HOLTEC BRITAIN

A Holtec International Company

Holtec Britain Ltd	HI-2240338
Sponsoring Company	**Document Reference**
1	23 September 2025
Revision No.	**Issue Date**
Report	Non-proprietary
Record Type	**Proprietary Classification**
ISO 9001	No
Quality Class	**Export Control Applicability**

Record Title:

PSR Part B Chapter 4 Control and Instrumentation Systems

Proprietary Classification

This record does not contain commercial or business sensitive information.

Export Control Status

Export Control restrictions do not apply to this record.

Revision Log

Revision	Description of Changes
0	First Issue to Regulators to support PSR v0
1	Second Issue to Regulators to support PSR v1
1.1	Review of CCI content in support of PSR v1

Table of Contents

List of Tables

List of Figures

4.1 INTRODUCTION

The Fundamental Purpose of the Generic Design Assessment (GDA) Safety, Security and Environment Case (SSEC) is to demonstrate that the generic Small Modular Reactor (SMR)-300 can be constructed, operated, and decommissioned on a generic site in the United Kingdom (UK) to fulfil the future licensee's legal duties to be safe, secure and to protect people and the environment, as defined in Holtec SMR GDA Preliminary Safety Report (PSR) Part A Chapter 1 Introduction [1].

The Fundamental Purpose is achieved through the Fundamental Objective of the PSR, which is to summarise the safety standards and criteria, safety management and organisation, as well as Claims, Arguments and intended Evidence (CAE) to demonstrate that the generic SMR-300 design risks to people are likely to be tolerable and As Low as Reasonably Practicable (ALARP).

Part B Chapter 4 of the PSR presents the CAE for the Instrumentation and Control (I&C) topic.

4.1.1 Purpose and Scope

The overarching SSEC Claims are presented in Part A Chapter 3 Claims, Arguments and Evidence [2].

This chapter (Part B Chapter 4) links to the overarching claim through Claim 2.2:

Claim 2.2: The design of the systems and associated processes have been developed taking cognisance of Relevant Good Practice (RGP) and substantiated to achieve their safety and non-safety functional requirements.

As set out in Part A Chapter 3 [2], Claim 2.2 is further decomposed across several engineering disciplines which are responsible for development of the design of relevant Structures, Systems and Components (SSC). This chapter presents the I&C aspects for the generic SMR-300, and therefore directly supports the claim focused on the overall design and architecture of the I&C systems, Claim 2.2.6.

Claim 2.2.6: The overall design and architecture of I&C SSCs ensure that safety functions and non-safety functions are delivered and faults arising from failures of the SSCs are minimised.

Further discussion on how the Level 3 claim is broken down into Level 4 claims and how the Level 4 claims are met is provided in sub-chapter 4.3.

This chapter will address areas within the GDA scope as defined in PSR Part A Chapter 2 General Design Aspects and Site Characteristics [3]. The scope of this chapter covers the reactor island I&C SSCs as set out in Section 4.2.1.

Sub-chapter 4.4 covers the codes and standards associated with the design of these I&C systems. Sub-chapter 4.5 covers the Defence in Depth (DiD) associated with the design of these I&C systems. Sub-chapter 4.6 covers the quality manufacturing and installation approach. Sub-chapter 4.7 covers the Examination, Inspection, Maintenance and Testing (EIMT). Finally, sub-chapter 4.8 provides a technical summary of how the claims for this

chapter have been achieved, together with a summary of key contributions from this chapter to the overall ALARP position. Sub-chapter 4.8 also discusses any GDA commitments that have arisen.

Excluded from the Part B Chapter 4 scope are the dedicated I&C systems, which are not part of the centralised I&C systems but are associated with particular plant systems. Safety justification for dedicated I&C systems will be added in future safety reports beyond the GDA process.

Also excluded from the Part B Chapter 4 I&C scope are the Radiological Protection Monitoring Systems which are covered by Part B Chapter 10 Radiological Protection [4]. The seismic detection instrumentation system is also excluded at this stage as information is not yet available.

Security and cyber security are also excluded from the Part B Chapter 4 scope and are addressed separately as part of the Generic Security Report (GSR) [5].

A master list of definitions and abbreviations relevant to all PSR Chapters can be found in Part A Chapter 2 General Design Aspects and Site Characteristics [3].

4.1.2 Assumptions

No assumptions have been identified for Part B Chapter 4. Any assumptions relevant to this topic that are identified in the future will be formally captured by the Commitments, Assumptions and Requirements (CAR) process [6]. Further details of this process are provided in Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance [7].

4.1.3 Interfaces with other SSEC Chapters

The I&C discipline interfaces with multiple plant systems and disciplines. The I&C architecture supports delivery of the safety features for those systems described in Part B Chapter 1 Reactor Coolant System and Engineered Safety Features [8], Part B Chapter 5 Reactor Supporting Facilities [9] and Part B Chapter 19 Mechanical Engineering [10].

The I&C systems provide monitoring and control in the Main Control Room (MCR) and Remote Shutdown Facility (RSF) to support Part B Chapter 9 Description of Operational Aspects/Conduct of Operations [11]. Safety functional requirements for I&C systems and faults associated with the I&C systems are identified and analysed in Part B Chapter 14 (Design Basis Accident Analysis) [12] and other safety analysis chapters.

Electrical supplies to the I&C systems are described in Part B Chapter 6 (Electrical Engineering) [13]. Human Factors (HF) will support the design of the I&C Human System Interfaces (HSIs) and HF related issues for the MCR and RSF, as covered in Part B Chapter 17 Human Factors [14]. Hazards are addressed in Part B Chapter 12 Nuclear Site Health and Safety and Conventional Fire Safety [15], Part B Chapter 22 Internal Hazards [16] and Part B Chapter 21 External Hazards [17]. I&C reliability figures are used in Part B Chapter 16 Probabilistic Safety Analysis (PSA) [18]. I&C ALARP arguments will inform the overall ALARP claims in Part A Chapter 5 Summary of ALARP [19].

4.2 DESCRIPTION OF I&C SSC

The initial starting point for identifying the I&C SSC is HPP-8002-0012, SMR-300 Systems, Structures, and Components Classification [20], and the Institute of Electrical and Electronics Engineers (IEEE) Standard Criteria for Safety Systems for Nuclear Power Generating Stations American National Standards Institute (ANSI)/IEEE-603-1991 [21]. These give the basic criteria for safety-related electrical and I&C systems and equipment. Electrical and I&C system equipment and components are classified as Class 1E or Non-Class 1E.

The SMR-300 I&C (including the associated HSI) is a two-safety division configuration intended to meet current industry standards and United States Nuclear Regulatory Commission (USNRC) requirements. The SMR-300 I&C encompasses the safety and non-safety I&C systems of a nuclear power plant, including HSI, and the interface to plant sensors and controlled plant components (e.g., pumps, valves, electrical breakers).

The SMR-300 I&C achieves DiD by providing separate systems for monitoring and control, protection and diverse actuation functions with appropriate redundancy, independence, diversity, determinism, segregation, fail-safe design and simplicity. Modern digital technology is employed for high availability, to reduce human performance error, and to optimise Operation and Maintenance (O&M).

The SMR-300 I&C design is for a twin reactor unit design. Each unit will have separate I&C systems for control and protection of the plant. The MCR and RSF provisionally have one operator console that includes screens dedicated for each unit.

A limited number of plant non-safety systems are shared between the two units, and these will be controllable from either of the units' Plant Control Systems (PCSs).

4.2.1 I&C Systems

In accordance with the overall hierarchy of SMR-300 documentation, the SMR-300 Specification – Instrumentation and Controls [22] sets out the overall I&C requirements including regulatory requirements and standards for the I&C systems.

The following systems are identified as I&C SSCs for this chapter of the PSR. They are described in the system design documents (SDDs) referenced.

- Plant Safety System (PSS) [23].
- Plant Control System (PCS) [24].
- Diverse Actuation System (DAS) [25].
- Post-Accident Monitoring System (PAM) [26].
- In-Core Instrumentation System (IIS) [27].
- Ex-Core Instrumentation System (EIS) [28].

Note that the DAS SDD for the SMR-300 will be available later, after step 2 of GDA, due to the decision to modify the DAS design from a microprocessor-based system to a non-computerised hardware-based system. See section 4.2.3.3 for more details.

Further detailed design documents for each I&C system are produced based on the requirements in the SDDs and these are identified as System Requirement Specifications

(SRS) and are produced by the I&C system supplier, Mitsubishi Electric Corporation (MELCO). The SRSs are not in the design reference point and only the PSS SRS is referenced in this chapter to provide additional design information.

[REDACTED]

The I&C systems capture plant parameters and provide information to the operator to allow plant monitoring, manual control and safety actions when required. In addition, certain control and safety actions are provided automatically to control and regulate the plant systems during normal plant operation and provide reactor protection against abnormal conditions to bring the reactor to a safe shutdown state. Safety functions are those actions required to achieve the system responses assumed in the safety analyses and those credited to achieve safe shutdown of the plant.

The I&C interfaces via inputs and outputs with the plant SSCs to monitor plant parameters and control components such as valves, pumps, etc. to deliver the required safety and non-safety functions. The detailed interfaces are, or will be, described within the PSR sections discussing the individual plant SSCs.

The SMR-300 I&C/HSI consists of three main systems PSS, PCS and DAS that operate independently to deliver the required safety functions. The IIS and EIS provide the reactor flux and other reactor parameter measurements. The HSI is provided by parts of each of the three main I&C systems as shown in the I&C architecture diagram in Figure 3.

Brief I&C system descriptions are presented in Table 1, with more detail provided in the following sub-sections.

Table 1: Instrumentation & Control SSCs

I&C SSC	Description
Plant Safety System	The PSS monitors all safety instrumentation and has automatic and manual actuation for Reactor Trip (RT) and Engineered Safety Features (ESFs). The PSS is the credited Class 1E system to mitigate Design Basis Accidents (DBAs) and achieve safe shutdown.
Diverse Actuation System	The Non-Class 1E DAS monitors safety instrumentation and controls safety and non-safety components to mitigate DBAs and achieve safe shutdown, should there be a concurrent Common Cause Failure (CCF) in the PSS. The Non-Class 1E DAS provides a diverse means of RT and ESF actuation [REDACTED]
Plant Control Systems	The PCS directly monitors non-safety plant instrumentation, controls non-safety plant components, and receives safety plant instrumentation signals via digital data and communication from the PSS. [REDACTED]. The PCS HSI is the primary operator interface for all normal and abnormal plant conditions. The PCS HSI is the preferred way to operate the plant because it utilises advanced Graphical User Interface (GUI), rapid navigation, advanced alarm processing, and computer-based procedures that improve operator performance and reduce the potential for human performance error.
Post-Accident Monitoring System	The PAM is a grouping of instrumentation and displays that operators use for monitoring plant parameters following an accident condition. [REDACTED] The parameters are displayed on operational Visual Display Units (VDUs) in the control room to be used in response to a plant accident.
Ex-Core Instrumentation System	The primary function of the ex-core nuclear instrumentation is to protect the reactor core from overpower by monitoring the neutron flux to allow the generation of appropriate alarms and reactor trips to shut down the reactor when required. Neutron flux levels are also used to determine operating permissives (or interlocks). The EIS provides indication in the MCR, and signals are provided to the PAM.

I&C SSC	Description
In-Core Instrumentation System	The IIS provides information on the neutron flux distribution and fuel assembly outlet temperatures at designated locations in the core. The IIS performs no protective or plant control functions and is primarily used to demonstrate compliance to Technical Specification limits. In-core monitoring enhances plant operation through continuous, real-time monitoring of actual core conditions. The IIS consists of fixed neutron flux and temperature monitoring systems that permit measurement of localised neutron flux and temperature variations within the reactor core. The IIS sensor cabling enters from the top of the Reactor Pressure Vessel (RPV).
Human System Interface (Part of PCS, PSS & DAS)	The HSI uses VDUs in the MCR and RSF. A VDU provides displays and corresponding soft controls. The HSI consists of: • Non-safety Operational VDUs (O-VDUs) and non-safety Large Display Panel (LDP) for normal and abnormal plant operation, part of PCS. • Safety VDUs (S-VDUs), part of PSS. • Conventional switches for system-level initiation for regulatory compliance (e.g. Regulatory Guide (RG) 1.62 [29]). • Non-safety DAS HSI (D-HSI). Part of DAS. The S-VDUs and O-VDUs are in the MCR and the RSF. O-VDUs may also be provided for information only (i.e. no control or alarm acknowledgement capability) at the Technical Support Centre (TSC), details to be confirmed. The SMR-300 I&C/HSI System provides digital data to the plant's Information Processing System (IPS). This includes Safety Parameters Display System (SPDS) data to support emergency response operations (the same data as provided on O-VDUs). This SPDS information is displayed at the Emergency Operations Facility (EOF) via EOF computers and displays. The EOF computers and displays are part of the plant's IPS, which is not in the scope of the GDA. The PSS HSI is provided for Class 1E regulatory compliance, and it provides the first backup operator interface for failure of the PCS. The DAS HSI is the second backup operator interface for failure of the PSS.

4.2.2 Plant Safety System

The PSS is a two-division Class 1E system designed to mitigate DBAs and achieve safe shutdown. Although subject to the overall project category/classification work this would typically be a Class 1 system in the UK in accordance with BS EN 61226 [30]. The analysis described in PSR Part B Chapter 14 [12] has given the PSS a preliminary Class 1 classification and the codes and standards review has confirmed broad equivalence between Class 1E and Class 1 – see section 4.4.6 Claim 2.2.6.1 -A2.

4.2.2.1 Design Intent

The PSS is the primary means of providing reactor safety I&C functions. It monitors plant parameters to ensure that the plant operation is within the limits defined by the safety analysis for Design Basis Events (DBE) [REDACTED].

The PSS provides:

- Automatic RT and ESF operation in abnormal conditions at appropriate plant conditions and operating modes.
- Manual actuation of safety functions.
- Safety related plant information on displays in the MCR and RSF [REDACTED].
- Prioritisation for outputs between the PSS and DAS and between the PSS and PCS.
- Automated Testing that does not inhibit performance of safety functions.
- Maintenance and Operating Bypass Facilities.

In addition, the PSS I&C design:

- Includes appropriate redundancy, independence, and segregation.
- Is diverse from the DAS (because the DAS is specifically designed to be diverse from the PSS in order to ensure the delivery of the necessary safety functions should a common cause failure make the PSS inoperable).
- Has the required environmental qualifications.
- Facilitates maintenance, detection and diagnosis of failure, repair or replacement.
- Provides the required reliability and performance.

