A Holtec International Company

Holtec Britain Ltd	HI-2240338
Sponsoring Company	**Document Reference**
0	30 September 2024
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 & Instrumentation

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

Table of Contents

List of Figures

No table of figures entries found.

List of Tables

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 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, claims, arguments and intended evidence 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 Instrumentation & Control (I&C) Structures, Systems and Components (SSCs) presents the Claims, Arguments and intended Evidence (CAE) for the design of the I&C SSCs that underpin the design of the Generic SMR-300.

4.1.1 Purpose and Scope

The Overarching SSEC Claims are presented in HI-2240334, Holtec SMR GDA PSR 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 SSCs. This chapter presents the I&C aspects for the Generic SMR-300 and therefore directly supports a 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 Subchapter 4.3.

This chapter will address areas within the GDA Scope as defined in HI-2240333, Holtec SMR GDA 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 2.1.

This chapter covers the codes and standards associated with the design of these SSCs (subchapter 4.4), the defence-in-depth associated with the design of the SSCs (subchapter 4.5) the quality manufacturing and installation approach (subchapter 4.6), and the examination, inspection, maintenance and testing of the SSCs (subchapter 4.7). Finally, a

summary of considerations against the ALARP principle is provided, together with any Forward Actions (FAs) or commitments that have arisen (subchapter 4.8).

The current GDA scope excludes dedicated I&C SSCs, which are not part of the centralised I&C systems but associated with particular plant systems. Safety justification for dedicated I&C systems will be added in future safety reports beyond the GDA process.

Excluded from the Part B Chapter 4 I&C scope are the Radiological Protection Monitoring Systems which are covered by HI-2240341, Holtec SMR GDA PSR 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 not addressed as part of this PSR chapter and are addressed separately as part of the Generic Security Report (GSR).

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

There are no assumptions made in this PSR chapter.

4.1.3 Interfaces with other PSR 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 HI-2240337, Holtec SMR GDA PSR Part B Chapter 1 Reactor Coolant System and Engineered Safety Features [5], HI-2240777, Holtec SMR GDA PSR Part B Chapter 5 Reactor Supporting Facilities [6] and HI-2240356, Holtec SMR GDA PSR Part B Chapter 19 Mechanical Engineering [7].

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) [8]. Safety functional requirements for I&C systems and faults associated with the I&C systems will be identified and analysed in Part B Chapter 14 (Design Basis Accident Analysis) [9] Electrical supplies to the I&C systems are described in Part B Chapter 6 (Electrical engineering) [10]. Human Factors (HF) will review 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) [11]. Hazards are addressed in Part B Chapters 12 (Nuclear Site Health and Safety) [12], 21 (Internal Hazards) [13] and 22 (External Hazards) [14]. I&C reliability figures are used in Part B Chapter 16 (Probabilistic Safety Analysis) [15]. I&C ALARP arguments will inform the overall ALARP claims in Part A Chapter 5 (Summary of ALARP) [16].

4.2 DESCRIPTION OF I&C SSCS

The initial starting point for identifying the I&C SSCs is HPP-160-3004, SMR-160 Systems, Structures and Components Classification Standard [17], and the Institute of Electrical and Electronic Engineers (IEEE) Standard Criteria for Safety Systems for Nuclear Power Generating Stations ANSI/IEEE-603-1991 [18]. 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. An SMR-300 version of HPP-160-3004 is to be produced, but no significant changes are anticipated.

(REDACTED)

The SMR-300 I&C/HSI achieves defence-in-depth by providing separate systems for monitoring and control, protection and diverse actuation functions with appropriate redundancy, independence, diversity, determinism, 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 has 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.

4.2.1 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, but these are being updated to reflect the developing SMR-300 I&C design.

- Plant Safety System (PSS) [19]
- Plant Control Systems (PCS) [20]
- Diverse Actuation System (DAS) [21]
- Post- Accident Monitoring System (PAMS) [22]
- In-Core Instrumentation System (IIS) [23]
- Ex-Core Instrumentation System (EIS) [24]

(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 and 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 In-core and Ex-core Instrumentation Systems 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 Appendix B.

