiation High, and
F) Main Steam Line Tunnel Temperature High.

SSLC RPS/MSIV manually initiates MSIV closure by following.

G) Manual MSIV closure

(iv) Testability

I. RPS

The RPS has the following provisions for testing:

A) Manual actuation test of scram pilot valve,
B) Automatic actuation test of scram pilot valve,
C) Detector operation test, and
D) Control rod scram test.

II. MSIV

The MSIV has the following provisions for testing:

A) Automatic actuation test of MSIV,
B) Detector operation test, and
C) MSIV close test.

(b) ECCS/ESF

(i) Overview

The detectors are divided into four divisions each with one or more sensor for each variable to be measured. Each of the four trip divisions gathers sensor signals via the RMU to determine in the DTM if an abnormal plant state has occurred. The DTM outputs from the four divisions are shared with those of the other divisions in the SLUs of the three divisions containing mechanical plant. These three dual redundant SLU logic channels each actuate the mechanical equipment associated with one of the three ECCS/ESF divisions via an output RMU if at least 2-out-of-4 DTM inputs are voting to trip.
Figure 14.6-3 shows the system architecture of SSLC (ECCS/ESF).

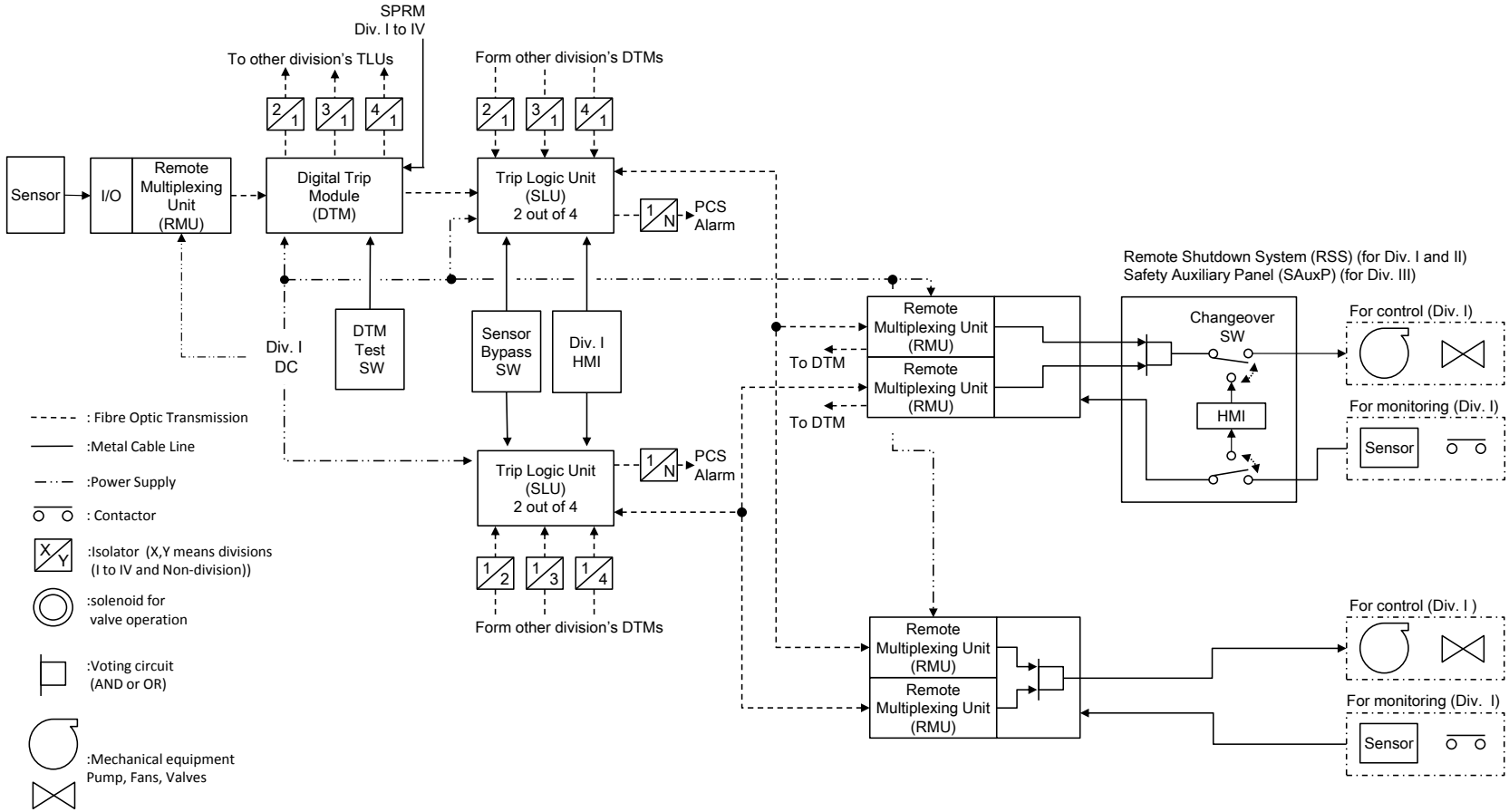


Figure 14.6-3: System Architecture of SSLC (ECCS/ESF)

(ii) Function at Failure

The design follows the fail-as-is principal with the exception of the PCIS (Primary Containment Isolation System) that follows a fail-safe approach. For example the ECCS/ESF (PCIS) will result in a "fail safe" when power source is lost. Note, the exception to the PCIS fail-safe approach is the RCIC which is fail-as-is to prevent isolation of function to add water to the core.

(iii) Initiation Logic

The initiation logic of the SSLC (ECCS/ESF) functions is set out below.

I. ECCS/ESF initiation

SSLC ECCS/ESF automatically initiates ECCS/ESF when the following conditions are detected in at least 2-out-of-4 divisions:

A) Reactor Water Level Low,
B) Drywell Pressure High,
C) HVAC Reactor Zones Exhaust Radiation High,
D) Refuelling Area Exhaust Radiation High,
E) System Leak Flow Rate High,
F) Equipment Room Temperature,
G) System Process Line Pressure Low, and
H) System Process Line Differential Pressure High.

SSLC ESF/ECCS manually initiates ECCS/ESF by the following.

I) Manual initiation switches for ECCS/ESF

(iv) Testability

Each detector and the voting logic for the ECCS/ESF can be tested by the injection of test signals and use of test switches.

(3) Platform

FPGA technology has been adopted for the UK ABWR to meet diversity requirements; hence the SSLC is implemented by using FPGA in the νCOSS® with diverse communications, sensors, and development personnel compared with the Class 3 HIACS platform and the Class 2 HWBS platform. Further details of the νCOSS® platform, its safety justification and the development process, which adopts formal methods, is included in the Basis of Safety Cases on Safety System Logic and Control System [Ref-6] and Topic Report on Class 1 Platform [Ref-15].

(4) Sensors and Input Processing

Sensors are required for measurement of:

(a) Neutron Flux,
(b) Pressure,
(c) Level,
(d) Flow,
(e) Temperature, and
(f) Radiation

The preferred sensors for the UK ABWR SSLC are 'dumb' with a simple design and significant operational history supporting a record of proven-in-use. However, there are two exceptions to this, the

Neutron Monitoring System and the Radiation Monitoring System that by necessity contain complex processing electronics. The sensors and measuring systems selected for the UK ABWR will follow the same principles and will be chosen post GDA phase. Sensors and Input Processing is described in section 14.7.3.

(5) Actuators

The equipment actuated by the SSLC (RPS/MSIV) includes:

(a) The AC (Alternating Current) and DC (Direct Current) actuators for reactor scram
  (i) Solenoid-operated scram pilot valves – de-energise to actuate (AC).
  (ii) Solenoid valves of the Backup Trip System – energise to actuate (DC).

Either is able to cause the loss of the air pressure causing the hydraulic pressure to drive the control rods into the core.

(b) The AC actuators for Main Steam Isolation Valve closure
  (i) Solenoid-operated pilot valves opening a trip valve.

(c) The systems actuated by the SSLC (ECCS/ESF) include:
  (i) High-Pressure Core-Flooder System, Reactor Core Isolation Cooling System,
  (ii) Low-Pressure Flooder System,
  (iii) Automatic Depressurisation System,
  (iv) Emergency Diesel Generators , and
  (v) Primary Containment Isolation System which control isolation valves other than the main-steam isolation valves

(6) Human-Machine Interface

The HMI for the SSLC is located in the Main Control Room (MCR). There are class 1 displays for safety located on the Main Control Console (MCC) and on the Wide Display Panel (WDP); these and the associated controls are Class 1 equipment developed specifically for UK ABWR.

Examples of displays and controls available for operation are as below.

(a) Display items
  (i) Reactor Water Level,
  (ii) Reactor Pressure,
  (iii) Drywell Pressure,
  (iv) Neutron Flux,
  (v) Suppression Pool Temperature, and
  (vi) Main Steam Line Radiation.

  Actuator Condition such as
  (vii) Valve Open/Close, and
  (viii) Pump ON/OFF.

(b) Controlled items, operated using push buttons
  (i) RHR (Residual Heat Removal System),
  (ii) HPCF (High Pressure Core Flooder System), and
  (iii) RCIC (Reactor Core Isolation Cooling System).

Additional information on the Human-Machine Interface is available in Generic PCSR Chapter 21.

(7) Support systems
The support systems required by the SSLC include:

(a) Power sources, and
(b) HVAC.

Other dependencies include the hydraulic system for the control rods and the Condensate Storage Tank which is a water reservoir for injection, the Reactor Building Cooling Water System and the Reactor Building Service Water System that act as the heat sink for the RHR heat exchangers, Instrument Air System and Nitrogen System and the emergency diesel generators.

Further details of these systems are given in Section 14.9 Support Systems.

14.6.2.2 Remote Shutdown System

(1) Overview

Two Remote Shutdown Panels (RSP) of manual displays and controls are provided outside the main control room to ensure that cold shutdown from hot shutdown of the reactor can be achieved in the event that the main control room becomes uninhabitable following a reactor scram. Each RSP can control one division of ECCS/ESF equipment. The functional and equipment requirements of the RSS C&I are to allow direct manual control of the mechanical plant of divisions I and II of the SSLC from the RSS via RSP I for Division I and RSP II for Division II. RSP I and RSP II are segregated to prevent the simultaneous loss from an internal hazard.

(2) System Architecture Interfaces and Layout

Figure 14.6-4 shows the Remote Shutdown System (RSS) C&I configuration.

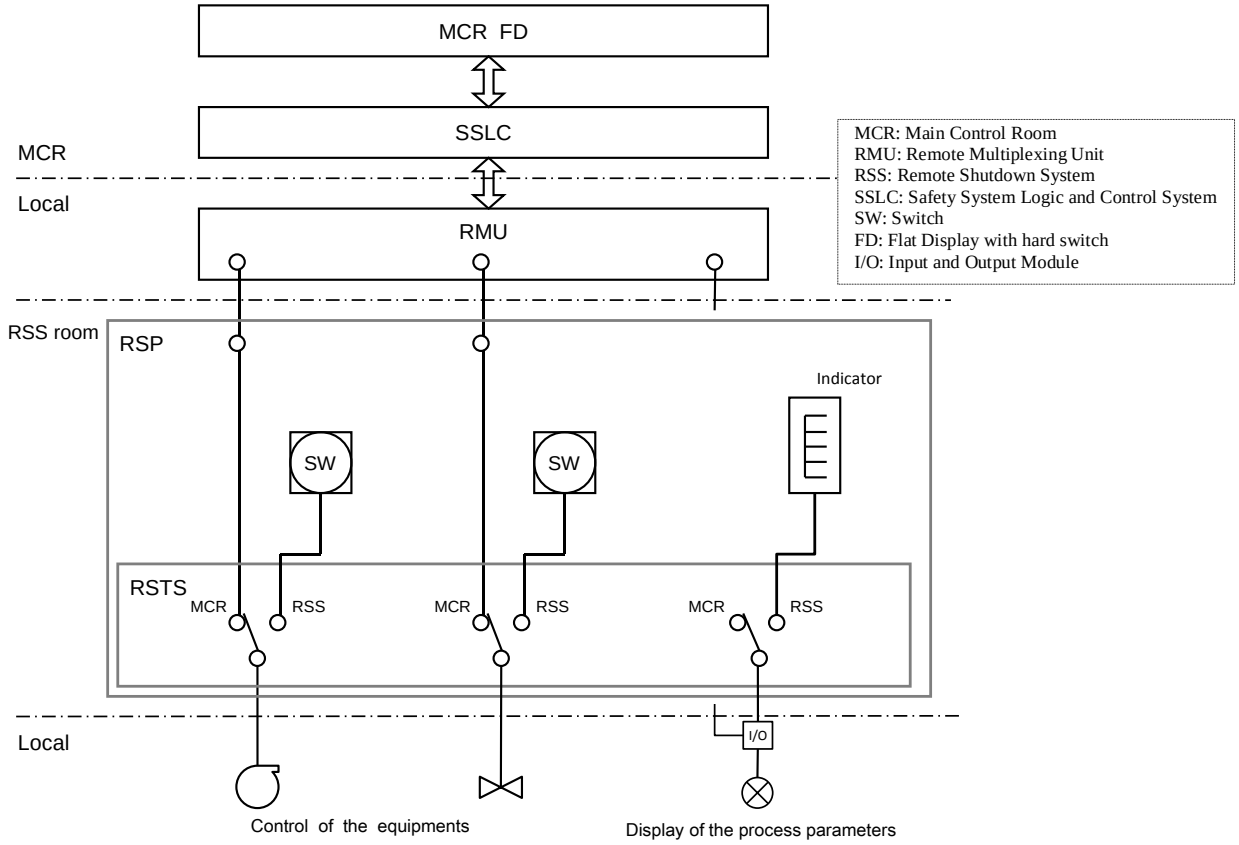


Figure 14.6-4: RSS C&I configuration

(a) Two Remote Shutdown Panels (RSP) are placed in Remote Shutdown System Panel Rooms that are independent from the Main Control Room (MCR).
(b) The operation from RSP is enabled by switching the Remote Shutdown Transfer Switch (RSTS) from the MCR side to the RSS side. The RSTS is installed on the RSP. Once the RSTS is operated, the manually initiated operations from RSP are independent from the MCR operation.
(c) An alarm is generated in the MCR when the RSTS is switched to the RSS side.
(d) Each RSP operates a separated division of the SSLC and are separated to prevent simultaneous failure from a hazard.
(e) The indication of plant parameters assigned to the RSS is enabled by switching the RSTS.

(3) Platform

The panels are implemented using hardwired logic with hard switches and analogue indication that are diverse to the *v*COSS® platform for a SSLC and HIACS platform of the Plant Control System.

(4) Sensors and Input Processing
The following plant parameters are displayed on each RSP:

(a) Level,
(b) Pressure,
(c) Flow, and
(d) Temperature.

(5) Actuators
The following actuators can be operated by each RSP:

(a) RCIC (Division I only) HPCF (Division II only) pump and valves,
(b) RHR pump and valves,
(c) SRVs,
(d) RCW (Reactor Building Cooling Water System) / RSW (Reactor Building Service Water System) pumps and valves, and
(e) Emergency power supply circuit breakers.

(6) Human-Machine Interface

The HMI is located in each RSS panel room, full details are provided in the Topic Report on SSLC [Ref-25]. In addition to the sensors listed in Point 4, the following actuator conditions are displayed on each HMI:

(a) Display items
  (i) Reactor Water Level,
  (ii) Reactor Pressure,
  (iii) ECCS Flow Quantity,
  (iv) Condensate Storage Tank Water Level, and
  (v) RHR Heat Exchanger Inlet Temperature.

  Actuator condition such as
  (vi) Valve Open/Close, and
  (vii) Pump ON/OFF.

(b) Controlled items, operated by hardwired switch
  (i) Pumps, valves, and
  (ii) Circuit breaker.

(7) Support Systems
Same as (7) of section 14.6.2.1 of this chapter.

14.6.2.3 Safety Auxiliary Panel (SAuxP) for the SSLC

(1) Overview

The SAuxP for the SSLC, in conjunction with the manual actuation of reactor trip and MSIV closure from the Main Control Console, provides a means of maintaining the safety system defence-in-depth in the event of a CCF of SSLC in conjunction with a large break LOCA (Loss of Coolant Accident). The SAuxP provides hardwired control of the division III ECCS equipment, for example, high pressure injection and also isolation of the CUW and RCIC to complete isolation of the RPV boundary.

(2) System Architecture Interfaces and Layout

The SAuxP is located in Main Control Room. Figure 14.6-5 shows the Safety Auxiliary Panel C&I configuration.

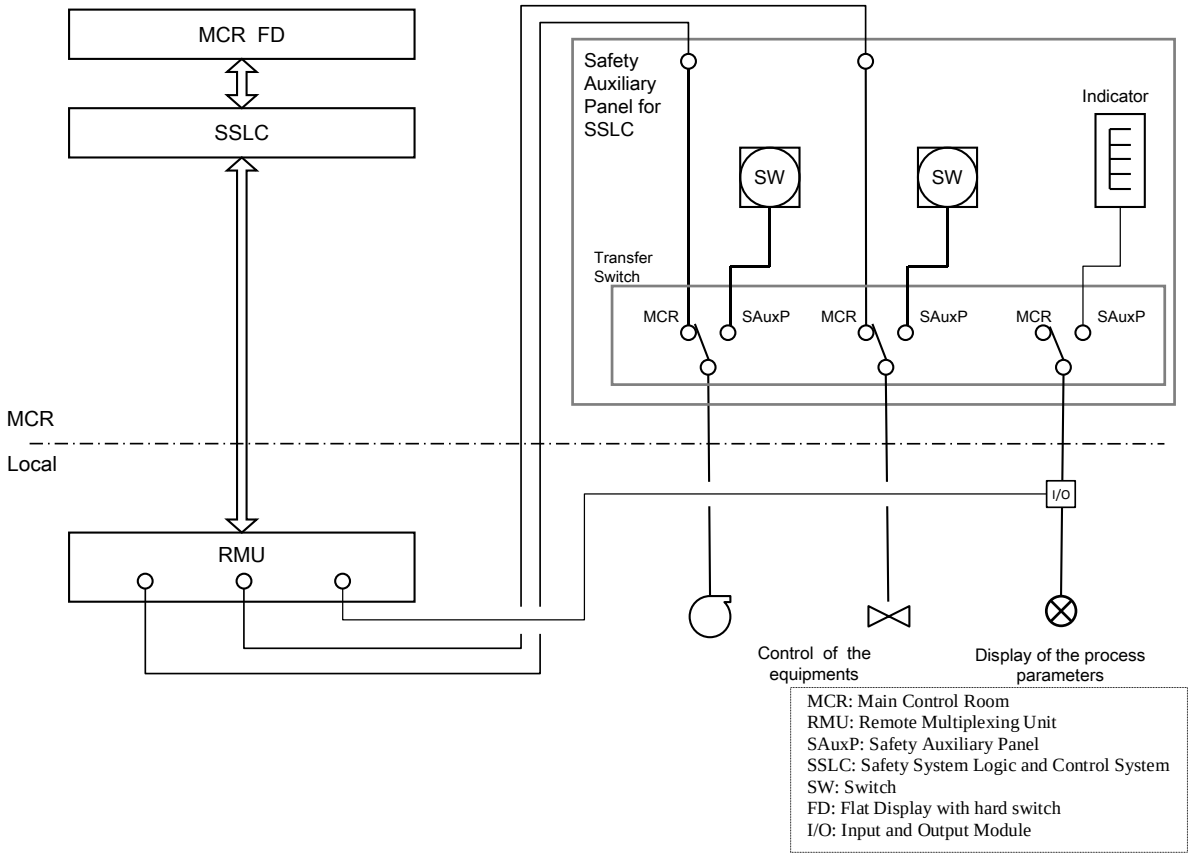


Figure 14.6-5: Safety Auxiliary Panel C&I configuration

(3) Platform

The equipment in the panel uses hardwired logic that is diverse to the νCOSS® platform for a SSLC and HIACS platform of the Plant Control System.

(4) Sensors and Input Processing
The following plant parameters are displayed on the SAuxP:

(a) Level, and
(b) Pressure.

(5) Actuators
The following actuators can be operated by the SAuxP:

(a) CUW, RCIC isolation valve,
(b) HPCF pump, valve,
(c) RHR pump and valves, and
(d) RCW / RSW pumps and valves.

(6) Human-Machine Interface

The HMI is located in Main Control Room.

Examples of displays and controls used for operations are as below.

(a) Display items
    (i) Reactor Water Level, and
    (ii) Reactor Pressure.

    Actuator condition such as
    (iii) Valve Open/Close, and
    (iv) Pump ON/OFF.

(b) Control items, operated by hardwired switch
    (i) Pumps, and
    (ii) Valves.

(7) Support systems
Same as (7) of sub-section 14.6.2.1 of this chapter.

Further details are provided in the Basis of Safety Cases on SSLC [Ref-6].

14.6.3 Hardwired Backup System

The Hardwired Backup System (HWBS) is a Class 2 system and is the secondary means of protecting against frequent design basis faults; it also provides protection against infrequent faults, beyond design basis accidents and severe accidents. The HWBS is implemented via controls in the Control-Building and Backup-Building (B/B) (see Figure 14.6-6). The system provides a defence in the case of CCF of the SSLC and the Plant Control System (PCntlS) that are based on complex technology as it is hardwired solid state based with diverse signal converters and comparators to those of the SSLC and PCntlS.

(1) Overview

The HWBS is independent (separated and isolated) and diverse from Class 1 main protection system. The system is based on diverse technology (analogue devices and relay logic) using diverse means of fault detection as appropriate. Its role is to provide diverse safety functions to those provided by the SSLC. The high level safety functions covered are specified in Generic PCSR Chapter 24, described in Table 24.3-1. The main fundamental safety functions performed by the HWBS are:

(a) Reactivity Control:
  (i) Standby Liquid Control (SLC),
  (ii) Recirculation Pump Trip (RPT),
  (iii) Feed-Water stop, and
  (iv) Alternative Rod Insertion (ARI).
(b) Fuel Cooling:
  (i) Reactor Depressurisation Control Facility (RDCF), and
  (ii) Flooder System of Specific Safety Facility (FLSS).
(c) Long Term Heat Removal:
  (i) Filtered Containment Venting System, and
  (ii) Hardened Vent Line.

The Hardwired Backup System is supported by Class 2 electrical supplies and HVAC.

(2) System Architecture Interfaces and Layout

Figure 14.6-6 shows the architecture of HWBS.

The automatic SLC (Standby Liquid Control System), ARI (Alternative Rod Insertion), RPT (Recirculation Pump Trip) and Feedwater Stop provide the functionality for the mitigation of a CCF of the RPS. The SLC, ARI, RPT and Feedwater Stop functions receive signals directly from a diverse set of sensors that are electrically independent from the sensors used by the Class 1 RPS. The system also has two mechanical trains for core cooling using the Flooding System of Specific Safety facility (FLSS) in the Backup-Building, that is diverse and independent from the Class 1 ECCS for mitigation of a CCF of the Class 1 ECCS. Manual operation from B/B control panel is enabled by switching of the transfer switch from the MCR side to the B/B side. The transfer switch is installed on B/B control panel, activation of the switch means operation from B/B is independent from the MCR.

Further details are provided in the Basis of Safety Cases on Hardwired Backup System [Ref-7].

