A Holtec International Company

Holtec Britain Ltd	HI-2240340
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 9 Description of Operational Aspects/Conduct of Operations

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

Table of Contents

List of Tables

9.1 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, commissioned, 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 Part A Chapter 1 Introduction [1].

The Fundamental Purpose is achieved through the Fundamental Objective of the Preliminary Safety Report (PSR), which is to summarise the safety standards and criteria, safety management and organisation, claims, arguments and evidence to demonstrate that the generic SMR-300 design risks to people are likely to be tolerable and As Low as Reasonably Practicable (ALARP) [1].

This chapter of the PSR outlines the approach to plant operations and the undertaking of operations. These are not expected to be outlined in full at the GDA stage, as they are developed by the licensee in the site licensing phase as the detailed information about the reactor's operation evolves. However, general approaches, methodologies and principles are outlined for operational management of the generic SMR-300 so that the eventual conduct of operations is integrated into the plant design.

Part B Chapter 9 of the PSR Description of Operational Aspects and Conduct of Operations presents the Claims, Arguments and Evidence (CAE) for the description of operational aspects and conduct of operations Structures, Systems and Components (SSC) that underpin the design of the generic SMR-300.

9.1.1 Purpose and Scope

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

This chapter (Part B Chapter 9) links to the overarching claim through Claim 2.3:

Claim 2.3: The design and safety assessment of the Generic Holtec SMR-300 considers the entire reactor lifecycle.

As set out in Part A Chapter 3 [2], Claim 2.3 is further decomposed across several disciplines which support the development of through-life management arrangements.

This chapter presents the Conduct of Operations aspects for the generic SMR-300 and therefore directly supports a claim focused on the appropriate arrangements to safely manage people and plant, Claim 2.3.1.

Claim 2.3.1: Appropriate arrangements to safely manage people and plant during the operation of the Generic Holtec SMR-300 are suitably mature.

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 9.2.

Part B Chapter 9 Description of Operational Aspects and Conduct of Operations presents a discussion of:

- An overview of the operational aspects of the generic SMR-300 and its conduct of operations (see sub-chapter 9.2).
- The CAE relevant to conduct of operations (see sub-chapter 9.3).
- The overall design of the Main Control Room (MCR) and Remote Shutdown Facility (RSF) (see sub-chapter 9.4).
- The definition of limits and conditions within the SSEC, and the production of Operating Documentation (see sub-chapter 9.5).
- The Examination, Inspection, Maintenance and Testing (EIMT) activities that are relevant for the generic SMR-300 (see sub-chapter 9.6).
- A technical summary of how the claims within this chapter have been met; the contribution from this chapter to support the demonstration that risks are likely to be tolerable and ALARP for the generic SMR-300 design, and any GDA commitments that have arisen (see sub-chapter 9.7).

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.

9.1.2 Assumptions

There are no assumptions raised in relation to Part B Chapter 9.

9.1.3 Interfaces with other SSEC Chapters

Operational aspects and conducts of operations interface with numerous chapters of the PSR to varying degrees, notably within maintenance considerations and Human Factors (HF) sections, a number of the key chapters are listed below, this is a non-exhaustive list:

The Reference Design and Reference Plant are stated in Part A Chapter 2 [3].

Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance [4] addresses the lifecycle management of the reference design and its interactions with the reference plant. It also includes the organisational and management arrangements at the GDA stage, which will evolve to support the establishment of a licensee. These arrangements will change to support the relevant lifecycle stage, and ultimately support the conduct of operations.

Part A Chapter 5 Summary of ALARP and SSEC [5] presents the ALARP methodology and ALARP justifications for the generic SMR-300, this provides the basis for the concluding sub-chapter, which provides an ALARP summary.

The requirements for EIMT will be captured in the following chapters:

Part B Chapter 1 Reactor Coolant System (RCS) and Engineered Safety Features (ESF) will present the Reactor Coolant System and connected SSCs that must allow reliable operation and control to maintain safety of the plant.

Part B Chapter 2 Reactor [6] includes the Fuel and Core SSCs that must allow reliable operation and control to maintain safety of the plant.

Part B Chapter 4 Control and Instrumentation Systems [7] presents the Instrumentation & Control (I&C) SSCs to provide reliable means for monitoring and control to maintain safety of the plant.

Part B Chapter 5 Reactor Supporting Facilities [8] includes Reactor supporting SSCs that must allow reliable operation and control to maintain safety of the plant.

Part B Chapter 6 Electrical Engineering [9] includes Electrical SSCs that must allow reliable operation and provide power to maintain the safety of the plant.

Part B Chapter 10 Radiological Protection [10] covers Radiological Protection SSCs and arrangements (e.g. zoning/entry restrictions) that must allow reliable operation and control to maintain normal operational safety of the plant.