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

Table 1: REDACTED

REDACTED

4.2.2 (REDACTED)

4.3 I&C CLAIMS, ARGUMENTS, EVIDENCE

The primary purpose of a Claims, Arguments, Evidence approach is to capture the golden thread of a safety case narrative demonstrating how relevant arguments and evidence are brought together to justify that a high-level or fundamental claim is true. In the context of the Generic SMR-300, that is how the Fundamental Purpose of the SSEC (presented in Part A Chapter 1 [1] is achieved.

The CAE provides a golden thread from the Fundamental Purpose through the SSEC via the objectives set out for each of the PSR, Preliminary Environmental Report (PER) and Generic Security Report (GSR). The overarching SSEC claims and the philosophy of their architecture are presented in PSR Part A Chapter 3 [2]. This chapter links to the overarching claims through Claim 2 and Claim 2.2:

Claim 2: The design and safety assessment shows that the Generic Holtec SMR-300 can be constructed, commissioned, operated and decommissioned on a generic site in the UK with risks that are tolerable and As Low As Reasonably Practicable (ALARP).

This chapter contributes directly to Claim 2.2, which is focused on the demonstration of the design and that the SSCs that form the design, are developed to ensure they meet the relevant safety requirements and appropriate codes and standards.

Claim 2.2: The design of the systems and associated processes have been developed taking cognisance of relevant good practice 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 SSCs. This chapter presents the I&C aspects for the Generic SMR-300 and therefore directly supports a claim focused on the overall design and architecture of I&C SSCs, 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 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 into account the 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 defence in depth (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 examined, inspected, maintained, and tested (EIMT) throughout their operational life to ensure they continue to provide the required safety functions. The maturity of evidence for this claim will be limited at a PSR stage.

Table 2 shows in which section of this PSR chapter these claims are addressed.

Table 2: **CAE Chapter sections:**

Claim No	Claim	Chapter Section
2.2.6.1	The I&C SSCs are designed using appropriate codes and standards taking into account the cognisance of relevant good practice (RGP) and operational experience (OPEX).	4.4 Codes, Standards & Methodologies

Claim No	Claim	Chapter Section
2.2.6.2	The I&C system design incorporates defence in depth (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

The CAE route map for this Chapter is summarised in Appendix A and a further update on claim decomposition, argument development and evidence maturity will be provided in PSR Revision 1 at the end of Step 2.

4.4 CODES, STANDARDS AND METHODOLOGIES

Claim 2.2.6.1: The I&C SSCs are designed using appropriate codes and standards taking into account the 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 4.2 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 detail in the System Design Documents (SDDs) [19] [20] [21] [22] [23] [24]. The US/UK Regulatory Framework and Principles Report [25] has identified Safety Assessment Principles (SAPs) and NRC General Design Criteria (GDC) for Nuclear Power Plant [26] and provides a comparison against the US regulatory framework.

In some cases, the 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 (RP) is to comply with both the NRC endorsed version and the latest version.

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.	US NRC, “10CFR50 Appendix A to part 50 - General Design Criteria for Nuclear Power Plants” [26] In particular, parts 13 I&C, 19 control room, and 20-29 for the protection system.	2011
2.	US NRC Regulatory Guides [27]	Various
3.	US NRC, NUREG-0800, Chapter 7, Instrumentation and Controls [28]	2017

#	Title of Code/Standard Reference	Rev/Date
4.	IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603. [18]	1991 (2018)
5.	IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2 [29]	2016
6.	IEEE/IEC 60780-323, “IEC/IEEE International Standard - Nuclear facilities – Electrical equipment important to safety -- Qualification," [30]	2016
7.	IEEE Std. 379, “IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” [31]	2014
8.	IEEE Std. 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,” [32]	2018
9.	IEEE, 497-2016, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations [33]	2016
10.	IEEE Standard 730, IEEE Standard for Software Quality Assurance Plans [34]	2014
11.	US 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 [35]	2020
12.	US NRC, NUREG CR-6991, Design practices for communications and workstations in highly integrated control rooms [36]	2009
13.	US NRC, NUREG CR-6082, Data Communications [37]	1993

The RP will review the design against UK RGP including the standards listed in Table 4, show compliance by submitting documents that are currently available and identify where additional work is required to demonstrate compliance with UK RGP.