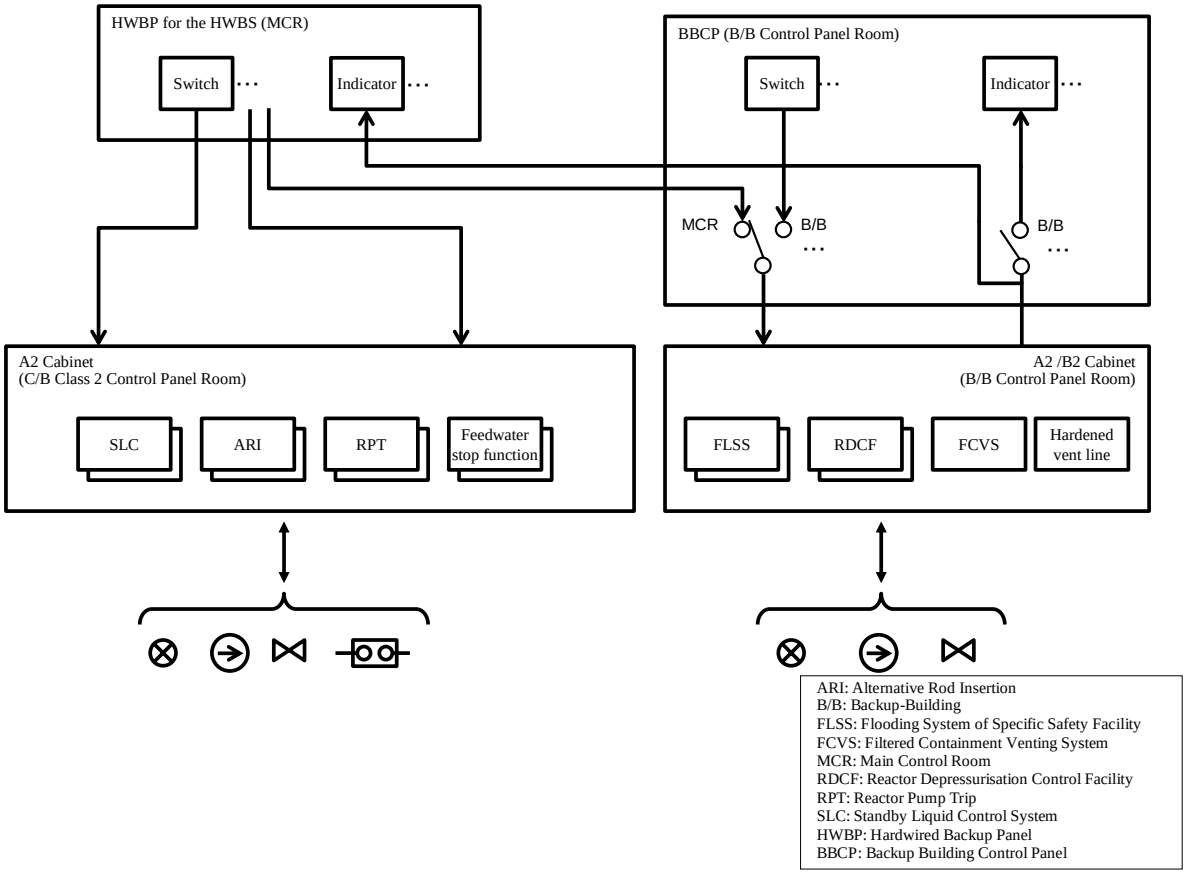
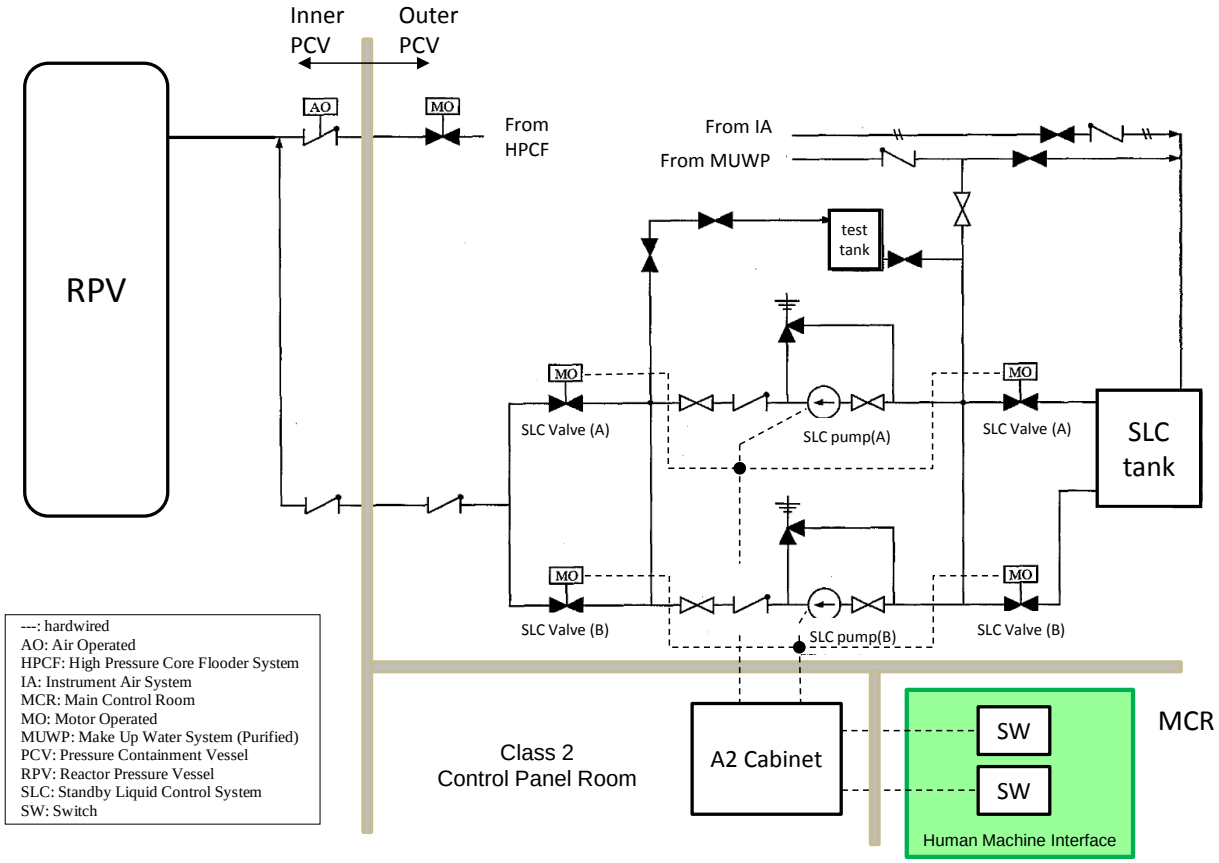


Figure 14.6-6: C&I architecture of Hardwired Backup System

14.6.3.1 Standby Liquid Control System

(1) Overview

The SLC provides the second means of reactivity control and is the principal means of reactivity control of the HWBS. To support the SLC function, the RPT and Feedwater Stop functions assist producing negative reactivity. The SLC configuration is shown in Figure 14.6-7. The mechanical system consists of components such as a storage tank, pumps, a test tank, piping and valves that are automatically initiated in response to a demand.



- SLC pump and SLC valve are operated manually from MCR
- SLC system has automatic initiation

Figure 14.6-7: Configuration of Standby Liquid Control System

(2) System Architecture Interfaces and Layout

The SLC is separated both physically and electrically from the SSLC (RPS) and CRD System. Operation of the SLC can be initiated both automatically and manually from the Main Control Room. Two channels of pumps and inlet and outlet valves are provided to ensure that the boric solution can be injected reliably when required. (See Figure 14.6-7)

(3) Platform

The SLC is implemented using sensors, hardwired trip modules and hardwired logic that is diverse to the νCOSS®. Details are provided in the Basis of Safety Cases on Hardwired Backup System [Ref-7].

(4) Sensors and Input Processing

The following sensors are associated with the SLC function:

(a) Level,
(b) Pressure, and
(c) .

The sensors and processing equipment will be hardwired and diverse from that used by the SSLC and will be installed to be independent from SSLC. Further information is given in the Basis of Safety Cases on Hardwired Backup System [Ref-7].

(5) Actuators

The following actuators are operated by the HWBS for the SLC function (this includes the relay based start-up circuit):

(a) SLC valves, and
(b) SLC pumps.

(6) Human-Machine Interface

The HMI for the SLC is Hard Wired Backup Panel (HWBP) located in Main Control Room (see Generic PCSR Chapter 21, section 21.4). Examples of the display and control provisions for operational purposes are given below.

(a) Display items
  (i) Reactor Water Level,
  (ii) Reactor Pressure,
  (iii) SLC Storage Tank Level, and
  (iv) System Pressure.

  Actuator condition such as
  (v) Valve Open/Close, and
  (vi) Pump ON/OFF.

(b) Control items, operated by hardwired switch
  (i) SLC valves, and
  (ii) SLC pumps.

(7) Support Systems

The support systems required for the HWBS controlling of SLC include:

(a) Power sources, and
(b) HVAC.

14.6.3.2 Alternative Rod Insertion

(1) Overview

The SSLC initiates rod insertion by operation of the control rod Hydraulic Control Units (HCU) via two sets of solenoid valves. Should an Anticipated Transient Without Scram (ATWS) event occur due to a failure of the SSLC-RPS and its associated solenoid valves, the HWBS ARI provides an alternate means of rapidly inserting the control rods by opening exhaust valves installed on the instrumentation air system of the HCUs. Supporting the HWBS ARI function is the HWBS Reactor Pump Trip (RPT) function to provide additional negative reactivity for an ATWS event. This capability is included in the HWBS to provide defence in depth as the HWBS primary means of achieving reactivity control is through the initiation of the SLC.

The initiation of rod insertion by the ARI C&I is accomplished independently and by diverse means from the C&I of the RPS using independent sensors, logic and exhaust valves. The ARI provides a third means, in addition to the two of the SSLC-RPS, of operating the HCUs using solenoid valves to vent the instrument air from the headers. Figure 14.6-8 shows schematic C&I configuration of shutdown function diversity.

It is acknowledged that the CRs and the HCUs are shared between the SSLC and the HWBS.

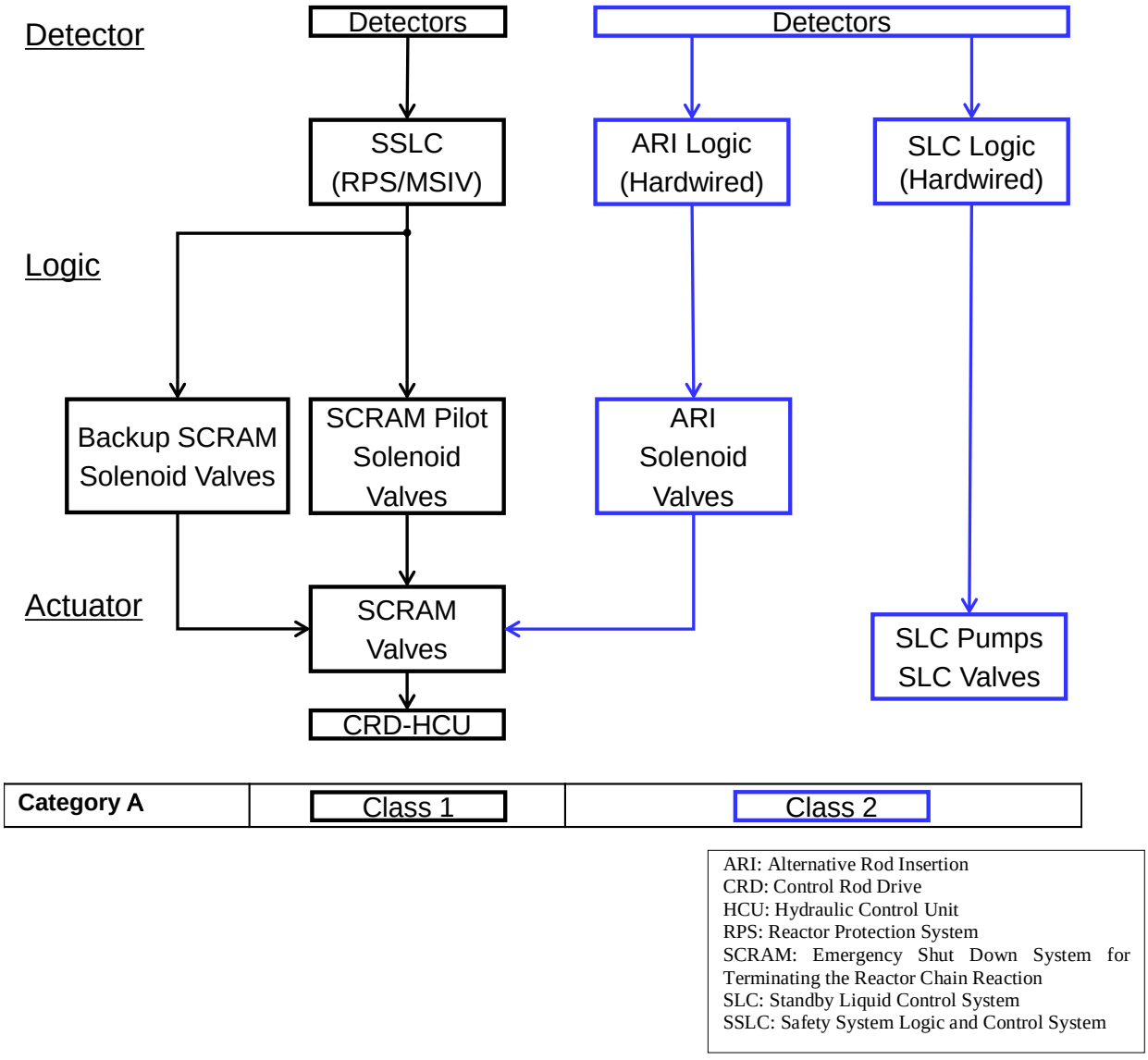


Figure 14.6-8: Schematic C&I configuration of shutdown function diversity

(2) System Architecture Interfaces and Layout

Figure 14.6-9 shows the architecture for the diverse provision of the ARI and the RPT for implementation of the reactor shutdown function.

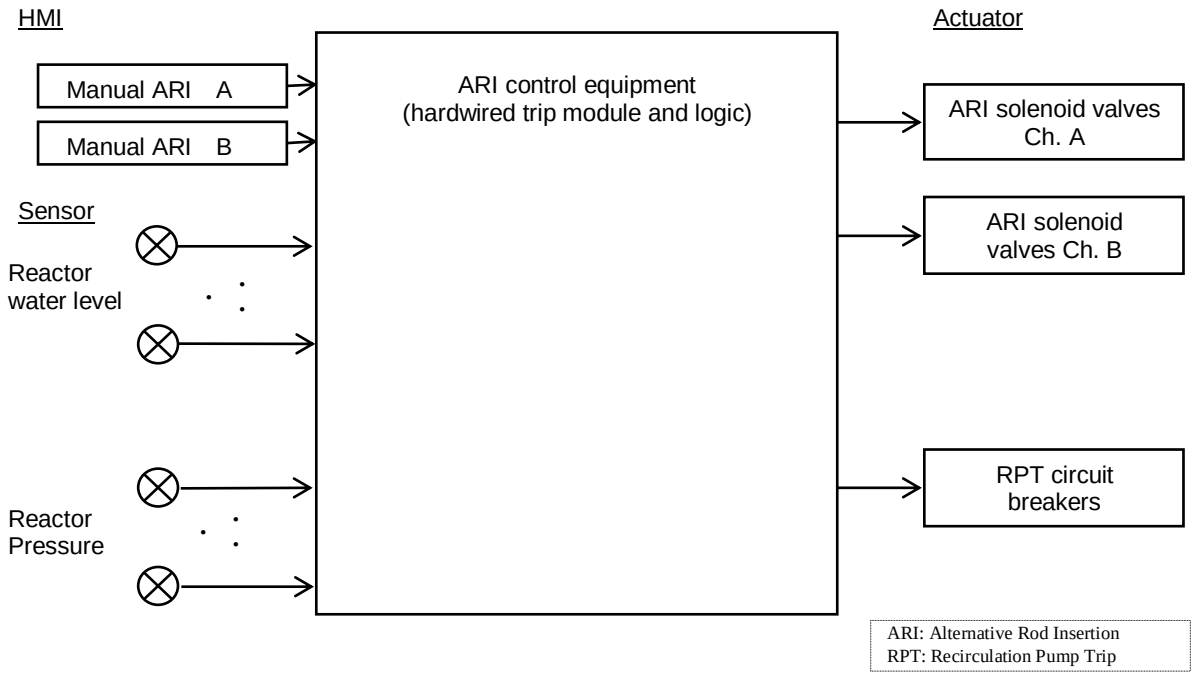


Figure 14.6-9: C&I Architecture of Alternative Rod Insertion (ARI)

(3) Platform

The ARI and the RPT are implemented using the hardwired trip modules and hardwired logic that is diverse to the νCOSS® platform for SSLC. Details are provided in Basis of Safety Cases on Hardwired Backup System [Ref-7].

(4) Sensors and Input Processing

The following sensors are associated with the ARI function:

(a) Level, and
(b) Pressure.

The sensors and processing equipment are diverse from that used by the SSLC and will be installed to be independent from the SSLC (within the safety constraints of the integrity of the reactor pressure boundary).

(5) Actuators

The equipment actuated by the ARI and the RPT includes.

(a) ARI solenoid valves
The operation of the solenoid valve will result in venting of instrument air from the headers and opening of the HCU resulting in hydraulic insertion of the rods.

(b) RPT circuit breakers
The operation of the RPT circuit breakers will result in isolation of the electrical circuit for the Recirculation Internal Pumps (RIPs).

(6) Human-Machine Interface

The HMI for the ARI is located in main control room.
Examples of display and control provision for operational purposed are given below:

(a) Display items
(i) Reactor Water Level, and
(ii) Reactor Pressure.

(b) Control items, operated by hardwired switch
(i) ARI solenoid valves.

(7) Support Systems
The support systems required for the HWBS controlling of ARI include:
(a) Power sources, and
(b) HVAC.

14.6.3.3 FLSS and RDCF

(1) Overview

The Flooding System of Specific Safety Facility (FLSS) and Reactor Depressurisation Control Facility (RDCF) provide an alternative means of maintaining reactor core cover by water to that provided by the ECCS High and Low pressure core flooders (RCIC, HPCF and LPFL) actuated by the SSLC. As shown in Figure 4.6-10:

(a) The SSLC (ECCS/ESF) provides Safety Class 1 means of providing core flooding (RCIC, HPCF, ADS and LPFL).

(b) The FLSS and RDCF are assigned Safety Class 2, which is diverse and independent from the Class 1 ECCS SSCs.

(c) Class 2 FLSS and RDCF are automatically initiated by the HWBS and can also be manually controlled from the Main Control Room (MCR) and the Backup-Building (B/B) using the SA C&I system HMI and powered from the B/B electric power supplies that are diverse and independent from Class1 SSLC.

Figure 14.6-10 shows the Schematic C&I Architecture of FLSS and RDCF.

In addition, the FLSS provides an alternative means of making up for water into the Spent Fuel Pool (SFP).

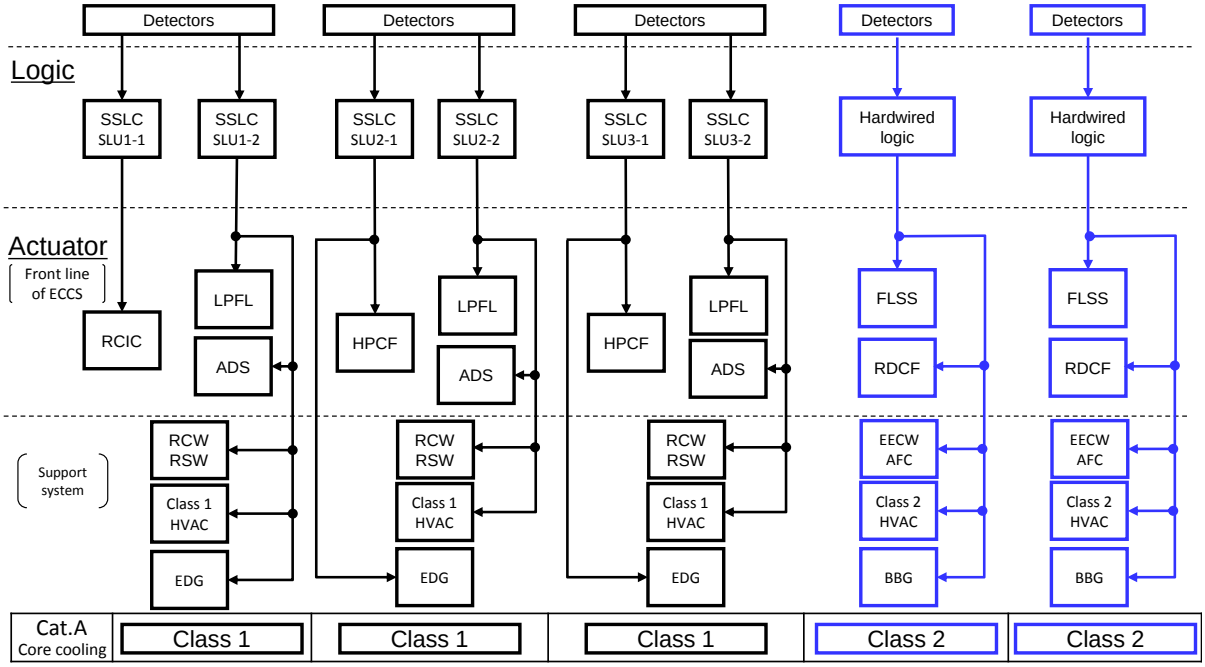


Figure 14.6-10: Schematic C&I Architecture Class 1 RCIC, HPCF, ADS and LPFL and Class 2 of FLSS and RDCF

ADS: Automatic Depressurisation System, AFC: Air Fin Coder, B/B: Backup-Building, BBG: Backup Building Generator
EDG: Emergency Diesel Generator, EECW: Emergency Equipment Cooling Water, FLSS: Flooding System of Specific Safety Facility
HPCF: High Pressure Core Flooder System, HVAC: Heating Ventilating and Air Conditioning System, LPFL: Low Pressure Flooder System
R/B: Reactor Building, RCIC: Reactor Core Isolation Cooling System, RCW: Reactor Cooling Water System
RSW: Reactor Building Service Water System, SLU: Safety Logic Unit, SSLC: Safety System Logic and Control System
RDCF: Reactor Depressurisation Control Facility

(2) System Architecture Interfaces and Layout

The C&I equipment of FLSS and RDCF includes hardwired logic, switches, indicators and electric power supplies from the Backup Building Generator (BBG) that are diverse and independent from the Class 1 SSLC-ECCS C&I equipment. The HMI for operating and monitoring the FLSS and RDCF is located in MCR and B/B control room.

Further detail of the system architecture is described in Basis of Safety Cases on Control and Instrumentation Architecture [Ref-5] and its implementation is described in the Basis of Safety Cases on the Hardwired Backup System [Ref-7].

(3) Platform

The FLSS and RDCF are implemented using hardwired trip modules and hardwired logic that is diverse to the νCOSS® SSLC platform.

(4) Sensors and Input Processing

The following sensors are associated with the FLSS function:
(a) Level,
(b) Pressure, and
(c) Flow.

The sensors and processing equipment are diverse from that used by the SSLC and will be installed to be independent from the SSLC (within the safety constraints of the integrity of the reactor pressure boundary). This is described in Basis of Safety Cases on Hardwired Backup System [Ref-7].

(5) Actuators

Startup circuits (relay based) for:
(a) FLSS pumps, and
(b) FLSS and RDCF valves.

(6) Human-Machine Interface

The HMI for the FLSS and RDCF is the Hardwired Backup Panel (HWBP) located in MCR (see Generic PCSR Chapter 21, section 21.4) and also Backup Building Control Panel (BBCP) in the B/B control room (see Generic PCSR Chapter 21, section 21.6); further details are provided in the Basis of Safety Cases on Hardwired Backup System [Ref-7].
Example of displays and controls available for operation are as below:

(a) Display items
  (i) Reactor Water Level,
  (ii) Reactor Pressure,
  (iii) FLSS Pressure, and
  (iv) FLSS Flow Quantity.

  Actuator condition such as
  (v) Valve Open/Close, and
  (vi) Pump ON/OFF.

(b) Control items, operated by hardwired switch

(i) FLSS pumps,
(ii) FLSS valves, and
(iii) SRVs.

(7) Support systems
The support systems required for the HWBS controlling of FLSS and RDCF include:
(a) Power sources, and
(b) HVAC.

14.6.3.4 Containment Venting

(1) Overview

Containment venting using Filtered Containment Venting System (FCVS) and Hardened Vent Line are installed to release the residual heat, transferred from the RPV to the PCV by the RDCF, to the environment as an alternative long heat removal. The function prevents damage to the PCV by over pressure and prevents the release of radioactive material to the environment during severe accident management should there be a loss of the Class 1 ECCS cooling function.

(2) System Architecture Interfaces and Layout

The C&I equipment for the Containment venting including the hardwired logic, switches, indicators and the electric power supplies (BBG) are diverse and independent from Class 1 ECCS C&I equipment. The HMI for operating and monitoring the Containment venting is located in the MCR and the B/B control room.

Further details of the system architecture are described in Basis of Safety Cases on Control and Instrumentation Architecture [Ref-5] and its implementation is described in the Basis of Safety Cases on Hardwired Backup System [Ref-7].

(3) Platform

The Containment venting is implemented using hardwired trip modules and hardwired logic that is diverse to the SSLC νCOSS® platform.

(4) Sensors and Input Processing

The following sensors are associated with the FCVS and Hardened Vent Line function:

(a) Pressure.

The sensors and processing equipment are diverse from that used by the SSLC and will be installed to be independent from the SSLC (within the safety constraints of the integrity of the reactor pressure boundary). This will be described in Basis of Safety Cases on Hardwired Backup System [Ref-7].

(5) Actuators

Startup circuits (relay based) for:

(a) The Containment venting valves.

(6) Human-Machine Interface

The HMI for the Containment venting is the HWBP located in the main control room (see Generic PCSR Chapter 21, section 21.4) and the BBCP in B/B control room (see Generic PCSR Chapter 21, section 21.6); further details are provided in the Basis of Safety Cases on Hardwired Backup System [Ref-7].

Example of displays and controls available for operation are as below:

(a) Display items
  (i) D/W Pressure, and
  (ii) S/C Pressure.

Actuator condition such as
(i) Valves Open/Close.

(b) Control items, operated by hardwired switch:
(i) The Containment venting valves.

(7) Support Systems
The support systems required for the HWBS controlling of Containment venting include:
(a) Power sources, and
(b) HVAC.

14.6.3.5 Hardwired Backup Panel (HWBP) for the HWBS

(1) Overview

The Hardwired Backup Panel (HWBP) for the HWBS provides hardwired control and monitoring of the Category A / Class 2 equipment.

(2) System Architecture Interfaces and Layout

The HWBP for the HWBS is located in main control room (see Generic PCSR Chapter 21, section 21.4). Figure 14.6-6 shows the HWBP C&I configuration.

(3) Platform

The equipment in the panel uses hardwired based technology.

(4) Sensors and Input Processing

(a) Level, and
(b) Pressure.

(5) Actuators

(a) SLC pumps, valves,
(b) ARI solenoid valves,
(c) RPT circuit breakers,
(d) Feedwater Stop Function,
(e) FLSS pumps,
(f) FLSS and RDCF valves, and
(g) Containment venting valves.

(6) Human-Machine Interface

The HMI is located in main control room.
Examples of displays and controls used for operations are as below.

(a) Display items
  (i) Reactor Water Level, and
  (ii) Reactor Pressure.

  Actuator condition such as
  (iii) Valve Open/Close, and
  (iv) Pump ON/OFF.

(b) Control items, operated by hardwired switch:
  (i) Pumps, and
  (ii) Valves.

(7) Support Systems
The support systems required for the HWBP include:
(a) Power sources, and
(b) HVAC.

14.6.4 Safety Auxiliary Control System

(1) Overview

Safety Auxiliary Control System (SACS) controls and monitors the systems which implement the Category B or C safety functions that support the SSLC's safety functions as a defence-in-depth measure and that are used after the SSLC initiates safety-protection operations. As the SACS, which is providing Safety Functions at Category B and C, it is a safety Class 2 system (B2 not A2). Please note that the systems controlled by the SACS are not formally claimed in the design basis accident analysis (see Generic PCSR Chapter 24) as either primary or diverse secondary safety measures.

The systems controlled and monitored by the SACS are:

(a) Standby Gas Treatment System (SGTS),
(b) High Pressure Nitrogen Gas Supply System (HPIN),
(c) Suppression Pool Clean-up System (SPCU),
(d) Off Gas system isolation, and
(e) Post Accident Monitoring System (PAM).

The SACS is implemented by the same technology platform as the SSLC and uses the same support systems (including HVAC and electrical supplies).