4.2.2.2 System Description

The PSS is:

- Qualified to Class 1E.
- Based on the Mitsubishi Electric Corporation (MELCO) Total Advanced Controller (MELTAC) Nplus S platform.
- Powered from the Class 1E I&C power distribution system.
- Powered from DC batteries (sized for 72 hours operation) following loss of alternating current (AC) supplies.
- Located in separate division I&C Rooms, the MCR and RSF.

The PSS architecture is shown in the SDD [23]. The main sub-systems of the PSS are:

- Reactor Protection Processor (RPP).
- Component Control Processor (PSS-CCP).
- Safety Human System Interface:
  - Safety Visual Display Unit (S-VDU).
  - Safety Visual Display Unit Processor (S-VDU-P).
- PSS Engineering tool that implements maintenance functions on the safety system.

The PSS platform and these subsystems are described further in the following subsections.

4.2.2.2.1 PSS Platform

[REDACTED]

4.2.2.2.2 Field Programmable Gate Arrays (FPGAs)

[REDACTED]

4.2.2.2.3 PSS-Reactor Protection Processor

[REDACTED]

The RPP is a computer rack made up of microprocessor, communication and supporting electronic modules. It provides:

[REDACTED]

- 2 divisions A and B, each implementing two-out-of-four (2oo4) voting logic.

- Division A receives signals from safety sensors of measurement channels U and X while Division B receives signals from safety sensors of measurement channels Y and Z.
- Data is transferred between the two divisions in order to perform the 2oo4 vote.

[REDACTED]

4.2.2.2.4 PSS-Component Control Processor

[REDACTED]

4.2.2.2.5 Plant Safety System-Human System Interface

[REDACTED]

4.2.2.2.6 PSS Inputs/Outputs

[REDACTED]

4.2.2.2.7 PSS – Prioritisation

[REDACTED]

4.2.2.2.8 Communication Networks

[REDACTED]

[REDACTED]

Figure 1: Signal flow from the PCS to PSS

4.2.2.2.9 Communication Independence

[REDACTED]

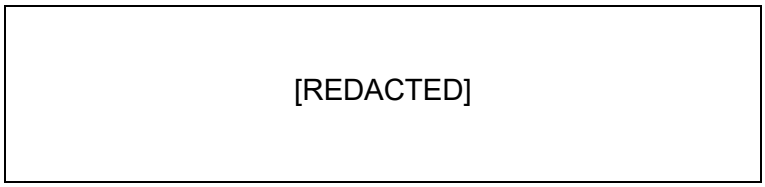

Figure 2: Communication Independence of the PSS

4.2.2.2.10 PSS Engineering Tool

The PSS engineering tool is a stand-alone computer using Personal Computer (PC) technology running engineering tool software. There is a PSS engineering tool for each PSS division. [REDACTED]

4.2.2.2.11 System Boundaries and Interfaces

[REDACTED]

4.2.2.2.12 Duty in Normal Operating Conditions and Fault Conditions

[REDACTED]

4.2.2.2.13 Reliability and Single Failure Criteria

[REDACTED]

4.2.2.2.14 Performance

[REDACTED]

4.2.2.2.15 Hazards

[REDACTED]

- Fire: PSS divisions are located in different fire zones.

[REDACTED]

4.2.3 Diverse Actuation System

Note that the following description relates to the design reference point (DRP) proposals for DAS. As part of GDA Step 2, Holtec Britain (HB) have raised a design challenge paper [31] and it has been decided to change the DAS design to a non-computerised hardware platform as described in the Design Decision Paper [32].

The DAS [REDACTED] provides the functions of the PSS in the event that the PSS fails to operate.

4.2.3.1 Design Intent

The DAS provides a diverse means of delivering the required safety functions for RT and ESF in the event that the PSS divisions fail to operate, e.g. due to some CCF.

The DAS:

- Provides manual operator action for the safety functions.
- Initiates safety functions after DAS actuation conditions are exceeded. Note there is an additional margin between PSS and DAS actuation setpoints.
- Maintains plant conditions within specified acceptance criteria for associated DBEs.
- Provides Anticipated Transient without Scram (ATWS) mitigation capability from MCR.
- Provides a Diverse Reactor Trip function.
- Mitigates Anticipated Operational Occurrence (AOO) assuming PSS fails to trip the reactor.

It also:

- Facilitates safety instrumentation signal sharing.
- Provides sufficient diversity between PSS and DAS.
- Provides MCR display and controls for manual system-level actuation of critical safety functions and monitoring of parameters.
- Has appropriate environmental qualifications.
- Facilitates maintenance, detection and diagnosis of failure, repair, or replacement.
- Provides indication of system unavailability during maintenance and testing.

In order to achieve the required diversity and integrity, it also:

- Uses different development and testing teams from the PSS for the platform software.
- Does not utilise digital communication from/to other Digital I&C systems but uses hardwired connections and a separate RT output.

[REDACTED]

4.2.3.2 System Description

[REDACTED]

4.2.3.2.1 DAS Platform – [REDACTED]

[REDACTED]

4.2.3.2.2 Diverse Protection Processor

[REDACTED]

4.2.3.2.3 Diverse Actuation System - Human System Interface

[REDACTED]

4.2.3.2.4 DAS Inputs/Outputs

[REDACTED]

4.2.3.2.5 Communication Networks

[REDACTED]

4.2.3.2.6 DAS Engineering Tool

[REDACTED]

4.2.3.2.7 System Boundaries and Interfaces

[REDACTED]

The key interfaces to the DAS are described in the DAS SDD [25].

4.2.3.2.8 Duty in Normal Operation and Fault Conditions

[REDACTED]

4.2.3.2.9 Reliability and Single Failure Criteria

[REDACTED]

4.2.3.2.10 Performance

[REDACTED]

4.2.3.2.11 Hazards

[REDACTED]

4.2.3.3 DAS Design Challenge

[REDACTED]

4.2.3.3.1 Classification of DAS

[REDACTED]

4.2.3.3.2 Codes and standards analysis

[REDACTED]

4.2.3.3.3 Justification for use of shared functional equipment

[REDACTED]

4.2.3.3.4 Justification for use of shared sensing equipment

[REDACTED]

4.2.3.3.5 Justification of PIMs design

[REDACTED]

4.2.3.3.6 Loss of all computer systems

[REDACTED]

4.2.3.3.7 Display of PAM information

[REDACTED]

4.2.3.3.8 DAS Reactor Trip

[REDACTED]

4.2.4 Plant Control System

The PCS provides the primary interface to the operator in the MCR in normal and fault conditions. It monitors non-safety and safety parameters and provides information displays, alarms and touchscreen control commands to operate the plant systems. The PCS is classified as a non-safety system in the SMR-300 design.

4.2.4.1 Design Intent

The PCS monitors plant parameters to provide information to the operator in the MCR and RSF and provides automatic and manual control facilities for the plant systems.

The PCS provides:

- Monitoring and display of plant system parameters to the Operator in the MCR and RSF.
- Alarms to alert the operator to abnormal plant and equipment conditions.
- Manual actuation of plant systems using touchscreen commands on the VDUs.
- Automatic control of plant systems to maintain the plant within the normal operating envelope.
- Data logging.
- Historian functionality.
- [REDACTED]

The PCS is not credited to perform any action during DBA.

In addition, the PCS I&C design:

- Includes appropriate redundancy to support operational requirements.
- Has the required environmental qualifications.
- Facilitates maintenance, detection and diagnosis of failure, repair or replacement.
- Provides the required reliability and performance.

[REDACTED]

4.2.4.2 System Description

The PCS is:

- A Non-Class 1E system.
- Based on the MELTAC-RX platform.
- Powered from Non-Class 1E I&C Power distribution System (ICE).
- [REDACTED]

The PCS architecture is shown in the PCS SDD [24].

The main sub-systems of the PCS are:

- Component Control Processors (CCPs).
- VDU Processors for Alarms, Operational, and Procedure displays for the Supervisor and Operator in the MCR and RSF. A Large Display Panel (LDP) screen is also provided in the MCR.
- PCS Engineering tool that implements maintenance functions on the system.

The PCS platform and these subsystems are described further in the following subsections.

4.2.4.2.1 PCS Platform

[REDACTED]

4.2.4.2.2 PCS-Component Control Processors

[REDACTED]

4.2.4.2.3 Plant Control System-Human System Interface

[REDACTED]

4.2.4.2.4 PCS Inputs/Outputs

[REDACTED]

4.2.4.2.5 Communication Networks

[REDACTED]

4.2.4.2.6 PCS Engineering Tool

[REDACTED]

4.2.4.2.7 System Boundaries and Interfaces

[REDACTED]

4.2.4.2.8 Duty in Normal Operating Conditions and Fault Conditions

[REDACTED]

4.2.4.2.9 Reliability and Single Failure Criteria

[REDACTED]

4.2.4.2.10 Performance

[REDACTED]

4.2.4.2.11 Hazards

[REDACTED]

4.2.5 Main Control Room & Remote Shutdown Facility

The MCR provides the central location for monitoring and control of the plant. The RSF is provided for circumstances when the MCR is not usable. It allows the operator to shut down and monitor the reactor. The I&C systems provide the VDUs and manual controls in both rooms. See PSR Part B Chapter 9 Conduct of Operations [11] for an overview of the MCR and RSF.

The VDUs consist of VDU processors, which are in the [REDACTED], and VDU panels (e.g. liquid crystal displays), which are located in the control rooms. Hereafter, this combination of a VDU processor and panel is referred to as a VDU. A VDU provides displays and corresponding touchscreen soft controls.

The MCR is common for both units, with each unit having a large display panel (LDP), one Safety Console (SC) for each division, a DAS console, and an Operator Console (OC). An additional common OC is provided for the Senior Reactor Operator (SRO). The RSF is common to both units and has one OC and one SC per unit.

A summary of the MCR and RSF I&C is provided below, followed by a description of the HSI for the PSS, DAS and PCS.

4.2.5.1 Main Control Room

The MCR I&C:

- Is computerised with one supervisor console and one operator console, each with screens dedicated to each unit.
- Provides S-VDUs and non-safety O-VDUs.
- Includes a large display processor and large display panel for each unit.
- Has minimal conventional switches; only system-level initiation switches for regulatory compliance (e.g. RG1.62 [29]) and switches for transfer to the RSF.

[REDACTED]

4.2.5.2 Remote Shutdown Facility

The RSF I&C:

- Is computerised and is provided for circumstances when the MCR is not usable.
- Provides S-VDUs and non-safety O-VDUs.
- Provides Manual Initiation Switches (MIS) for RT as per MCR.
- Has minimal conventional switches; only system-level initiation switches for regulatory compliance (e.g. RG 1.62 [29]) and switches for transfer from MCR.

The RSF includes:

[REDACTED]

4.2.5.3 Other Locations

O-VDUs are also provided for information only (i.e. no control or alarm acknowledgement capability) at the TSC.

The PCS provides digital data to the plant's Information Processing System (IPS). This includes Safety Parameter Display System (SPDS) data to support emergency response operations (the same data as provided on O-VDUs). This SPDS information is displayed at the emergency operations facility (EOF) via EOF computers and displays. The EOF computers and displays are part of the plant's IPS.

4.2.5.4 I&C Systems Human System Interfaces

The features of the SMR-300 I&C/HSI systems are summarised as follows:

4.2.5.4.1 Plant Safety System Human System Interface

The PSS-HSI is made up of:

- PSS Visual Display Unit Processor (S-VDU-P).
- PSS Visual Display Unit (S-VDU).
- MIS.
- Manual Transfer Switches (MXS).

[REDACTED]

4.2.5.4.2 Diverse Actuation System Human System Interface

As part of the commitment (C_I&C_082) to provide a non-computerised DAS, the design of the DAS HSI will be changed and is likely to be discrete analogue and digital indications and controls. The following description relates to the design reference point (DRP) proposals for DAS.

[REDACTED]

4.2.5.4.3 Plant Control System Human System Interface

The PCS-HSI is made up of display processors and touchscreen VDUs.

The Supervisor Console in the MCR is provided with.

- PCS Alarm Visual Display Unit Processor (A-VDU-P) and Alarm VDU (A-VDU).
- PCS Operational Visual Display Unit Processor (O-VDU-P) and VDU (O-VDU).
- PCS Procedural Visual Display Unit Processor (P-VDU-P) and Procedural VDU (P-VDU).

The Operator Console in the MCR is similar but has two Operational processors and VDUs per unit. The Operator Console configuration is also provided in the RSF.

The operator console is where plant operation is conducted from. Note that the supervisor console is a read only console and provides no control functions.

A PCS Large Display Panel VDU Processor (LDP-VDU-P) is provided for overview displays in the MCR.

[REDACTED]

4.2.6 Reactor Pressure Vessel I&C Ex-core & In-core SSC

SMR-300 I&C design includes specialised instrumentation for reactor parameters monitoring, which include In-core and Ex-core instrumentation, consisting of sensors, detectors, amplifiers, and signal processing logic units. The following section presents the general description of their functions, and their interface with the PSS, DAS, and PCS.

4.2.6.1 Ex-Core Instrumentation

The ex-core instrumentation system (EIS) monitors the reactor power level by detecting neutron leakage from the reactor core with fixed neutron detectors located external to the Reactor Pressure Vessel (RPV). Three ranges of safety related instrument channels are used to provide measurement of neutron flux from the reactor core: Source Range (SR), Intermediate Range (IR), and Power Range (PR). Each range has four redundant channels. The three measurement ranges cover the entire operating range of the reactor from refuelling operations to ‘at power’ conditions. The ranges overlap to ensure proper coverage.

The safety functions of the EIS are to:

- Monitor Neutron Flux from shutdown to full power operation.
- Monitor the rate of change of neutron flux in the Power Range.
- Monitor power distribution in the Power Range.
- Monitor Neutron Flux during a DBA.

Safety functions are provided by Class 1E qualified equipment.

The non-safety functions of the EIS are to:

- Provide Neutron Flux indications, recordings, and alarms from shutdown to full power operation.
- Provide Reactor Power information to the reactor control system.
- Provide nuclear flux data to the plant historian.
- Provide audible count rate and alarms during shutdown and refuelling.
- Provide startup rate monitoring.

[REDACTED]

4.2.6.2 In-Core Instrumentation

The in-core instrumentation system (IIS) is provided by Instrument Assemblies (IAs) designed to be inserted into the centre of a fuel assembly lattice in designated instrumentation tubes.

The IIS safety function is the IA’s role in maintaining the reactor pressure boundary. Otherwise, the IIS and IAs provide non-safety functions.