Part B Chapter 12 Nuclear Site Health and Safety (NSHS) and Conventional Fire Safety [11] considers how operations will ensure safety and risk reduction of non-radiological hazards. Holtec's Construction (Design and Management) (CDM) Strategy [12] has been published, along with the NSHS Safety Management System Report [13], which sets out the means by which the CDM Strategy is to be implemented. The CDM Strategy and NSHS Safety Management System define the roles of the CDM Regulations 2015 (CDM 2015) Duty Holders. Holtec are clear that they will discharge the duties of Designer beyond GDA. The safety of operators during maintenance activities will ultimately be assessed using principles developed in this chapter for operational activities.

Part B Chapter 13 Radioactive Waste Management [14] describes operations for managing the solid, liquid, and gaseous wastes generated by the generic SMR-300 and is deemed to be essential to normal operations.

Part B Chapter 14 Design Basis Analysis (Fault Studies) [15] will derive the operating limits and conditions from the Fault Studies used in the development of operating documentation (e.g. Technical Specifications)

Part B Chapter 15 Beyond Design Basis Accident (BDBA), Severe Accident Analysis, and Emergency Preparedness [16] will ultimately inform Emergency Operating Procedure and Severe Accident Management Guidelines which will form the conduct of operations.

Part B Chapter 16 Probabilistic Safety Assessment (PSA) [17] informs EIMT as a potential input to proof testing intervals of SSC.

Part B Chapter 17 Human Factors [18] provides an overview and assessment of the Human Factors Engineering (HFE) process being applied to the United States (US) SMR-300 reference plant design of the systems and associated processes have been developed taking cognisance of Relevant Good Practice (RGP). Beyond GDA, HF will undertake Staffing and Qualification (S&Q) analyses to ensure that the staffing levels are sufficient to always maintain safe operations, in normal and accident conditions. It is important to align the concept of operations with the Human Factors Integration (HFI) process.

Part B Chapter 18 Structural Integrity [19] identifies the requirements for EIMT, including Pre-Service and In-Service inspections of Structural Integrity SSCs.

Part B Chapter 19 Mechanical Engineering [20] presents the requirements for EIMT of Mechanical Engineering SSCs.

Part B Chapter 20 Civil Engineering [21] will present the requirements for EIMT of Civil Engineering SSCs.

Part B Chapter 23 Reactor Chemistry [22], chemistry associated with Chemical Specifications (e.g. control of the reactor chemistry should allow operations such as determining the concentration of soluble boron in the Reactor Coolant System).

Part B Chapter 24 Fuel Transport and Storage [23], the fuel route will define the refuelling operations, dry storage system operational procedures and arrangements. EIMT aspects will be considered for the fuel route and dry storage systems.

9.2 OVERVIEW OF OPERATIONAL ASPECTS AND CONDUCT OF OPERATIONS

This sub-chapter outlines the normal operating modes that are relevant to the generic SMR-300. It also identifies the fuel route, transport, and storage and lifting operations that will ultimately be subject to operating limits and conditions. These will remain subject to development beyond this GDA stage and will inform the scope of the future SSEC, which will in turn, derive the limits that require incorporation into the operating documentation, to operate the plant safely. The production of operating documentation is discussed further in sub-chapter 9.5, which will be undertaken in the site licensing stage.

As the generic SMR-300 design is still under development, the final operating regime for normal operations is yet to be fully defined. Future revisions of the SSEC will reflect the ongoing development of the normal operating regime.

The majority of information available in relation to the Operating Philosophy of SMR-300 at GDA relates to staffing arrangements within the MCR and RSF facilities of the plant. Limited information was available regarding the Operating Philosophy for the Fuel Handling Area (FHA), Containment Structure (CS) and Containment Enclosure Structure (CES), which has been summarised as far as practicable for GDA Step 2.

[REDACTED]. An Operating Philosophy Review Report [24] has been undertaken, which is summarised throughout this chapter.

An SMR-300 Concept of Operations (Con Ops) will be produced towards the end of 2025 as part of the Holtec International HFE Project Management Plan (PMP) [25], in line with NRC HFE process for HFE programme management [26] after sufficient Task Analysis is available to support S&Q analysis. The SMR-300 Con Ops will provide the overall philosophy for how the operating crew is organised and how it monitors and controls the plant during normal operations, off-normal conditions and emergencies.

As the Con Ops is still in production, information currently available to summarise the SMR-300 Operating Philosophy for UK GDA is distributed across high-level documentation. The Operating Philosophy Review Report [24] therefore summarises the available information on operator roles and responsibilities, staffing levels and key facilities for SMR-300 operation.

9.2.1 Normal Operating States and Plant Modes

Normal operations are defined in the International Atomic Energy Agency (IAEA) Nuclear Safety and Security Glossary [27] as ‘operations within specified operational limits and conditions’. Normal operation includes all the operating modes permitted at the facility, e.g., startup and shutdown states and temporary situations arising due to maintenance and testing. They also include minor deviations from desired operating conditions provided these are appropriately justified in the safety case (i.e., they include what the IAEA terms Anticipated Operational Occurrences (AOO) [27]).