(2) System Architecture Interfaces and Layout

The SACS is taken from the existing J-ABWR design meaning its functions and property requirements are known but the functions are separated (no diversity requirement) from those of the SSLC. This is to avoid mixing of functions of different safety functional categories in the SSLC. Figure 14.6-11 shows the architecture of SACS and includes sensors, RMUs, cables, controllers, actuators and HMIs that are the same component types as the SSLC. The SACS is isolated from and separated from the SSLC with its equipment in its own cabinets. It is also isolated from other C&I systems maintaining the requirement for separation but providing status data to the PCS. The equipment cabinets for the SACS are located in Control Building (C/B).

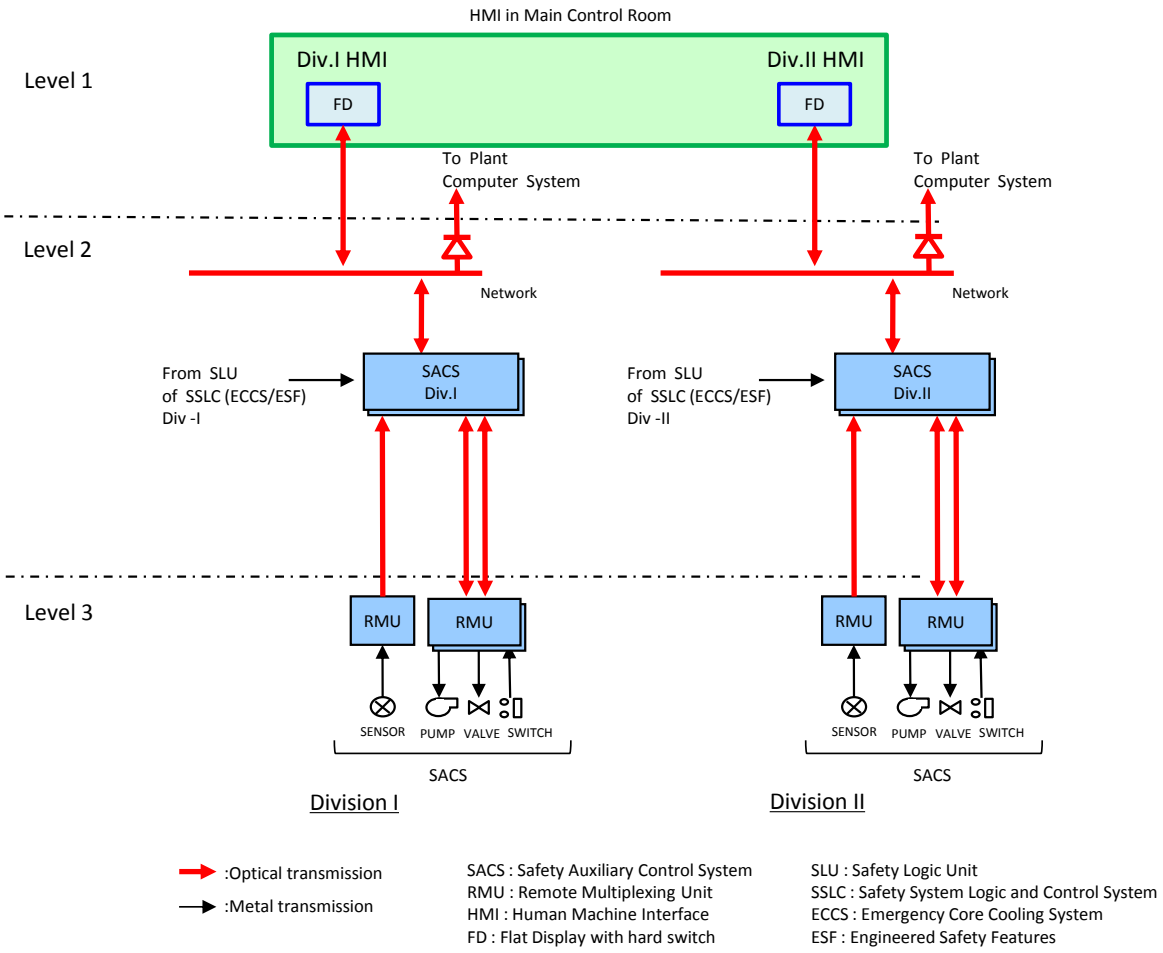


Figure 14.6-11: C&I architecture of Safety Auxiliary Control System

(3) Platforms

The SACS is implemented using the νCOSS® platform

(4) Sensors and Input Processing
- (a) Pressure,
- (b) Level,
- (c) Flow,
- (d) Temperature,
- (e) Radiation level, and
- (f) Hydrogen and Oxygen concentration.

(5) Actuators
- (a) Pumps,
- (b) Valves,
- (c) Fans, and
- (d) Heaters of the systems.

(6) Human-Machine Interface

The HMI of the SACS are located on Main Control Console (MCC) and Wide Display Panel (WDP) in the main control room (see Generic PCSR Chapter 21, section 21.4). Examples of display and control item are as below.

(a) Display items
  (i) D/W Pressure and System Pressure,
  (ii) Reactor Water Level and System Water Level,
  (iii) System Flow Quality,
  (iv) Temperature of the equipment room and system,
  (v) Radiation level of the equipment room and Primary Containment Vessel,
  (vi) Hydrogen and Oxygen concentration of the Primary Containment Vessel, and
  (vii) Hydrogen concentration of the system.

  Actuator condition of
  (viii) Pump ON/OFF,
  (ix) Valve Open/Close,
  (x) Fan ON/OFF, and
  (xi) Heater ON/OFF.

(b) Control items, operated using push buttons
  (i) SGTS valves, fans and heaters,
  (ii) HPIN valves,
  (iii) SPCU pumps and valves, and
  (iv) OG isolation valves.

(7) Support Systems
The support systems required for the SACS include:
(a) Power sources, and
(b) HVAC.

Details are provided in Basis of Safety Cases on Safety Auxiliary Control System [Ref-8].

14.6.5 Plant Control System

The functions performed by the Plant Control System (PCntlS) are directly classified as Safety Class 3 equipment using the approach to classification specified in Generic PCSR Chapter 5, section 5.6.4. The major plant control sub-systems are identified in Figure 14.6-12 as:

(i) Automatic Power Regulator (APR),
(ii) Rod Control and Information System (RCIS),
(iii) Recirculation Flow Control (RFC),
(iv) Electro-Hydraulic Turbine Control System (EHC), and
(v) Feedwater Flow Control System (FDWC).

The systems are Class 3 and details of the system are provided in Basis of Safety Cases on Plant Control System [Ref-9].

(1) Overview

The plant control system is the means of controlling the major parameters of the reactor, e.g. pressure, level, recirculation flow and power. It has five major control loops and a rod withdrawal block system that are implemented using microprocessor technology. Figure 14.6-12 provides an overview of the plant control system that is described in detail in the Basis of Safety Cases on Plant Control System [Ref-9]. The figure indicates the use of dual and triple redundancy for the major control loops for (i) to (v). Also, Figure 14.6-13 gives a system outline drawing of the reactor control systems.

(i) APR

The APR System is used to control reactor power during reactor startup, power generation, and reactor shutdown, by appropriate commands to the RCIS for changing rod positions, or to the RFC for changing reactor recirculation flow.

Further details of the C&I is provided in Basis of Safety Cases on Plant Control System [Ref-9].

(ii) RCIS

The RCIS controls reactor power and power profile by moving the control rods, using the Fine Motion Control Rod Drives (FMCRD), either by automatic or manual initiation by the operator. The control-rod positions are adjusted to raise power, mainly for compensating for reactivity changes and adjusting the power distribution following prolonged fuel burn up. In addition, in cases where power-control is required over a large range, they are adjusted in conjunction with flow adjustments by the RFC in order to control the power. The control rods are driven into or withdrawn from the core by individual motor drives.

Further details of the C&I is provided in Basis of Safety Cases on Plant Control System [Ref-9].

(iii) RFC

The RFC controls reactor power during operation to obtain a target reactor power by changing the reactor coolant recirculation flow within predetermined ranges.

An adjustment in the recirculation flow utilises the characteristic that the reactor power varies approximately in direct proportion to the recirculation flow. The recirculation flow is adjusted by varying the speed of the Recirculation Internal Pumps (RIPs) using Adjustable Speed Drives (ASDs)

associated with each RIP motor. Further details of the C&I is provided in Basis of Safety Cases on Plant Control System [Ref-9].

(iv) EHC

The Turbine-Control Systems control the reactor pressure both in normal plant operation and in transient conditions such as during reactor scram and turbine generator trip.

The electro-hydraulic turbine control system responds to the input from the APR to provide automatic control. The control maintains a constant reactor pressure during power operation. The system controls the reactor pressure by adjusting the opening of the turbine steam control valves and turbine bypass valves in response to reactor pressure, turbine speed and power signals. The turbine bypass valves allow steam to be bypassed directly to the condenser, without being passed through the turbine. The turbine bypass system has a capacity of about 33 percent of the rated steam flow and can process steam within the bypass capacity during startup and shutdown operations and power operations against the generator load variation.

Further details of the C&I is provided in Basis of Safety Cases on Plant Control System [Ref-9].

(v) FDWC

The FDWC maintains the water level in the reactor pressure vessel within predetermined ranges during power operation and expected plant transients.

Automatic controls are exercised to ensure that a constant reactor water level is maintained at all times during power operation; this is achieved by balancing feedwater flow with steam consumption.

The Reactor Feedwater Control System uses a three-element control algorithm for this purpose. The feedwater control receives input signals from the: feedwater flow rate, main-steam flow rate and reactor water level. The feedwater flow rate is adjusted automatically either by adjusting the speed of the turbine-driven feedwater pumps or by adjusting the opening of the feedwater control valve (FCV) provided on the discharge side of the motor-driven feedwater pump. The flow rate is controlled to maintain a predetermined water level. In case of low power, a single-element feedwater control is exercised using the water level signal to maintain a predetermined water level by adjusting the opening of the FCV on the discharge side of the motor-driven reactor feedwater pump or the opening of the CUW blow down control valve.

A further detail of the system is provided in Basis of Safety Cases on Plant Control System [Ref-9].

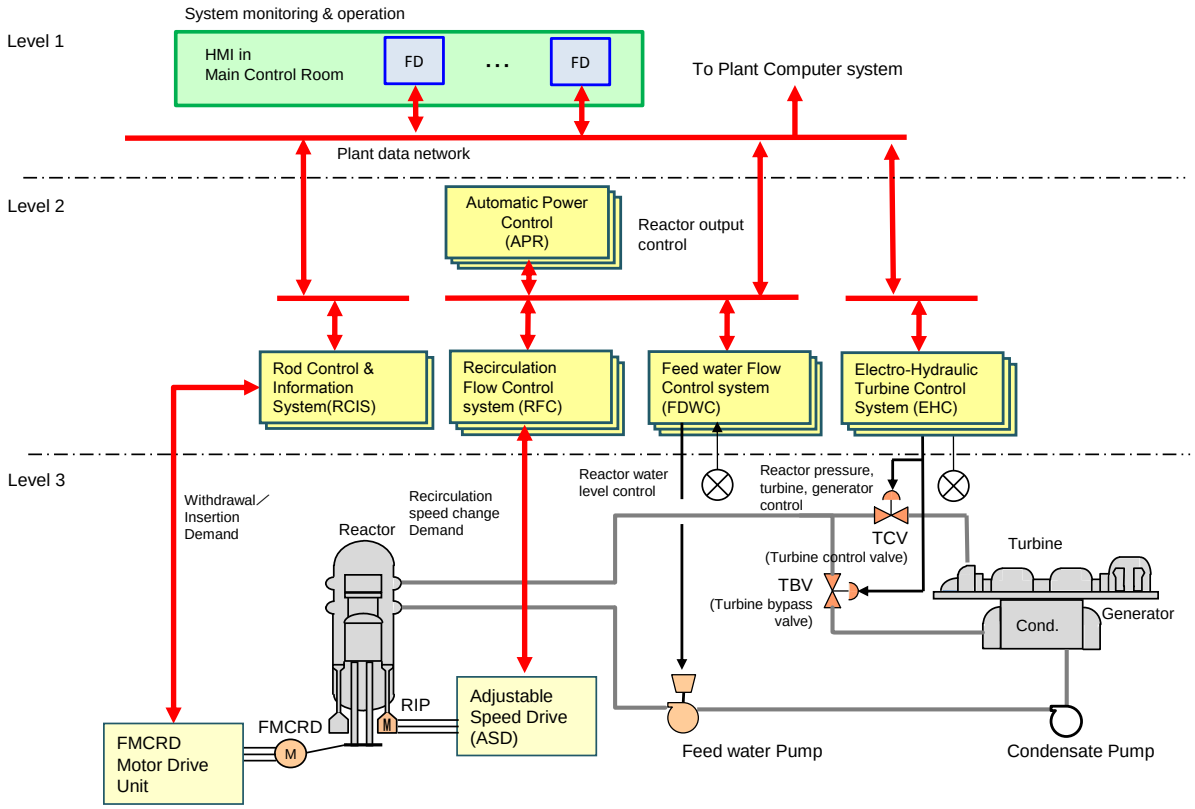


Figure 14.6-12: C&I Architecture of Plant Control System

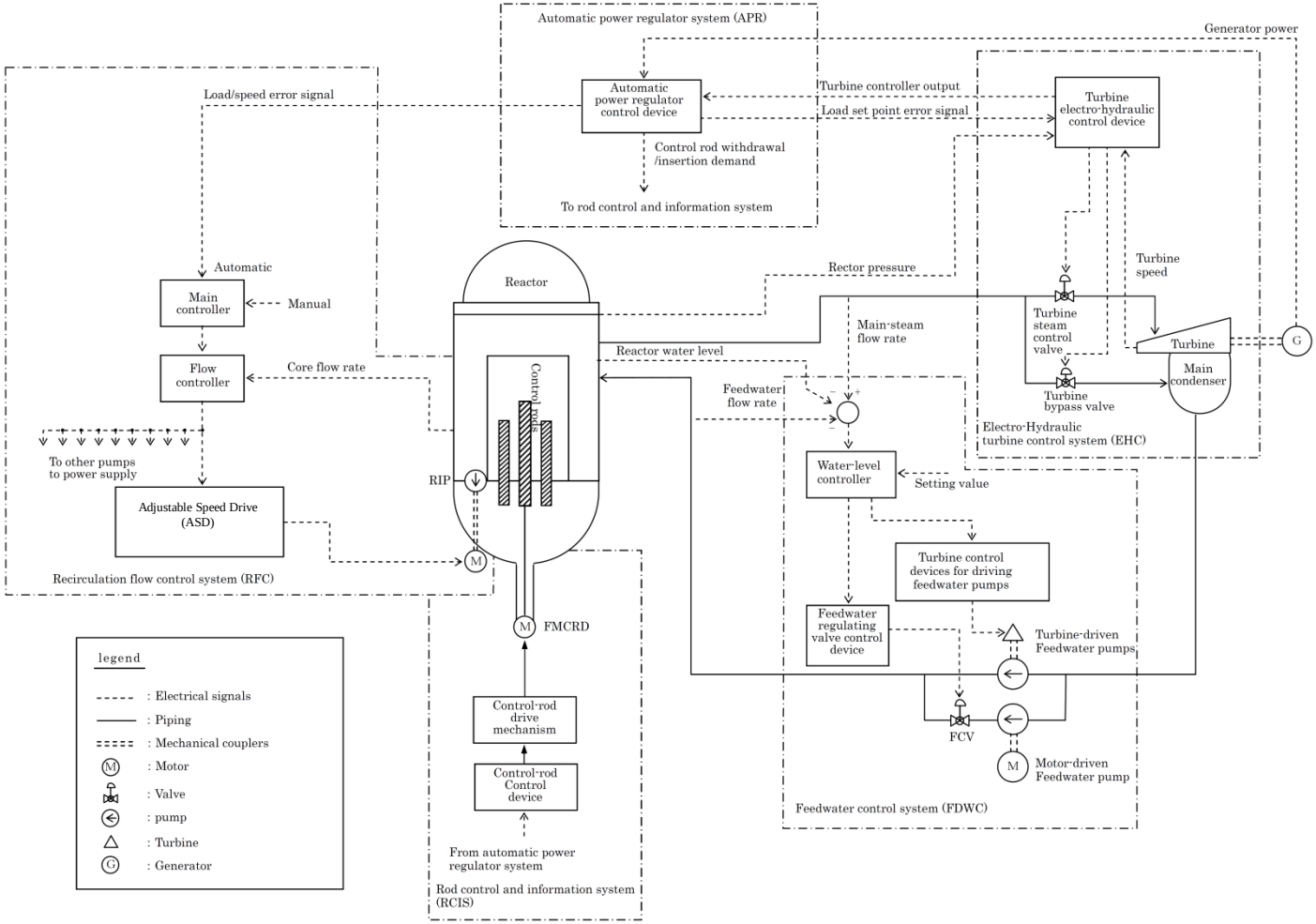


Figure 14.6-13: System outline drawing, reactor control systems

(2) System Architecture Interfaces and Layout

The system architecture is shown in Figure 14.6-12. Its interfaces are shown in Figure 14.5-1.

(3) Platforms

The platform to be used for the main control systems is HIACS, a microprocessor-based platform which has significant operating experience in safety and control system applications in J-ABWR. HIACS is programmed using Function Block Diagram (FBD), a Problem Oriented Language with extensive experience of use.

Details of program languages and communications applied in HIACS are provided in Topic Report on Class 3 Platform [Ref-16].

(4) Sensors and Input Processing

(a) Level,
(b) Pressure,
(c) Flow, and
(d) Position.

(5) Actuators

(a) Feedwater pump, valve,
(b) Turbine steam control valve, Turbine bypass valve,
(c) FMCRD, and
(d) RIP.

(6) Human-Machine Interface

The HMI is located on Main Control Console (MCC) in the MCR (see Generic PCSR Chapter 21, section 21.4). Details are provided in Basis of Safety Cases on Plant Control System [Ref-9].
Examples of displays and controls available are as below

(a) Display items
  (i) Reactor Water Level,
  (ii) Reactor Pressure,
  (iii) Core Flow Rate,
  (iv) Feedwater Flow Rate,
  (v) Main Steam Line Flow Rate, and
  (vi) Rod Position Information.

(b) Control items, operated used flat displays:
  (i) Feedwater pump, valve,
  (ii) Turbine steam control valve, Turbine bypass valve,
  (iii) FMCRD, and
  (iv) RIP.

(7) Support Systems
The support systems required for the PCntlS include:
(a) Power sources, and
(b) HVAC.

14.6.6 Severe Accident C&I System

(1) Overview

Severe Accident C&I (SA C&I) System is required to be able to monitor those parameters which, in the event of the severe accident, are necessary to understand the accident conditions and facilitate actions to mitigate the consequences of the accident. The instrumentation is required to monitor the accident status of the core and spent fuel pool cooling, containment of radio-activity and radioactive discharges.

The SA C&I System also provides equipment to deliver the safety functions to control and monitor the systems for severe accident management; this is largely mobile equipment that can be connected to the plant to provide means of mitigating the consequences of severe accidents.

The SA C&I is supported by the Class 2 electrical and HVAC systems located in the Backup-Building and Class 3 or lower additional supplies that are available from mobile plant.

Further details are presented in the BSCs on SA C&I System [Ref-10].

(2) System Architecture Interfaces and Layout

SA C&I System monitors the plant parameters and allows manual operations to mitigate the consequences of a severe accident. Figure 14.6-14 provides an overview of the SA C&I System including the mobile plant. The operation from BBCP is enabled by switching of the transfer switch from the MCR side to the B/B side. The transfer switch is installed on the BBCP, when activated the operation from B/B is isolated from any MCR interference.

The major SA C&I sub-systems are:
(a) Reactor Depressurisation Control Facility (RDCF),
(b) Flooder System of Specific Safety Facility (FLSS),
(c) Flooder System of Reactor Building (FLSR) (mobile plant),
(d) Filtered Containment Venting System (FCVS), and
(e) Alternate Heat Exchange Facility (AHEF) (mobile plant).

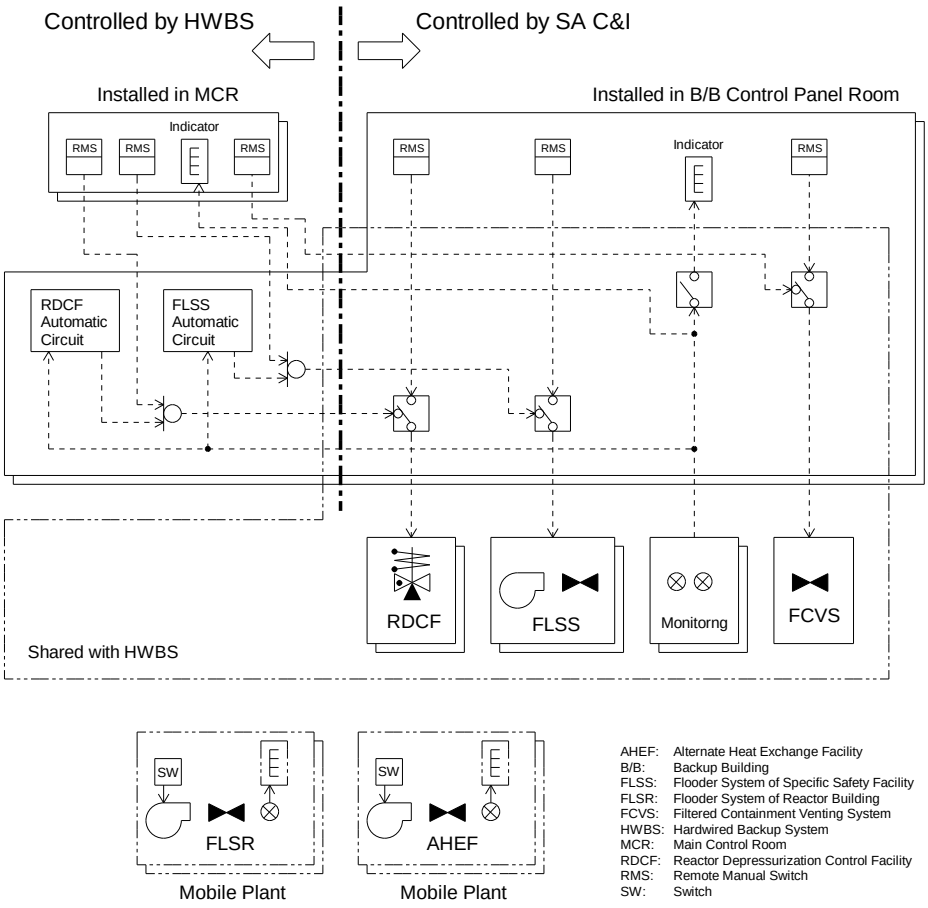


Figure 14.6-14 Schematic Architecture of SA C&I System

(3) Platforms

The SA C&I shared with the HWBS is on a hardwired logic platform. The C&I on the mobile plant is on an embedded system platform.

(4) Sensors and Input Processing

The sensors qualified for severe conditions and selected to cover the extreme range of the parameters of the severe accident.

(a) Level,
(b) Pressure,
(c) Radiation, and
(d) Temperature.

(5) Actuators

(a) FLSS pumps,
(b) FLSS and RDCF valves,
(c) Containment venting valves, and
(d) Mobile Equipment.

The actuators associated with the SA C&I consist predominantly of mobile equipment that can be connected to the plant to provide means of mitigating the consequences of severe accidents.

(6) Human-Machine Interface

Severe accident instrumentation is displayed on HWBP in Main Control Room, and on BBCP in the control room in Backup-Building once the transfer has taken place (see Generic PCSR Chapter 21, section 21.4 and 21.6). There are also HMIs on the mobile equipment. Details are given in the BSCs on SA C&I System [Ref-10].

(a) Display items
  (i) Reactor Water Level,
  (ii) Reactor Pressure,
  (iii) Radiation level of the Primary Containment Vessel, and
  (iv) Temperature of the Primary Containment Vessel and RPV surface.
  Actuator condition such as
  (v) Valve Open/Close, and
  (vi) Pump ON/OFF.

(b) Control items, operated by hardwired switch:
  (i) Pumps, and
  (ii) Valves.

(7) Support Systems
The support systems required for the SA C&I System include:
(a) Power sources, and
(b) HVAC.

14.6.7 Reactor / Turbine Auxiliary Control Systems

The Reactor / Turbine Auxiliary Control System (ACS) is the means of providing control for the turbine, the generator and their major auxiliaries such as cooling water. The Reactor / Turbine Auxiliary Control System is divided into two parts; the Reactor Auxiliary Control System and the Turbine Auxiliary Control System. Figure 14.6-15 provides an overview of the duplex redundant auxiliary control system for the reactor and turbine. The majority of these systems are directly classified as Class 3 or not classified and implemented using digital (HIACS) technology. The ACS is supported primarily by the normal battery backed electrical supplies and HVAC. The ACS is installed in the Main Control Room (MCR) of the Control Building (C/B). Details of these systems are provided in the BSCs on ACS [Ref-11].