The IIS non-safety functions consist of:

- Core exit temperature instrumentation.
- Reactor vessel water level instrumentation.
- In-core nuclear instrumentation.

The in-core nuclear instrumentation consists of Self-Powered Neutron Detector (SPND) assemblies that include an outer sheath containing detector and thermocouple. The SPND assemblies are spaced both radially and axially to be able to fully describe the three-dimensional (3D) power distribution while maintaining a low uncertainty. Since the in-core instrumentation does not provide protection functions, these detectors do not need to be fast responding.

[REDACTED]

4.2.7 Post-Accident Monitoring

In the SMR-300 there is no separate, independent post-accident monitoring I&C system. [REDACTED]. There are no Type A parameters. Type B and C parameters are displayed by the [REDACTED] and the Type D, E, and F parameters are displayed by the [REDACTED]. See Table 5 for the definition of parameter types and Regulatory Guide 1.97 [33].

The United States (US)/IAEA approach to post-accident monitoring differs from the approach taken in the UK. [REDACTED].

To demonstrate risks have been reduced to ALARP Holtec will:

- Review the US/IAEA requirements for post-accident monitoring signals on the basis that they are specified, and the UK approach is goal setting.
- Review the US/IAEA expectations against the SMR-300 fault studies/severe accident analysis (SAA). This will consider aspects such as the impact of the PSS being unavailable in a post-accident scenario.

A commitment (C_I&C_083) has been raised to address these points – see section 4.8.3.

4.3 I&C CLAIMS, ARGUMENTS AND EVIDENCE

This chapter presents the I&C aspects for the generic SMR-300 and therefore directly supports Claim 2.2.6.

Claim 2.2.6: The overall design and architecture of I&C SSCs ensures that safety functions and non-safety functions are delivered and faults arising from failures of the SSCs are minimised.

Claim 2.2.6 has been further decomposed within Part B Chapter 4 across the development lifecycle, to provide confidence that the relevant requirements for I&C systems and I&C architecture will be met during all lifecycle phases. This has been achieved by breaking down Claim 2.2.6 into four further sub-claims as follows:

Sub-claim 2.2.6.1 The I&C SSCs are designed using appropriate codes and standards taking cognisance of relevant good practice (RGP) and Operational Experience (OPEX).

This sub-claim shows that the design addresses the requirements in the appropriate codes and standards during the design phase and takes account of relevant good practice in existing designs and operational experience.

Sub-claim 2.2.6.2 The I&C system design incorporates Defence in Depth to protect against anticipated operational occurrences and accident conditions.

This sub-claim shows that the I&C architecture and I&C system design phase supports the overall DiD approach with suitable I&C systems providing the required safety and non-safety functions for their associated DiD level and that they also operate as required if other I&C systems fail to operate.

Sub-claim 2.2.6.3 I&C SSCs achieve the design intent through quality manufacturing and installation processes.

This sub-claim shows that the design is implemented according to the design intent and that the I&C systems can provide the required functionality in the site environment, noting that the maturity of evidence for this claim will be limited at a PSR stage.

Sub-claim 2.2.6.4 Examination, inspection, maintenance and testing regimes provide confidence in the design and continued operation of the I&C systems for their design lifetime.

This sub-claim ensures that the I&C systems are initially tested appropriately at site including through I&C system commissioning and subsequently that they are subject to EIMT throughout their operational life to ensure they continue to provide the required safety functions. The maturity of evidence for this claim is limited at a PSR stage.

Table 2 shows the breakdown of Claim 2.2.6 and identifies in which chapter of this PSR these claims are demonstrated to be met to a maturity appropriate for PSR v1.

Table 2: Claims Covered by Chapter B4

Claim No.	Claim	Chapter Section
2.2.6.1	The I&C SSCs are designed using appropriate codes and standards taking cognisance of relevant good practice (RGP) and operational experience (OPEX).	4.4 Codes, Standards & Methodologies
2.2.6.2	The I&C system design incorporates DiD to protect against anticipated operational occurrences and accident conditions.	4.5 Defence in Depth
2.2.6.3	I&C SSCs achieve the design intent through quality manufacturing and installation processes.	4.6 Quality Manufacturing and Installation
2.2.6.4	Examination, inspection, maintenance and testing regimes provide confidence in the design and continued operation of the I&C systems for their design lifetime.	4.7 Examination, Inspection, Maintenance, and Testing

Appendix A provides a full Claims, Arguments and Evidence mapping for Chapter B4, which includes any lower-level claims, arguments and evidence needed to support the claims in the table above. This includes identification of evidence available at PSR v1 and aspects for future development of evidence to support these claims beyond PSR v1.

4.4 I&C CODES, STANDARDS AND METHODOLOGIES

Claim 2.2.6.1: The I&C SSCs are designed using appropriate codes and standards taking cognisance of relevant good practice (RGP) and operational experience (OPEX).

This section identifies the codes and standards used in developing the I&C system design, the relevant good practice considered, and the operational experience taken into account.

4.4.1 Codes and Standards

The I&C systems have been designed in accordance with the main codes and standards identified in Table 3.

The codes and standards have been selected in accordance with the SSC safety classification outlined in Section 4.4.2 Safety Categorisation and Classification. The codes and standards identified reflect the functional and reliability requirements of the SSCs.

Codes and standards that have been applied in the design of the I&C systems of the SMR-300 are identified in the I&C system SDDs [23] [24] [25] [26] [27] [28]. The US/UK Regulatory Framework and Principles Report [34] has identified Safety Assessment Principles (SAPs) and US Nuclear Regulatory Commission (U.S.NRC) General Design Criteria (GDC) for Nuclear Power Plant [35] and provides a comparison against the US regulatory framework.

The applicable US and UK I&C standards are identified. UK standards that are considered by ONR to represent RGP (as set out in Table 4) have been compared with U.S.NRC guides and associated standards to establish if there is an equivalent standard in the US. This has been carried out mostly at a clause-by-clause level. Differences between the two sets of documents have been identified. The identified differences have been reviewed by the Requesting Party (RP) and any significant differences confirmed or rejected. The confirmed differences will be used to inform the development of the I&C design and/or further design justification work beyond GDA. Ultimately, for each I&C system an evaluation of compliance of the system to US expectations will be undertaken. This will allow traceability of the design through US codes and standards and the UK/US codes and standards comparison to demonstrate compliance with UK RGP.

In some cases, the U.S.NRC has endorsed an older version of some standards e.g. IEEE, and a newer version has been issued. The intention of the Requesting Party is to comply with both the U.S.NRC endorsed version and the latest version (date noted in brackets) for standards.

Table 3: Main Codes, Standards, and Regulations Utilised for Development of the SMR-300 I&C Design

#	Title of Code/Standard Reference	Rev/Date
1.	U.S.NRC, 10CFR50 Appendix A to part 50 - General Design Criteria for Nuclear Power Plants [35] In particular, parts 13 I&C, 19 control room, and 20-29 for the protection system.	2021
2.	U.S.NRC Regulatory Guides [36].	Various
3.	U.S.NRC, NUREG-0800, Chapter 7, Instrumentation and Controls [37].	2016
4.	IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603 [21].	1991 (2018)
5.	IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2 [38].	2016

#	Title of Code/Standard Reference	Rev/Date
6.	IEEE/IEC 60780-323, IEC/IEEE International Standard - Nuclear facilities – Electrical equipment important to safety -- Qualification [39].	2016
7.	IEEE Std. 379, IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems [40].	2000 (2014)
8.	IEEE Std. 384, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits [41].	1992 (2018)
9.	IEEE, 497, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations [42].	2016
10.	IEEE Standard 730, IEEE Standard for Software Quality Assurance Plans [43].	2014 (not endorsed)
11.	U.S.NRC, Branch Technical Position (BTP) 7-19, Guidance for Evaluation of Defense in Depth and Diversity to Address Common Cause Failure due to Latent Defects in Digital Safety Systems [44].	2024
12.	U.S.NRC, NUREG/CR-6991, Design practices for communications and workstations in highly integrated control rooms [45].	2009
13.	U.S.NRC, NUREG/CR-6082, Data Communications [46].	1993

Table 4: Identified Applicable Standards Relevant to the I&C Topic in the UK Context

#	Title of Code/Standard Reference	Rev/Date
1.	IAEA – Specific Safety Guide SSG-39 – Design of Instrumentation and Control systems for Nuclear Power Plants [47].	2016
2.	BS EN 61513 – Nuclear power plants - Instrumentation and control important to safety — General requirements for systems [48].	2013
3.	BS EN 61226 - Nuclear power plants — Instrumentation and control systems important to safety —Classification of instrumentation and control functions [30].	2021
4.	BS EN 60880 - Nuclear power plants - Instrumentation and control systems important to safety. Software aspects for computer-based systems performing category A functions [49].	2009
5.	BS EN 62566 - Nuclear power plants — Instrumentation and control important to safety — Development of HDL-programmed integrated circuits for systems performing category A functions [50].	2014
6.	BS EN 60987 - Nuclear power plants - Hardware design requirements for computer-based systems [51].	2021
7.	BS EN 62138 - Nuclear power plants — Instrumentation and control systems important to safety - software aspects for systems performing Cat B or C functions [52].	2019
8.	BS EN 63413 - Nuclear Power Plants - Instrumentation and control systems important to safety - Platform qualification [53].	2024 (Currently out for public comment)
9.	BS IEC 62671 - Nuclear power plants - Instrumentation and control important to safety - Selection and use of industrial digital devices of limited functionality [54].	2013
10.	BS EN 60671- Nuclear power plants- Instrumentation and control systems important to safety – Surveillance testing [55].	2011
11.	BS EN 60709 - Nuclear power plants- Instrumentation and control systems important to safety – Separation [56].	2019
12.	BS EN 60780-323 - Nuclear facilities Electrical equipment important to safety– Qualification [57] (identical to IEC/IEEE 60780-323:2016).	2017
13.	BS EN IEC/IEEE 60980-344 – Nuclear facilities – Equipment important to safety – Seismic qualification [58].	2021
14.	BS EN 62003 – Nuclear power plants. Instrumentation, control and electrical power systems. Requirements for electromagnetic compatibility testing [59].	2020
15.	BS EN 61500 Nuclear power plants- Instrumentation and control systems important to safety – Data communication in systems performing category A functions [60].	2019
16.	BS EN 62340 - Nuclear power plants- Instrumentation and control systems important to safety – Requirements for coping with common-cause failure (CCF) [61].	2010

Although primarily for the use of the regulator, due account has also been taken of the relevant Office for Nuclear Regulations (ONR) SAPs [62] and Technical Assessment Guides (TAGs) available on the ONR website.

4.4.2 Safety Category & Classification

Safety category and classification is discussed here as it has an impact on the codes and standards to be used.

I&C SSCs have had their safety related and non-safety related functional requirements identified and appropriate safety class assigned by following the procedure SMR-300 Systems, Structures, and Components Classification [20]. The safety classification of an item is either safety-related or non-safety-related depending upon the design function it performs during a DBE.

There are differences in the approach to safety categorisation and classification between the U.S.NRC Regulatory Guides [36] and other national and international standards.

The differences in the approach to safety categorisation and classification have been identified via the gap analysis [63] and the US/UK regulatory framework and principles report [34]. For I&C although there is some broad alignment, different categorisation and classification approaches are applied and compliance with different standards documents are required. The preliminary fault schedule (PFS) as described in PSR Part B Chapter 14 has assigned a preliminary classification of Class 1 to the PSS and Class 2 to the DAS, but the PFS is to be developed further post GDA, and the category and classification confirmed and or clarified. I&C RGP standards have been reviewed and equivalent US standards requirements identified, see section 4.4.6 for details.

A summary of the standards used in the categorisation and classification of I&C systems for the Palisades project is provided in the following paragraphs.

I&C classification has been performed following applicable US standards – e.g. ANSI/IEEE-603-1991 [21].

The intent of the IEEE definition of Class 1E, as given in ANSI/IEEE-603-1991 [21] is identical to the U.S.NRC definition of safety-related. ANSI/IEEE-603-1991 [21] gives the basic criteria for safety-related electrical and I&C systems and equipment. Electrical and I&C system equipment and components are classified as Class 1E or Non-Class 1E in accordance with definitions stated in IEEE Std.603 [21].

In general, the equipment and components that perform safety-related functions are designated as Class 1E and the equipment and components that do not perform any safety-related functions are designated as Non-Class 1E. IEEE-603 Standard [21] is endorsed by Regulatory Guide 1.53 [64] as a method acceptable to the U.S.NRC for complying with 10 Code of Federal Regulations (CFR) 50 Appendix A General Design Criteria [35],10 CFR 50.49 [65], and 10 CFR 50.55a [66], with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of safety systems for nuclear power plants.

I&C systems and components that employ digital computers and programs are required to be designed and qualified in accordance with IEEE Standard 7-4.3.2 [38] and Regulatory Guide

1.152 [67] requirements. IEEE Standard 7-4.3.2 [38] contains computer-specific requirements to supplement the criteria and requirements of IEEE Standard 603 [21]. The I&C design complies with these standards as identified in this chapter and the supporting references.

Design and qualification of accident monitoring instrumentation are required to be in accordance with Regulatory Guide 1.97 [33]. Those accident monitoring instruments that are relied upon to initiate safety functions are designated as Class 1E. In general, all other accident monitoring functions of the instruments are Non-Class 1E since their indications are not relied upon for any manual operator actions to mitigate the consequences of DBAs. However, the guidance in Regulatory Guide 1.97 [33] and IEEE Std. 497 [42] to meet the applicable GDCs requires some of the accident monitoring instrumentation to be designated as Class 1E. The I&C design complies with these standards as identified in this chapter and the supporting references.

From SMR-300 Systems, Structures, and Components Classification [20] SMR Class C is applicable to all safety related[1] I&C SSCs. This classification requires safety I&C systems and SCCs to meet ANSI/IEEE-603-1991 Class 1E standards which provides assurance that the deterministic and probabilistic requirements, associated with the safety function they support, can be met. Further information on the review of UK RGP codes and standards and the compliance of the design with the relevant US standards is provided in section 4.4.6 Codes and Standards CAE.

4.4.3 Relevant Good Practice and Operational Experience

See also Section 4.8.2.1 for information about the use of RGP and OPEX.

As part of the current GDA process the experience of previous GDAs and the relevant challenges made by the ONR to other RPs have been reviewed and the relevant I&C related issues identified.