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. [38]	2016
2.	BS EN 61513 - Nuclear power plants - Instrumentation and control important to safety — General requirements for systems. [39]	2013
3.	BS EN 61226 - Nuclear power plants — Instrumentation and control systems important to safety —Classification of instrumentation and control functions. [40]	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. [41]	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. [42]	2014
6.	BS EN 60987 - Nuclear power plants - Hardware design requirements for computer-based systems. [43]	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 [44]	2019
8.	BS EN 63413 - Nuclear Power Plants - Instrumentation and control systems important to safety - Platform qualification [45]	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 [46]	2016
10.	BS EN 60671- Nuclear power plants- Instrumentation and control systems important to safety – Surveillance testing [47]	2011
11.	BS EN 60709 - Nuclear power plants- Instrumentation and control systems important to safety – Separation [48]	2019
12.	BS EN 60780 - Nuclear facilities Electrical equipment important to safety– Qualification [49]	2017
13.	BS EN 60980-344 – Nuclear facilities – Equipment important to safety – Seismic qualification [50]	2021

#	Title of Code/Standard Reference	Rev/Date
14.	BS EN 62003 – Nuclear power plants. Instrumentation, control and electrical power systems. Requirements for electromagnetic compatibility testing. [51]	2020
15.	BS EN 61500 Nuclear power plants- Instrumentation and control systems important to safety – Data communication in systems performing category A functions [52]	2019
16.	BS EN 62340 - Nuclear power plants- Instrumentation and control systems important to safety – Requirements for coping with common-cause failure (CCF) [53]	2010

Although primarily for the use of the regulator, due account will also be taken of the relevant Office for Nuclear Regulations (ONR) SAPs [54] and Technical Assessment Guides (TAGs) available on the ONR website.

4.4.2 Safety Category & Classification

I&C SSCs have had their safety related and non-safety related functional requirements identified and appropriate safety class assigned by following the procedure HPP-160-3004 SMR-160 Systems, Structures, and Components Classification Standard [17] which references the US NRC Regulatory Guide 1.26, Revision 6 [55] and related documents. The safety classification of an item is either safety-related or non-safety-related depending upon the design function it performs during a Design Basis Event (DBE).

There are differences in the approach to safety categorisation and classification between the NRC Regulatory Guides [27] and other national and international standards.

The differences in the approach to safety categorisation and classification have been identified via the gap analysis [56] and the US/UK regulatory framework and principles report [25].

The project methodology for safety categorisation and classification (Ref Chapter A.2) will be developed during Step 2 of the GDA. This will address any gaps identified in SSEC Revision 0 relating to categorisation and classification to ensure appropriate compliance with standards and that regulatory expectations are addressed.

A summary of the standards used in the categorisation and classification of I&C systems is provided below.

I&C classification has been performed following applicable US standards – e.g., ANSI/IEEE-603-1991 [18].

(REDACTED)

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. This has informed the gap analysis and the forward action plans already identified and discussed in section 4.8.2.1.

The ONR identified lessons learned from previous GDAs for I&C are as follows:

- 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.
- 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.
- 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.
- It is common 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.
- 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.
- 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 (ICBM's), and environmental qualifications. Consideration should be given of the potential for common cause failures to occur where Smart Devices are used in multiple points in the C&I architecture.
- The GDA assessment should be based on a generic design. Site-specific design features should not be taken into account in the GDA assessment.

These have been taken into consideration in identifying the forward actions, which are managed as set out in section 4.8, and will be more fully addressed in Revision 1 of this chapter.

(REDACTED)

4.4.4 Codes, Standards and Methodology Summary

The previous sections show that the I&C design is using appropriate nuclear standards as required in the US. Relevant UK standards have been identified, and a comparison against these standards will be carried out as part of step 2 of GDA. RGP and OPEX have been used to inform the gap analysis and identify forward actions. The codes and standards claim will 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.

Defence in depth 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 defence in depth.

These levels are defined in the IAEA document 'Safety of Nuclear Power Plants: Design SSR-2/1' [57] and developed in the ONR Safety Assessment Principles for Nuclear Facilities [54] 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.

The following sections describe how Defence in Depth is demonstrated for the I&C topic.

4.5.1 (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 [19] [20] [21] [22] [23] [24].

I&C SSCs and their safety and non-safety functions, as identified to date are presented in Table 5 below. These have been identified by following the US categorisation process leading to the safety / non safety categorisation. These are based on the SMR-160 design and will be reviewed and updated as the SMR-300 design is further developed.