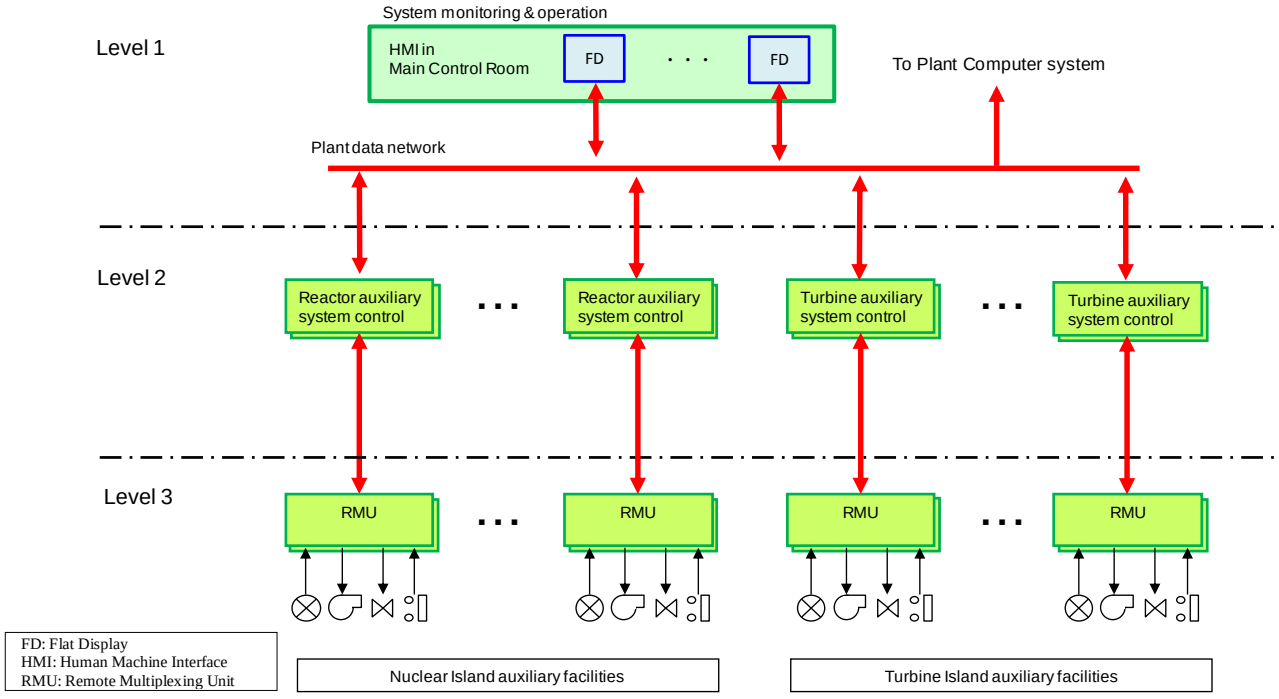


Figure 14.6-15: C&I Architecture of Reactor / Turbine Auxiliary Control System

14.6.7.1 Reactor Auxiliary Control System

(1) Overview

The Safety Class 3 reactor auxiliary control system is a dual redundant system using a microprocessor platform (HIACS); it includes the following sub-systems:

(a) NB (Nuclear Boiler System): controls the valves related main steam line,
(b) RRS (Reactor Recirculation System): controls the purge water flow for the RIPs,
(c) CUW (Reactor Water Clean-up System): provides continuous purifying for reactor water,
(d) MUWC (Makeup Water Condensate System): supplies purified water for plant operation,
(e) CRD (Control Rod Drive System): operates control rods positions,
(f) RD (Radioactive Drain transfer System): transfers radioactive drain to Radwaste systems,
(g) IA (Instrument Air System): supplies compressed clean air to plant instruments,
(h) DWC (Drywell Cooling System): keeps air condition of the drywell,
(i) HVAC (Heating Ventilating and Air Conditioning System): maintains temperature and humidity of the building environment and prevent the leakage of radioactive air from buildings.
(j) LDS (Leak Detection System): detects a leakage of coolant,
(k) AC (Atmospheric Control System): injects nitrogen into the PCV, and
(l) SAM (Sampling and Post-Accident Sampling System): SAM measures the necessary data to verify the plant condition.

The system information and manual controls are linked to flat displays on the main control console in the MCR. They also provide an input to the plant computer system.

Further detail is given in Generic PCSR Chapter 12, section 12.3 to 12.4 and Chapter 16, 16.3 to 16.5.

(2) System Architecture Interfaces and Layout

Further details are provided in the BSCs on ACS [Ref-11].

(3) Platforms

The system is built on the HIACS platform that is described in detail in Topic Report on Class 3 Platform [Ref-16].

(4) Sensors and Input Processing

Further details are provided in the BSCs on ACS [Ref-11].

(5) Actuators

Further details are provided in the BSCs on ACS [Ref-11].

(6) Human-Machine Interface

The main HMI for the ACS is located on Main Control Console (MCC) and Wide Display Panel (WDP) in the MCR using flat displays (see Generic PCSR Chapter 21, section 21.4).

(7) Support Systems

The support systems required for the Reactor ACS include:

(a) Power sources, and
(b) HVAC.

14.6.7.2 Turbine Auxiliary Control System

(1) Overview

The turbine auxiliary control system is a dual redundant system using a microprocessor platform (HIACS), it includes the following sub-systems:

(a) MS (Turbine Main Steam System): Steam supply to the turbine system,
(b) CFDW (Condensate System, Feedwater System): Feedwater supply to the reactor,
(c) AO (Air Off Take System): Vacuum rise and vacuum retention of the condenser,
(d) HD/HV (Feedwater Heater Drain System/Feedwater Heater Vent System): Drain pumping up to the condensate system,
(e) Main Turbine: Steam energy conversion to rotative force,
(f) EHC (Electro-Hydraulic Turbine Control System): Control the auxiliary for EHC controls,
(g) TGS (Turbine Gland Steam System): Gland seal steam supply,
(h) LO (Turbine Lubricating Oil System): Supply lubricating to the turbine and generator bearings.
(i) MSR (Moisture Separator Reheater): Improve the thermal efficiency of the plant,
(j) ES (Extraction Steam System): Steam supply to the Heater,
(k) TBP (Turbine Bypass System): Excess steam bypass to the condenser,
(l) AS (Turbine Auxiliary Steam System): Steam supply to auxiliary systems,
(m) GEN (Generator): Rotative force conversion to electricity,
(n) CW (Circulating Water System): Cooling water supply to the condenser,
(o) TCW (Turbine Building Cooling Water System): Cooling water supply to the turbine building facilities,
(p) TSW (Turbine Building Service Water System): Cooling water supply to the turbine building cooling water system,
(q) HS/HSCR (Heating Steam System / Heating Steam Condensate Water Return System): Clean steam supply to the equipment operating with house steam, and
(r) OG (Off-gas System): Minimise the release of radioactive noble gases and iodine to the environment.

The system information and manual controls are linked to flat displays on the main control console and the back panel in the MCR. They also provide an input to the plant computer.

Further detail is given in Generic PCSR Chapter 17, section 17.3 to 17.10.

Further details of the Reactor / Turbine Auxiliary Control Systems are provided in the BSCs on ACS [Ref-11].

(2) System Architecture Interfaces and Layout

Further details are provided in the BSCs on ACS [Ref-11].

(3) Platforms

The system is built on the HIACS platform that is described in detail in Topic Report on Class 3 Platform [Ref-16].

(4) Sensors and Input Processing

Further details are provided in the BSCs on ACS [Ref-11].

(5) Actuators

Details are provided in the BSCs on ACS [Ref-11].

(6) Human-Machine Interface

The main HMI for the ACS is located on Main Control Console (MCC) and Wide Display Panel (WDP) in the MCR using flat displays (see Generic PCSR Chapter 21, section 21.4).

(7) Support Systems
The support systems required for the Reactor ACS include:

(a) Power sources, and
(b) HVAC.

14.6.8 Plant Computer System

(1) Overview

Plant Computer System (PCS) is used for monitoring, recording and displaying; it is not used to directly control the plant. The information provided enables the nuclear power plant to be operated efficiently and to achieve an economic nuclear fuel burn up.

Key functions provided by the PCS include:

(a) Plant performance calculation,
(b) Plant monitoring support functions,
(c) The support functions for plant operation (e.g. guidance for plant operation),
(d) Data recording, and
(e) Data transmission outside the PCS.

A complete list can be found in the BSCs on the Plant Computer System [Ref-12].

The PCS is supported by the Class 3 normal electrical supplies and the HVACs.

(2) System Architecture Interfaces and Layout

The Plant Computer System role includes supporting the control room displays and operator interface with the control system, providing data logging and alarm functions. The configuration of the dual redundant plant computer system is shown in Figure 14.6-16 including its interfaces to the other systems. Its interfaces are also shown in Figure 14.5-1. The plant computer system is for monitoring, recording and display; it drives the Plant level Flat Displays for current, trend and related information. Further information is described in Basis of Safety Cases on Plant Computer System [Ref-12].

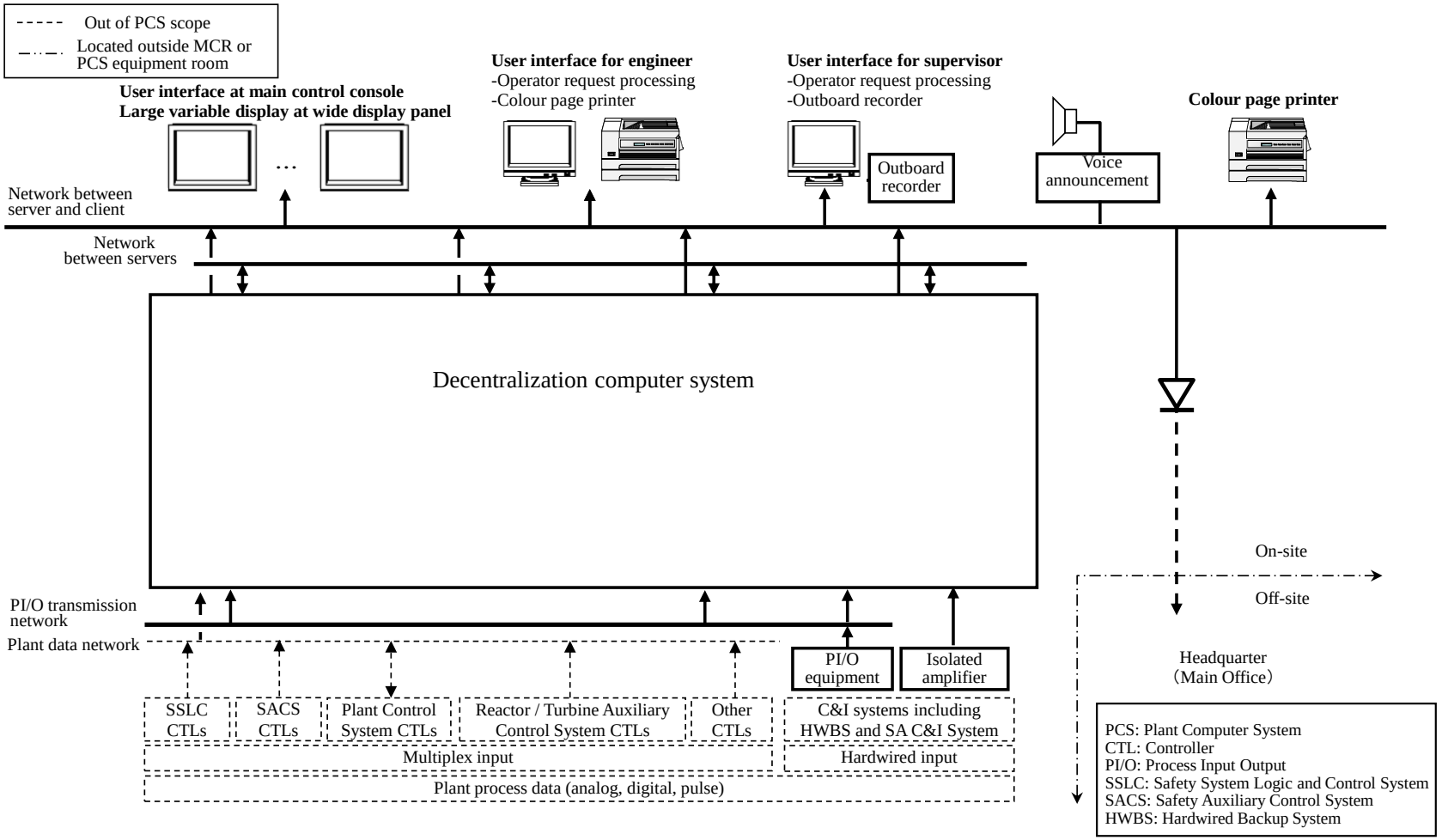


Figure 14.6-16: C&I Architecture of Plant Computer System

The PCS also has other equipment such as colour page printer, I/O (Input/Output) equipment, isolated amplifier, high-speed input device, user interfaces, voice announcement devices, firewalls. The PCS equipment is installed in the computer room of the Control Building (C/B).

(3) Platforms

Industrial PCs with Linux based real time OS.

(4) Sensors and Input Processing

Further details are provided in the BSCs on PCS [Ref-12].

(5) Actuators

N/A

(6) Human-Machine Interface

Further details are provided in the BSCs on PCS [Ref-12].

(7) Support systems
The support systems required for the Reactor PCS include:

(a) Power sources, and
(b) HVAC.

14.6.9 Others

The 'Other' C&I Systems include the following:
(1) Traversing In-core Probe (TIP),
(2) Area Radiation Monitoring System (ARM),
(3) Process Radiation Monitoring System (PRM),
(4) Radwaste (RW) C&I system, and
(5) Embedded systems (e.g. R/B overhead crane and Fuel Handling Machine (FHM)).

The Others System is described below:

(1) Traversing In-core Probe (TIP)

The TIP is a device that is used to calibrate the Local Power Range Monitor (LPRM). TIP provides the mutual calibration of the LPRM detectors in the range of 10 to 100 percent of the reactor rated output, and provides space distribution data of the neutron flux in the core to the core performance calculator.

(2) Area Radiation Monitoring System (ARM)

The ARM is a system for measuring and monitoring the gamma equivalent dose rate in management (controlled) areas of nuclear power plant. The ARM is installed to properly carry out the management of the dose to staff in the restricted access areas / the management areas of the plant. In the event of an accident, the system provides radiation monitoring for managing building entry by radiation workers, the ARM will measure the environmental gamma dose equivalent rate where necessary.

(3) Process Radiation Monitoring System (PRM)

The purpose of PRM is monitoring the operating state of the plant and the environmental release of radioactive waste during the various operation modes. To achieve this, the PRM measures the radioactivity content in the process fluid (liquid and gas). Measuring the radiation level in the process fluid also provides indication of the release of radioactive material to the environment at the time of an accident.

(4) Radwaste (RW) C&I system

This system collects data on the radioactive waste generated during plant operation and/or plant stoppage, performs processing, and recovers treated water for plant use water, or releases treated water externally. For solid waste, the system performs separate data collection and storage by waste forms, and after reducing radioactivity, supports the solidification process.

(5) Embedded systems

The C&I embedded as part of the plant equipment (e.g. R/B overhead crane and FHM) will also be considered as part of the C&I but not as part of this Architecture. These embedded systems are clarified in the list of Embedded C&I and SMART devices in SC1 or SC2 systems [Ref-31]. Further description of embedded systems used for the plant equipment important to safety throughout the ABWR facility, including fuel route, access control, hazard barrier and EDG control, is developed in section 14.8 of this chapter.

14.7 Sensors and Pre-Processing, Actuators

14.7.1 Introduction

Safe and efficient reactor operation relies on timely accurate plant information that is obtained from sensors measuring the plant conditions and by having sufficient suitable actuators to bring about the required control and safety functions.

Sensors

Key control and safety measurements for the ABWR include neutron flux, reactor pressure, reactor water level (differential pressure), radiation level as well as flow (differential pressure), temperature and position measurements. With some exceptions, the necessary indicating and recording instruments are installed in the MCR.

The reactor safety instrumentation is for the main (SSLC) and the backup (HWBS) safety systems. The reactor plant process instrumentations are connected to the PCntlS. Descriptions of the sensors are provided in section 14.7.3 of this chapter.

Each of the sensors are assigned the same safety category as the safety category of function they support and hence have the same class as the C&I system platform. The sensors also maintain the independence and diversity requirements of the systems they input to. For example, the reactor water level measurement is used for all 3 diverse systems: the SSLC, HWBS and PCntlS, however each reactor water level measurement is independent and diverse to prevent a failure affecting more than one system by a CCF.

Actuators

Actuators are required to initiate operation of plant items such as the control rods, pumps and valves. The actuators on the ABWR initiate operation of such equipment where electric power, hydraulic pressure and mechanical stored energy are the prime movers. While the majority use electric signals some use instrument air and nitrogen to initiate action. Descriptions of the actuators are provided in section 14.7.4 of this chapter.

The design of the ABWR seeks to avoid the need for dual control of equipment; however, in practice this cannot always be achieved. For example, the control rods are used for control of power and power distribution (by the control system using the fine motion control rod drives) and protection (by the SSLC using hydraulic insertion) although the two drive systems are independent with the hydraulic drive having precedence. ABWR controls the protection system equipment by the reactor protection system (SSLC RPS) C&I only, not by using both the protection and control C&I systems. For the control rod drives the protection action is prioritised in the design of the mechanical arrangement of the systems and not by using logic to prioritise between commands from the safety and the control systems. For example, the hydraulic actuation that drives the control rods into the core is independent of the fine motion control rod drives acting directly on the rods to move them. It is important to note the UK ABWR does not use Priority Actuation Logic C&I systems. As described in the control rod example above where dual control and protection is used then it is resolved by the inherent mechanical and electrical design of the system, not by use of complex priority actuation logic C&I.

14.7.2 Requirements

The measurement and hence sensor requirements are identified as part of the BSCs of the individual systems. These requirements include their performance (including reliability, accuracy and response time), environmental robustness (temperature, pressure, seismic and radiation) and diversity separation and independence. Requirements for diversity independence and separation may arise from other sources e.g. requirements for each safety class described in IEC61226 and is taken into account.

The design of the instrumentation fully considers the provisions for various operation modes (see Generic PCSR Chapter 5) and the response to anticipated operational occurrences to:

(1) Maintain and control, within an appropriate expected range, process parameters to ensure the integrity of the core, reactor coolant pressure boundary, reactor containment boundary and the associated systems.
(2) To monitor the plant parameters within an expected range of fluctuations so that necessary functional safety measures can be initiated.

As described in Section 14.6.6 of this chapter, particular instrumentation is also required to be able to monitor those parameters which, in the event of an accident, are necessary to understand the accident and to decide on and take remedial action, in an appropriate manner. This instrumentation design will cover sufficient range for accident and severe accident conditions so that a proper indication and record of these parameters can be produced. The severe accident monitoring instruments are designed to withstand the conditions encountered in a severe accident.

14.7.3 Sensors and Pre-Processing

The reactor power is measured by suitable neutron-flux detectors over a range of about 9 decades, i.e. from the startup range to the power range. All of the neutron-flux detectors are located inside the core. Two types of detectors are used for neutron-flux monitoring, both are fission-chamber type detectors but one is for the startup range, and the second for the power range. Details of each type of neutron-flux detectors are described in Topic Report on NMS [Ref-32].

The Neutron Monitoring System is designed to provide measurement for the SSLC (RPS) safety system so that when there is a potential for fuel damage due to excessive reactor power generated during abnormal operational transients, the SSLC (RPS) can prevent the fuel damage by detecting this phenomena in advance and initiating a trip (scram) of the reactor. In addition, there is a requirement that the neutron monitoring system includes a rod block monitor so that control rod withdrawal is blocked before the acceptable fuel design limits are exceeded, above the predetermined reactor power.

The Process Radiation Monitoring System (including Safety Process Radiation Monitoring System) is provided to allow determination of the content of radioactive material in various gaseous and liquid process streams. One of the objectives of this system is to initiate the SSLC action to limit the potential release of radioactive substances from the primary and secondary containments if predetermined radiation levels are exceeded.

The reactor plant process instrumentation consists of instrumentation such as the Reactor Vessel Instrumentation (RVI), the Recirculation System instrumentation, the Reactor Feed-water System instrumentation, the Main-Steam System instrumentation and the Control-Rod Drive System instrumentation. The instrumentation measures and indicates variables such as temperature, pressure, flow rate and water level for the SSLC, HWBS and control system; each has their own sensors that preserve the independence and diversity of and are powered by the system to which they are attached.

With some exceptions, the necessary indicating and recording instruments are all installed in the main control room.

Some of the instrumentation piping headers for measuring the reactor pressure and water level are shared by the safety systems and the other control systems. The installation is designed so that the functionality of the safety systems will not be affected by any electrical failures, short circuits, ground faults, broken wires, instrumentation piping failures or other faults or failures associated with the other systems or the detectors dedicated to the other systems. A schematic example of the interconnections of the reactor water level instruments are shown in Figure 14.7-1. A description and substantiation of this arrangement, including detailed locations and system interconnections, is developed in the BSCs on C&I Architecture [Ref-5] and the Topic Report on Reactor Pressure Vessel Instrument System [Ref-33].

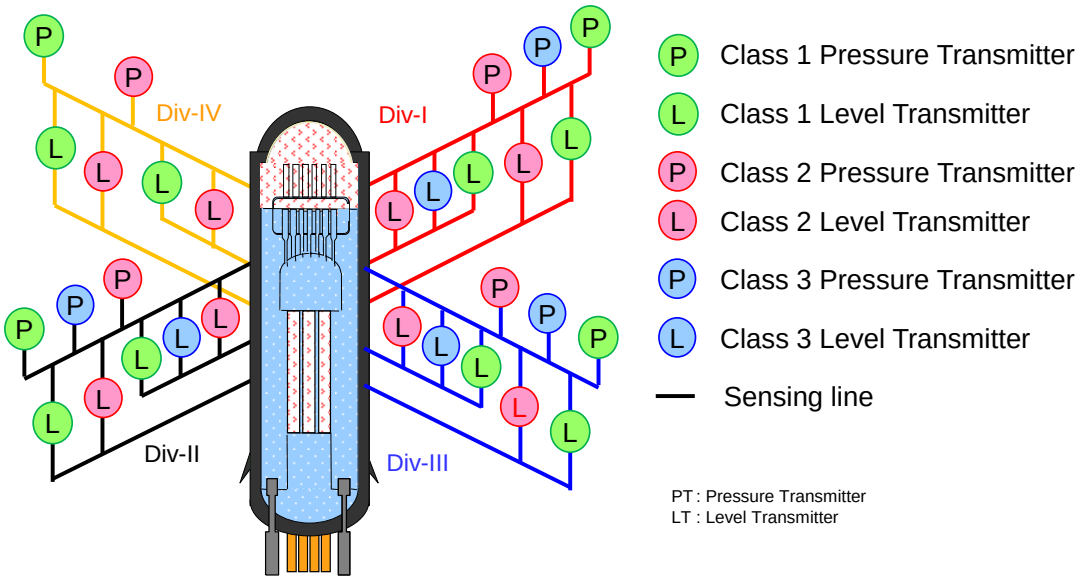


Figure 14.7-1: Schematic of interconnections of reactor water level instruments

14.7.4 Actuators

There are actuators for implementation of each function of the main and backup safety systems. The actuators of the main (Class 1) and the backup (Class 2) safety systems are required to be diverse and independent.

There are Class 1 and 2 actuators for implementing reactor shutdown, and emergency core cooling Functions.

14.8 Embedded C&I Systems

Although the focus of this chapter is on reactor C&I systems, there are other C&I systems important to safety used throughout an ABWR facility. Many of these systems are closely tied to a supplier's technology and detailed supplier information will not be known until the site specific phase of the project after the completion of GDA. However because of the importance of the fuel route and embedded C&I to the overall safety of ABWR facility high level principles for their design architecture have been developed and are summarised in this section. Fuel route C&I is largely based on the design of interlocks and alarms and the design principles for this topic can readily be translated to areas such as access control barriers to, for example, entry to radiologically classified areas.

14.8.1 Fuel Route C&I

The two main systems featured in the fuel route safety case, see Generic PCSR Chapter 19, are the Reactor Building Crane (RBC) and the Fuel Handling Machine (FHM) where safety important C&I is required. There are other systems but identical C&I design principles have been applied to those used for the RBC and FHM.

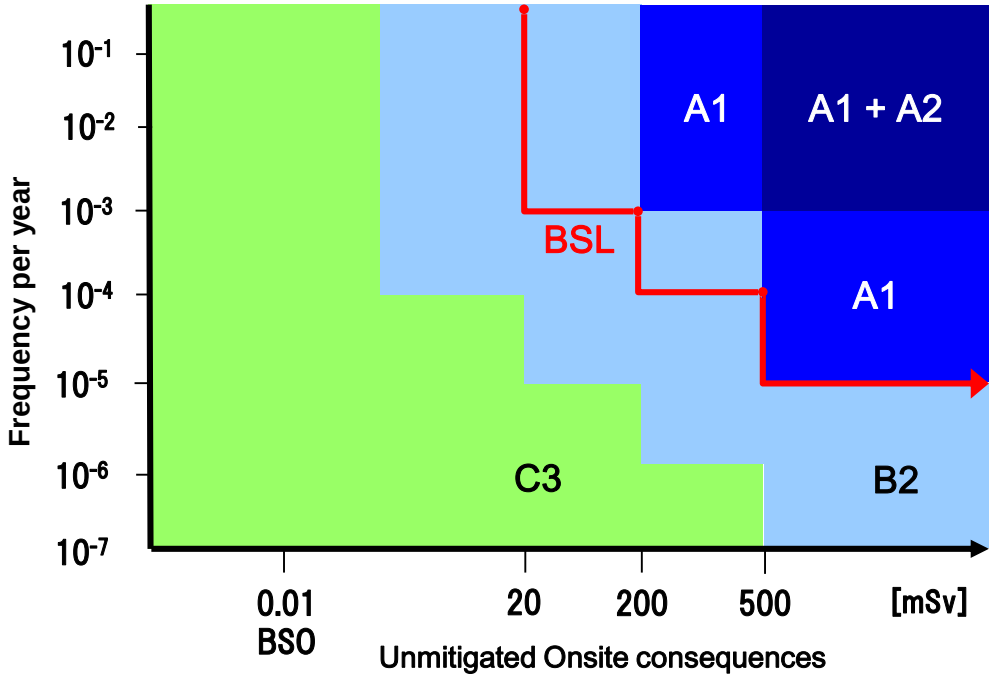


Figure 14.8-1 Unmitigated Dose Target Diagram

Figure 14.8-1 shows the unmitigated dose versus frequency target diagram for onsite radiological consequences taken from Hitachi-GE's UK ABWR NSEDPs [Ref-1], there is a similar diagram for offsite consequences. The above diagram show deterministic rules applied for the protection of unmitigated faults. For example if the unmitigated consequences were in the top right hand corner then the Safety Function is Category A and the protection required is two completely independent systems at Safety Class 1 (A1) and Safety Class 2 (A2) and is shown as 'A1 + A2'. To align the design with the considerable defence-in-depth through redundancy and diversity achieved for the reactor systems the main C&I design principle is also based on achieving using, where necessary, three independent C&I platforms.