The ONR's identified lessons learned from previous GDAs for I&C are identified below, along with a summary of how they have been addressed:

- RPs should fully understand regulatory expectations for the C&I safety case to be presented in a claims, arguments and evidence (CAE) format to support the safety case head document. As the role of the C&I systems is that of actuating safety systems the claims should be established from the requirements of the safety systems primarily arising from the fault schedule. Claims should also be established for the capability of the C&I systems to withstand faults, and internal and external hazards.
    - Response: This chapter adopts a CAE format to support the safety case. The claims include delivering the safety functional requirements which have been derived to date from the fault analysis in the US noting that the UK fault schedule [68] is still preliminary and does not identify safety functional requirements. See section 4.5.2. Specific claims are not established for the withstand of faults and internal and external hazards, but these are addressed in the arguments related to the claim concerning codes and standards.

[1] safety related SSC in this context is the US meaning which is equivalent to a UK safety SSC.

- There is a requirement for overall risk to be demonstrated to be ALARP. This generally means that a number of options will have been shown to have been considered, and why the design selected is ALARP.
    - Response: The I&C design has been challenged by Holtec Britain and subsequently by ONR in particular where the proposed DAS utilises a microprocessor-based system that, although different to the PSS, was overall judged to be too similar and difficult to justify. Options have been considered and the decision taken to adopt a non-computerised DAS. Other areas of the design such as the use of shared sensors and actuators are to be further reviewed and options will be considered as part of the ongoing I&C design development.
- Many designs have been presented to ONR where the layers of protection are not demonstrated to be independent and adequately diverse. Particular challenges include common electrical supplies, common microprocessors/software, shared sensors and communications from lower class systems to higher class systems.
    - Response: The proposed DAS has been judged by Holtec Britain to not be adequately diverse. A non-computerised DAS is now to be developed. Sensors and outputs are shared between the PSS and the DAS. In developing the new DAS proposals, work is being carried out to assess if the DAS can claim different sensors from the PSS for the same initiating event. In addition, design options for separate, diverse sensors and less sharing of input and output equipment will be considered. A Diversity and Defence in Depth Assessment is planned to demonstrate independence and adequate diversity post Step 2. In the event that the further work proposed does not result in an adequate demonstration of diversity and independence then optioneering will be undertaken to identify and implement any improvements which are reasonably practicable. [REDACTED].
- It is common in previous GDA assessments for excessive risk reduction claims to be made for software-based and other C&I systems. Guidance on limits that will be accepted by ONR is in NS-TAST-GD-046 [69].
    - Response: The claims to be made for the I&C systems are expected to be aligned with the ONR guidance on limits. It is currently envisaged to claim ~1E-4 pfd for the PSS and ~1E-3 pfd for the DAS but these claims will need to be further substantiated e.g. by detailed reliability analysis. Note that these are high confidence values and the PSA is likely to use best estimate values which are more optimistic.
- Where priority systems are used to enable more than one class of system to take a safety action, it is important that the RP is able to demonstrate that the risks arising from common cause failure, and spurious actuation are demonstrated to be acceptable.
    - Response: The proposed design uses software in the Class 1E PSS to monitor and prevent any incorrect PCS demands by prioritising the PSS demands. Simple hardware logic (not FPGAs) in the PIMs ensures the safety action is carried out should either the PSS or the DAS demand a safe state for an ESF. The DAS has a separate and independent RT output. The PSA modelling of the I&C does include some consideration of CCF and failure of the I&C systems as an initiating event – see Section 4.4.6, Claim 2.2.6.1 – A4 I&C Failure Causing Faults, for more detail.

- The RP should specify the intended approach to Smart Device qualification and confirm this is suitable for each safety class within the GB context. This should cover Production Excellence (PE), Independent Confidence Building Measures (ICBMs), and environmental qualifications. Consideration should be given for the potential of common cause failures to occur where Smart Devices are used in multiple points in the C&I architecture.
    - Response: The need to identify and qualify Smart Devices used in each safety class is recognised. At present the design is not sufficiently developed to identify specific devices either within the I&C architecture design or elsewhere with the overall design of the SMR-300, e.g. within electrical items of equipment such as Uninterruptible Power Supplies (UPS). It is intended to avoid the use of Smart devices where practicable. An approach to Smart Device qualification will be developed as part of the future I&C work beyond Step 2 and the potential for common cause failures to occur due to the use of Smart Devices in multiple points of the design will be considered.
- The GDA assessment should be based on a generic design. Site-specific design features should not be taken into account in the GDA assessment.
    - Response: Site-specific design features have not been taken into account in this PSR chapter.

These lessons learned have been taken into consideration in reviewing the I&C design, comparing the UK RGP/US standards and identifying the future work areas, and commitments which are managed as set out in Section 4.8 of this chapter.

[REDACTED]

4.4.4 Equipment Grouping Separation and Cabling

The SMR-300 design standard for grouping and separation [70] identifies the relevant US regulatory requirements and provides specific requirements for electrical and I&C equipment and cabling in Section 5.5 with electrical and I&C examples in Appendix A.

In summary, safety classified systems must be separated from non-safety systems by appropriate distance, barriers, or isolation devices and the PSS divisions and associated cabling must be separated by appropriate distance, barriers, or isolation devices.

As part of future codes and standards work beyond GDA the adequacy of the approach set out in the design standard will be justified.

4.4.5 Fail Safe Design

Ideally the I&C safety systems should be fail-safe, i.e. they should have no unsafe failure modes and failures should be detected and result in a safe state.

4.4.6 Codes and Standards CAE

Claim 2.2.6.1 has been further decomposed into five arguments to address how each of the claim subject areas are addressed during the I&C design and subsequent lifecycle stages. The I&C systems have been designed using applicable US nuclear codes and standards (A1). These standards have been compared against UK RGP and any differences identified (A2) and these differences have been reviewed and sentenced (A3). The I&C design is informed

by OPEX (A4), and the design development, testing, installation and commissioning phases will be controlled to ensure compliance with appropriate standards (A5).

Claim 2.2.6.1 – A1: The I&C systems have been designed using applicable US nuclear Codes and Standards

Evidence for Claim 2.2.6.1 – A1

The I&C has been designed using US standards and is subject to review as part of the US licensing activities, in particular for the Palisades SMR-300 project. The list of standards is captured in project documents and managed through the development lifecycle to ensure compliance or adequate justification. Ultimately, regulatory scrutiny by U.S.NRC of the I&C design and project compliance documents will be used to justify compliance with US standards.

SMR-300 Project References for Design and Licensing
The project references for design and licensing report [71] identifies the standards used for each discipline and I&C standards are listed in Section 8 of that report.

I&C Codes and Standards Initial Analysis Report
The I&C Codes and Standards Initial Analysis report [72] Section 4 identifies the relevant US I&C Codes and Standards used in developing the I&C design. These include the standards used by MELCO in developing their design.

Existing compliance information
At present compliance information demonstrating how the I&C design meets the US standards is not yet complete. The requirements are captured in each I&C system SDD and will subsequently be traced through the design lifecycle to confirm compliance. At present MELCO have provided compliance documents for the two key I&C standards (IEEE 603 and IEEE 7-4.3.2) in the reports Regulatory Compliance Evaluation (IEEE 603) [73] and Regulatory Compliance Evaluation (IEEE 7-4.3.2) [74]. These do not address application-level requirements compliance which are to be developed by Holtec International. MELCO have also developed a compliance report against RG 1.152 in report Regulatory Compliance Evaluation (RG 1.152) [75].

A shortfall that has already been identified is that the microprocessor-based Diverse Actuation System (DAS is not adequately diverse from the PSS to comply with the U.S.NRC guidance in NUREG/CR-7007. This has been addressed in a UK I&C Architecture Challenge Paper [31] and a related Design Decision Paper [32].

Claim 2.2.6.1 – A2: Comparison between UK I&C codes and standards and US nuclear I&C Codes and Standards has been carried out to identify any differences.

Evidence for Claim 2.2.6.1. – A2

Codes & Standards Initial Analysis Report
The Codes and Standards initial analysis report [72] compares the UK RGP codes and standards documents against the U.S.NRC set of requirements and guidelines. It identifies equivalent US requirements and any differences between the two document sets.

In general, there is equivalence between the US and UK RGP nuclear I&C standards and guidance document sets, although the mapping is not always that straightforward. In some areas the terminology used is different and in others the approach is different albeit with the same objective. The requirements for Class 1E systems and Class 1 systems in the UK are broadly similar but differ in some detail. Similarly, the requirement for Class 3 systems and non-1E systems are broadly equivalent.

The difference in the categorisation and classification approaches in the US and UK means that certain standards requirements, particularly for Class 2 systems providing Category B functions, are not as readily identifiable in the US. In some areas the requirements are simply different.

The initial analysis report has been subject to further review as set out in the next argument – A3.

Claim 2.2.6.1 – A3: Gaps identified through I&C codes and standards review have been subject to a sentencing process, and any gaps are identified and tracked.

Evidence for Claim 2.2.6.1 – A3

GDA Reference Design Process
The GDA Reference Design Process [76] enables any significant differences between the UK and US standards and UK RGP to be reviewed and challenged and where necessary design challenges and design changes to be proposed and agreed or rejected.

I&C Codes and Standards Analysis Review
The differences identified between the US and UK standards in the initial review [72] have been reviewed by HB to confirm / reject their significance and potential impact on the I&C design [77]. That report identifies the results of the review and identifies items that should be taken forward into future I&C design / design substantiation activities.

In summary these include differences in the approach to:

- Diversity (BS EN 61226).
- Class 1 Software (BS EN 60880).
- Modification (BS EN 60880, BS EN 61500).
- Surveillance testing (BS EN 60671).
- Independence (BS EN 62340).
- Fail-safe Design (BS EN 62340, BS EN 61513).
- Data communications modification (BS EN 61500).
- Hardware Requirements (BS EN 60987).
- Separation Requirements (BS EN IEC 60709).
- General requirements (performance, design margins) (BS EN 61513).

A significant difference was identified in the approach to Hardware Description Language (HDL) programmed devices where little or no equivalence was identified for the detailed requirements in BS EN 62566 and detailed work on that standard was halted on that basis. Further work is proposed to establish the way forward to review and justify the use of such devices post GDA.

The US standards mostly apply to safety categorised (1E) systems which are broadly aligned with Class 1 in the UK. This potentially makes the demonstration of compliance with UK RGP for lower classified systems (Class 2 and 3) as less clear and well defined.

In response to these confirmed differences the RP will:

[REDACTED]

The overall approach to codes and standards will demonstrate and justify compliance with the US documents, identify any differences between UK RGP and the US documents and allow those differences to be reviewed, justified or design changes developed as set out above. An appropriate level of review has been carried out as part of step 2 GDA, and further detailed work will continue. On that basis future safety submissions will be able to demonstrate that the I&C production process is of sufficient quality to support the safety claims made on the overall I&C architecture and the individual I&C systems.

Claim 2.2.6.1 – A4: I&C system design is informed by OPEX from PWR reactor I&C designs and takes benefit of modern technology to improve safety & minimise faults arising from I&C failures.

Evidence for Claim 2.2.6.1 – A4

MELCO operational experience

The I&C design has been carried out by MELTAC and is based on their established I&C platforms. The MELTAC Nplus platform (the basis for Nplus S), has been used in protection systems in 32 PWRs in service in total in Japan (18) and China (14) with over 200 reactor-years of operation in total. The operational use of the equipment has provided feedback on the performance of the platform in service, including actual reliability data compared to calculated failure rate data. See Topical Report [78] section 7.

MELCO review international OPEX through their link with the Japan Nuclear Safety Institute (JANSI). A self-regulatory organization, JANSI, corporates with the domestic and overseas related organizations, gathers the latest information and shares to the plant manufacturers including MELCO. Meetings with JANSI are held regularly, MELCO checks whether the information has impact on their products and service each time when obtaining the information.

MELCO is a member of INPO and regularly obtains nonconformance information. While discussing with utilities and relevant companies, MELCO incorporates the nonconformance information into the related design as needed.

MELTAC Topical Report

The MELTAC Topical Report [78] describes the Nplus S platform and provides module reliability data in Section 7 based on parts count analysis which has been used to model the PSS in the PSA. The U.S.NRC has endorsed the Nplus S platform for use as a protection system based on the MELTAC Topical Report.

ONR I&C OPEX from GDAs

The ONR I&C OPEX from the GDA process has been taken into account and a response against each of the items is provided in Section 4.4.6.

The overall I&C architecture aligns with the common PWR I&C architecture of providing largely separate systems for control functions (PCS), protection systems (PSS) and a diverse actuation system (DAS) for circumstances where the protection system fails.

The platform used for the DAS in the reference design is based on microprocessor technology and so is the PSS platform albeit using a different MELCO product. This has led to the I&C challenge paper [31] and I&C decision paper [32]. The operational experience from existing licensed designs as set out in NUREG/CR-7007 [79] indicates that they are more diverse than the reference design and in Japan and China the MELTAC designs have used an analogue DAS. The digital platforms exhibit improved diagnostics and a reduced need for proof tests compared to conventional hardwired systems, but on balance the potential difficulties in demonstrating adequate diversity in the DAS microprocessor-based design outweighed these benefits, and a decision has been taken to change to a non-computerised DAS.

I&C Failures causing Faults
Faults arising from failures of the I&C systems are minimised through appropriate quality in the development processes, the use of redundancy, voting and diversity along with appropriate failure detection mechanisms and responses as set out in this chapter B4 and supporting references for the I&C systems. Faults initiated by the I&C systems will be addressed as part of the Fault Studies and will continue to be developed post GDA – see PSR Part B Chapter 14 [12].

The PSA takes into account the potential for the I&C systems to initiate events as described in the Fault Tree Report for the PSS Section 8.9 [80]. The initiating events are described more generally in the PSA initiating events analysis document [81]. Potential sources of CCF are also identified in the Fault Tree Report (Section 8.10.3) but are limited to ‘active’ components such as relays. This has been identified as a limitation as part of the current PSA review but in any case, detailed modelling of I&C modules CCF would not normally be included in the PSA. Such analysis will be included as part of detailed reliability substantiation by the original equipment manufacturers, in this case by MELCO, but this will be post GDA.

Claim 2.2.6.1 – A5: Safety and non-safety functional requirements will be demonstrated by appropriate verification and validation activities or analysis processes and results.

Evidence for Claim 2.2.6.1 – A5

I&C Development Process
The overall I&C design development processes will be described in a document, but this will not be available in time for PSR Rev 1.

Verification and Validation Plans
As part of the Quality Assurance (QA) arrangements to be developed for the I&C systems production, an appropriate verification and validation plans will be developed to ensure that the I&C systems deliver the required safety and non-safety functions. These will include reviews and tests. See also – A6 below.