Table 5: REDACTED

REDACTED

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 4.2.2.2.10), DAS (section 4.2.3.2.7) and PCS (section 4.2.4.2.7). See also the electrical PSR Part B Chapter 6 [10].

Heating, Ventilation and Air Conditioning (HVAC) systems 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 [6].

4.5.4 (REDACTED)

4.5.5 (REDACTED)

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 summarized and referenced in the MELTAC topical report [58] for the PSS platform and have been assessed by the US 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 US 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 US NRC Regulatory Guides [27] 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 5 .

4.6.3 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 [8]. 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.

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 and maintenance 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 program 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 Summary

I&C systems will be commissioned in isolation to ensure correct connectivity and function prior to further testing as part of the plant commissioning. In operation, 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 subchapter provides an overall summary and conclusion of the I&C Chapter and how this Chapter contributes to the overall demonstration of ALARP for the Generic SMR-300. PSR Part A Chapter 5 [16] 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;
  - Demonstration against risk targets;
    - Evaluation of Risk (where applicable);
  - Risk Reduction Options
  - GDA Commitments and Forward Actions.
- Conclusion.

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

4.8.1 Technical Summary

PSR Chapter B Part 4, Revision 0 demonstrates that the I&C SSCs within the scope of this report will meet the high-level claims of the SSEC and that the SSCs can be substantiated at Pre-Construction Safety Report (PCSR) stage. This is demonstrated through achieving the following claim and associated sub claims:

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 US NRC requirements, NRC Regulatory Guides and IEEE standards as described in this chapter. Relevant good practice and operational experience has been considered and will be further reviewed as part of step 2 of the GDA.

The SMR-300 I&C architecture and I&C system design supports the overall defence in depth 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.

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,

PSR Revision 1 will demonstrate through further arguments and evidence that the I&C SSCs provide the required functions at the required integrity levels and faults arising are minimised.

4.8.2 ALARP Summary

4.8.2.1 Demonstration of Relevant Good Practice

The design of the SMR-300 I&C systems comply with the recognised good practices applicable in the US, where the present design follows codes and standards approved by the US 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: REDACTED

REDACTED

Although these RGPs and OPEX are recognised for the SMR-300 design, some of the design aspects might be interpreted differently in the UK.

As the Safety Classification approach is a crosscutting topic for all disciplines, it will be managed at a project level by developing a comprehensive safety categorisation and classification strategy. That strategy will feed back to the individual chapters and outline the approach for the current GDA and further action plan after Step 2 has concluded.

Dedicated reports which support the safety case by, for example, justifying the I&C architecture against UK RGP will be produced. Such reports include, but are not limited to:

- UK context I&C architecture report, presenting the case for the suitability of the I&C design against UK specific RGPs and that the design reduces risk to ALARP.

- Research output report will capture the results of research into the software assurance methods used in the nuclear industry in different countries, across other industrial sectors in the UK, within vendors within the UK and compliance assessment organisations. Techniques and methods in I&C design and architecture that assist in software assurance will be reviewed with academic establishments. The work will include the use and justification of SMART devices. The report will make recommendations for the approach to software assurance for the SMR-300 I&C design.

The list of reports might be extended to also include available studies and reports used in the regulatory interactions with US NRC, in order to substantiate the proposed design approach, as many of these design aspects might be considered to demonstrate RGP.

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

(REDACTED)

Forward actions will form the basis for setting out the process to justify any gaps from UK RGP. Forward actions have been collated and are managed via the process described in HI-2240335, Holtec SMR GDA PSR Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance [59].

4.8.2.2 Demonstration against risk targets

The numerical targets against which the demonstration of ALARP is considered can be found in PSR Part A Chapter 2 [3]. I&C SSCs, 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.

4.8.2.2.1 Evaluation of risk

Evaluation of risk is not directly applicable to the I&C SSCs. The safety classification of the I&C SSCs will be associated with a Probability of Failure on Demand (PFD) and Probability of Failure per Annum (PFA), which is then used to calculate the overall comparison against the risk targets as described above.

At this time, the evaluation of the normal operations and accident risks against Targets 1-9 has not been provided. This information will be presented in PSR Part B Chapter 10 ‘Radiological Protection’ [4] for normal operations, and PSR Part B Chapter 14 ‘Design Basis Accident Analysis’ [9], Chapter 15 ‘Beyond Design Basis and Severe Accident Analysis, and Emergency Preparedness’ [60], Chapter 16 ‘Probabilistic Safety Analysis’ [15] for accident conditions.