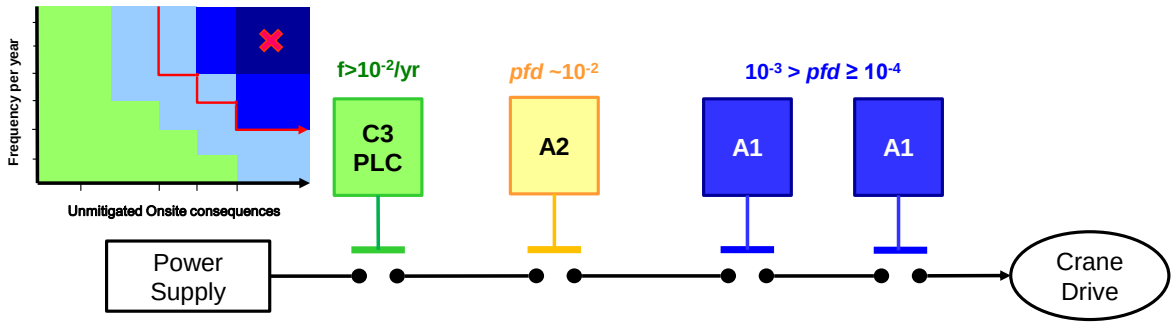


Figure 14.8-2 A1 + A2 Protection

Figure 14.8-2 shows a potential configuration on the FHM where an A1 + A2 protection is required from the C&I. The above diagram is a highly simplified version of what would be required and is used to illustrate the key design principles. The numbers at the top of the C&I symbols show the frequency of failure of the control system (*f*) and the probability of failure-on-demand (*pfd*) of the C&I-based safety interlocks. All C3 Programmable Logic Controllers (PLC) are assumed to fail frequently ($1x10^{-1}$/yr – $1x10^{-2}$/yr). The different colour of each main block indicates a completely diverse and independent C&I platform. In the above example the Class 3 control system will be based on PLC technology from, for example, the FHM supplier. The A1 system would have to be a fully duplex system to meet the single failure criterion. No planned maintenance would be undertaken on a crane when it is in operation and any fault detected prior to a potentially hazardous operation would stop the lift or crane movement from happening. This means that the single failure criterion is satisfied by two independent divisions of C&I equipment shown in the red boxes in the above diagram. In order to meet good safety principles and cyber security principles (not discussed further in this document) an important design principle is that the A1 C&I system should be hardwired. The reason for this difference with the reactor systems, where the HWBS is A2, is that the unmitigated consequences of all plant control systems faults always require A1 + A2 protection. However the unmitigated radiological consequences of many fuel route failures are much lower than the A1 + A2 threshold and therefore the C&I is often fully met by the use of an A1 system as shown in Figure 14.8-3. This configuration of an A1 protection will cover the majority of the cases. Even where A1 + A2 is required in some situations the A2 function is fulfilled by a mechanical interlock device.

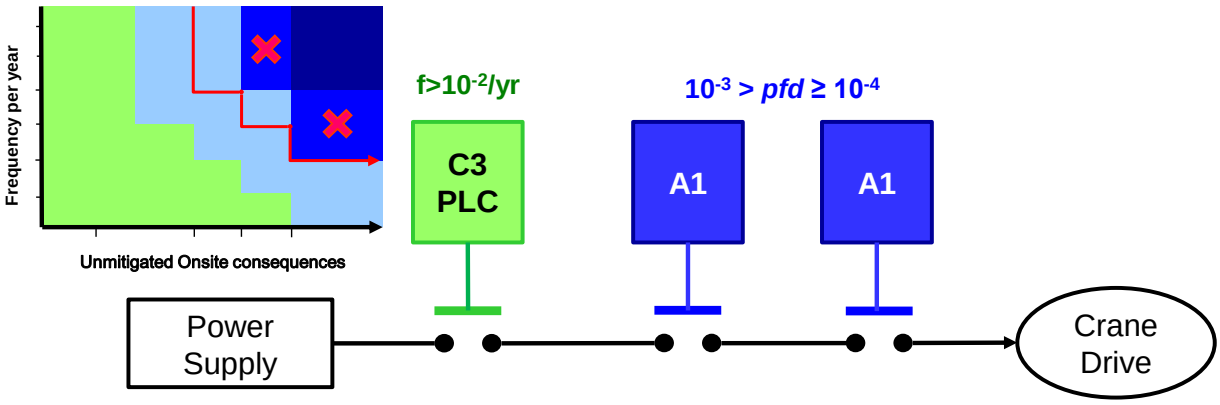


Figure 14.8-3 A1 Protection

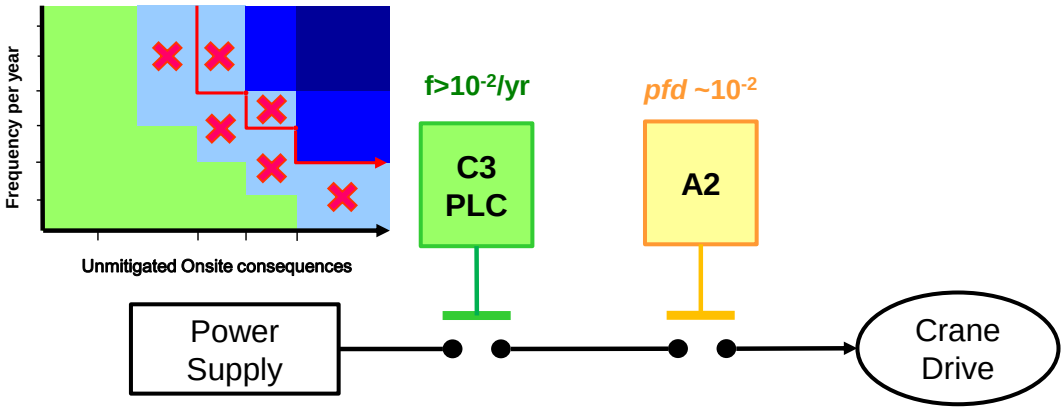


Figure 14.8-4 A2 Protection

An important part of GDA is to justify the viability of proposed C&I architectures shown in three Figures 14.8-2 to 14.8-4 and in particular the establishing the availability of hardwired technology for A1 safety functions on major systems such as the RBC and FHM. To establish the viability of the proposed C&I architectures a review was undertaken by holding discussions with two crane supplier Companies with considerable experience of supplying major lift systems such as RBCs. Both Companies showed that they had good hardwired safety grade technology, covering sensors, logic solver and actuators, that could satisfy all A1 functions on the RBC. Both offered relay technology for the logic solver but both considered that they could adapt their designs to use available Solid State Dynamic Logic similar to that of the HWBS if necessary.

Table 14.8-1 Technology Options

Option	Sub-System	Equipment Type Preference	Example System I/O		Number of Channels
1	Control	Safety Grade PLC	I/O	SMART sensors Input to motor control	1
	Protection A1	Relay Logic	I/O	Discrete components Contactors / relays	2
2	Control	Safety Grade PLC	I/O	SMART sensors Input to motor control	1
	Protection A1	Solid State Dynamic Logic	I/O	Discrete components Contactors / relays	2
3	Control	Safety Grade PLC	I/O	SMART sensors Input to motor control	1
	Protection A1	Solid State Dynamic Logic	I/O	Discrete components Contactors / relays	2
	Protection A2	Relay Logic	I/O	Discrete components Contactors / relays	1

The viable technology options for different configurations of the fuel route C&I for systems such as the RBC and FHM are raised and studied during GDA. The option study will be continued post GDA phase by a future licensee to develop and evolve the fuel route C&I design in the site specific phase of the project. Generic PCSR Chapter 19 provides more detailed information on fuel route mechanical engineering systems and plant layout.

14.8.2 Access Control and Hazard Barrier

For example entry control systems will require alarms and door interlocks. Other doors such as fire or other hazard barriers will also require alarms and potential interlocks. These systems will follow the same approach to the design of interlocks and alarms as described in section 14.8.1 of this chapter on fuel route.

14.8.3 EDG Control

An example of embedded C&I can be taken from the electrical power supply system (EPS, Generic PCSR Chapter 15). In the event of a loss of offsite power supply the Class 1 embedded C&I sends a signal to the EPS to start the Emergency Diesel Generators (EDGs). In responding to this command for each EDG, the embedded C&I will ensure it successfully starts and continues to operate stably and reliably. Each EDG will have technology such as electronic engine management systems, lube oil systems, automatic voltage regulators etc. as a part of the overall package provided by a future EDG supplier. As the supplier for such technology will not be selected until the site specific phase of the project design details for embedded C&I have not yet been established. However as a part of GDA design rules have been developed to be used in future equipment specification documents to ensure that the embedded C&I is fully aligned with its safety functional role.

The principles are as follows:

(1) If the embedded C&I is essential for the operation of the system, it is supporting (e.g. EDG) it will have the same safety class. For example the EDG system is Safety Class 1 and therefore essential embedded C&I will be Safety Class 1.
(2) Where important principles such as fail-safe or fail-as-is are specified for the safety system these will be fully implemented within the embedded C&I systems.
(3) Embedded C&I will be designed to safely interface with the main C&I systems that initiate their actuation. In the example of the EDGs the main interface will be with the SSLC.
(4) Embedded C&I systems will conserve and support the overall C&I architecture for claims on independence. For example for the A2 systems controlled by the HWBS there will also be a strong expectation that the embedded C&I will also be hardwired. A good example is the backup building diesel generators.
(5) Where embedded C&I uses SMART devices they will go through the full production excellence and independent confidence methodology for their Safety Class as described in 14.11.5 of this chapter.
(6) An embedded C&I system essential for the operation of the system it is supporting will be fully qualified to perform its safety functional roles under specified environmental conditions. For example where a system such as an EDG requires being seismically qualified its embedded C&I will be also be seismically qualified.

14.9 C&I Support Systems

14.9.1 Introduction

This section presents the support system required by the C&I systems. The support systems include:
(1) Electrical power supplies (Generic PCSR Chapters 15 and Chapter 16, section 16.6.2),
(2) Instrument air and nitrogen (Generic PCSR Chapter 16, section 16.4.1),
(3) Water Cooling,
(4) HVAC systems (Generic PCSR Chapter 16, section 16.5), and
(5) Fire Protection.

The support systems provide support in accordance with the Category of the safety function and Class of the C&I system. The support systems are by default the same class as the systems that they are supporting (Claim SPC C&I 1).

14.9.2 Systems

(1) Electrical power supplies for the C&I

There are three major electrical systems supporting the C&I; Class 1 for the SSLC, Class 2 for the HWBS, both are diesel backed supplies and the Class 3 station supply. The electrical power supplies are designed according to the need to maintain functionality for each of the applicable systems in the event of failure of the normal power supplies, e.g. due to loss of offsite power or station blackout.

Each of the C&I systems (SSLC, HWBS, etc.) is provided with an electrical power supply which is consistent with the classification of the supported C&I systems.

The three divisions of 6.9 kV Safety Class 1 Electrical Power System (EPS) is normally supplied via the Safety Class 3 buses which are connected to the off-site power source. The divisions of 6.9 kV Safety Class 1 EPS are supported by three Emergency Diesel Generators (EDGs) and the Diverse Additional Generator (DAG). The EDGs are available under Loss Of Off-Site Power (LOOP) conditions to support the C&I. The DAG is available under Station Black Out (SBO) conditions to support the C&I.

The two divisions of 690V B/B Class 2 EPS is normally supplied from Safety Class 3 buses via transformers which are connected to the off-site power source. The 690V B/B Class 2 EPS are supported by the Backup-Building Generators (BBGs). The BBGs are diverse from the EDGs. The BBGs are available under LOOP and SBO conditions to support the B/B Class 2 C&I.

The provision of local electrical supplies for C&I system are shown in Generic PCSR Chapter 15, sections 15.4.1 to 15.4.9, and are summarised below.

C&I System	C&I Electrical Supply
SSLC	• Each SSLC division is supplied from an independent division of the 4 division Safety Class 1 uninterruptible AC power supplies (UPSs) and the 4 division Safety Class 1 DC Power Supplies. • Each division of the Safety Class 1 C&I Power System is supported by dedicated Safety Class 1 Battery which is available under LOOP conditions.
HWBS	• Each HWBS division is supplied from an independent division of the B/B Class 2 AC and DC Electrical Power Supplies. • Each division of the B/B Class 2 DC Electrical Power Supplies is supported by a dedicated B/B Class 2 Battery which is available under LOOP conditions.
SACS	• Each SACS division is supplied from an independent division of the 4 division Safety Class 1 uninterruptible AC power supplies (UPS) or the 4 division Safety Class 1 DC Power Supplies. • Each division of the Safety Class 1 C&I Power System is supported by dedicated Safety Class 1 Battery which is available under LOOP conditions.
PCntlS	• PCntlS is supplied from the 2 channels of the Safety Class 3 AC dedicated C&I supplies. • The Safety Class 3 AC dedicated C&I supplies and are normally supplied via the Safety Class 1 Electrical System.
SA C&I	• Each SA C&I division is supplied from an independent division of the B/B Class 2 AC and DC Electrical Power Supplies. • Each division of the B/B Class 2 DC Electrical Power Supplies is supported by a dedicated B/B Class 2 Battery which is available under LOOP conditions.
ACS	• ACS is supplied from the 2 channels Safety Class 3 AC dedicated C&I supplies. • The Safety Class 3 AC dedicated C&I supplies and Safety Class 3 DC System are normally supplied via the off-site power.
PCS	• PCS is supplied from one of the 2 channels Safety Class 3 AC uninterruptible AC power supplies (UPS). • Each division Safety Class 3 AC UPS is supported by Safety Class 3 Battery system which is available under LOOP conditions. • The Safety Class 3 AC UPS are normally supplied via the off-site power.

The reliability of the electrical power supplies for C&I systems and their related mechanical plant are sufficiently to meet the targets claimed in the PSA and include electrical protection so that a partial system fault would not affect other systems. The architecture and redundancy allows the design targets, e.g. N+2 for Class 1 and diversity between the Class 1 and B/B Class 2 safety supplies, to be met as well as for equipment isolation and maintenance.

Details of the electric power supplies are described in Generic PCSR Chapter 15, section 15.1, 15.3 to 15.5.

(2) Instrument Air and Nitrogen supplies

The air supply systems consist of an Instrument Air System and a station Service Air System. They supply the compressed air needed to operate the reactor. As the air inside the containment vessel is normally replaced with nitrogen gas during startup and power operation, the air-operated valves inside the containment vessel are supplied with nitrogen, and compressed air is supplied as a backup. Fail-safe designs are adopted in the air and nitrogen operated valves.

The compressed gas supply for SSLC controlled actuation circuits (scram, MSIV, ADS and isolation valves) are supplied from accumulators and pipework that are designed and is implemented to Class 1 standards.
The supporting equipment maintaining the pressure of the pneumatic reservoirs is implemented at a lower class, the C&I is in the SACS with dual redundancy at Class 2. Details of the air and nitrogen supplies are described in Generic PCSR Chapter 16, section 16.4.1: Compressed Air System.

(3) Water Cooling System

The Water Cooling System (such as RCW and RSW) is established to remove heat from both safety and no direct safety related reactor auxiliary components including some of the turbine auxiliary components.

The Water Cooling System has three independent electrical divisions and contains redundancy so that single failure of any electrical component in a system division will not interfere with the required safety action of the affected system.

The RCW supplies cooling water to plant auxiliaries. The RSW removes heat from the RCW by supplying service water from the ultimate heat sink to the RCW Heat Exchanger. They have equipment in divisions I, II and III. They are controlled by the SSLC ECCS/ESF which will automatically initiate the system in response to a LOCA or LOOP event or high Suppression Pool temperature. Manual control is also possible from the SSLC Class 1 HMI, SAuxP in the MCR and RSS.

The Water Cooling System is described in detail in Generic PCSR Chapter 16, section 16.3.2: Reactor Building Cooling Water Systems.

(4) HVAC

Temperature and humidity in the main control room and the reactor building is be controlled by Heating, Ventilation and Air Conditioning (HVAC) system to maintain the C&I equipment within its declared operating envelope and to provide a suitable environment for the operators. The HVAC also has a role in preventing the spread of radioactive contamination. The heating, ventilation and air conditioning system for the main control room and the C&I equipment areas control temperature and humidity and minimises radiation ingress in the event of accidents.

The HVAC system architecture supports the segregated divisional architecture of the C&I systems.

For the SSLC, a 4 division Class 1 system, there are three divisions of Class 1 HVAC equipment, with HVAC for the 4^{th} division of C&I being supplied by combinations of divisions I, II and III as required. They are supplied by the Class 1 electrical system.

For the HWBS, a 2 division Class 2 system, there are two Class 2 HVAC systems, which are powered from the Class 2 power supply to provide diversity from the Class 1 HVAC. They provide cooling to the Control Building and Backup-Building where HWBS C&I is located.

For the PCntlS, HVAC is provided by the MCR HVAC system, which is powered by Class 1 supplies. These HVACs are separate from the Class 1 HVAC used for the SSLC. The same policy applies to the ACS and PCS.

More detail of HVAC systems are described in Generic PCSR Chapter 16, section 16.5: Heating Ventilating and Air Conditioning System.

(5) Fire Protection for C&I systems and equipment

Redundant safety C&I systems and equipment are segregated by fire barriers, distance or the provision of fire detection and fighting system in order to prevent fire from spreading to other divisions and the failure of redundancy. Fire retardant cabling is used to reduce the risk of a cable fire.

Details of the Fire Protection are described in Generic PCSR Chapter 16, section 16.6.1: Fire Protection Systems.

14.9.3 Justification

The justification of Support Systems for the C&I Systems follows the same Claims Argument and Evidence approach used for the C&I as developed the Basis of Safety Cases on Control and Instrumentation Architecture [Ref-5].

The justification of the Support Systems, adequacy of their design and qualification is provided in the respective sections of the PCSR and supporting safety case document; this includes defence against single failures and CCF, independence, redundancy and providing same class for support system with C&I system.

14.10 Management Systems

14.10.1 Introduction

Hitachi-GE has a suite of management systems, processes and procedures that govern requirements, design, development, implementation, integration, verification and validation activities related to C&I. These are backed-up by comprehensive quality assurance activities. Details are described in Figure 3 of the project wide QUALITY MANAGEMENT PLAN [Ref-34].

These management systems, processes, procedures and quality assurance activities are applied to all platforms and to C&I applications/systems.

14.10.2 QA

A life cycle approach to quality assurance is applied to the C&I. Relevant quality assurance activities are applied at all phases of the C&I lifecycle see Generic PCSR Chapter 4, section 4.3.1: Hitachi-GE Safety and Quality Policy.

14.10.3 Safety Lifecycle

Quality control methodologies that are applied to the C&I system important to safety throughout the life cycle of the system are established, implemented, and documented. The process applied for C&I is identified in the C&I Design Process Plan [Ref-42] and this then refers to the relevant supporting process documents.

An IEC 61513 compatible lifecycle approach to the safety contribution of C&I is applied. This starts from the establishment of safety requirements for C&I from the Fault Studies and PSA activities. The categorisation of functionality and the classification of systems and equipment will grade some of the lifecycle activities and set the design and implementation requirements.

More detail about the life cycle activities is included in subsequent sections of this document.

14.10.4 Requirements Capture

The C&I safety requirements are underpinned by the Fault Studies and PSA activities (see Generic PCSR Chapters 24 and 25 respectively). These define the required safety measures and control the allocation of safety measures to C&I. A C&I Top Requirements document is created. This is reviewed and validated against the output of the Fault Studies and PSA activities carried out by the Safety Team.

C&I Requirements for individual systems are documented, according to the requirement management process which is defined in the C&I Design Process Plan [Ref-42].

14.10.5 Overall Lifecycles

Hitachi-GE has a suite of management systems, processes and procedures that govern requirements, design, development, implementation, integration, verification and validation activities related to C&I. These management systems, processes and procedures provide a life cycle for the C&I provision. The C&I Design Process Plan [Ref-42] includes a list of the management systems, processes and procedures and their application to individual C&I platforms and C&I systems.

Although some of the management system, process and procedure documents only exist in Japanese the C&I Design Process Plan [Ref-42] has provided the title and a short description of the contents of each document in English.

The approach is based upon IEC 61513. Hitachi-GE is using its existing management systems, processes and procedures for the design of C&I provisions where appropriate. However, processes compliant with the requirements of IEC nuclear standards have been introduced where required. Hitachi-GE will continue to review its existing management systems, processes and procedures post GDA phase against:

(1) Relevant international standards, including relevant IEC standards.
(2) Its understanding of UK good practice.
(3) Its understanding of UK regulatory expectations.

Any identified gaps will be addressed through justification of the existing approach, through changes or through compensatory measures.

The C&I life cycle includes the following steps;

1. Planning Phase (Plant Requirement)

All C&I activities and provisions for a UK ABWR project will be planned and coordinated by the C&I Engineering Team. The phase will follow an established suite of processes and procedures for the planning and co-ordination activities; these are documented in the C&I Design Process Plan [Ref-42]. This step identifies the overall functional and performance requirements of the C&I systems, identify the categorisation of C&I functions and review any system constraints.

Compliance with the documented process and procedures is subject to quality assurance activities such as management control, peer review, record keeping and periodic audit defined in the QUALITY MANAGEMENT PLAN [Ref-34].

2. Requirement Phase
2-1 C&I Architecture Requirement

The overall C&I architecture is designed to implement the overall requirement specifications of the C&I systems and to provide adequate measures against CCF Potential.

2-2 Functional Assignment

Following the overall C&I architecture design, the safety functions are assigned to the individual C&I systems and the functionality, constraints, boundaries and interfaces with other systems, interfaces with humans and environmental conditions are developed.

2-3 Design Analysis.

The reliability, defence against CCF and Human Factor requirements are assessed at this stage.

3. Design Phase (System Specification and detailed design)

The system architecture design is developed in order to implement the system requirements specification.

Following this the hardware and system or application software is developed (including the platform development activities – for the SSLC and HWBS). The application function requirements are then verified to confirm that the system requirements are captured in the detailed design.

A typical process is identified in the C&I Design Process Plan [Ref-42], and for each C&I platform a complete plan [Ref-46] will be produced which is commensurate with the requirements of the class of that system.

The design process is also described in detail in Generic PCSR Chapter 4, section 4.7: Safety in the Design Phase.

4. Implementation Phase (Integration)

During this stage the individual hardware and software components which make-up the system are integrated. Detailed implementation (manufacture) processes are defined for hardware, software and configuration of complex components and are referenced in the C&I Design Process Plan [Ref-42].

4-1 Hardware Implementation

A hardware implementation plan is prepared for each C&I system and the detailed system design is implemented using an established suite of processes and procedures that are identified in the BSCs documents for each platform and C&I system.

The assembled system hardware is verified against the detailed design documentation. Details of this verification activity are defined in the C&I Design Process Plan [Ref-42].

4-2 Software Implementation

Software implementation is described in section 14.11 and in relevant sub-sections of section 14.6 of this chapter.

4-3 Configurations of Complex Components

The configuration of complex components (such as ASIC (Application Specific Integrated Circuit) and FPGA) has many properties similar to the production and use of application software. This is particularly relevant to the FPGA-based platform for the SSLC and SACS systems. Hence there are appropriate management systems, processes and procedures established for producing the configuration databases (or similar) for complex components. Information on configuration management for the νCOSS® FPGA-based platform for Class 1 systems is included in the suite of development process documentation.

Further information is included in Section 14.11 of this chapter.

4-4 Integration

Integration activities are implemented to manage the integration of ‘software’ into the hardware of final systems.

An integration plan is prepared for each C&I system. This follows the established suite of processes and procedures in place for the C&I system integration activities. These processes and procedures are documented and are described in the system BSCs documents.

The integration plan (and the identified processes and procedures) includes a significant verification component. The functionality and properties of the integrated hardware, software and configuration data are verified against the detailed design documentation.

5. Examination Phase (Factory test)
5-1 System Validation

Validation processes are defined to confirm that the constituent parts of a C&I application or C&I system meet requirements. Details of the validation activities are defined in the C&I Design Process Plan [Ref-42].

6. Loading Phase (Site install and system test)

The C&I systems are installed in the site and tested their functionality.

7. Modification

Modification process is defined to control changes to the C&I requirements, design or implementation. This is one of the processes listed in the C&I Design Process Plan [Ref-42].

8. Commissioning Phase

In this phase, the final system is commissioned on site. Each activity and test is planned and documented.

Commissioning includes validation activities for components, equipment, sub-systems, C&I systems and the complete C&I Architecture installed on site. Commissioning is described in Generic PCSR Chapter 29: Commissioning and in Chapter 4, section 4.9: Safety in the Commissioning Phase.

9. Operation and Maintenance Phase

Operation and Maintenance are described in Generic PCSR Chapter 30: Operation and in Chapter 4, section 4.10: Safety in the Operational Phase.

10. Decommissioning Phase

Decommissioning process is defined to cover the end of life and decommissioning of C&I equipment or systems. Decommissioning is considered in detail in Generic PCSR Chapter 31.

The design and installation of the C&I takes into account decommissioning by seeking to ensure that those systems; e.g. radiation monitoring for personal protection, operate separately from those used for reactor operation.
C&I equipment is to be reviewed for the application to decommissioning activities before the end of generation. (For example, the radiation monitoring and plant monitoring)

Decommissioning of the majority of the C&I equipment (in particular the electronics) is achievable without any specific considerations. The amount of potentially radioactively contaminated material is minimised by locating equipment away from high radiation areas. Consequently most of the C&I equipment can be decommissioned by the reverse process of the construction without the need to access high radiation zones.

14.11 Hardware and Software Development and System Justification

14.11.1 Introduction

This section describes the hardware and software development processes and sets out the justification which shows the design development processes of the platforms applied to UK ABWR are valid and meet relevant IEC standards and regulatory expectations.

14.11.2 General Descriptions of Platforms for UK ABWR

There are three types of platforms for the UK ABWR: νCOSS® for Class 1 system, hardwired technology for the HWBS of Class 2 systems and HIACS for Class 3 control systems. In νCOSS®, FPGA based technology is applied as it is regarded as diverse from the microprocessor based HIACS. Each platform is comprised of hardware modules such as CPUs (Central Processing Units), IO (Input/Output) modules, network modules and power supplies. Application specific modules are also provided which are adapted to the platforms in the UK ABWR. In addition, dedicated engineering workstations and PADT (Programming and Debugging Tool) are used to support each platform to perform programming.