Analysis Reports

For characteristics that are not demonstrable by tests but require analysis, suitable processes e.g. reliability analysis will be defined and carried out to ensure and demonstrate that the I&C systems meet the associated requirements.
As part of the I&C lifecycle development, the I&C systems will be subject to a number of verification and validation activities as set out in a verification and validation plan, or equivalent documents including testing at various stages. These will typically include unit tests, integration tests, works acceptance tests, site installation, site acceptance tests, I&C commissioning, and plant commissioning (see Claim 2.2.6.1 – A6).

Claim 2.2.6.1 – A6: Design development, installation, commissioning and testing activities will be controlled using appropriate quality processes.

Evidence for Claim 2.2.6.1 – A6

PSS platform – MELTAC Topical Report
The Topical Report [78] Section 6 describes the quality arrangements for the development of the MELCO Nplus S platform, basic software which includes FPGAs that are used for the PSS platform, its compliance with relevant US requirements and any exceptions. The topical report references the following manuals:

MELTAC Platform Software Program Manual
The MELTAC Platform Software Program Manual [82] identifies the PSS platform software lifecycle plans and other documents and their compliance, e.g. to IEEE standards.

MELTAC Application Software Manual
The MELTAC Application Software Manual [83] describes the application lifecycle which is summarised in Fig 3.2-1 Overview, and the V&V activities which are summarised in Fig 3.10-2 of that document.

PCS & DAS platform
[REDACTED]

Note that the development process for the new DAS is not yet fully developed.

The application-level software will be based on the processes used in previous projects for MELCO activities and their requirements, e.g. the application software manual above, along with any additional Holtec input and verification activities requirements.

The overall I&C design and development processes will be described in a document, but this will not be available in time for PSR Rev 1.

Commissioning Plans (post GDA)
Commissioning plans or similar documents will identify the required commissioning tests for the I&C systems. In particular, I&C system commissioning tests will demonstrate that the I&C systems operate correctly in isolation and in combination in the site environment. They will also demonstrate that the I&C systems are correctly connected to the plant inputs and outputs prior to undertaking any associated plant commissioning tests.

Evidence (post GDA)
Evidence is to be developed, for example quality plans, configuration control processes, verification/validation process and will be completed post GDA step 2. Evidence will be developed to demonstrate that the processes are controlled using appropriate quality control arrangements including design reviews, quality plans, verification and validation plans, and commissioning plans.

Evidence will be developed to document the appropriate quality control processes that ensure that applicable standards are applied to all the phases of the lifecycle and that the relevant requirements have been addressed.

Commissioning is often considered in the UK as an independent measure that provides additional confidence in the I&C systems to be able to perform their allocated safety functions at the required integrity. It can be seen as additional to the normal verification and validation carried out as part of the development process. The detailed arrangements for the commissioning, the levels of independence to be provided and any further independent activities that provide confidence in the I&C systems are yet to be established; the arrangements and justification for such independent activities will be developed post GDA.

4.4.7 Codes, Standards and Methodology Summary

The SMR-300 I&C systems have been designed using applicable US nuclear codes and standards. These have been compared against UK RGP and any differences identified, and these differences have been reviewed and sentenced. Where significant issues have been identified, these have been escalated as challenge papers and have resulted in Design Decisions, which are captured as GDA Commitments (see Section 4.8.3), to implement in any future UK deployment.

The I&C safety and non-safety functional requirements will be demonstrated through the development and implementation of verification and validation plans. The I&C design is informed by OPEX, and the design development, testing, installation and commissioning phases will be controlled to ensure compliance with appropriate standards and quality arrangements. However, details of the design, Configuration Management and Version Control (CMVC), quality plans and the verification and validation plans and processes are still evolving and will be presented post GDA step 2. The current arrangements are considered suitably mature for this stage of the design process. The codes and standards claim is judged to be demonstrated on that basis.

4.5 DEFENCE IN DEPTH

Claim 2.2.6.2: The I&C system design incorporates Defence in Depth to protect against anticipated operational occurrences and accident conditions.

DiD is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. The independent effectiveness of the different levels of defence is a necessary element of DiD.

These levels are defined in the IAEA document 'Safety of Nuclear Power Plants: Design SSR-2/1' [84] and developed in the ONR Safety Assessment Principles for Nuclear Facilities [62] as follows:

- **Level 1 Prevention of abnormal operation and failures by design**: Conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels.
- **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.
- **Level 3 Control of faults within the design basis to protect against escalation to an accident**: Engineered safety features, multiple barriers and accident or fault control procedures.
- **Level 4 Control of severe plant conditions in which the design basis may be exceeded, including protecting against further fault escalation and mitigation of the consequences of severe accidents**: Additional measures and procedures to protect against or mitigate fault progression and for accident management.
- **Level 5 Mitigation of radiological consequences of significant releases of radioactive material**: Emergency control and on- and off-site emergency response.

Note that defence against cyber security threats is covered in the GSR [5]. The potential for cyber attacks to cause a CCF is recognised and the mitigations against such events are described in the GSR.

The following sections describe how DiD is demonstrated for the I&C topic.

4.5.1 I&C Architecture

4.5.1.1 Overview

The SMR-160 I&C design is the basis for the SMR-300 I&C design which is still being developed. An I&C architecture white paper [85] describes the I&C architecture.

The I&C architecture including HSI is comprised of three main I&C systems for each unit, the PSS, DAS and PCS. The PSS operates independently of the PCS and DAS. Where these systems are interconnected then design measures are provided to reduce the risks of fault propagation and CCF. A diagram of the I&C architecture is presented in Figure 3.

In normal operation, plant conditions are monitored by all three systems, information is presented to the operator in the MCR via VDUs and plant systems are automatically or

manually controlled via the PCS. Where plant conditions move away from normal conditions, alarms are raised initially and/or automatic control action is taken to maintain the plant inside the normal operating envelope by the PCS.

The PSS consists of two divisions and monitors all safety instrumentation to provide automatic and manual actuation for RT and ESF under abnormal conditions to bring the plant to a safe shutdown state. In order to cater for situations where the PSS might fail to operate, the DAS also monitors safety parameters to provide a diverse method of operating the RT and ESF.

Each of the three main I&C systems has VDUs provided in the MCR to inform the operator of the plant conditions and the status of the I&C systems. The PCS and PSS also provide VDUs in the RSF. The PCS HSI is the primary operator interface for all normal and abnormal plant conditions, with the PSS providing Class 1E information and acting as a backup to the PCS. The DAS displays provide further back up should the PSS displays fail. [REDACTED]

MIS are provided in the MCR and RSF to manually initiate RT and ESF.

At an architecture level the three I&C systems provide DiD against operational occurrences and DBAs:

- PCS provides normal duty operation and the response to Anticipated Operational Occurrences (AOOs (DiD Level 1 & 2).
- PSS provides protection in response to DBAs, with DAS acting as a backup in case of PSS failure to operate (DiD Level 3).
- [REDACTED]

The three I&C systems are connected within the architecture. Inputs to the PCS and PSS are hardwired to input modules either locally or to remote I/O. [REDACTED]. The DAS has no other input modules, but a separate direct wired output for RT.

[REDACTED]

Communications between the safety divisions and among the systems within a safety division are in accordance with U.S.NRC ISG 04 for Highly Integrated Control Rooms [86] and IEEE 7-4.3.2 [38] and IEEE 603 [21].

4.5.1.2 Defence in Depth, Common Cause Failure & Diversity

Diversity is provided within the I&C system architecture to mitigate the risk of common mode failure (CMF) and common cause failure (CCF).

The three I&C systems operate independently to provide the required monitoring, control and protection functions, with some interconnection to enable the sharing of measured values and actuation of plant components.

[REDACTED]

The risk of CCF, the diversity provided, and the DiD provided by the architecture has been reviewed and is presented in the report HI-2210230, Diversity and Defence in Depth Assessment for I&C Systems [87]. This provides an analysis of the design by separating it into independent ‘blocks’ and considering the diversity between those blocks and the risks of CCF.

The referenced report is an SMR-160 document and will be updated to provide an analysis of the SMR-300 design but this will be after GDA Step 2.

4.5.1.3 Shared Sensors and Outputs

As described above, the I&C architecture includes the use of some common items of equipment that are shared between the I&C systems. This is aligned with the overall design approach of providing simplicity and a minimum amount of instrumentation, control functions and control loops, consistent with providing the essential functional requirements of the systems.

[REDACTED]

4.5.2 Safety Functional Requirements

Safety functions and non-safety functions have been identified and allocated to the appropriate I&C SSCs within the I&C architecture. I&C Engineering has been applied to ensure that SSCs deliver their assigned requirements. This section presents the requirements that are relevant to the I&C systems. The requirements for the I&C SSCs are documented in the I&C system SDDs [23] [24] [25] [26] [27] [28].

I&C SSCs and their types of safety and non-safety functions, are presented in Table 5 below. These have been identified by following the US categorisation process leading to the safety / non safety categorisation.

Table 5: I&C SSCs Safety and Non-Safety functions

I&C SSC	Safety	Safety Functions	Non-Safety Functions
PSS functions	Safety Rated Class 1E	Perform coincidence logic voting logic for RT. Perform coincidence voting for ESF actuations. Actuate RT breakers for RT. Actuate ESF components for ESF actuations.	Provide information to the PCS. Digitally shares process data with the PCS for control, monitoring and recording purposes. [REDACTED] Performs Self-Diagnostics. Performs self-diagnostic testing and provides indication and alarm of any detected errors. [REDACTED]
PCS functions	Non-safety rated	The PCS is not credited to perform any safety function during DBA.	Provide manual and closed loop automatic control of SMR-300 plant processes. [REDACTED] Provide indication of process variables and status of the plant conditions. Alarm abnormal process conditions. Data logging. Historian. [REDACTED]
DAS functions	Non-safety rated	The DAS is not credited to perform any safety function.	[REDACTED] Provides diverse means to perform either the same function or different function, if a postulated CCF disables a safety function in PSS. Provide manual diverse actuation signal and monitoring of parameters supporting the critical safety functions performed by PSS.
PAM [REDACTED]	Non-safety rated	The PAM does not perform a credited safety function.	The high-level function of PAM instruments is to provide a reliable means of monitoring plant variables and systems by control room operators during accident situations. PAM

I&C SSC	Safety	Safety Functions	Non-Safety Functions
			instruments are split into six types used to perform distinct functions. Each of these functions is defined below: Type A Variables: Provide information essential for accomplishment of safety functions that require manual action during DBE. Note at present there are no Type A variables required. Type B Variables: Provide information to assess the process of accomplishing or maintaining plant safety functions. Type C Variables: Indicate a potential for breach or actual breach of fission product barriers. Type D Variables: Provide indication of the performance of safety systems, required auxiliary support features, and other systems required for safe shutdown. Type E Variables: Monitor the magnitude of release of radioactive material and the environmental conditions used to determine the impact of release. Monitor radiation levels and radioactivity in the plant environment and select areas that are required for plant recovery. Type F Variables: Provide indication of fuel damage and its direct effects.
EIS	Safety Rated	Monitor Neutron Flux from shutdown to full power operation. Monitor the rate of change of neutron flux in the Power Range. Monitor Power Distribution in the Power Range. Monitor Neutron Flux during DBA.	Provide Neutron Flux indication, recording, and alarms for shutdown to full power operation. Provide Reactor Power information to the reactor control system. Provide nuclear flux data to the plant historian. Provide ACR and alarms during shutdown and refuelling. Provide startup rate monitoring.
IIS	Non-safety rated	The IIS system safety design includes the IAs role in maintaining the reactor pressure boundary. Otherwise, the IAs are non-safety instruments.	Provide measurement of Core Exit Temperatures. Provide measurement of Reactor Flux. Provide measurement of Coolant Level above Active Fuel Zone.

The details of the actual functions to be provided by the PSS and DAS, for example the plant conditions which are monitored and will cause a RT or operate the required ESF outputs are provided in the PSS Logic Basis document [88] and the DAS Control Description document [89]. For the PCS, a similar document(s) will be produced to define the required control functions. The control functions will be developed and validated in part by using the plant simulator to provide feedback on the control system performance.

Note that the functions to be provided will subsequently be reviewed and potentially modified as part of the further development of the preliminary fault schedule (PFS) as set out in PSR Part B Chapter 14 [12].

4.5.3 Supporting Systems – Electrical & HVAC

The I&C systems are powered by the electrical systems as described in each section for PSS (Section 4.2.2.2.11), DAS (Section 4.2.3.2.7) and PCS (Section 4.2.4.2.7). See also the electrical PSR Part B Chapter 6 [13].

Heating, Ventilation and Air Conditioning (HVAC) systems or passive cooling arrangements are provided for the I&C rooms and the MCR/RSF to maintain the correct environmental conditions. These are described in PSR Part B Chapter 5 [9].

The C&I equipment rooms are supplied by the Non-Radiologically Controlled Area HVAC system (NRV) which is not claimed during a loss of offsite power event. The design intention is for NRV rooms to meet these criteria without power provided to the NRV, therefore the NRV is not credited during accident scenarios. To demonstrate suitability of the system, analysis is being conducted that assesses the heat rise in these rooms as well as associated design work on related HVAC systems which are active during normal operation. This is expected to be mature and concluded outside of GDA step 2 timescales. See associated commitment C_MEC_028 in PSR Part B Chapter 19 [10].

4.5.4 Location of Equipment

[REDACTED]

4.5.5 Defence in Depth CAE

Claim 2.2.6.2 has been further decomposed into six arguments to address how each of the claim subject areas are addressed during the I&C design and subsequent lifecycle stages.

Plant safety functions have been suitably allocated to I&C systems (A1). I&C system design was reviewed against UK RGP to ensure it satisfies UK fault schedule needs, and any gaps are identified and appropriately tracked (A2). I&C system functional, non-functional, performance and reliability requirements have been specified (A3). I&C systems are designed to meet their functional, non-functional and performance requirements for their specified operational life (A4). I&C system design takes internal and external hazard withstand requirements into account (A5). I&C system design takes into account the ageing and obsolescence of I&C systems and components (A6).

Claim 2.2.6.2 – A1: Plant safety functions are suitably allocated to I&C systems.

Evidence for Claim 2.2.6.2 – A1

PSR Chapter A2 [3] describes the high-level US approach to functional classification. The Plant-Level Function Identification and Decomposition Report [90] performs a functional decomposition against the plant goals of ensuring safety and generating power and derives high-level functions to meet these goals and then processes to meet these functions. Note this is an SMR-160 document and the SMR-300 document will only be available after this version of the PSR.

This is then used to analyse the system-level functional requirements, which are presented in lower-tier documentation. For the I&C Systems, these lower-tier documents are:

PSS Logic Basis.
The PSS Logic Basis document [88] captures the safety and non-safety functions that the PSS is required to deliver.