4.8.2.3 Risk reduction options

This is a placeholder to identify and review any relevant Position Papers and Design Decision Papers with a view to demonstrate which option(s) is/are ALARP.

It will summarise those option evaluations, and it will briefly explore if other risk reduction options have or could be considered and either:

- Present the ALARP argument for why those options have not been implemented.
- Present the ALARP argument for why those options will be implemented in future.
- Create a Forward Action to consider the option(s) at some future point (noting this still must be a point where a meaningful design improvement could be made).

The process for the assessment of risk reduction options is presented in HPP-3295-0017-R0, Holtec SMR-300 Generic Design Assessment Reference Design Process and GDA Prospective Design Change Register [61]. Part A Chapter 5 of this PSR 'ALARP Summary' [16] considers the holistic risk-reduction process for the Generic SMR-300.

4.8.2.4 GDA commitments and Forward Actions

There are no GDA commitments identified for Part B Chapter 4 I&C.

Forward Actions have been collated and are managed via the process described in PSR Part A Chapter 4, 'Lifecycle Management of Safety and Quality Assurance' [59]. PSR Chapter A5 'ALARP Summary' [16] describes the contribution of the forward actions to the ALARP argument.

4.8.3 Conclusions

This chapter summarises the overall centralised I&C architecture and I&C systems design. It identifies the claims and arguments that will 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, evidence will be provided to substantiate these claims and arguments.

It is recognised that there are different Codes, Standards and Methodologies and practices between the UK and US. Forward Actions have been identified to review these different approaches and for developing a design justification which is consistent with UK-recognised RGP and requirements. This will be carried out in accordance with the ALARP principle.

Similarly, Forward Actions have also been identified to resolve the key technical differences between the US and UK justification for I&C systems, e.g. research into the approach to software assurance. 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 [16].

It is therefore judged that the safety of the I&C design will be able to be demonstrated subject to resolution of the outstanding items and future action plans.

4.9 REFERENCES

[1] “Holtec Britain, "HI-2240332, Holtec SMR GDA PSR Part A Chapter 1 Introduction," Revision 0, August 2024”.

[2] “Holtec Britain, "HI-2240334, Holtec SMR GDA PSR Part A Chapter 3 Claims, Arguments and Evidence," Revision 0, August 2024”.

[3] “Holtec Britain, "HI-2240333, Holtec SMR GDA PSR Part A Chapter 2 General Design Aspects and Site Characteristics," Revision 0, August 2024”.

[4] “Holtec Britain, "HI-2240341, Holtec SMR GDA PSR Part B Chapter 10 Radiological Protection," Revision 0, August 2024”.

[5] “Holtec Britain, "HI-2240337, Holtec SMR GDA PSR Part B Chapter 1 Reactor Coolant System and Engineered Safety Features" Revision 0, August 2024”.

[6] “Holtec Britain, "HI-2240777, Holtec SMR GDA PSR Part B Chapter 5 Reactor Supporting Facilities," Revision 0, August 2024”.

[7] “Holtec Britain, "HI-2240356, Holtec SMR GDA PSR Part B Chapter 19 Mechanical Engineering," Revision 0, August 2024”.

[8] “Holtec Britain, "HI-2240340, Holtec SMR GDA PSR Part B Chapter 9 Description of Operational Aspects/Conduct of Operations," Revision 0, August 2024”.

[9] HI-2240345 Holtec SMR GDA PSR Part B Chapter 14 Safety/Design Basis Accident Analysis Rev 0 August 2024.

[10] “Holtec Britain, "HI-2240339, Holtec SMR GDA PSR Part B Chapter 6 Electrical Engineering," Revision 0, August 2024”.

[11] HI-2240348 Holtec SMR GDA PSR Part B Chapter 17 - Human Factors, Rev 0 August 2024.

[12] HI-2240343 Holtec SMR GDA PSR Part B Chapter 12 Nuclear Site Health and Safety and Conventional Fire Safety, Rev 0, August 2024.

[13] “Holtec Britain, "HI-2240351, Holtec SMR GDA PSR Part B Chapter 22 Internal Hazards," Revision 0, August 2024”.