The platforms, including their dedicated PADT, are developed in accordance with appropriate IEC standards and are justified based on the UK specific principles and guidance.

Detailed technical information on the platforms is included in the Basis of Safety Cases on the Control and Instrumentation Architecture [Ref-5] to provide suitable evidence that the UK ABWR C&I systems are designed and will be manufactured, tested, installed and commissioned in accordance with standards appropriate to a system's safety class.

14.11.3 Design and Development

The overall design development of the systems important to safety for the UK ABWR complies with the requirements defined in IEC 61513. A lifecycle of the Hardware Description Language (HDL) development for νCOSS® is developed to comply with the requirements of IEC 62566 for Class 1 and the software development will comply with IEC 62138 for the HIACS. The hardware development for νCOSS® is compliant with IEC 60987.

14.11.3.1 Development of νCOSS® for Class 1 systems

The development process for the νCOSS® for Class 1 systems is based on the requirements of IEC 61513 and IEC 62566.
In developing the Class 1 platform, diversity to the Class 2/3 platforms is taken into account. Specifically, a plan to address platform-related diversity attributes shown in NUREG CR/6303 such as design diversity, human diversity, equipment diversity and software diversity are established in the beginning of the Class 1 platform development, and diversity evaluation against Class 2 HWBS and Class 3 HIACS platforms has been performed during the GDA. The detailed development of this process and supporting procedures has also been undertaken during the GDA. Further details of the development processes including verification and validation activities are provided in the Basis of Safety Cases on SSLC [Ref-6] and its supporting references.

14.11.3.2 Development of HIACS for Class 3 systems

(1) Design -

The software requirements documentation is available before the design and implementation of software development begin. Basically, a top down approach is applied to the software design. The end of the design phase is marked by the preparation of the software design specification. Serving as the basis for the subsequent software implementation.

(2) Implementation -

A function block diagram is applied to the application software. Function block diagram supports a simple software structure and allows the developers to take into account the C&I requirements, which are also shown by symbolic descriptions.

(3) Verification -

The verification activities are undertaken as part of the software development by staff not performing the software production. The software verification plan is prepared and issued prior to starting software verification activities.

Further details of the design processes used to develop the HIACS platforms are given in the Topic Report on Class 3 Platform [Ref-16]. Details of the processes for system development are given in the Basis of Safety Cases for the relevant system, e.g. [Refs-5 and 9].

14.11.3.3 Justification

The development processes and procedures have been justified by showing they meet modern practice for that class of system, and that they are compliant with current nuclear specific standards, i.e. IEC standards.

The quality of the safety systems using complex components will be demonstrated by the Production Excellence activities and Independent Confidence Building Measures that is considered good practice in the UK, e.g., SAP, 2014 Edition, Revision 0, ESS.27 and NS-TAST-GD-046, April 2017, Rev 3.

(1) Production Excellence (PE)
Production Excellence requires a demonstration of excellence in all aspects of production of the software (HDL for FPGAs) and the system, covering initial specification through to the finally commissioned system, comprising the following elements:

(a) Thorough application of technical design practice consistent with current accepted standards for the development of HDL for FPGA and software for computer-based safety systems.
(b) Implementation of an adequate quality assurance programme and plan in accordance with appropriate quality assurance standards.
(c) Application of a comprehensive testing program formulated to check every system function.

C&I design and implementation substantiation information is often not fully available and therefore complete until well into the site specific design, construction and commissioning stages of the site specific project post GDA phase. In recognition of this fact, a series of support documents in addition to this PCSR provides a summary of what information is available for GDA and analysis of the methodologies that will be used to provide a suitable safety case later during the site specific phase post GDA phase.

(2) Independent Confidence Building Measures (ICBM)
Independent Confidence Building Measures are applied to systems based on complex technology to provide an independent and thorough assessment of a safety system's fitness for purpose. This comprises the following elements:

(a) Complete and preferably diverse check of the finally validated product by a team that is independent of the systems suppliers, including:
  (i) independent product check providing a searching analysis of the product, and
  (ii) independent check of the design and production process, including activities needed to confirm the realization of the design intention.
(b) Independent assessment of the test programme, covering the full scope of test activities.

The ICBMs complement the PE activities and will include for Class 1 SSLC independent inspection and analysis and the statistical testing of the final system. The ICBMs methodology will be identified and pilot exercises have been completed during GDA to show that the selected approach for analysis can be applied within the project constraints. The complete set of ICBM activities will be completed post GDA phase under the control of the future licensee. The concept of ICBM activities for the Class 1 platform is provided in the Topic Report on ICBM for FPGA [Ref-14].

(3) Compensatory Measures

If the production excellence assessment identifies weaknesses in the production process, compensating measures are applied. The type of compensating measures will depend on the specific weaknesses found. Compensating measure adopts methods independent of ICBM activities, and also ICBM activities are executed after executing all compensating measures.

14.11.4 SMART devices

A SMART device is a device that contains a FPGA, ASIC, CPLD, microprocessor (and therefore contains both hardware and software) and is programmed to provide specialised capabilities, often measuring or controlling a process variable.

Principally, the use of SMART devices is avoided for the delivery of Category A safety functions by Class 1 systems. If the use of SMART devices cannot be avoided then they will be justified in a manner consistent with the class of the system that they are deployed in. A two legged approach will be used based on:

(1) Production Excellence, and
(2) Independent Confidence Building Measures.

If there are weaknesses in these legs, e.g. due to lack of information or noncompliance with standards requirements them compensatory measures will be introduced to counteract the weakness.

It is anticipated that all SMART devices selected for use will be developed to a recognised life-cycle. Then, a graded approach will be taken according to the Class of system the device is to be used in. For example for devices to be used in Class 1 systems consistency (consistency as it is unlikely that SMART devices will have been developed to nuclear standards and be compliant) with IEC standard 61513 and 60987 will be sought. For those SMART devices in Class 2 and 3 systems any software and its development would be expected to be consistent with IEC 62138. Please note that avoidance of all SMART devices will be a strong requirement for all embedded C&I for equipment controlled by the HWBS.

SMART devices justification will be completed on a case by case basis on device selection. However, an exercise was undertaken during GDA to demonstrate viability of the techniques. This

exercise has been completed successfully demonstrating the viability of the techniques and this has shown that proportionate approach can be taken according to the class of the device; i.e. most stringent for Class 1.

Further information on the justification of SMART devices can be found in the Topic Report on SMART Devices [Ref-13].

14.11.5 Design Tools

The development process for Class 1 systems on the νCOSS® will make use of design tools. The justification of these tools has been considered as part of the tool selection and development process. Further information on the design tools selected for Class 1 platform are provided in the Basis of Safety Cases on the SSLC [Ref-6] and its supporting references.

The development of Class 3 systems on the HIACS platform also makes use of software tools. These tools have been developed using the extant development practice, including ISO 9001 compliant process. The current and historic development practice will be reviewed as a compliance exercise. The base standards for these tools will be IEC 61513 and 62138. Details of these tools are described in the Topic Report on Class 3 Platform [Ref-16].

14.12 Assumptions, Limits and Conditions for Operation

14.12.1 Purpose

One purpose of this generic PCSR is to identify constraints that must be applied by a future licensee of the UK ABWR plant to ensure safety during normal operation, fault and accident conditions. Some of these constraints are maximum or minimum limits on the values of system parameters, such as pressure or temperature, whilst others are conditional, such as prohibiting certain operational states or requiring a minimum level of availability of specified equipment. They are collectively described in this GDA PCSR as Assumptions and Limiting Conditions for Operation (LCOs). The general principles for the identification of Assumptions, Limits and Conditions for Operation (LCOs), are described in Generic PCSR Chapter 4, section 4.12.

This section provides a summary of the Assumptions and LCOs that apply specifically to the scope of this chapter of the PCSR.

14.12.2 LCOs specified for C&I systems

In order to ensure that the C&I system is operated within safety limits and the design requirements from the safety case are met during the operating regime, appropriate Limit Conditions of Operation (LCO) are and corrective actions (measures) are defined to follow when the LCOs are not met. This information is described in the Basis on Safety Cases (listed below) and ultimately reflected in the Generic Technical Specifications [Ref-45], which are transferred to the utility owner to operate the plant as intended in the safety case.

The LCOs shown in [Ref-45] are identified from the safety cases of each C&I:

(1) SSLC including safety system platform and application [Ref-6]
- The SSLC functions are operable.

(2) Hardwired Backup System (HWBS) [Ref-7]
- The HWBS functions are operable.

(3) Safety Auxiliary Control System (SACS) [Ref-8]
- The SACS functions are operable.

(4) Plant Control System (PCntlS) [Ref-9]
- The PCntlS functions are operable.

(5) Severe Accident C&I System [Ref-10]
- The SA C&I system are operable.

(6) Reactor / Turbine Auxiliary Control System [Ref-11]
- To be determined with consideration for the previous plant experience by site specific design post GDA phase.

(7) Plant Computer System [Ref-12]
- To be determined with consideration for the previous plant experience by site specific design post GDA phase.

These safety cases identify the safety functions (FSFs, HLSFs) defined by Fault Study, relevant C&I Safety Function Claims, key SSCs implementing the C&I Safety Function Claims, relevant

surveillance requirements and the LCOs shown in [Ref-45]. Further information is given in the arguments and evidence for SPC 8 in each system BSC.

14.12.3 Assumptions for C&I system

(1) Class 1 SSLC and Class 2 HWBS platform

The requirements, specifications and the justification methods for the Class 1 SSLC platform have been discussed, and the specifications and justification methods were submitted to the regulator during GDA. The development of the SSLC platform will continue post GDA phase.

The requirements for the Class 2 HWBS platform have been discussed during GDA and simple hardwired technology confirmed. Some Class 2 HWBS platforms have been reviewed and judged to satisfy the safety functional and non-safety functional requirements for HWBS. The final platform applied for the HWBS platform will be selected, designed and developed in more detail post GDA phase.

(2) Class 1 Human-Machine Interface

The expectations for the Class 1 Human-Machine Interfaces have been discussed during GDA. During GDA, potential options have been raised for the justification of operability from a human factors perspective and the high level strategy for Class 1 HMI has been decided. The detailed technology applied for Class 1 HMI will be selected post GDA phase.

(3) SMART device

The expectations for SMART devices have been discussed and an exercise was undertaken during GDA to demonstrate viability of the justification techniques. The assumed application of SMART devices has been shown during GDA and the actual application of SMART devices will be confirmed in the site-specific detailed design phase; post GDA.

(4) Frequency of test and maintenance

The test and maintenance frequencies proposed for developing the safety case are based on J-ABWR practices. These frequencies will be studied and refined using PSA insights post GDA phase.

(5) Countermeasures against spurious all control rod insertion fault

Potential options for the countermeasure against spurious all control rod insertion fault have been raised and discussed during GDA. The selection of the final design for the countermeasure against the spurious all control rod insertion fault will be implemented post GDA phase.

14.13 Summary of ALARP Justification

This section presents a high level overview of how the ALARP principle has been applied for Generic PCSR Chapter 14 on C&I and how this topic contributes to the overall ALARP argument for the UK ABWR.

Generic PCSR Chapter 28 (ALARP Evaluation) presents the high level approach taken for demonstrating ALARP across all aspects of the design and operation. It presents an overview of how the UK ABWR design has evolved, the further options that have been considered across all technical areas resulting in a number of design changes and how these contribute to the overall ALARP case. The approach to undertaking ALARP Assessment during GDA is described in the GDA ALARP Methodology [Ref-36] and GDA Safety Case Development Manual [Ref-37]. For C&I this consists of the following steps:

- Establishing the Role of C&I in controlling risks to safety from the UK ABWR.
- Undertaking a gap analysis of the reference J-ABWR C&I design to UK relevant good practice.
- Undertaking an options analysis for closing gaps.
- Selecting and implementing the optimal ALARP solution.

14.13.1 Establishing the Role of C&I in Controlling the Risks to Safety From the UK ABWR

The fault studies chapters 24, 25 and 26 provide an overview of the safety functional claims for all safety structures, systems and components in the safety analyses of the UK ABWR. These chapters also show that C&I systems make a major contribution to safety at all five levels of the defence-in-depth defined in Generic PCSR Chapter 5, section 5.5. The mapping of the C&I systems to these levels of defence-in-depth (see Generic PCSR Chapter 5, section 5.5) are as follows:

- Class 3 Plant Control Systems (PCntlS) – Level 1 (Expected Events) and Level 2 (Foreseeable Events).
- Class 1 Safety System and Logic Control (SSLC) – Level 3 (Frequent and Infrequent Design Basis Faults).
- Class 2 Hard-Wired Backup System (HWBS) – [1]Level 3 (Design Basis Faults).
- Class2/3 Severe Accident (SA) C&I – Level 4 and 5 Severe Accidents.

The above list shows that the C&I systems play a very significant role in the safety of the UK ABWR. Similarly there is a significant interplay between C&I and the human based safety claims specified in Generic PCSR Chapter 27. This is reflected in Generic PCSR Chapter 21 on the Human-Machine Interface (HMI) where the C&I provides the information required for all of the UK ABWR HMIs.

The above means that C&I systems plays a critical role in supporting all aspects of safe operations at a UK ABWR site.

[1] For C&I this covers a special class of design basis fault involving a frequent design fault and a coincident common cause failure of the Class 1 SSLC or, for example fuel routes, the coincident failure of the Class 1 protection.

14.13.2 Undertaking a gap analysis of the reference J-ABWR C&I design to UK relevant good practice

It was established early in the GDA process that UK relevant good practice for C&I for nuclear power plant (NPP) was provided by three independent C&I platforms. This can be best understood by analysing the following equation:

$$f_{acc}=f_{PCntlS}.p_{SSLC}.p_{HWBS} \quad \ldots\ldots 1$$

Where:

- f_{acc} is the accident frequency.
- f_{PCntlS} is the frequency of the failure of the plant control system leading to the accident.
- p_{SSLC} is the probability of failure-on-demand of the SSLC.
- p_{HWBS} is the probability of failure on demand of the HWBS.
- the '.' represents multiplication.

For the PCntlS the target reliability, $f_{PCntlS,}$ as a frequency of failure per year (/yr) is within the limits of $1x10^{-1}$/yr -$1x10^{-2}$/yr.

For the SSLC its probability of failure-on-demand, p_{SSLC} , is conservatively assumed to be $1x10^{-4}$.

For the HWBS its probability of failure-on-demand, p_{HWBS}, is conservatively assumed to be $1x10^{-2}$.

Best estimate analysis in the PSA (see Generic PCSR Chapter 25) would result in lower figures of probabilities of failure-on-demand for both the SSLC and HWBS. Equation 1 shows that in order to get an accident with a radiological consequence requires the initiating event of the PCntlS starting an accident sequence and then the common cause failure of both the SSLC and HWBS. The multiplication of the frequencies and probabilities in equation 1 means that all three systems are required to independent.

Independence has been considered in accordance with UK NPP relevant good practice, and other important expectations such as standards and application of the single failure criterion – leading to the following principles:

(1) High standards of segregation and separation of three main C&I systems.
(2) High standards of electrical isolation.
(3) Where data networks are used, high standards of data isolation with strict one-way communication enforced by data-diodes between the Class 1 system and the PCntlS, and also use of one-way diodes between the PCntlS and the wider NPP computer-based networks.
(4) Each of the three main C&I systems based on platforms employing diverse technology.
(5) A strong expectation that at least one system would employ simple hard-wired technology.
(6) The Class 1 platform should preferably only control Category A safety functions.
(7) The Class 1 platform has to meet N+2 version of the single failure criterion.

UK ABWR is developed from base design J-ABWR for satisfying the UK NPP relevant good practice and UK expectations.
The above is not a comprehensive list of requirements for independence, which are covered elsewhere in this chapter and in its supporting BSCs and TRs (see reference section). Similarly this chapter and its supporting references do provide more information for safety claims on meeting the single failure criterion and on matters such as code and standards compliance.

14.13.3 Selecting and implementing the optimal ALARP solution

The reference J-ABWR design had strong claims on satisfying principles of separation (1) and isolation (2). For (3) the data network-based two-way communication between a lower safety class system and a higher safety class system with an appropriate electrical isolation is allowed for the J-ABWR. Considering diversity (4), the J-ABWR uses the same platform technology (HIACS) for the PCntlS and the SSLC. The J-ABWR hardwired controls are consistent with UK expectations from the perspective of independence (satisfying point 5 above) however, many controls required manual actuation in fewer than 30 minutes therefore there was a gap against point (6) above. Also the J-ABWR HIACS-based SSLC platform was not designed in accordance with the listed standards (8).

The considerations of the development for UK ABWR from the comparison between UK relevant good practice and the base line J-ABWR were therefore, as follows:

(1) Strengthening of diversity between the PCntlS and the SSLC.
(2) Re-consideration of use of two-way data communication networks between the Class 1 SSLC and the [2]Class 3 PCS, and use of two-way communication with NPP data networks not involved in plant control.
(3) Strengthening of automation in many of the manual hardwired backup functions.
(4) Strengthening of separation of Safety Categories; to separate Category B and C safety functions controlled by the J-ABWR SSLC.
(5) Strengthening the redundancy of the SSLC control circuit; adding of the SSLC control circuit redundancy for some safety functions to meet N+2 single failure criterion.
(6) Re-confirmation and re-structuring (if necessary) of C&I design life cycle based on the overall IEC 61513:2013 framework and additionally it wasn't designed using IEC 60880:2006 for software or IEC 61508:2010 for systematic measures.

14.13.4 Undertaking an options analysis for closing gaps

For the strengthening of diversity between the PCntlS and the SSLC, there were four main options:

(1) Change the design of the PCntlS.
(2) Introduce the newly developed Hitachi νSAFE® platform for the role of the Class 1 SSLC.
(3) Select a separate major supplier of Class 1 technology.
(4) Develop a new SSLC platform enforcing diversity with the HIACS based PCntlS.

The first option was not selected as it does not solve the other gaps revealed with using HIACS platform for the Class 1 SSLC, for example, the application of modern high integrity safety system standards such as IEC 61513:2013 Class 1 and IEC 61508 [3]SIL 3 and 4. It was also considered that completely changing both the PCntlS and the SSLC platform technologies at the same time was neither desirable nor reasonably practicable. The J-ABWR PCntlS technology has evolved from J-BWR analogue PCntlS to the use of the HIACS platform for the J-ABWR over a period of five

[2] The J-AWR does not use the Class 3 terminology for its PCS and instead is the same as the practice in the USA and refers to such systems as non-safety related.

[3] The terminology 'Safety Integrity Level (SIL)' is taken from IEC 61508:2010. The UK ABWR classifies its C&I systems from IEC 61226:2009 using Safety Classes 1, 2 and 3. Throughout this Chapter Safety Class 1 is equivalent to SILs 3 and 4, Safety Class 2 is equivalent to SIL 2 and Safety Class 3 is equivalent to SIL 1.

decades of very dependable performance. The J-ABWR PCntlS HIACS-based technology has provided many years of trouble free operation and is used more widely in many other industrial applications.

For the second option an analysis soon showed that νSAFE® used the same microprocessor technology and shared some of the software with the HIACS technology. νSAFE® was also designed to meet IEC 61508:2010 SIL2 for a single division configuration and also for systematic measures. This fell short of the IEC 61508: SIL3 for a single division configuration and SIL 4 for systematic measures expected for a Class 1 C&I system for a UK NPP. Also in view of the lack of both software and hardware diversity any change to νSAFE® would involve a complete re-design of the platform and would largely be the same as developing a new platform (see option 4).

The third option was reviewed however it was soon showed not to be practicable to undertake because there could be no certainty of avoiding common parts between HIACS and any new third party platform. Additionally no other commercial Class 1 platform was available optimised for ABWR safety functions.

The fourth option was selected because it could resolve the independence gaps and would allow development of a new Class 1 platform design to fully resolve the gaps to the N+2 architecture principle. Additionally, re-use of the same platform technology would allow Category B and C functions to be separated from the SSLC by implementing them as a separate new system. This new system is called the Safety Auxiliary Control System (SACS) and it is fully described in its BSCs [Ref-8] and TR [Ref-38].

The opportunity provided by developing the new platform for the SSLC allowed the best design lifecycle techniques to be used. To ensure full independence a decision was taken to avoid the combination of microprocessors and software and instead field programmable gate array (FPGA) technology was chosen for the new Class 1 FPGA SSLC platform – this new technology has the commercial name vCOSS®.

A decision was taken to use mathematically rigorous formal verification and equivalence checking process for the design of the Class 1 SSLC νCOSS® platform, information on this topic can be found in the BSCs on the SSLC [Ref-6], the TR on the SSLC [Ref-25] and the TR on Class 1 Platform [Ref-15]. Another good example of optimising the design to reduce the risk to ALARP is to ensure that the SSLC can readily be statistically tested for up to at least 50,000 tests. Statistical testing is judged to be one of the best techniques in the group of techniques assigned to the independent confidence building phase for justifying that the SSLC meets its reliability targets.

The architecture of the SSLC was chosen to ensure full compliance with N+2. Removing the lower safety category functions and placing them in the SACS was a part of this process. An analysis of all other SSLC safety functions revealed that it was only the design of the final actuation circuits for the automatic depressurisation system (ADS) that required strengthening to meet N+2. A full options analysis was undertaken to select an ADS solution that fully met the N+2 criterion while keeping the number of additional components, and therefore additional complexity, to the minimum required to achieve the ADS safety function.

It should be noted that the fuel pool cooling system, MCR HVAC and PCIS are N+1 compliant and therefore for these and only these functions the SSLC is N+1. For information on the PCIS see table 24.4-1 and for the fuel pool cooling system 24.10.2.1 both from Generic PCSR Chapter 24 and Chapter 16, section 16.5 for MCR HVAC. Appendix A of the GDA Safety Case Development Manual [Ref-37] provides more information on the rationale for N+1.

For isolation of the data communication networks there is only one effective option and that is by using one-way data diodes. These one-way data diodes will be selected to show that they are fully tolerant to all credible failure modes and to all malicious forms of cyber-attack. The expectations on the isolation of the data communication networks is shown in Section 6.2.3.3.3 of IEC 61513 and more information on the cyber-security can be found in the Generic PCSR Chapter 1.

As stated above the J-ABWR does have hard-wired controls, although they are manually initiated and do not constitute an integrated system. To ensure risks from this system were ALARP Hitachi-GE decided to re-design the existing J-ABWR manual controls into an overall integrated Category A, Class 2 system. This system is the Hard-Wired Backup System (HWBS). Additionally the latest fault studies results (see Generic PCSR Chapters 24, 25 and 26) for the UK ABWR were used to optimise the design of the HWBS.

Options for implementing the HWBS were initially between static hard-wired logic and dynamic hard-wired logic. For many reasons, including inherent testability and better fault tolerance, dynamic hard-wired logic has been specified for the HWBS. This is fully in line with UK relevant good practice where dynamic hard-wired logic has been used in the UK fleet of operational NPP in all Advanced Gas Cooled Reactors and the Sizewell B reactor in Class 1 roles for almost 4 decades. This technology has been shown to be highly reliable, robust and fault tolerant.

Two dynamic hard-wired logic options were considered for further ALARP analysis of the HWBS platform from two different suppliers. Both platforms were found to be equivalent, and capable of meeting the requirements of the UK ABWR, therefore for commercial reasons Hitachi-GE decided not to foreclose on either supplier option during GDA. One of the options from a supplier has been analysed in greater detail to ensure that all of the performance requirements for the HWBS can be met. This is shown in the BSCs on HWBS [Ref-7], TR on HWBS [Ref-39] and the TR on HWBS Platform TR [Ref 40]. The HWBS platforms will be selected post GDA and more detail will then be added to the safety case to cover the design process, development process, qualification, testing and maintenance.

14.13.5 Broader C&I Systems ALARP Analysis

The above ALARP analysis is focussed on the main reactor C&I systems and their underpinning platform technologies. A full analysis of UK relevant good practice was also undertaken and the results implemented on matters such as embedded C&I and on SMART devices. Hitachi-GE has and will continue to implement UK regulatory expectations for such systems on production excellence as specified in ONR's TAG 46. From TAG 46 it has also undertaken pilot studies on the independent confidence building measures for the SSLC vCOSS® platform as well full pilot studies on implementing independent confidence building measures on a Safety Class 1 and Safety Class 2 demonstration SMART devices [Refs-15, 16, 13]. These studies have shown that a comprehensive range of independent confidence building measures have been demonstrated as suitable and feasible, and will be ready to be used in the site specific phase of the project.

For other non-reactor systems the same platform technologies as the main reactor systems may be used or other platform technologies will be used that provide very low risks of failure propagation commensurate with that achieved for the reactor for a similar hazard potential and level of risk. For examples on the fuel route please see the ALARP Assessment Report for Fuel Route [Ref-41].

14.13.6 Concluding Remarks on demonstrating that Risks are ALARP for the UK ABWR C&I Systems

Hitachi-GE has undertaken a comprehensive programme of work during GDA to demonstrate that the risks to safety from failures of the C&I systems for the UK ABWR are ALARP. This work is based on an in-depth gap analysis by comparing UK relevant good practice for NPP C&I systems against the reference design for the J-ABWR.

Where gaps were found design changes were proposed and have been implemented at a level of detail consistent with the requirements of GDA. In undertaking the changes, for the majority of cases, an option analysis process was followed to ensure an outcome that has reduced risks to an ALARP level. Where an option analysis was not undertaken it is demonstrated that the selected solution represented the best that is currently available.

Both Faults Studies (Generic PCSR Chapter 24) and PSA (Generic PCSR Chapter 25) show that the UK ABWR C&I as a key set of essential support systems play a critical role in ensuring the risks to safety from the UK ABWR are ALARP. This chapter and its supporting references have shown that the design of the UK ABWR C&I has been optimised to reduce the risk of significant failure across different C&I platforms to a very low level. Therefore a very low level of risk of common cause failure from the UK ABWR C&I makes a significant contribution to the overall claim that the risks from the UK ABWR are ALARP.