DAS Control Description

The DAS control description document [89] captures the safety and non-safety functions that the DAS is required to deliver.

PCS Functions
The PCS will have similar document(s) to those for the PSS and DAS produced to define the PCS functional requirements, but this is not yet available.

PSR Part B Chapter 14.3 [12]
Describes the US approach to Deterministic Safety Analysis (DSA). DSA is the analysis of the plant response to transients and postulated accidents and is used to ascertain (identify) and evaluate (quantify) SMR-300 relevant initiating events within the design basis of the power plant. The DSA is used to assess, using the identified safety-classified components (SCCs), if initiating scenarios challenge and threaten plant safety and determine the limiting conditions of the plant.

PSR Part B Chapter 14.3 also presents the proposed approach to UK Design Basis Accident Analysis (DBAA). UK DBAA utilises the output of the DSA but involves a broader UK context aligned approach, to identify and evaluate potential accidents that occur within the design basis of a nuclear facility (i.e. transients, internal events, internal and external hazards). In this approach, the adequacy of the design and the suitability and effectiveness of its safety measures are assessed against a specific set of deterministic rules. This is supported by production of a Fault and Protection Schedule which provides a clear and auditable link between potential faults, the sequences of events that could follow, and the safety measures designed to mitigate or prevent those events.

A limited UK DBAA (for six faults only) has been undertaken at GDA Step 2 to commence identification of UK equivalent categorisation of Safety Functions (SFs) and UK equivalent classification of candidate SSCs, that deliver these Safety Function(s) see the DBAA Summary Report [91].

Given the limited UK DBAA work undertaken to date, the final UK equivalent categorisation and classification is not yet available [91]. The ongoing work to develop the I&C architecture and design to address these expectations is discussed in Section 4.2.3.3 in this chapter for the new DAS. The preliminary fault schedule has identified the PSS as Class 1, see section 4.2.2. The UK DBAA work will be further progressed post-GDA Step 2 to comprehensively assess all relevant faults and hazards and complete the UK Categorisation and Classification work. A commitment has been raised in PSR Part B Chapter 14 (C_Faul_103) to address this further work. This may lead to changes to the I&C systems, classification and justification and such changes will be addressed post GDA step 2.

The output of the UK DBAA work will also be used to produce a consolidated list of Safety Functional Requirements (SFRs) and performance requirements, which will be captured within an engineering schedule. Further details on the approach to development of the engineering schedule is provided in PSR Part B Chapter 19 [10].

Claim 2.2.6.2 – A2: I&C system design has been reviewed against UK RGP to ensure it satisfies UK fault schedule needs, and any gaps are identified and appropriately tracked.

Evidence for Claim 2.2.6.2 – A2

I&C Challenge Paper/Decision Paper
As part of the GDA step 2 work the I&C architecture was reviewed and a number of key issues were identified including the diversity of the DAS technology, the common equipment shared

between the PSS and the DAS and the sharing of sensors between the PSS and the DAS. The I&C architecture challenge paper [31] and the I&C decision paper [32] were produced to capture the issues and the decision and commitment C_I&C_082 has been raised.

Interface between PCS & PSS
[REDACTED]

PAM
The PAM displays are currently provided in the [REDACTED] (Type D, E, F) and the [REDACTED] (Type B, C). There is no separate dedicated PAM I&C system. This is not considered RGP in the UK and further work is required post GDA to explore the options for either justifying the existing design or modifying the design. See Section 4.2.7 in this chapter B4 and commitment C_I&C_083.

Claim 2.2.6.2 – A3: I&C system functional, non-functional, performance and reliability requirements have been specified.

Evidence for Claim 2.2.6.2 – A3

I&C System SDDs
The I&C system requirements have been specified in the SDDs [23] [24] [25] [26] [27] [28]. Note that this includes the SDD for the existing DAS and an SDD for the new DAS will be produced after Step 2 of the GDA.

Note that for reliability requirements the overall claims on the I&C systems are not yet finalised. [REDACTED]

Claim 2.2.6.2 – A4: A4 I&C systems are designed to meet their functional, non-functional and performance requirements for their specified operational life.

Evidence for Claim 2.2.6.2 – A4

I&C System Design
The I&C development process provides a design response to the I&C SDDs. The I&C SDDs are produced by Holtec International and capture the I&C system overview and requirements. The SDDs are then used by MELCO to produce System Requirements Specifications (SRS) which provide further design detail in response to the SDDs. These SRS documents have now been produced but are beyond the DRP and for the DAS a revised SRS will be required to reflect the commitment (C_I&C_082) to revise the design.

Design Life
The operational life of the plant is identified as 80 years and if systems cannot achieve that design life then they are required to ensure that they can be upgraded or replaced at the required intervals – see Top Level Design Requirements, Design Life Section 3.3 [92].

The I&C systems will not have a design life of 80 years, but 20-30 years at best, see Topical Report [78] Section 6.1.6. Many existing nuclear stations have had successful I&C replacement projects to address problems with ageing I&C systems, including replacement with MELCO products and this provides confidence that such systems can be successfully replaced. See operational experience document [93].

Claim 2.2.6.2 – A5: I&C system design takes internal and external hazard withstand requirements into account.

Evidence for Claim 2.2.6.2 – A5

I&C Qualification

The I&C equipment and systems are qualified to withstand the effects of environmental variations, such as temperature, humidity, ingress protection, and electromagnetic interference according to their location and the anticipated environment. The I&C equipment and systems are qualified to appropriate seismic levels depending on their function and location. The level of qualification is identified in the relevant subsections of Section 4 4.2.2.2.15, 4.2.3.2.11, and 4.2.4.2.11 of this PSR Chapter 4 and the overall requirement for appropriate qualification is set out in the SDDs (References 19 to 24). See also Section 5 of the topical report [78] for the PSS platform qualification.

I&C Location

[REDACTED]

Claim 2.2.6.2 – A6: I&C system design takes into account the ageing and obsolescence of I&C systems and components

Evidence for Claim 2.2.6.2 – A6

SMR-300 Top Level Plant Design Requirements

The top level plant design requirements document [92] identifies a life of 80 years or that the systems can be replaced. The I&C equipment will not be supportable for more than 20-30 years, so will need to be replaced periodically throughout the life of the plant. The top level requirements include that all system components and equipment that are replaceable shall use the longest practical service life available for commercial equipment and materials. The system structures shall be designed for the full design life, with defined maintenance plans reflecting best available techniques.

PSS platform Topical Report

Section 6.1.6 Obsolescence Management of the Topical Report [78] describes the obsolescence management programme for the MELTAC platform. MELCO uses hardware parts which have excellent production continuity. Regardless, the product service life for nuclear applications covers 20 to 30 years, so it is inevitable that many parts will become unavailable. The section summarises the process used to determine the availability of parts and the process used to evaluate and utilise different parts for substitution. All changes to the MELTAC platform are done under MELCO's 10 CFR 50 Appendix B QAP.

Topical Report Section 7.4 Equipment (Parts) that Require Periodic Replacement to Maintain Reliability identifies the PSS platform items that periodically need to be replaced to maintain reliability such as capacitors within power supplies.

Ageing & Obsolescence Management Programme

It is envisaged that as part of future implementation phases beyond Step 2 of GDA an ageing and obsolescence management programme will be put in place to ensure that the I&C systems continue to deliver the required functionality and reliability throughout their operational life.

4.5.6 Defence in Depth Summary

The I&C architecture provides I&C systems that contribute to the DiD levels. The PCS provides monitoring and control of the plant to contribute to levels 1 and 2. The PSS provides RT and ESF functions to contribute to DiD level 3. The DAS provides a diverse means of RT and ESF actuation if the PSS were to fail to operate.

[REDACTED]

Connections between the systems are electrically isolated and designed to reduce the risk of failures and their propagation. The design has been analysed for diversity and DiD.

Safety and non-safety functions have been identified through the overall safety analysis in the US and allocated to the I&C systems within the I&C architecture. This allocation will continue to be reviewed and updated as the SMR-300 design progresses and the UK preliminary fault schedule (PFS) [68] is developed further beyond Step 2 of GDA.

Challenges associated with UK RGP such as connection between I&C systems of different classes have been reviewed and justification provided, or further work proposed. The DiD claim will be demonstrated on that basis.

4.6 QUALITY MANUFACTURING AND INSTALLATION PROCESSES

Claim 2.2.6.3: I&C SSCs achieve the design intent through quality manufacturing and installation processes.

The manufacturing and installation processes are controlled as part of the quality assurance arrangements for the I&C systems.

4.6.1 Manufacturing

The I&C systems described in this chapter are mainly designed and manufactured by Mitsubishi Electric Corporation in accordance with their quality assurance arrangements. These are summarised and referenced in the MELTAC topical report [78] for the PSS platform and have been assessed by the U.S.NRC for use in reactor protection systems. The application software is also developed by Mitsubishi in accordance with their software quality assurance plans in order to meet U.S.NRC requirements.

[REDACTED]

The QA arrangements provide a framework to ensure that the manufacturing of the systems achieves the design intent and meets the defined safety and non-safety requirements, including the requirements set out in U.S.NRC Regulatory Guides [36] and IEEE standards.

4.6.2 Installation

The I&C systems will be installed by the equipment supplier or approved contractors in accordance with their approved QA arrangements to ensure that the equipment is not damaged as part of the shipping, unloading, storage and installation processes. The arrangements will confirm that the I&C systems have been installed correctly in accordance with the design intent, are safe to power up and that they operate correctly in the site environment.

These arrangements will ensure the I&C systems are suitably prepared for I&C system commissioning tests to then be carried out prior to the wider plant commissioning tests. Construction and commissioning are addressed in PSR Part B Chapter 25 [94].

4.6.3 Manufacturing and Installation CAE

Claim 2.2.6.3 has been further decomposed into two arguments to address how each of the claim subject areas are addressed during the I&C design and subsequent lifecycle stages.

Quality of manufacturing of I&C SSCs is established through continuous QA and Quality Control (QC) of the manufacturing process (A1). Quality of installation for I&C SSCs is established through rigorous contractor selection and continuous QA and QC of the installation and commissioning process (A2).

Claim 2.2.6.3 – A1: Quality of manufacturing of I&C SSCs is established through continuous QA and QC of the manufacturing process.

Evidence for Claim 2.2.6.3 – A1

PSS Topical Report
The PSS Topical Report [78] describes the QA arrangements applied to the PSS platform in Section 6. The MELTAC platform was developed under a Japanese quality assurance programme compliant with ISO 9001 (MELCO's ISO 9001 QAP) and has undergone a one-time commercial grade dedication (CGD) by MELCO for use in US safety -related applications. The details of that CGD programme are provided in the Topical Report (Section 6.2) by reference. MELTAC is now maintained and manufactured under MELCO's 10 CFR 50 Appendix B QAP.

Section 6.1.8 of the Topical Report describes the MELTAC reliability database and how operational experience in terms of any problems or failures are captured and fed back into the design and/or manufacturing process.

Operational Experience
[REDACTED]

Claim 2.2.6.3 – A2: Quality of installation for I&C SSCs is established through rigorous contractor selection and continuous QA and QC of the installation and commissioning process.

Evidence for Claim 2.2.6.3 – A2

Evidence To be Developed post GDA
The I&C systems will be installed by the equipment supplier or approved contractors in accordance with approved QA arrangements to ensure that the equipment is not damaged as part of the shipping, unloading, storage and installation processes. The arrangements will confirm that the I&C systems have been installed correctly in accordance with the design intent, are safe to power up and that they operate correctly in the site environment.

4.6.4 Manufacturing and Installation Process Summary

The I&C systems will be manufactured and installed in accordance with appropriate QA arrangements to ensure that the design intent is implemented, and the I&C systems deliver the required functions in the site environment. The quality manufacturing and installation claim will be demonstrated on that basis.

4.7 EXAMINATION, INSPECTION, MAINTENANCE, AND TESTING

Claim 2.2.6.4: Examination, Inspection, Maintenance and Testing (EIMT) regimes provide confidence in the design and continued operation of the I&C systems for their design lifetime.

Examination, inspection, maintenance and testing (EIMT) is generically addressed in Part B Chapter 9 Conduct of Operations [11]. However, for I&C systems there are specific requirements.

As part of the I&C lifecycle development the I&C systems will be subject to a number of verification and validation activities as set out in a verification and validation plan, or equivalent documents including testing at various stages. These will typically include unit tests, integration tests, works acceptance tests, site installation, site acceptance tests, I&C commissioning, and plant commissioning (see Claim 2.2.6.1 – A5).

In particular, I&C system commissioning tests will demonstrate that the I&C systems operate correctly in isolation and in combination in the site environment. They will also demonstrate that the I&C systems are correctly connected to the plant inputs and outputs prior to undertaking any associated plant commissioning tests.

All phases of testing will take due account of the relevant standards and guidance.

The frequency of routine testing of the operational I&C systems will be defined based on the reliability analysis and for protection systems will be based on the required frequency to ensure that any unrevealed failures are detected to support the reliability claim.

Routine examination, inspection, and maintenance and testing arrangements will be defined and documented in accordance with manufacturers' recommendations and the relevant standards and guides.

It is anticipated that an I&C obsolescence programme would be established to ensure that obsolescence of the I&C equipment is addressed as the I&C systems age throughout the life of the station but details of this are outside of the scope of GDA.

4.7.1 EIMT CAE

Claim 2.2.6.4 has been further decomposed into one argument to address how each of the claim subject areas are addressed during the I&C design and subsequent lifecycle stages.

EIMT for the operational life of the I&C systems will be defined as informed by the design activities (A1)

Claim 2.2.6.4 – A1: EIMT for the operational life of the I&C systems will be defined as informed by the design activities.

Evidence for Claim 2.2.6.4 – A1

PSS TR

The Topical Report [78] Section 7.4 identifies life-limited components that have to be replaced at regular intervals for example power supply modules, fans, VDUs. Sections 6.1.3 and 6.1.4 identify that MELCO provides maintenance manuals and training for users.

Similar information will be developed for the other I&C platforms and systems.

Surveillance testing
Surveillance tests will be defined based on the extent of self-diagnostics coverage in order to ensure that equipment continues to provide the required functionality with the necessary reliability. It is currently envisaged that such tests will only be required during plant shutdowns for the PSS.

4.7.2 EIMT Summary

EIMT proposals are set out generically in Chapter B9 Conduct of Operations [11] and in particular section 9.6 of B9 outlines guidance for the requirements, design and scheduling of EIMT activities. EIMT proposals for the I&C systems will be defined post GDA. In operation, the examination, inspection, maintenance, and testing arrangements will ensure that the I&C systems continue to provide the required functions throughout their life. The EIMT claim will be demonstrated on that basis.