[14] “Holtec Britain, "HI-2240350, Holtec SMR GDA PSR Part B Chapter 21 External Hazards," Revision 0, August 2024”.

[15] HI-2240347 Holtec SMR GDA PSR Part B Chapter 16 Probabilistic Safety Assessment, Rev 0, August 2024.

[16] HI-2240336 Holtec SMR GDA PSR Part A Chapter 5 Summary of ALARP Rev 0 August 2024.

[17] Holtec HPP-160-3004 SMR-160 Systems, Structures, and Components Classification Standard, Rev 6, Dec 2021.

[18] IEEE 603-Standard Criteria for Safety Systems for Nuclear Power Generating Stations 1991 (NRC Endorsed) & 2018 (latest).

[19] Holtec, HI-2167088 System Design Description for Plant Safety System Rev 1, 08 March 2022.

[20] Holtec, HI-2188464 System Design Description for Plant Control System, Rev 2, 19 September 2023.

[21] Holtec, HI-2210177 System Design Description for Diverse Actuation System, Rev 0, 22 July 2021.

[22] Holtec, HI-2177603 System Design Description for Post-Accident Monitoring System Rev 1 15th May 2020.

[23] Holtec, HI- 2210416 System Design Description for In-core Instrumentation System Rev 1, 10th Jan 2023.

[24] Holtec, HI-2200467 System Design Description for Ex-Core Instrumentation System Rev 2 8th Sep 2023.

[25] Holtec Britain, HI-2240127 Holtec SMR-300 UK/US Regulatory Framework and Principles Report, Rev 0, February 2024.

[26] US NRC 10 CFR 50 Appendix A to part 50 General Design Criteria for Nuclear Power Plant 24th March 2021.

[27] US NRC Regulatory Guides - generic reference to the many guides [Online] Available at: https://www.nrc.gov/reading-rm/doc-collections/reg-guides/index.html#guides.

[28] US NRC NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Chapter 7 Instrumentation and Controls Rev 6 2016.

[29] IEEE Std 7-4.3.2 IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, 2016.

[30] IEC/IEEE 60780 - 323 Nuclear Facilities - Electrical equipment Important to safety - Qualification, 2016.

[31] IEEE 379 - IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, 2000.

[32] IEEE 384 - IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits, 2018.

[33] IEEE 497 - IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, 2016.

[34] IEEE 730 - IEEE Standard for Software Quality Assurance Processes, 2014.

[35] US NRC Branch Technical Position (BTP) 7-19 - Revision 8, Guidance for Evaluation of Defense-in-Depth and Diversity to Address Common Cause Failure due ot latent design defects in Digital Safety Systems, , Jan 2021.

[36] US NRC, NUREG CR-6991, Design practices for communications and workstations in highly integrated control rooms, 2009.

[37] US NRC, NUREG CR-6082, Data Communications 1993.

[38] IAEA Specific Safety Guide SSG-39 – Design of Instrumentation and Control systems for Nuclear Power Plants, 2016.

[39] BS EN 61513 - Nuclear power plants - Instrumentation and control important to safety — General requirements for systems, 2013.

[40] BS EN 61226 - Nuclear power plants - Instrumentation, control and electrical power systems important to safety - Categorization of functions and classification of systems 2021.

[41] BS EN 60880 - Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions, 2009.

[42] BS EN 62566 - Nuclear power plants — Instrumentation and control important to safety — Development of HDL-programmed integrated circuits for systems performing category A functions, 2012.

[43] BS EN 60987 - Nuclear power plants - Hardware design requirements for computer based systems, 2021.

[44] BS EN 62138 - Nuclear power plants — Instrumentation and control important safety - software aspects for systems performing Cat B or C functions, 2019.

[45] BS EN 63413 - Nuclear Power Plants - Instrumentation and control systems important to safety - Platform qualification - Ed.1.0 Out for public comment, 2024.

[46] BS EN 62671 - Nuclear power plants - Instrumentation and control important to safety - Selection and use of industrial digital devices of limited functionality 2016.

[47] BS EN 60671- Nuclear power plants- Instrumentation and control systems important to safety – Surveillance testing 2011.

[48] BS EN 60709 - Nuclear power plants- Instrumentation and control systems important to safety – Separation 2019.

[49] BS EN 60780 - Nuclear facilities Electrical equipment important to safety– Qualification 2017.