14.14 Conclusions

The safety claims and arguments given in this chapter demonstrate that the C&I systems for the UK ABWR fulfil their important safety roles to the level of reliability and integrity specified in the safety analysis chapters 24, 25 and 26. The work undertaken by Hitachi-GE on C&I described in this chapter has shown that there is a high degree of confidence that the C&I platforms meet all of their Safety Functional Claims and Safety Property Claims (see appendixes). For the Safety Class 1 SSLC this chapter describes the development a new C&I platform using the most mathematically rigorous and verifiable processes specified in international codes and standards. Another important element of the overall C&I architecture is the introduction of a simple but highly robust Safety Class 2 Hardwired Backup System (HWBS). The HWBS has been designed to keep the reactor safe even in the highly unlikely event of major common cause failures in both the Safety Class 1 SSLC and the Safety Class 3 Plant Control System.

The C&I systems perform a safety critical role for the UK ABWR and by designing three completely independent C&I systems with considerable defence-in-depth and fault tolerance these systems will ensure that the risks to safety from C&I failures are as low as is reasonably practicable. This chapter has also demonstrated that the same principles of independence and defence-in-depth apply to the C&I for the fuel route and other parts of the UK ABWR facility

By obtaining an early regulatory design acceptance confirmation that the C&I systems for the UK ABWR have a safe architecture and can meet all of the exacting UK regulatory expectations for production excellence and independent confidence building measures the likelihood of late and costly design changes for a future licensee are very low.

14.15 References

[Ref-1] UK ABWR Nuclear Safety and Environmental Design Principles (NSDEPs), GA10-0511-0011-00001 (XD-GD-0046), Rev.1, July 2016.

[Ref-2] International Electro technical Commission, "*Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions*", IEC 61226, Edition 3.0, July 2009.

[Ref-3] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Overall Human-machine Interface*", GA91-9201-0002-00109 (3E-GD-A0166), Rev. 1, April 2017.

[Ref-4] Hitachi-GE Nuclear Energy, Ltd., "*Conceptual Security Arrangements*", GA91-9101-0301-00001, Rev. B, August 2015.

[Ref-5] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Control and Instrumentation Architecture*", GA91-9201-0002-00022 (3D-GD-A0001), Rev. 4, June 2017.

[Ref-6] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Safety System Logic and Control System*", GA91-9201-0002-00073 (3D-GD-A0008), Rev. 4, June 2017.

[Ref-7] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Hardwired Backup System*", GA91-9201-0002-00029 (3D-GD-A0009), Rev. 2, January 2017.

[Ref-8] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Safety Auxiliary Control System*", GA91-9201-0002-00111 (3D-GD-A0016), Rev. 3, February 2017.

[Ref-9] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Plant Control System*", GA91-9201-0002-00070 (3D-GD-D010), Rev. 4, May 2017.

[Ref-10] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Severe Accident C&I System*", GA91-9201-0002-00110 (3D-GD-A0015), Rev. 3, June 2017.

[Ref-11] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Reactor / Turbine Auxiliary Control System*", GA91-9201-0002-00071 (3D-GD-A0010), Rev. 3, March 2017.

[Ref-12] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Plant Computer System*", GA91-9201-0002-00072 (3D-GD-A0011), Rev. 3, March 2017.

[Ref-13] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on SMART Devices*", GA91-9201-0001-00046 (3E-GD-A0177), Rev. 3, March 2017.

[Ref-14] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on ICBM for FPGA*", GA91-9201-0001-00051 (3E-GD-A0169), Rev. 3, March 2017.

[Ref-15] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Class 1 Platform*", GA91-9201-0001-00045 (3E-GD-A0058), Rev. 2, March 2017.

[Ref-16] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Class 3 Platform*", GA91-9201-0001-00044 (3E-GD-A0059), Rev. 1, March 2017.

[Ref-17] International Atomic Energy Agency, "*Safety of Nuclear Power Plants: Design*", NS-R-1, September 2000.

[Ref-18] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Fault Assessment*", GA91-9201-0001-00022 (UE-GD-0071), Rev.6, July 2017.

[Ref-19] United States Nuclear Regulatory Commission, "*Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*", (NUREG/CR-7007, ORNL/TM-2009/302), February 2010.

[Ref-20] United States Nuclear Regulatory Commission, "*Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems*", (NUREG/CR-6303, UCRL-ID-119239), December 1994.

[Ref-21] Vacant Number

[Ref-22] Japan Atomic Energy Commission, "*Regulatory Guide for Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities*", Regulatory Guide of Japan Atomic Energy Commission (Japanese), ISBN: 9784802814966, Edition 12, pp. 7-28, 2008. [Online (old edition)]: http://www.mext.go.jp/b_menu/hakusho/nc/t19900830001/t19900830001.html

[Ref-23] International Atomic Energy Agency, "*IAEA Safety Standards: Design of Instrumentation and Control Systems for Nuclear Power Plants*",SSG-39, April 2016.

[Ref-24] International Organization for Standardization, "*Quality management systems – Requirements*", ISO 9001:2008, Edition 4, November 2008.

[Ref-25] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Safety System Logic and Control System*", GA91-9201-0001-00052 (3E-GD-A0104), Rev. 3, June 2017.

[Ref-26] Hitachi-GE Nuclear Energy, Ltd., "*List of Safety Category and Class for UK ABWR*", GA91-9201-0003-00266 (AE-GD-0224), Rev. 4, August 2017.

[Ref-27] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Main Control Room Human-machine Interface*", GA91-9201-0002-00060 (3E-GD-A0029), Rev. 2, April 2017.

[Ref-28] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Remote Shutdown System Human-machine Interface*", GA91-9201-0002-00061 (3E-GD-A0030), Rev. 2, April 2017.

[Ref-29] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Backup Building Human-machine Interface*", GA91-9201-0002-00062 (3E-GD-A0031), Rev. 2, May 2017.

[Ref-30] Hitachi-GE Nuclear Energy, Ltd., "*Basis of Safety Cases on Radioactive Waste Human-machine Interface*", GA91-9201-0002-00063 (3E-GD-A0032), Rev. 1, August 2015.

[Ref-31] Hitachi-GE Nuclear Energy, Ltd., "*The list of Embedded C&I and SMART Devices in SC1 or SC2 systems*", GA91-9201-0003-00793 (3E-GD-A0206), Rev. 1, October 2016.

[Ref-32] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Neutron Monitoring System*", GA91-9201-0001-00054 (3E-GD-B017), Rev. 1, July 2016.

[Ref-33] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Reactor Pressure Vessel Instrument System*", GA91-9201-0001-00056 (3E-GD-A0129), Rev. 2, June 2017.

[Ref-34] Hitachi-GE Nuclear Energy, Ltd., "*QUALITY MANAGEMENT PLAN (For UK ABWR GDA Project)*", GA70-1501-0007-00001 (GNQA13-0066), Rev. 6, April 2015.

[Ref-35] Vacant Number

[Ref-36] Hitachi-GE Nuclear Energy, Ltd., *"GDA ALARP Methodology"*, GA10-0511-0004-00001 (XD-GD-0037), Rev.3, June 2017.

[Ref-37] Hitachi-GE Nuclear Energy, Ltd.,*"GDA Safety Case Development Manual"*, GA10-0511-0006-00001 (XD-GD-0036), Rev.3, June 2017.

[Ref-38] Hitachi-GE Nuclear Energy, Ltd., *"Topic Report on Safety Auxiliary Control System"*, GA91-9201-0001-00148 (3E-GD-A0289), Rev.1, March 2017.

[Ref-39] Hitachi-GE Nuclear Energy, Ltd.,*" Topic Report on Hardwired Backup System"*, GA91-9201-0001-00058 (3E-GD-A0105), Rev.2, January 2017.

[Ref-40] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Hardwired Backup System Platform"*, GA91-9201-0001-00153 (3E-GD-A0364), Rev.1, April 2017.

[Ref-41] Hitachi-GE Nuclear Energy, Ltd., *"ALARP Assessment Report for Fuel Route"*, GA91-9201-0003-00814 (AE-GD-0472), Rev.1, June 2017.

[Ref-42] Hitachi-GE Nuclear Energy, Ltd., *"C&I Design Process Plan"*, GA32-1502-0002-00001, (3D-GD-A0020), Rev.0, April 2017.

[Ref-43] Vacant Number

[Ref-44] Vacant Number

[Ref-45] Hitachi-GE Nuclear Energy, Ltd., *"Generic Technical Specifications"*, GA80-1502-0002-00001 (SE-GD-0378), Rev.3, August 2017.

[Ref-46] Hitachi-GE Nuclear Energy, Ltd., *"Safety Plan for NCFS-1"*, GA91-9920-0003-00001 (3E-GD-A0134), Rev.10, July 2017.

[Ref-47] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Safety Process Radiation Monitoring System*", GA91-9201-0001-00115 (3E-GD-K053), Rev.3, June 2017.

[Ref-48] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Process Radiation Monitoring System (Containment Radiation Monitor)*", GA91-9201-0001-00162 (3E-GD-K109), Rev.1, March 2017.

[Ref-49] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Process Radiation Monitoring System (Off-gas System Area Airborne Radiation Monitor)*", GA91-9201-0001-00255 (3E-GD-K153), Rev.0, March 2017.

[Ref-50] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Severe Accident C&I System*", GA91-9201-0001-00147 (3E-GD-A0290), Rev.2, June 2017.

[Ref-51] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Plant Control System*", GA91-9201-0001-00190 (3E-GD-D122), Rev.2, June 2017.

[Ref-52] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Reactor / Turbine Auxiliary Control System*" GA91-9201-0001-00149 (3E-GD-A0298), Rev.1, March 2017.

[Ref-53] Hitachi-GE Nuclear Energy, Ltd., "*Topic Report on Plant Computer System*", GA91-9201-0001-00152 (3E-GD-A0299), Rev.1, March 2017.

Appendix A1: SFC Claims Table

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
1	1	Control of Reactivity	1-1	Functions to prevent excessive reactivity insertion	-	-	-	-	N/A. This HLSF is achieved by the Mechanical Equipment system. The CRD through its FMCRD is the principal means to prevent excessive reactivity insertion by prevention of control rod ejection. The CRD is the principal means to prevent excessive reactivity insertion by mechanically preventing a CR drop event when the control rod is separated from the ball nut. The CRD through its FMCRD and the CR are the principal means to prevent excessive reactivity insertion by ensuring the bayonet coupling function (CR-FMCRD coupling). (Refer to Generic PCSR Chapter 12.2)	-	-
2			1-2	Functions to maintain core geometry	-	-	-	-	N/A. This HLSF is achieved by the Mechanical Equipment system. The core geometry is maintained by core support structure and fuel assembly. (Refer to Generic PCSR Chapter 11 and Figure 11.1-1)	-	-
3			1-3	Emergency shutdown of the reactor	FS1	RPS Scram (A1)	Fault Conditions	SSLC SFC 1-3.1	SSLC provides the functions to control the systems assigned as the first provision for the Category A Safety Function for emergency shutdown of the reactor.	A	1

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
4			1-4	Functions to maintain sub-criticality	FS2	SLC(A2)	-	-	N/A This HLSF is achieved by the Mechanical Equipment system. The CRD through its FMCRD is the principal means to deliver maintenance of core sub-criticality during normal operations. The CRD is the principal means to maintain the control rods inserted when shutdown by Scram in order to maintain the core sub-criticality. The SLC is the secondary means to maintain the reactor subcritical without CRs insertion by injecting the neutron absorbing solution into the reactor core in the event of ATWS design basis fault. (Refer to Generic PCSR Chapter 12.2)	-	-
5			1-5	Function of alternative reactivity control	FS2 FS3 FS4 FS5	SLC(A2) ATWS-RPT(A2) FWSTP(A2) ARI(A2)	Fault Conditions	HWBS SFC 1-5.1	HWBS provides the functions to control the systems assigned as the second provision for the Category A Safety Functions of alternative reactivity control.	A	2
6					-	-	Fault Conditions	PCntlS SFC 1-5.1	PCntlS provides the functions for alternative reactivity control.	-	3
7			1-6	Functions to circulate reactor coolant (functions to control reactivity of the core in normal operational states)	-	-	Normal Conditions	PCntlS SFC 1-6.1	PCntlS provides the functions to control the circulation of reactor coolant (functions to control reactivity of the core in normal operational states).	-	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
8					-	-	Normal Conditions	ACS SFC 1-6.1	ACS provides the functions to control the auxiliary system to support the reactor coolant circulation (which controls reactivity of the core in normal operational states).	-	3
9			1-7	Functions to plant instrument and control (except for safety protection function) (Functions to control reactivity of the core in normal operational states)	-	-	Normal Conditions	PCntlS SFC 1-7.1	PCntlS provides the functions to control the position of CRs (except for safety protection function) (functions to control reactivity of the core in normal operational states).	-	3
10			1-8	Functions to suppress reactor power increase with other system	-	-	Normal /Fault Conditions	PCntlS SFC 1-8.1	PCntlS provides the functions to suppress reactor power increase with other system.	-	3
11			1-9	Functions to maintain sub-criticality of spent fuel outside the reactor coolant system	-	-	-	-	N/A. This HLSF is achieved by the Mechanical Equipment system. The spent fuel storage rack maintains the fuel assemblies in a subcritical state. (See Generic PCSR Chapter 19.3)	-	-
12			1-10	Functions to maintain sub-criticality of spent fuel during processes of spent fuel removal from cask pit to storage area and during interim storage period	-	-	-	-	N/A This HLSF is achieved by the Mechanical Equipment system. Spent fuel assemblies will be maintained in a sub-critical state during normal operation as well as during and following frequent and infrequent faults and hazards. (Refer to Generic PCSR Chapter 32)	-	-

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
13	2	Fuel Cooling	2-1	Functions to cool reactor core	FS6 FS7 FS9 FS10	RCIC(A1) HPCF(A1) ADS(A1) LPFL(A1)	Fault Conditions	SSLC SFC 2-1.1	SSLC provides the functions to control the systems assigned as the first provision for the Category A Safety Function to cool the reactor core.	A	1
14					-	-	Fault Conditions	OCIS SFC 2-1.1	Other C&I system provides the functions to control the auxiliary system.	-	3
15			2-2	Function of alternative fuel cooling	FS11 FS12	Alternative SRV(A2) FLSS(A2)	Fault Conditions	HWBS SFC 2-2.1	HWBS provides the functions to control the systems assigned as the second provision for the Category A Safety Functions of alternative fuel cooling.	A	2
16					-	-	Fault Conditions	SA C&I SFC 2-2.1	SA C&I provides the functions to control the systems for severe accident management that implement Category B Safety Functions of alternative fuel cooling.	B	2/3
17			2-3	Function to make up reactor coolant with other system	-	-	Fault Conditions	ACS SFC 2-3.1	ACS provides the functions to control the systems to make up reactor coolant with other system.	-	3
18					-	-	Fault Condition	OCIS SFC 2-3.1	OCIS provides the function to control the systems to make up reactor coolant with other system, if available.	C	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
19			2-4	Function to cool spent fuel outside the reactor coolant system	-	-	Normal/ Fault Conditions	SSLC SFC 2-4.1	SSLC provides the functions to control the systems assigned as the first line provision for the Category A Safety Function to cool spent fuel outside of the reactor coolant system.	A	1
20			2-5	Functions to make up water for spent fuel pool	-	-	Fault Conditions	HWBS SFC 2-5.1	HWBS provides the functions to control the systems assigned as the second provision for the Category A Safety Functions to make up water for spent fuel pool.	A	2
21					-	-	Fault Conditions	SACS SFC 2-5.1	SACS provides the Category C Safety Functions to control make up water for the spent fuel pool.	C	3
22					-	-	Fault Conditions	SA C&I SFC 2-5.1	SA C&I provides the functions to control the systems for severe accident management that implement Category B Safety Functions to make up water for spent fuel pool.	B	2/3
23					-	-	Fault Conditions	ACS SFC 2-5.1	ACS provides the functions to control the systems to make up water for spent fuel pool.	-	3
24					-	-	Fault Conditions	OCIS SFC 2-5.1	OCIS provides the function to control the systems to make up water for spent fuel pool, if available.	C	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
25			2-6	Functions to maintain spent fuel temperature limit during processes of spent fuel removal from cask pit to storage area and during interim storage period	-	-	-	-	N/A This HLSF is achieved by the Mechanical Equipment system. (Refer to Generic PCSR Chapter 32)	-	-
26	3	Long term heat removal	3-1	Functions to remove residual heat after shutdown	FS13 FS14	SRV –Manual depressurization–(A1) RHR(A1)	Fault Conditions	SSLC SFC 3-1.1	SSLC provides the functions to control the systems assigned as the first line provision for the Category A Safety Function for long term heat removal.	A	1
27			3-2	Function of alternative containment cooling and decay heat removal	FS15	Containment venting(A2)	Fault Conditions	HWBS SFC 3-2.1	HWBS provides the functions to control the systems assigned as the second provision for the Category A Safety Functions of alternative containment cooling and decay heat removal.	A	2
28					-	-	Fault Conditions	SA C&I SFC 3-2.1	SA C&I provides the functions to control the systems for severe accident management which implement Category B Safety Functions of alternative containment cooling and decay heat removal.	B	2/3
29	4	Confinement/Containment of radioactive materials	4-1	Functions to form reactor coolant pressure boundary	-	-	-	-	N/A. This HLSF is achieved by the Mechanical Equipment system. The components within the RCPB ensure the pressure integrity of the boundary and preserve reactor coolant, loss of which would lead to consequences above the BSL. (Refer to Generic PCSR Chapter 12.1)	-	-

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
30			4-2	Functions to prevent overpressure within the reactor coolant pressure boundary	-	-	-	-	N/A. This HLSF is achieved by the Mechanical Equipment system. The safety valve function of the SRVs is the principal means to deliver overpressure protection of the RCPB under abnormal transients and accident conditions that could put excessive pressure on the boundary. (Refer to Generic PCSR Chapter 12.1)	-	-
31			4-3	Functions to contain reactor coolant outside the RCPB	-	-	-	-	N/A This HLSF is achieved by the Mechanical Equipment system. The pipework of the NB outside the Reactor Coolant Pressure Boundary (RCPB) beyond outboard MSIV contains reactor coolant and its rupture could lead to a release of radioactive material of dose consequences relatively low, but demanding Category A safety functions to mitigate them. The CUW piping outside the RCPB contains radioactive material. Rupture of this piping could lead to a release of radioactive material of dose consequences relatively low. The piping outside the RCPB contains material with low radioactivity. (Refer to Generic PCSR Chapter 12.3)	-	-
32							Normal /Fault Conditions	ACS SFC 4-3.1	ACS provides the monitoring functions of plant conditions to contain reactor coolant.	-	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
33			4-4	Functions to contain radioactive material	-	-	-	-	N/A. This HLSF is achieved by the Mechanical Equipment system. The instrumentation piping and sampling line implement the function to retain the reactor coolant.	-	-
34			4-5	Functions to reseat safety valves and relief valves	-	-	-	-	N/A This HLSF is achieved by the Mechanical Equipment system. The SRV re-seating function is a principal means to prevent excessive loss of reactor coolant when the SRV is spring-actuated for the delivery of the RCPB overpressure Protection. (Refer to Generic PCSR Chapter 12.3)	-	-
35			4-6	Functions to mitigate reactor pressure increase with other system (other than No.4-2)	-	-	Fault Conditions	OCIS SFC 4-6.1	Other C&I system provides the functions to control the systems to mitigates reactor pressure increase with other system (other than No.4-2).	C	3
36					-	-	Fault Conditions	PCntlS SFC 4-6.1	PCntlS provides the functions to mitigate the reactor pressure increase with other system.	-	3
37			4-7	Functions to confine radioactive materials, shield radiation, and reduce radioactive release	FS16 FS17	MSIV(A1) PCIS(A1)	Fault Conditions	SSLC SFC 4-7.1	SSLC provides the functions to control the systems assigned as the first provision for the Category A Safety Functions to confine radioactive materials, shield radiation, and reduce radioactive release.	A	1

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
38					-	-	Fault Conditions	SACS SFC 4-7.1	SACS provides the function to control the systems to reduce radioactive release.	B	2
39							Normal Condition	ACS SFC 4-7.1	ACS provides the functions to control the systems for containg radioactive material and for reducing release radioactive release.	-	3
40			4-8	Functions to minimise the release of radioactive gases	-	-	Fault Conditions	SACS SFC 4-8.1	SACS provides the functions to control the systems to minimise the release of radioactive gases.	B	2
41					-	-	Fault Conditions	SA C&I SFC 4-8.1	SA C&I provides the functions to control the systems for severe accident management to minimise the release of radioactive gases.	B	2/3
42			4-9	Functions to contain radioactive materials in the event of a severe accident	-	-	Fault Conditions	SA C&I SFC 4-9.1	SA C&I provides the functions to control the systems for severe accident management to contain radioactive materials.	B	2/3
43			4-10	Functions to prevent the dispersion of fission products into reactor coolant, spent fuel pool and canister	-	-	-	-	N/A This HLSF is achieved by the Mechanical Equipment system. Fuel assembly and its components are designed so that the effective dose received by any person is less than the prescribed limit, within the functions of relevant plant components. (See Generic PCSR Chapter 11.4)	-	-

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
44			4-11	Functions to store the radioactive materials as gaseous waste	-	-	Normal Conditions	ACS SFC 4-11.1	ACS provides the functions to control the systems to reduce the emission rate of radioactive materials sufficiently before discharging them to atmosphere.	-	3
45							Normal Conditions	SACS SFC 4-11.1	SACS provides the functions to control the systems to store the radioactive materials as gaseous waste.	B	2
46			4-12	Functions to store the radioactive materials as liquid wastes	-	-	Normal Conditions	ACS SFC 4-12.1	ACS provides the functions to control the systems to transfer liquid waste to the Liquid Waste Management System.	-	3
47					-	-	Normal Conditions	OCIS SFC 4-12.1	Other C&I system provides the support provisions for the Category C safety functions to store the radioactive materials as liquid wastes.	C	3
48			4-13	Functions to store the radioactive materials as solid wastes	-	-	Normal Conditions	OCIS SFC 4-13.1	Other C&I system provides the support provisions for the Category C safety functions to store the radioactive materials as solid wastes.	C	3
49			4-14	Functions to provide containment barrier during processes of spent fuel removal from cask pit to storage area and during interim storage period	-	-	-	-	N/A This HLSF is achieved by the Mechanical Equipment system. Containment of spent fuel will be maintained during various operation modes and following frequent and infrequent faults and hazards. (Containment) (See Generic PCSR Chapter 32)	-	-

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
50			4-15	Unused number	-	-	-	-	N/A This HLSF is achieved by the Mechanical Equipment System.	-	-
51			4-16	Functions to provide radiation shield during processes of spent fuel removal from cask pit to storage area and during interim storage period	-	-	-	-	N/A This HLSF is achieved by the Mechanical Equipment System.	-	-
52			4-17	Functions to maintain PCV atmosphere in an inert state for preventing hydrogen combustion			Normal /Fault Condition	ACS SFC 4-17.1	ACS provides the function to control the systems to maintain PCV atmosphere in an insert state for preventing hydrogen combusion.	-	3
53	5	Others	5-1	Functions to generate actuation signals for the engineered safety features and reactor shutdown system	-	-	Fault Conditions	SSLC SFC 5-1.1	SSLC provides the functions to generate actuation signals for the engineered safety features and reactor shutdown system as the first provision for the Category A Safety Functions.	A	1
54					-	-	Fault Conditions	HWBS SFC 5-1.1	HWBS provides the functions to generate actuation signals for the engineered safety features and reactor shutdown system as the second provision for the Category A Safety Functions.	A	2