4.8 CHAPTER SUMMARY AND CONTRIBUTION TO ALARP

This sub-chapter provides an overall summary and conclusion of the I&C Chapter and how this Chapter contributes to the demonstration of ALARP for the generic SMR-300. Chapter A5 [19] sets out the overall approach for demonstration of ALARP and how contributions from individual Chapters are consolidated.

This subchapter therefore consists of the following elements:

- Technical Summary.
- ALARP Summary
  - Demonstration of RGP.
  - Evaluation of Risk and Demonstration Against Risk Targets (where applicable).
  - Options Considered to Reduce Risk.
- GDA Commitments.
- Conclusion.

A review against these elements is presented below under the corresponding headings.

4.8.1 Technical Summary

PSR Part B Chapter 4 aims to demonstrate the following level 3 claim to a maturity appropriate for a PSR:

Claim 2.2.6: The overall design and architecture of I&C SSCs ensure that safety functions and non-safety functions are delivered and faults arising from failures of the SSCs are minimised.

The SMR-300 I&C design has been undertaken using best practice nuclear industry codes and standards to address U.S.NRC requirements, U.S.NRC Regulatory Guides and IEEE standards as described in this chapter. A review of UK RGP, in particular I&C standards against US requirements has been carried out and any differences identified and sentenced. Operational experience has been taken into account and related information for the I&C systems is summarised.

The SMR-300 I&C architecture and I&C system design supports the overall DiD approach providing systems for monitoring and control in normal operation, protection and diverse protection systems in the event of design basis accidents and displays for post-accident monitoring.

A significant change to the I&C architecture in terms of the technology to be used for the DAS has been proposed and accepted as a commitment for the fleet design. See commitment C_I&C_082 in section 4.8.3.

The SMR-300 I&C systems will be manufactured and installed in accordance with appropriate quality assurance arrangements to ensure the design intent is achieved and the systems operate adequately in the site environment.

EIMT will demonstrate the fitness for purpose of I&C SSCs through I&C system commissioning tests prior to plant commissioning. Once in operation, ongoing examination, inspection,

maintenance, and testing throughout the life of the I&C systems will ensure that the I&C systems continue to provide the required functionality.

The key requirement of the I&C SSCs is to provide the required safety and non-safety functions at the required integrity and that faults arising from failures of the SSCs are minimised. The required safety functions and non-safety functions are identified currently or will be identified for the I&C systems post GDA. The functions will be subject to confirmation and potentially update as the preliminary fault schedule is developed further post GDA – see PSR Part B Chapter 14 [12].

The I&C safety and non-safety functions will be demonstrated through appropriate verification and validation activities. The verification and validation activities are summarised in this chapter and further detail will be developed and justified post GDA.

Faults arising from failures of the I&C systems are minimised through the use of redundancy, voting and diversity along with appropriate design review, failure detection and responses. Faults initiated by the I&C systems will be addressed as part of the preliminary fault schedule and will continue to be developed post-GDA – see PSR Part B Chapter 14 [12].

4.8.2 ALARP Summary

4.8.2.1 Demonstration of RGP

The design of the SMR-300 I&C systems complies with the recognised good practices applicable in the US, where the present design follows codes and standards approved by the U.S.NRC and internationally recognised bodies such as the International Atomic Energy Agency (IAEA) and IEEE for use in nuclear safety systems.

The principal codes and standards identified within subchapter 4.4 are considered RGP by the UK nuclear industry. This is based on existing practices adopted on UK nuclear licensed sites, application in earlier and successful GDAs, as well as recognition as RGP by ONR SAPs and TAGs.

The I&C systems design employs the following RGPs presented in Table 6.

Table 6: I&C RGPs

[REDACTED]

Although these RGP and OPEX are recognised for the SMR-300 design, some of the design aspects might be interpreted differently in the UK. For such areas, review and further justification or design changes will be proposed as shown in the examples for the DAS technology and PAM displays.

The list of reports supporting the safety case includes available studies and reports used in the regulatory interactions with U.S.NRC, in order to substantiate the proposed design approach.

The I&C and other elements discussed in the scope of this I&C chapter that are considered to require further work to be able to fully claim compliance with UK RGP are as follows:

- Safety Categorisation and Classification approach to be completed against a comprehensive fault schedule.
- An updated diversity and DiD analysis will be completed for the SMR-300 I&C architecture.
- Development of an approach to identification and justification of Smart devices.
- Human Factors Engineering of HSI, as reported in PSR Part B Chapter 17 [14], where relevant RGP adherence & design management process is outlined.
- Security review and analysis as reported in the GSR.
- Codes and standards further detailed comparison and review .
- Appropriate use of ALARP in design decisions.

Note that the above points are not considered fundamental shortfalls but work items that will be addressed as part of normal business and are therefore not identified as specific commitments.

4.8.2.2 Evaluation of Risk and Demonstration Against Risk Targets (where applicable)

The numerical targets against which the demonstration of ALARP is considered can be found in PSR Part A Chapter 2 [3]. I&C SSC, through the defined safety functions, will contribute to the demonstration of ALARP by comparison against the risk targets in two ways:

- By fulfilling safety functions for normal operations (e.g. monitoring and control functions) and thereby contributing to achieving Targets 1-3.
- By achieving their safety classification as a duty system or a protection system, where claimed, they will contribute to the achievement of accident risk, Targets 4-9.

Evaluation of risk is not directly applicable to the I&C SSCs. The safety classification of the I&C SSCs will be informed by the fault studies categorisation of functions provided by the systems and an appropriate Probability of Failure on Demand (PFD) and Probability of Failure per Annum (PFA) identified and justified for each I&C system. These values will then be used to calculate the overall comparison against the risk targets as described above.

The evaluation of the normal operations and accident risks against Targets 1-9 is summarised in PSR Part A Chapter 5 [19]. Further information is presented in PSR Part B Chapter 10 ‘Radiological Protection’ [4] for normal operations, and PSR Part B Chapter 14 ‘Design Basis Accident Analysis’ [12] for accident conditions.

4.8.2.3 Options Considered to Reduce Risk

This section identifies and reviews relevant I&C Design Challenge Papers and Design Decision Papers which have been identified following the GDA Design Reference Point (DRP1), with a view to demonstrate which options are ALARP. It summarises the option evaluations and briefly explores if other options have or could be considered to reduce risk. It presents the ALARP argument for why options have not been implemented, why options will be implemented in the future and the GDA Commitment to consider the option(s) at a future point (noting this still must be a point where a meaningful design improvement could be made).

DAS design and I&C Architecture

[REDACTED]

Commitment:

C_C&I_082: Design Challenge Paper 'I&C Architecture' (HI-2240612) associated with PSR Part B B4 Claim 2.2.6.2 'The I&C system design incorporates Defence in Depth to protect against anticipated operational occurrences and accident conditions' is with the Design Authority for Design Decision. This Design Challenge relates to differences between the US and UK Regulatory regimes in the I&C discipline and the potential need for a design change to the DAS.

A Commitment is raised to progress this Design Challenge through the Design Management process (HPP-3295-0017-R1.0) to completion. Notably, the DAS design will be modified to use a non-computerised, simple hardware-based DAS which is adequately diverse from the technology used in the PSS. The use of shared equipment between the PSS and DAS will also be reviewed and options considered. The design of the output interface modules (PIM) will also be reviewed and justified. Target for Resolution - Issue of Pre-Construction SSEC.

Post-Accident Monitoring

[REDACTED]

The approaches in the US and UK are different and, in the UK, regulatory preference is for a separate system to align with DiD requirements. See Section 4.2.7.

To demonstrate risks have been reduced to ALARP Holtec will in the future:

- Review the US / IAEA requirements for post-accident monitoring signals on the basis that they are specified, and the UK approach is goal setting.
- Review the US / IAEA expectations against the SMR-300 fault studies / severe accident analysis (SAA. This will consider aspects such as the impact of the PSS being unavailable in a post-accident scenario.

Commitment:

C_C&I_083: The US / IAEA approach to post accident monitoring differs from the approach taken in the UK. The lack of a dedicated PAM results in the design not falling within one layer of Defence-in-Depth. The UK regulator prefers a dedicated PAM that falls within Level 4 of Defence-in-Depth. A Commitment is raised to review US / IAEA requirements for post-accident monitoring signals. This will consider the US / IAEA expectations against the SMR-300 fault studies / severe accident analysis (SAA). It will also consider aspects such as the impact of the PSS being unavailable in a post-accident scenario. Target for Resolution - Issue of Pre-Construction SSEC.

The process for the assessment of risk reduction options is presented in 'HPP-3295-0017, Design Management Process' [76].

4.8.3 GDA Commitments

GDA Commitments which relate to this chapter have been formally captured in the Commitments, Assumptions and Requirements process [6]. Further details of this process are provided in Part A Chapter 4 [7]. The GDA Commitments raised in Part B Chapter 4 are:

C_C&I_082: Design Challenge Paper 'I&C Architecture' (HI-2240612) associated with PSR B4 Claim 2.2.6.2 'The I&C system design incorporates Defence in Depth to protect against anticipated operational occurrences and accident conditions' is with the Design Authority for Design Decision. This Design Challenge relates to differences between the US and UK Regulatory regimes in the I&C discipline and the potential need for a design change to the DAS. A Commitment is raised to progress this Design Challenge through the Design Management process (HPP-3295-0017-R1.0) to completion. Notably, the DAS design will be modified to use a non-computerised, simple hardware-based DAS which is adequately diverse from the technology used in the PSS. The use of shared equipment between the PSS and DAS will be reviewed and design options considered. The design of the output interface modules (PIM) will also be reviewed and justified. Target for Resolution - Issue of Pre-Construction SSEC.

C_C&I_083: The US / IAEA approach to post accident monitoring differs from the approach taken in the UK. The lack of a dedicated PAM results in the design not falling within one layer of Defence-in-Depth. The UK regulator prefers a dedicated PAM that falls within Level 4 of Defence-in-Depth. A Commitment is raised to review US / IAEA requirements for post-accident monitoring signals. This will consider the US / IAEA expectations against the SMR-300 fault studies / severe accident analysis (SAA). It will also consider aspects such as the impact of the PSS being unavailable in a post-accident scenario. Target for Resolution - Issue of Pre-Construction SSEC.

4.8.4 Conclusion

This chapter summarises the overall centralised I&C architecture and I&C systems design. It identifies the claims, arguments and currently available evidence that form the basis of the safety case for the I&C topic throughout the lifecycle of SMR-300 to a maturity aligned to a preliminary safety report.

As the design and safety case are developed, further evidence will be provided to substantiate these claims and arguments.

The I&C design has been reviewed against UK RGP in terms of the differences between the UK and US standards and appropriate justification has been provided or further activities have been identified to support justification beyond Step 2 of GDA.

Further work has been identified to review and resolve the key technical differences between the US and UK justification for I&C systems. These activities will also be developed in accordance with the principles of ALARP and the ALARP considerations are discussed in the context of the overall SMR-300 design in an overarching ALARP summary statement in Part A Chapter 5 [19].

It is therefore judged that the safety of the I&C design will be demonstrated, subject to completion of the commitments, resolution plans and the outstanding items and planned future work.

4.9 REFERENCES

[1] Holtec Britain, “HI-2240332, Holtec SMR GDA PSR Part A Chapter 1 Introduction,” Revision 1, July 2025.

[2] Holtec Britain, “HI-2240334, Holtec SMR GDA PSR Part A Chapter 3 Claims, Arguments and Evidence,” Revision 1, July 2025.

[3] Holtec Britain, “HI-2240333, Holtec SMR GDA PSR Part A Chapter 2 General Design Aspects and Site Characteristics,” Revision 1, July 2025.

[4] Holtec Britain, “HI-2240341, Holtec SMR GDA PSR Part B Chapter 10 Radiological Protection,” Revision 1, July 2025.

[5] Holtec Britain, HI-2240878, SMR-300 Generic Security Report, Rev 0, June 2025.

[6] Holtec Britain, “HPP-3295-0013, Holtec SMR-300 Generic Design Assessment Capturing and Managing Commitments, Assumptions and Requirements,” Revision 1, 2024.

[7] Holtec Britain, “HI-2240335, Holtec SMR GDA PSR Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance,” Revision 1, July 2025.

[8] Holtec Britain, “HI-2240337, Holtec SMR GDA PSR Part B Chapter 1 Reactor Coolant System and Engineered Safety Features,” Revision 1, July 2025.

[9] Holtec Britain, “HI-2240777, Holtec SMR GDA PSR Part B Chapter 5 Reactor Supporting Facilities,” Revision 1, July 2025.

[10] Holtec Britain, “HI-2240356, Holtec SMR GDA PSR Part B Chapter 19 Mechanical Engineering,” Revision 1, July 2025.

[11] Holtec Britain, “HI-2240340, Holtec SMR GDA PSR Part B Chapter 9 Description of Operational Aspects/Conduct of Operations,” Revision 1, July 2025.

[12] Holtec Britain, “HI-2240345, Holtec SMR GDA PSR Part B Chapter 14 Design Basis Accident Analysis (Fault Studies),” Revision 1, July 2025.

[13] Holtec Britain, “HI-2240339, Holtec SMR GDA PSR Part B Chapter 6 Electrical Engineering,” Revision 1, July 2025.

[14] Holtec Britain, “HI-2240348, Holtec SMR GDA PSR Part B Chapter 17 Human Factors,” Revision 1, July 2025.

[15] Holtec Britain, "HI-2240343, Holtec SMR GDA PSR Part B Chapter 12 Nuclear Site Health and Safety and Conventional Fire Safety," Revision 1, July 2025.

[16] Holtec Britain, "HI-2240351, Holtec SMR GDA PSR Part B Chapter 22 Internal Hazards," Revision 1, July 2025.

[17] Holtec Britain, "HI-2240350, Holtec SMR GDA PSR Part B Chapter 21 External Hazards," Revision 1, July 2025.

[18] Holtec Britain, "HI-2240347, Holtec SMR GDA PSR Part B Chapter 16 Probabilistic Safety Assessment," Revision 1, July 2025.

[19] Holtec Britain, "HI-2240336, Holtec SMR GDA PSR Part A Chapter 5 Summary of ALARP," Revision 1, July 2025.

[20] Holtec International, "HPP-8002-0012 SMR-300 Systems, Structures, and Components Classification," Revision 0, February 2025.

[21] Institute of Electrical and Electronics Engineers, "IEEE 603-2018, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," 1991 (NRC Endorsed) & 2018 (latest).