[50] BS EN 60980-344 – Nuclear facilities – Equipment important to safety – Seismic qualification 2021.

[51] BS EN 62003 Nuclear power plants. Instrumentation, control and electrical power systems. Requirements for electromagnetic compatibility testing 2020.

[52] BS EN 61500 Nuclear power plants- Instrumentation and control systems important to safety – Data communication in systems performing category A functions 2019.

[53] BS EN 62340 - Nuclear power plants- Instrumentation and control systems important to safety – Requirements for coping with common-cause failure (CCF) 2010.

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

[55] U.S. NRC regulatory guide 1.26, Revision 6 Quality Group Classifications and Standards for Water, Steam, and Radioactive-Waste Containing Components of Nuclear Power Plants, December 2021.

[56] MML, 100110593-ENG1-0037, GDA Step 1 Gap Analysis, Revision 0, February 2024.

[57] IAEA SSR-2/1Safety of Nuclear Power Plants: Design IAEA Rev 1 2016.

[58] HI-2188331, Safety System Digital Platform - MELTAC - Topical Report (JEXU-1041-1008 Rev 2), Revision 1, 5th May 2023.

[59] HI-2240335, Holtec SMR GDA PSR Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance, Rev 0, August 2024.

[60] HI-2230346 Holtec SMR GDA PSR Part B Chapter 15 Beyond Design Basis and Severe Accident Analysis, and Emergency Preparedness, Rev 0, August 2024.

[61] HPP-3295-0017, Holtec SMR-300 Generic Design Assessment Reference Design Process and GDA Prospective Design Change Register, R0, May 16th 2024.

[62] USNRC, NUREG CR-6303 Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems (NUREG/CR–6303, UCRL–ID–119239) Dec 1994.

[63] Regulatory Guide 1.97 Revision 5 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants, April 2019.

[64] HI-2210230 Diversity and Defence in Depth Assessment for I&C systems, Rev 0, 27 July 2021.

[65] US NRC Regulatory Guide 1.53 Revision 2 - Application of the Single-Failure Criterion to Safety Systems, November 2003.

[66] NRC RG1.180 Guidelines for evaluating electromagnetic and radio frquency interfernce in safety-related instrumentation and control systems, Rev 2 Dec 2019.

[67] NRC RG1.209 Environmental qualification of safety-related computer based instrumentation and control systems in Nuclear Power Plant, March 2007.

[68] NRC RG1.62 Manual Initiation of Protective Actions, Rev 1 June 2010.

[69] NRC Interim Staff Guidance (ISG) 04 for Highly Integrated Control Rooms Rev 1 2009.

[70] USNRC, US NRC RG 1.152 Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants Rev 4 July 2023.

[71] US NRC Safety Evaluation Report (SER), Safety Evaluation for Mitsubishi Electric Total Advanced Controller (MELTAC) Platform Topical Report and Supporting Documents, November 2018.

[72] HI-2220583 SMR-160 I&C Architecture White Paper Rev 0 20 Sept 2022.

[73] US NRC 10 CFR 50.49 Environmental qualification of electric equipment important to safety for nuclear power plants, March 2021.

[74] US NRC 10 CFR 50.55a Codes and Standards, September 25th 2023.

[75] IEEE 627 - IEEE Standard for Qualification of Equipment used in Nuclear Facilities, 2019.

4.10 LIST OF APPENDICES

Appendix A I&C CAE Route Map

Table 7: Chapter B4 CAE Route Map

Overarching SSEC Claim	Chapter Claim/s	Chapter Sub-claim/s	Chapter Section
Claim 2.2 – System/Process Design and Substantiation The design of the systems and associated processes have been developed taking cognisance of relevant good practice and substantiated to achieve their safety and non-safety functional requirements.	**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.	**Sub-claim 2.2.6.1** 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 and Methodologies
		Sub-claim 2.2.6.2 The I&C system design incorporates Defence in Depth to protect against anticipated operational occurrences and accident conditions	4.5 Defence in Depth
		Sub-claim 2.2.6.3 I&C SSCs achieve the design intent through quality manufacturing and installation process.	4.6 Quality Manufacturing and Installation Processes
		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.	4.7 Examination, Inspection, Maintenance and Testing

Appendix B (REDACTED)

REDACTED