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
55					-	-	Fault Conditions	SACS SFC 5-1.1	SACS provides the functions to generate actuation signals for the engineered safety features for the Category B Safety Functions.	B	2
56			5-2	Supporting functions especially important to safety	-	-	Normal /Fault Conditions	SSLC SFC 5-2.1	SSLC provides the functions to control the support systems assigned to the first provision for the Category A Safety Functions.	A	1
57			5-3	Function of alternative supporting system	-	-	Fault Conditions	HWBS SFC 5-3.1	HWBS provides the functions to control the support systems for the second provision for the Category A Safety Functions.	A	2
58							Fault Conditions	SACS SFC 5-3.1	SACS provides the functions to control the alternative supporting systems for the delivery of the Category B Safety Function.	B	2
59					-	-	Fault Conditions	SA C&I SFC 5-3.1	SA C&I provides the functions to control the support systems for the delivery of the Category B Safety Functions.	B	2/3
60					-	-	Fault Conditions	OCIS SFC 5-3.1	Other C&I system provides the functions to control the alternative supporting systems for the delivery of the Category B Safety Function.	B	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
61			5-4	Monitoring functions of plant conditions to support operator actions	-	-	Fault Conditions	SSLC SFC 5-4.1	SSLC provides the monitoring functions of plant conditions to support operator actions.	A	1
62					-	-	Fault Conditions	HWBS SFC 5-4.1	HWBS provides the monitoring functions of plant conditions to support operator actions.	A	2
63					-	-	Fault Conditions	SACS SFC 5-4.1	SACS provides the monitoring functions of plant conditions to support operator actions.	B	2
64					-	-	Fault Conditions	SA C&I SFC 5-4.1	SA C&I provides the monitoring functions of plant conditions to support operator actions.	B	2/3
65					-	-	Normal Conditions	ACS SFC 5-4.1	ACS provides the functions to monitor plant conditions in normal operation.	-	3
66					-	-	Normal Conditions	OCIS SFC 5-4.1	Other C&I system provides the monitoring functions of plant conditions to support operator actions.	C	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
67			5-5	Functions to shut down safely from outside the control room	-	-	Fault Conditions	SSLC SFC 5-5.1	RSS provides the functions to control the systems to shutdown safely from outside the main control room.	A	1
68			5-6	Functions to handle fuel and heavy equipment safely	-	-	Normal Conditions	OCIS SFC 5-6.1	Other C&I system provides the Category A safety functions to handle fuel safely.	A	1
69			5-7	Functions to limit the effect of hazard	-	-	Normal Conditions	OCIS SFC 5-7.1	Other C&I system provides the support provisions for the Category B or C safety functions to limit the effect of hazard.	B	2
70			5-8	Functions to clean up reactor coolant	-	-	Normal Conditions	ACS SFC 5-8.1	ACS provides the functions to control the systems to clean up reactor coolant.	-	3
71					-	-	Normal Conditions	OCIS SFC 5-8.1	Other C&I system provides the functions to control the auxiliary system which implements the Category C safety functions to clean up reactor coolant.	C	3
72			5-9	Functions to clean up water except for reactor coolant	-	-	Normal Conditions	SACS SFC 5-9.1	SACS provides the functions to control the systems to clean up water except for reactor coolant.	C	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
73					-	-	Normal Conditions	OCIS SFC 5-9.1	Other C&I system provides the functions to control the auxiliary system which implements the Category C safety functions to clean up water except for reactor coolant.	C	3
74			5-10	Functions to supply electric power (except for emergency supply)	-	-	Normal Conditions	PCntlS SFC 5-10.1	PCntlS provides the functions to supply electric power (except for emergency supply).	-	3
75					-	-	Normal Conditions	ACS SFC 5-10.1	ACS provides the functions to control the auxiliary system to supply electric power (except for emergency supply).	-	3
76			5-11	Supporting functions to supply power (except for emergency supply)	-	-	Normal Conditions	ACS SFC 5-11.1	ACS provides the functions to control the auxiliary system to supply power (except for emergency supply).	-	3
77							Normal Condition	OCIS SFC 5-11.1	Other C&I provides the function to control the auxiliary systems which implements the Category B or C to supply power.	B	3
78			5-12	Supporting functions for management of normal operation	-	-	Normal Conditions	PCS SFC 5-12.1	PCS performs the support functions periodically, or as occasion demands, in order to maintain efficient and safe operation of the nuclear power plant.	-	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
79			5-13	Auxiliary functions for plant operation	-	-	Normal Conditions	ACS SFC 5-13.1	ACS provides the functions to control the auxiliary system for plant operation.	-	3
80					-	-	Fault Conditions	SACS SFC 5-13.1	SACS provides the functions to control the systems which support the SSLC to cool reactor core.	C	3
81			5-14	Supporting functions for on-site emergency preparedness	-	-	Fault Conditions	OCIS SFC 5-14.1	Other C&I system provides the supporting functions for on-site emergency preparedness.	C	3
82					-	-	Fault Conditions	OCIS SFC 5-14.2 （ERF C&I SFC 5-14.1）	ERF C&I system collates and distributes plant status information to various response facilities both on and offsite in the event of an emergency.	C	3
83					-	-	Fault Conditions	OCIS SFC 5-14.3	Other C&I system provides the supporting functions for fire protection system.	C	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
84			5-15	Functions to control hydrogen concentration in fault conditions	-	-	-	-	N/A This HLSF is achieved by the Mechanical Equipment. Shielding and contamination control will be maintained to operators and the public during various operation modes as well as during and following frequent and infrequent faults and hazards. (See General PCSR Chapter 31)	-	-
85			5-16	Functions to provide handling and retrievability during processes of spent fuel removal from cask pit to storage area and during interim storage period	-	-	-	-	N/A This HLSF is achieved by the Mechanical Equipment. Handling and retrieval of spent fuel will be maintained during refueling outage, and faults and hazards will be shown to be of acceptably low frequency. (See General PCSR Chapter 31)	-	-
86			5-17	Function to provide structural support to SSCs	-	-	-	-	N/A This HLSF is achieved by the Mechanical Equipment system or civil works and structures. (See Generic PCSR Chapter 10)	-	-

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
87			5-18	Function to maintain internal building environment appropriate for SSC	-	-	Fault Conditions	SSLC SFC 5-18.1	SSLC ECCS/ESF HVAC function maintains the control building and reactor building environment in case of an accident.	A	1
88					-	-	Fault Conditions	HWBS SFC 5-18.1	HWBS provides the functions to maintain internal building environment appropriate for SSCs.	A	2
89							Fault Conditions	SACS SFC 5-18.1	SACS provides the functions to maintain the internal building environment in case of an accident	B	2
90					-	-	Fault Conditions	SA C&I SFC 5.18-1	SA C&I provides the functions to maintain internal building environment appropriate for SSCs.	B	2/3
91					-	-	Normal Conditions	ACS SFC 5-18.1	ACS provides the functions to maintain the internal building environment during the normal operation.	-	3
92			5-19	Monitoring functions of radioactive discharge to the environment	-	-	Fault Conditions	SA C&I SFC 5-19.1	SA C&I provides the monitoring functions of radioactive discharge to the environment.	B	2/3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
93							Fault Conditions	OCIS SFC 5-19.1	Other C&I system provides the monitoring functions of radioactive discharge to the environment.	C	3
94			5-20	Functions to maintain availability of CRs hydraulic insertion function and to recover CRs to normal unlatched state after rapid insertion			Normal Condition	ACS SFC 5-20.1	ACS provides the functions to control the systems for supporting the deliver of reactor rapid shutdown.	-	3
95							Normal Condition	PCntlS SFC 5-20.1	PCntlS provides the functions to control the systems for recovering CRs to normal unlatched state after rapid insertion.	-	3
96			5-21	Function to retain water for provision of radiation shield during the refueling process					N/A This HLSF is achieved by the Mechanical Equipment.	-	-
97			5-22	Function to limit deceleration loading to canister containment boundary during credible cask drop faults			-	-	N/A This HLSF is achieved by the Mechanical Equipment.	-	-
98			5-23	Monitoring functions of occupational and public radiation exposures			Normal Condition	OCIS SFC 5-23.1	Other C&I system provides the monitoring functions of occupational and public radiation exposures.	C	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Control and Instrumentation System (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
99			5-24	Functions to limit worker access into high dose area					N/A		

Appendix A2: FS and Initiating Fault / Event ID Linkage Table

*: Refer to Appendix A1 for the reflect SFCs.

No*.	Front System	Initiating Fault / Event ID	Remarks
FS1	RPS Scram (A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.1, 4.2.2, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 5.1.1, 5.2.1, 5.3.1, 5.3.4, 1.4.2, 3.1.1, 2.1.2, 11.2, 11.3, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.1.2,	
FS2	SLC(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.1, 4.2.2, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.2, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.2, 11.3, 11.4.1, 11.5, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1	
FS3	ATWS-RPT(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.4, 1.5, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.4.1, 4.2.5.1, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 1.4.2, 3.1.1, 2.1.2, 11.2, 11.3, 11.4.1, 11.5, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1	
FS4	FWSTP(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.4, 1.5, 1.7, 1.8, 2.1, 2.2, 2.3, 4.2.3.1, 4.2.4.1, 4.2.5.1, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 1.4.2, 2.1.2, 11.3, 11.5, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1	
FS5	ARI(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.1, 4.2.2, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.2, 11.3, 11.4.1, 11.5, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1	

*: Refer to Appendix A1 for the reflect SFCs.

No*.	Front System	Initiating Fault / Event ID	Remarks
FS6	RCIC(A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.3, 10.1, 10.2, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 2.1.2, 11.1, 11.2, 11.3, 11.5, 11.8.1, 11.10.1, 11.11.1,, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.6, 18.1.1, 18.2.1, 18.3.1	
FS7	HPCF(A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.2, 5.1.3, 5.2.2, 5.2.3, 5.3.2, 5.3.3, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 2.1.2, 11.1, 11.2, 11.3, 11.4, 11.5, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.3.2, 13.3.3, 13.3.4, 13.4.1, 13.4.2, 13.4.3, 13.4.4, 13.4.5, 13.4.6, 13.5.1.1, 13.5.1.2, 13.5.1.3 13.5.1.4, 13.5.1.5, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.2, 13.5.2.3, 13.5.2.4, 13.5.2.5, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.2, 13.5.3.3, 13.5.3.4, 13.5.3.5, 13.5.3.6, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.8.1.1, 13.8.1.2, 13.8.1.3, 13.8.1.4, 13.8.1.5, 13.8.1.6, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.5, 13.8.2.6, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.10.1, 13.10.2, 13.10.3, 13.10.4, 13.10.5, 13.10.6, 13.11.1, 13.11.2, 13.11.3, 13.11.4, 13.11.5, 13.11.6 13.12.1, 13.12.2, 13.13.1, 13.13.2, 13.14.1, 13.14.2, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.2, 13.17.3, 13.17.4, 13.18.1, 13.18.2, 13.18.3, 13.18.4, 11.4.2.1, 11.4.2.2, 11.4.2.3, 17.1.2.1, 17.1.2.2, 17.1.2.4, 17.2.2.1, 17.2.2.2, 17.2.2.4, 17.3.2.1, 17.3.2.2, 17.3.2.4, 17.4.2.1, 17.4.2.2, 17.4.2.3, 17.4.2.4, 17.4.2.5, 17.4.2.6, 17.5.2.1, 17.5.2.2, 17.5.2.3, 17.5.2.4, 17.5.2.5, 17.5.2.6, 18.1.2.1, 18.1.2.2, 18.1.2.3, 18.1.2.4, 18.1.2.5, 18.1.2.6, 18.2.2.1, 18.2.2.2, 18.2.2.3, 18.2.2.4, 18.2.2.5, 18.2.2.6, 18.3.2.1, 18.3.2.2, 18.3.2.3, 18.3.2.4, 18.3.2.5, 18.3.2.6	
FS8	SRV -Safety valve function- (A1)	No claim	
FS9	ADS(A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.2, 5.2.2, 5.3.2, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.3, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1	

*: Refer to Appendix A1 for the reflect SFCs.

No*.	Front System	Initiating Fault / Event ID	Remarks
FS10	LPFL(A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.2.2, 5.3.2, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.2, 11.3, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.3.2, 13.3.6, 13.5.1.1, 13.5.1.2, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.2, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.2, 13.5.3.6, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.8.1,1, 13. 8.1,2, 13. 8.1,3, 13.8.1.4, 13.8.1.5, 13.8.1.6, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.5, 13.8.2.6, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.10.1, 13.10.2, 13.10.3, 13.10.4, 13.10.5, 13.10.6, 13.11.1, 13.11.2, 13.11.3, 13.11.4, 13.11.5, 13.11.6 13.12.1, 13.12.2, 13.13.1, 13.13.2, 13.14.1, 13.14.2, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.2, 13.17.6, 13.18.1, 13.18.2, 13.18.6, 17.1.2.1, 17.1.2.2, 17.1.2.6, 17.2.2.1, 17.2.2.2, 17.2.2.6, 17.3.2.1, 17.3.2.2, 17.3.2.6, 17.4.2.1, 17.4.2.2, 17.4.2.6, 17.5.2.1, 17.5.2.2, 17.5.2.6, 18.1.2.1, 18.1.2.2, 18.1.2.6, 18.2.2.1, 18.2.2.2, 18.2.2.6, 18.3.2.1, 18.3.2.2, 18.3.2.6	Requirements as LPFL (B2) are below: 1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.2, 5.1.2, 5.2.2, 5.3.2, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.3, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.5.1.2, 13.5.1.6, 13.5.1.7 Remark: Requirements as LPFL (A1) are below: 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 11.2, 13.3.1, 13.3.2, 13.3.6, 13.5.1.1, 13.5.2.1, 13.5.2.2, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.2, 13.5.3.6, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.8.1,1, 13. 8.1,2, 13. 8.1,3, 13.8.1.4, 13.8.1.5, 13.8.1.6, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.5, 13.8.2.6, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.10.1, 13.10.2, 13.10.3, 13.10.4, 13.10.5, 13.10.6, 13.11.1, 13.11.2, 13.11.3, 13.11.4, 13.11.5, 13.11.6 13.12.1, 13.12.2, 13.13.1, 13.13.2, 13.14.1, 13.14.2, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.2, 13.17.6, 13.18.1, 13.18.2, 13.18.6, 17.1.2.1, 17.1.2.2, 17.1.2.6, 17.2.2.1, 17.2.2.2, 17.2.2.6, 17.3.2.1, 17.3.2.2, 17.3.2.6, 17.4.2.1, 17.4.2.2, 17.4.2.6, 17.5.2.1, 17.5.2.2, 17.5.2.6, 18.1.2.1, 18.1.2.2, 18.1.2.6, 18.2.2.1, 18.2.2.2, 18.2.2.6, 18.3.2.1, 18.3.2.2, 18.3.2.6
FS11	Alternative SRV (RDCF)(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.3, 11.5, 11.6, 11.7, 11.8.1, 11.9, 11.10.1, 11.11.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.3.6, 13.4.1, 13.4.6, 13.5.1.1, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.6, 13.6.1,1, 13.6.1,5, 13.6.1,6, 13.6.2,1, 13.6.2,5, 13.6.2,6, 13.6.3,1, 13.6.3,5, 13.7.1, 13.7.6, 13.12.1, 13.12.2, 13.17.1, 13.17.6, 13.18.1, 13.18.6, 11.6.1, 11.6.6, 11.7.1, 11.7.4, 11.8.2.1, 11.8.2.6, 11.10.2.1, 11.10.2.6, 11.11.2.1, 11.11.2.6, 11.12.2.1, 11.12.2.6, 17.1.2.1, 17.1.2.6, 17.2.2.1, 17.2.2.6, 17.3.2.1, 17.3.2.6, 17.4.2.1, 17.4.2.6, 17.5.2.1, 17.5.2.6, 18.1.2.1, 18.1.2.6, 18.2.2.1, 18.2.2.6, 18.3.2.1, 18.3.2.6	Requirements as RDCF (B2) are below: 4.2.5.1, 4.2.5.2, 4.5, 4.6, 5.3, 7.1, 8.1, 8.2, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 5.1.1, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.4, 11.3, 11.6, 11.7, 11.8, 17.2.1, 18.3.1, 4.2.6, 4.5, 4.6, 5.3, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 5.1.1, 5.2.1, 5.3.1, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 11.3, 11.6, 11.7, 11.8, 17.2.1, 18.3.1 13.4.1, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.6, 17.5.2.1, 17.5.2.6, 18.3.2.1, 18.3.2.6

*: Refer to Appendix A1 for the reflect SFCs.

No*.	Front System	Initiating Fault / Event ID	Remarks
FS12	FLSS(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2,, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.2, 11.3, 11.4.1, 11.5, 11.6, 11.7, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.3.2, 13.3.3, 13.3.4, 13.3.5, 13.3.6, 13.4.1, 13.4.2, 13.4.3, 13.4.4, 13.4.5, 13.4.6, 13.5.1.1, 13.5.1.2, 13.5.1.3, 13.5.1.4, 13.5.1.5, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.2, 13.5.2.3, 13.5.2.4, 13.5.2.5, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.2, 13.5.3.3, 13.5.3.4, 13.5.3.5, 13.5.3.6, 13.6.1.1, 13.6.1.2, 13.6.1.3, 13.6.1.4, 13.6.1.5, 13.6.1.6, 13.6.2.1, 13.6.2.2, 13.6.2.3, 13.6.2.4, 13.6.2.5, 13.6.2.6, 13.6.3.1, 13.6.3.2, 13.6.3.3, 13.6.3.4, 13.6.3.5, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.8.1.2, 13.8.1.3, 13.8.1.4, 13.8.1.5, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.5, 13.8.2.6, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.10.1, 13.10.2, 13.10.3, 13.10.4, 13.10.5, 13.10.6, 13.11.1, 13.11.2, 13.11.3, 13.11.4, 13.11.5, 13.11.6, 13.12.1, 13.12.2, 13.13.1, 13.13.2, 13.14.1, 13.14.2, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.2, 13.17.3, 13.17.4, 13.17.5, 13.17.6, 13.18.1, 13.18.2, 13.18.3, 13.18.4, 13.18.5, 13.18.6, 11.4.2.1, 11.4.2.2, 11.4.2.3, 11.6.1, 11.6.2, 11.6.3, 11.6.4, 11.6.5, 11.6.6, 11.8.2.1, 11.8.2.2, 11.8.2.3, 11.8.2.4, 11.8.2.5, 11.8.2.6, 11.10.2.1, 11.10.2.2, 11.10.2.3, 11.10.2.4, 11.10.2.5, 11.10.2.6, 11.11.2.1, 11.11.2.2, 11.11.2.3, 11.11.2.4, 11.11.2.5, 11.11.2.6, 11.12.2.1, 11.12.2.2, 11.12.2.3, 11.12.2.4, 11.12.2.5, 11.12.2.6, 17.1.2.1, 17.1.2.2, 17.1.2.3, 17.1.2.4, 17.1.2.5, 17.1.2.6, 17.2.2.1, 17.2.2.2, 17.2.2.3, 17.2.2.4, 17.2.2.5, 17.2.2.6, 17.3.2.1, 17.3.2.2, 17.3.2.3, 17.3.2.4, 17.3.2.5, 17.3.2.6, 17.4.2.1, 17.4.2.2, 17.4.2.3, 17.4.2.4, 17.4.2.5, 17.4.2.6, 17.5.2.1, 17.5.2.2, 17.5.2.3, 17.5.2.4, 17.5.2.5, 17.5.2.6, 18.1.2.1, 18.1.2.2, 18.1.2.3, 18.1.2.4, 18.1.2.5, 18.1.2.6, 18.2.2.1, 18.2.2.2, 18.2.2.3, 18.2.2.4, 18.2.2.5, 18.2.2.6, 18.3.2.1, 18.3.2.2, 18.3.2.3, 18.3.2.4, 18.3.2.5, 18.3.2.6,	Requirements as FLSS (B2) are below: 4.2.5.1, 4.2.5.2, 4.5, 4.6, 5.3, 7.1, 8.1, 8.2, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 5.1.1, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 11.2, 11.3, 17.2.1, 18.3.1, 13.3.3, 13.3.4, 13.3.5, 13.3.6, 13.4.1, 13.4.3, 13.4.4, 13.4.5, 13.5.1.2, 13.5.1.3, 13.5.1.4, 13.5.1.5, 13.5.1.6, 13.5.1.7, 13.5.2.3, 13.5.2.4, 13.5.2.5, 13.5.3.1, 13.5.3.2, 13.5.3.3, 13.5.3.4, 13.5.3.5, 13.5.3.6, 13.6.1.2, 13.6.1.3, 13.6.1.4, 13.6.1.5, 13.6.1.6, 13.6.2.3, 13.6.2.4, 13.6.3.3, 13.6.3.4, 13.7.3, 13.7.4, 13.7.5, 13.8.1.2, 13.8.1.3, 13.8.1.2, 13.8.1.3, 13.8.1.4, 13.8.1.5, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.6, 13.9.1, 13.9.2,13.9.4, 13.9.6, 13.10.1, 13.10.2, 13.10.4, 13.10.6, 13.11.1, 13.11.2, 13.11.4, 13.11.6, 13.13.1, 13.13.2, 13.14.1, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.3, 13.17.4, 13.17.5, 13.18.3, 13.18.4, 13.18.5, 11.6.3, 11.6.4, 11.6.5, 18.2.2.3, 18.2.2.4, 18.2.2.5, 11.10.2.4, 11.10.2.5, 11.11.2.4, 11.11.2.5, 11.12.2.3, 11.12.2.4, 11.12.2.5, 18.3.2.1, 18.3.2.3, 18.3.2.4, 18.3.2.5, 18.3.2.6,
FS13	SRV –Manual depressurization– (A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.2, 10.1, 10.2, 10.3, 10.4, 5.1.1, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 11.1, 11.3, 11.5, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.3.6, 13.4.1, 13.4.6, 13.5.1.1, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.6, 13.7.1, 13.7.6, 13.12.1, 13.12.2, 13.17.1, 13.17.6, 13.18.1, 13.18.6, 11.7.1, 11.7.4, 17.1.2.1, 17.1.2.6, 17.2.2.1, 17.2.2.6, 17.3.2.1, 17.3.2.6, 17.4.2.1, 17.4.2.6, 17.5.2.1, 17.5.2.6, 18.1.2.1, 18.1.2.6, 18.2.2.1, 18.2.2.6, 18.3.2.1, 18.3.2.6	

*: Refer to Appendix A1 for the reflect SFCs.

No*.	Front System	Initiating Fault / Event ID	Remarks
FS14	RHR(A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 11.1, 11.2, 11.3, 11.4.1, 11.5, 11.6, 11.7, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1 13.3.1, 13.3.2, 13.3.3, 13.3.4, 13.3.5, 13.3.6, 13.4.1, 13.4.2, 13.4.3, 13.4.4, 13.4.5, 13.4.6, 13.5.1.1, 13.5.1.2, 13.5.1.3, 13.5.1.4, 13.5.1.5, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.2, 13.5.2.3, 13.5.2.4, 13.5.2.5, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.2, 13.5.3.3, 13.5.3.4, 13.5.3.5, 13.5.3.6, 13.6.1.1, 13.6.1.2, 13.6.1.3, 13.6.1.4, 13.6.1.5, 13.6.2.1, 13.6.2.2, 13.6.2.3, 13.6.2.4, 13.6.2.5, 13.6.2.6, 13.6.3.1, 13.6.3.2, 13.6.3.3, 13.6.3.4, 13.6.3.5, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.8.1.2, 13.8.1.3, 13.8.1.4, 13.8.1.5, 13.8.1.6, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.5, 13.8.2.6, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.10.1, 13.10.2, 13.10.3, 13.10.4, 13.10.5, 13.10.6, 13.11.1, 13.11.2, 13.11.3, 13.11.4, 13.11.5, 13.11.6, 13.12.1, 13.12.2, 13.13.1, 13.13.2, 13.14.1, 13.14.2, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.2, 13.17.3, 13.17.4, 13.17.5, 13.17.6, 13.18.1, 13.18.2, 13.18.3, 13.18.4, 13.18.5, 13.18.6, 11.4.2.1, 11.4.2.2, 11.4.2.3, 11.6.1, 11.6.2, 11.6.3, 11.6.4, 11.6.5, 11.6.6, 11.7.1, 11.7.3, 11.7.4, 11.8.2.1, 11.8.2.2, 11.8.2.3, 11.8.2.4, 11.8.2.5, 11.8.2.6, 11.10.2.1, 11.10.2.2, 11.10.2.3, 11.10.2.4, 11.10.2.5, 11.10.2.6, 11.11.2.1, 11.11.2.2, 11.11.2.3, 11.11.2.4, 11.11.2.5, 11.11.2.6, 11.12.2.1, 11.12.2.2, 11.12.2.3, 11.12.2.4, 11.12.2.5, 11.12.2.6, 17.1.2.1, 17.1.2.2, 17.1.2.3, 17.1.2.4, 17.1.2.5, 17.1.2.6, 17.2.2.1, 17.2.2.2, 17.2.2.3, 17.2.2.4, 17.2.2.5, 17.2.2.6, 17.3.2.1, 17.3.2.2, 17.3.2.3, 17.3.2.4, 17.3.2.5, 17.3.2.6, 17.4.2.1, 17.4.2.2, 17.4.2.3, 17.4.2.4, 17.4.2.5, 17.4.2.6, 17.5.2.1, 17.5.2.2, 17.5.2.4, 17.5.2.5, 17.5.2.6, 18.1.2.1, 18.1.2.2, 18.1.2.3, 18.1.2.4, 18.1.2.5, 18.1.2.6, 18.2.2.1, 18.2.2.2, 18.2.2.3, 18.2.2.4, 18.2.2.5, 18.2.2.6, 18.3.2.1, 18.3.2.2, 18.3.2.3, 18.3.2.4, 18.3.2.5, 18.3.2.6,	
FS15	Containment venting(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.2, 11.3, 11.4.1, 11.5, 11.6, 11.7, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.4.1, 13.5.2.1, 13.5.3.1, 13.6.2.1, 13.6.3.1, 13.7.1, 13.8.1.1, 13.8.2.1, 13.9.1, 13.10.1, 13.11.1, 13.12.2, 13.17.1, 13.18.1, 11.6.1, 11.8.2.1, 11.10.2.1, 11.11.2.1, 11.12.2.1, 17.1.2.1, 17.2.2.1, 17.3.2.1, 17.4.2.1. 17.5.2.1, 18.1.2.1, 18.2.2.1, 18.3.2.1	Requirements as Containment venting (B2) are below: 4.5, 4.6, 5.3, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 5.1.1, 5.1.2, 5.1.3, 5.2.2, 5.2.3, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 11.4.1, 11.5, 18.3.1, 13.4.1, 13.5.3.1, 13.8.1.1, 13.8.2.1, 13.9.1, 13.10.1, 13.11.1, 13.17.1, 13.18.1, 17.5.2.1, 18.3.2.1
FS16	MSIV(A1)	2.1, 2.2, 2.3, 3.1, 4.6, 5.1, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 2.2.1, 2.3.1, 5.1.3, 3.1.1, 2.1.2, 11.2, 11.4.1, 11.8.1, 11.9, , 15.1.1, 15.1.2, 15.1.3, 17.6, 18.1.1, 18.2.1, 18.3.1	MSIV closure due to initiator (No description of Cat./Class) are below: 11.10.1, 11.11.1, 11.12.1, 18.1.1

*: Refer to Appendix A1 for the reflect SFCs.

No*.	Front System	Initiating Fault / Event ID	Remarks
FS17	PCIS(A1)	2.1, 2.2, 2.3, 3.1, 4.6, 5.1, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.2, 5.2.2, 5.3.2, 1.1.1, 1.4.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.2, 18.1.1, 18.2.1, 18.3.1	

Appendix B: SPC Claims Table

	SPC	Safety Properties Claims (SPC) Contents
1	C&I SPC 1	The safety functions allocated to C&I systems and their support systems have been categorised and the SSCs classified in accordance with their significance to safety.
2	C&I SPC 2	The C&I achieves the reliability requirements assigned to the SSCs which C&I controls.
3	C&I SPC 3	The C&I System has sufficient defence in depth to meet relevant operating conditions.
4	C&I SPC 4	The C&I systems have the appropriate level of redundancy to protect against single failure.
5	C&I SPC 5	The C&I is robust to specified internal hazards.
6	C&I SPC 6	The C&I is robust to specified external hazards.
7	C&I SPC 7	The C&I has adequate performance to execute the assigned nuclear safety functions and meet operational requirements.
8	C&I SPC 8	The C&I continues to meet its functional safety requirements throughout its operational life.
9	C&I SPC 9	The design, development and implementation processes of the C&I SSCs comply with standards and good practice set by their classification and the systems' role in the architecture.

Appendix C: Document Map