[22] Holtec International , PS-8002-0047 SMR-300 Specification - Instrumentation and Controls, R0, Feb 2025.

[23] Holtec International, "HI-2240668, System Design Description for Plant Safety System," Revision 0, January 2025.

[24] Holtec International, "HI-2240655, System Design Description for Plant Control System," Revision 0, June 2024.

[25] Holtec International, "HI-2210177, System Design Description for Diverse Actuation System," Revision 0, July 2021.

[26] Holtec International, "HI-2241173, System Design Description for Post-Accident Monitoring System," Revision 0, January 2025.

[27] Holtec International, "HI-2240848, System Design Description for In-core Instrumentation System," Revision 0, 2025.

[28] Holtec International, "HI-2240847, System Design Description for Ex-Core Instrumentation System," Revision 0, 2025.

[29] United States Nuclear Regulatory Commission, "Regulatory Guide 1.62, Manual Initiation of Protective Actions," Revision 1, June 2010.

[30] British Standards Institution, “BS EN IEC 61226:2021 Nuclear power plants. Instrumentation, control and electrical power systems important to safety. Categorization of functions and classification of systems,” 2021.

[31] Holtec Britain, “HI-2240612, UK SMR-300 GDA Design Challenge - I&C Architecture [DC01],” Revision 0, September 2024.

[32] Holtec International, “HI-2241522, Decision Paper on the SMR-300 Diverse Actuation System,” Revision 0, April 2025.

[33] United States Nuclear Regulatory Commission, “Regulatory Guide 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” Revision 5, April 2019.

[34] Holtec Britain, “HI-2240127, Holtec SMR-300 US/UK Regulatory Framework and Principles Report,” Revision 1, February 2024.

[35] United States Nuclear Regulatory Commission, “10 CFR 50 Appendix A to Part 50 General Design Criteria for Nuclear Power Plants,” March 2021.

[36] United States Nuclear Regulatory Commission, “Regulatory Guides - generic reference to the many guides,” [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/reg-guides/index.html#guides.

[37] United States Nuclear Regulatory Commission, “NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Chapter 7 Instrumentation and Controls,” Revision 6, 2016.

[38] Institute of Electrical and Electronics Engineers, “7-4.3.2-2016 - IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations,” 2016.

[39] International Electrotechnical Commission/Institute of Electrical and Electronics Engineers, “IEC/IEEE 60780-323-2016 Internaional Standard - Nuclear Facilities -- Electrical equipment important to safety -- Qualification,” 2016.

[40] Institute of Electrical and Electronics Engineers, “379-2000 - IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” 2000.

[41] Institute of Electrical and Electronics Engineers, “384-2018 - IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,” 2018.

[42] Institute of Electrical and Electronics Engineers, “497-2016 - IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations,” 2016.

[43] Institute of Electrical and Electronics Engineers, “730-2014 - IEEE Standard for Software Quality Assurance Processes,” 2014.

[44] United States Nuclear Regulatory Commission, “Branch Technical Position (BTP) 7-19 - Guidance for Evaluation of Defense-in-Depth and Diversity to Address Common Cause Failure due ot latent design defects in Digital Safety Systems,” Revision 8, January 2021.

[45] United States Nuclear Regulatory Commission, “NUREG/CR-6991, Design practices for communications and workstations in highly integrated control rooms,” 2009.

[46] United States Nuclear Regulatory Commission, “NUREG/CR-6082, Data Communications,” 1993.

[47] International Atomic Energy Agency, “IAEA Specific Safety Guide No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants,” 2016.

[48] British Standards Institution, “BS EN 61513:2013 Nuclear power plants. Instrumentation and control important to safety. General requirements for systems,” 2013.

[49] British Standards Institution, “BS EN IEC 60880 Nuclear power plants. Instrumentation and control systems important to safety. Software aspects for computer-based systems performing category A functions,” 2009.

[50] British Standards Institution, “BS EN 62566:2014 Nuclear power plants. Instrumentation and control important to safety. Development of HDL-programmed integrated circuits for systems performing category A functions,” 2014.

[51] British Standards Institution, “BS EN IEC 60987:2021 Nuclear power plants. Instrumentation and control important to safety. Hardware design requirements for computer-based systems,” 2021.

[52] British Standards Institution, “BS EN IEC 62138:2019 Nuclear power plants. Instrumentation and control systems important to safety. Software aspects for computer-based systems performing category B or C functions,” October 2019.

[53] British Standards Institution, “BS EN IEC 63413 Nuclear Power Plants - Instrumentation and control systems important to safety - Platform qualification,” Edition 1.0 (out for public comment), 2024.

[54] British Standards Institution, “BS IEC 62671:2013 Nuclear power plants. Instrumentation and control important to safety. Selection and use of industrial digital devices of limited functionality,” 2013.

[55] British Standards Institution, “BS EN 60671:2011 Nuclear power plants. Instrumentation and control systems important to safety. Surveillance testing,” 2011.

[56] British Standards Institution, "BS EN IEC 60709:2019 Nuclear power plants. Instrumentation and control systems important to safety. Separation," 2019.

[57] British Standards Institution, "BS EN 60780-323:2017 Nuclear facilities. Electrical equipment important to safety. Qualification 2017 (identical to IEC/IEEE 60780-323 2016)," 2017.

[58] British Standards Institution, "BS EN IEC/IEEE 60980-344:2021 Nuclear facilities. Equipment important to safety. Seismic qualification," 2021.

[59] British Standards Institution, "BS EN IEC 62003:2020 Nuclear power plants. Instrumentation, control and electrical power systems. Requirements for electromagnetic compatibility testing," 2020.

[60] British Standards Institution, "BS EN IEC 61500:2019 Nuclear power plants. Instrumentation and control systems important to safety. Data communication in systems performing category A functions," 2019.

[61] British Standards Institution, "BS EN 62340:2010 Nuclear power plants. Instrumentation and control systems important to safety. Requirements for coping with common-cause failure (CCF)," 2010.

[62] Office for Nuclear Regulation, "Safety Assessment Principles for Nuclear Facilities," 2014 Edition Revision 1, January 2020.

[63] Mott MacDonald Limited, "100110593-ENG1-0037, GDA Step 1 Gap Analysis," Revision 0, February 2024.

[64] United States Nuclear Regulatory Commission, "Regulatory Guide 1.53, Application of the Single-Failure Criterion to Safety Systems," Revision 2, November 2003.

[65] United States Nuclear Regulatory Commission, "10 CFR 50.49 Environmental qualification of electric equipment important to safety for nuclear power plants," March 2021.

[66] United States Nuclear Regulatory Commission, "10 CFR 50.55a Codes and Standards," September 2023.

[67] United States Nuclear Regulatory Commission, "Regulatory Guide 1.152, Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants," Revision 4, July 2023.

[68] Holtec Britain, HI-2241323 Preliminary Fault Schedule Report, Rev 1, May 2025.

[69] Office for Nuclear Regulation , NS-TAST-GD-046 ONR Technical Assessment Guide Computer Based Safety Systems, Issue 7, Dec 2023.

[70] Holtec International, “HPP-8002-3017, SMR-300 Design Standard for Grouping and Separation,” Revision 0, March 2024.

[71] Holtec Intenational, “HI-2240448, SMR-300 Project References for Design and Licensing,” Revision 1, November 2024.

[72] Holtec Britain, “HI-2250202, I&C Codes and Standards - Initial Analysis Report,” Revision 0, July 2025.

[73] MELCO, “HI-2241397, Regulatory Compliance Evaluation (IEEE 603),” Revision 0, February 2025.

[74] MELCO, HI-2241398, Regulatory Compliance Evaluation (IEEE 7-4.3.2), Rev 0, February 2025.

[75] MELCO, HI-2241399, Regulatory Compliance Evaluation (RG 1.152), Rev 0, February 2025.

[76] Holtec Britain, “HPP-3295-0017, Design Management Process,” Revision 1, 2024.

[77] Holtec Britain, “HI-2250203, I&C Codes and Standards Analysis Review,” Revision 0, July 2025.

[78] MELCO, “HI-2188331, Safety System Digital Platform - MELTAC - Topical Report,” (JEXU-1041-1008 Revision 2), Revision 1, May 2023.

[79] United States Nuclear Regulatory Commission, “NUREG/CR-7007 Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems,” February 2010.

[80] Holtec International, “HI-2241212, SMR-300 Level 1 PSA System Notebooks and Fault Tree Report for Plant Safety System,” Revision 0, June 2025.

[81] Holtec International, “HI-2240421, SMR-300 PSA Initiating Events Analysis,” Revision 0, July 2024.

[82] MELCO, “HI-2188332 (JEXU-1041-1016), MELTAC Platform Software Program Manual,” Revision 1, May 2023.

[83] MELCO, “HI-2188333 (JEXU-1041-1032), MELTAC Platform Application Software Program Manual,” Revision 1, May 2023.

[84] International Atomic Energy Agency, “IAEA No. SSR-2/1, Safety of Nuclear Power Plants: Design,” Revision 1, 2016.

[85] Holtec International, “HI-2220583, SMR-160 I&C Architecture White Paper,” Revision 0, September 2022.

[86] United States Nuclear Regulatory Commission, “DI&C-ISG-04 (ML083310185), Digital Instrumentation and Controls, Task Working Group #4: Highly-Integrated Control Rooms - Communication Issues (HICRc) Interim Staff Guidance,” Revision 1, March 2009.

[87] Holtec International, “HI-2210230, Diversity and Defence in Depth Assessment for I&C systems,” Revision 0, July 2021.

[88] Holtec International, “HI-2240747, SMR-300 Plant Safety System Logic Basis,” Revision 0, August 2024.

[89] Holtec International, “HI-2240456, Diverse Actuation System Control Description,” Revision 0, August 2024.

[90] Holtec Intenational, “HI-2220167, Plant Level Function Identification and Decomposition Report,” Revision 0, July 2022.

[91] Holtec Britain, “HI-2241577, SMR-300 GDA UK DBAA Summary Report,” Revision 0, February 2025.

[92] Holtec International, “HI-2240251, SMR-300 Top Level Plant Design Requirements,” Revision 3, January 2025.

[93] MELCO, JEXK-0120-2413 Response to MELCO Operating Experience Requirements, Rev C, May 2025.

[94] Holtec Britain, “HI-2240354, Holtec SMR GDA PSR Part B Chapter 25 Construction and Commissioning Approach,” Revision 1, July 2025.

4.10 LIST OF APPENDICES

Appendix A PSR Part B Chapter 4 CAE Route Map

Evidence with tick bullet points indicates that these are available at PSR v1, and evidence with an open bullet indicates evidence is in development and will be available after PSR v1.

Table 7: PSR Part B Chapter 4 CAE Route Map

REDACTED

Appendix B I&C Architecture

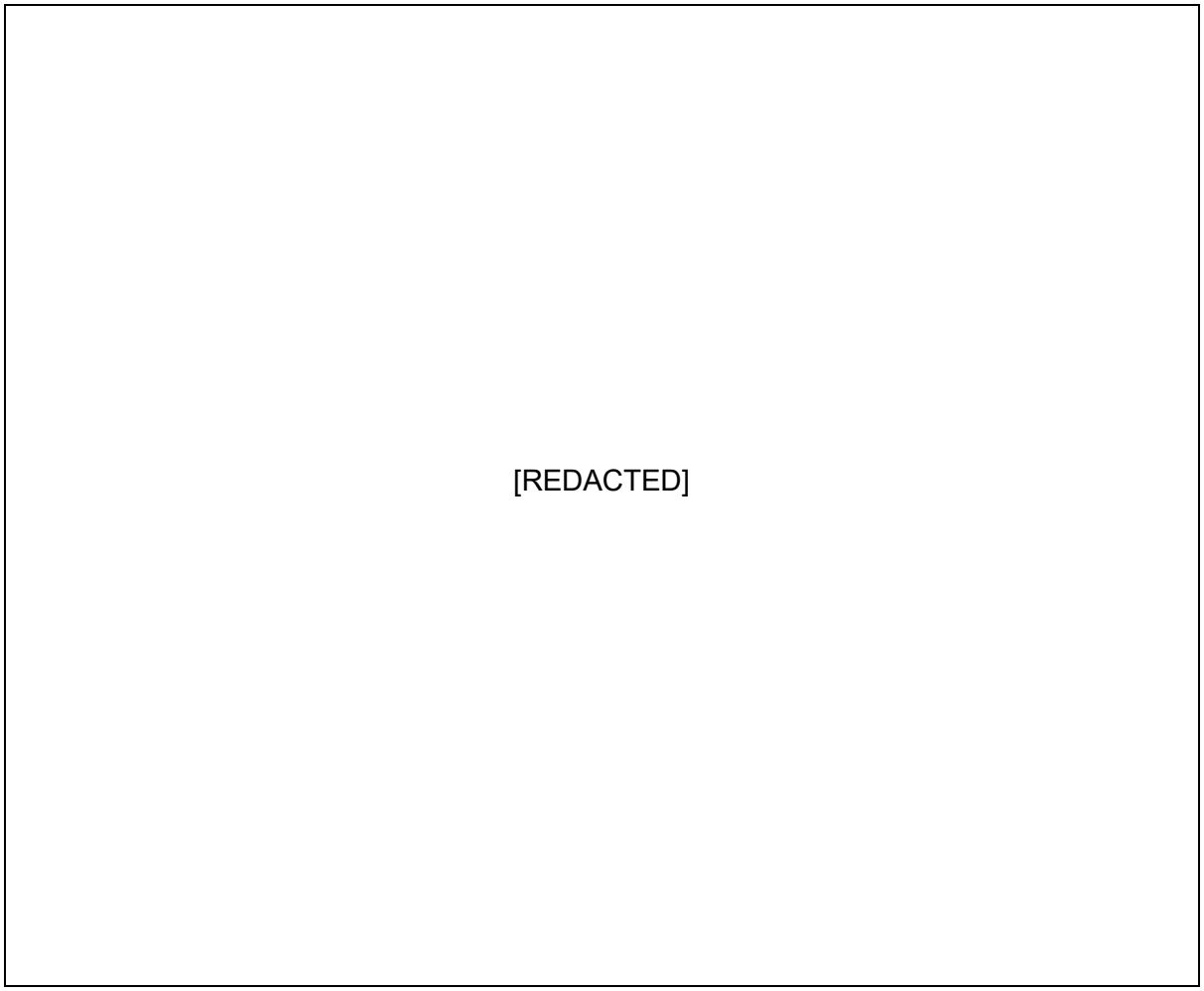

Figure 3: I&C Architecture