Normal operation of the generic SMR-300 is defined as when the plant is within its specified operating conditions/limits. The typical plant operating modes are defined in the Standard Technical Specifications to comply with 10 Code of Federal Regulations (CFR) 50 [28] paragraph 50.36 Technical Specifications. As the operating modes have not yet been fully defined, the typical Mode 1 Power Operations mode has been split to coincide with the licensing basis events definitions in the Standard Review Plan NUREG-0800 Chapter 15.

The alignment with UK plant condition classes is shown in Part B Chapter 14 Design Basis Analysis (Fault Studies) [15]. Holtec have defined abnormal plant conditions to align with those AOOs occurring once per reactor lifetime.

The SMR-300 plant modes of operation defined in SMR-300 Top Level Plant Design Requirements [29] are summarised in Table 1. These align with modes found at currently operating Pressurised Water Reactors (PWR).

Table 1: Modes of Operation for SMR-300

[REDACTED]

9.2.1.1 Power Operation

Power Operation is the phase where the SMR-300 is generating power and is defined as Plant Mode 1 [29]. During normal operation, primary coolant is driven by Reactor Coolant Pumps (RCP) and high pressure, superheated steam is produced in the once-through Steam Generator (SGE) and directed to a turbine generator. Feedwater is returned to the SGE with the use of condensate and feedwater pumps.

The plant control scheme is designed for operation with the SGE and is based on a "feed forward" strategy. A change in the electrical grid load is automatically compensated by the turbine control valves opening or closing to admit steam to the turbine at a constant speed to keep the active power variations within the limits mandated by the national grid code. The generic SMR-300 is designed to accommodate the following operational occurrences without causing a reactor trip or ESF actuation signal:

- ± 5%/minute ramp load change between 15% and 100% power.
- 100% generator load rejection and transition to house load operation.

- Loss of a single feedwater pump.

This enables SMR-300 to accommodate load changes without causing reactor trip or emergency shutdown features. If a trip of both the RCPs occurs during normal operation, coolant flow is driven by natural circulation.

9.2.1.2 Startup

Startup is the process for moving the reactor into a critical state and beginning normal operation (power generation) up to a Reactor Power of 5% and is defined as Plant Mode 2 [29].

Actions to prepare the plant for entry into Plant Mode 2 include increasing the temperature of the RCS to the required temperature prior to criticality using RCPs and establishing that coolant chemistry requirements to progress in plant startup have been met.

Once the RCS is at normal operating pressure and temperature, control rods are withdrawn to criticality. Rods are further withdrawn to the point of adding heat and power is raised to that for Power Operation Mode. Steam is bypassed around the main steam isolation valve to warm up the steam lines and the steam turbine. Steam is admitted to the turbine for turbine warmup and the turbine generator is synchronised to the grid at a minimum power level.

For SMR-300, Units 1 and 2 are intended to be started in sequence through preparation of shared systems. These systems include demineralised water for dilution of the RCS, auxiliary steam to supply gland sealing steam, needed to draw a vacuum in the condenser and potentially feedwater heating, as well as the waste gas system to supply cover gas to the Chemical and Volume Control System (CVC) holdup tanks for moving water.

9.2.1.3 Shutdown Operations

Shutdown operation is the process for stopping power generation through a controlled shutdown of a reactor. Control rods are fully inserted manually to enter Plant Mode 3. The SGE and RCPs are initially used to remove the decay heat. The steam produced by the SGE after reactor shutdown is sent directly to the condenser through the turbine bypass valves. The condensate from the condenser is returned to the SGE using the main feedwater system. The RCPs are used to ensure thermal equilibrium of the RCS. When RCS pressure is reduced to below the Residual Heat Removal System (RHR) operating pressure, RHR is placed in service to continue decay and sensible heat removal from the core. The RHR heat exchangers are sized to cool the RCS to [REDACTED]. There are three Plant Modes [29] associated with shutdown operation:

- Plant Mode 3: Hot Standby.
- Plant Mode 4: Safe Shutdown.
- Plant Mode 5: Cold Shutdown.

9.2.1.4 Refuelling Operations

An outage is the period where the reactor is shut down to perform refuelling and maintenance activities, which will require additional staff and specialist contractors. It is defined as Plant Mode 6 [29].

The generic SMR-300 is designed to operate on a nominal 18-month fuel cycle with approximately one-third of the fuel assemblies in the core discharged every refuelling outage. The refuelling process for the generic SMR-300 is similar to a conventional Boiling Water Reactor (BWR) given the orientation and close proximity of the Spent Fuel Pool (SFP) to the reactor. Placing the SFP adjacent to the Reactor Pressure Vessel (RPV) eliminates the complexity and maintenance associated with conventional PWR fuel up-ending and transferring equipment to facilitate transfer of fuel between the containment and the fuel handling building.

A high-level summary of the SMR-300 refuelling operations are as follows:

- New fuel is loaded into a Multi-Purpose Canister (MPC) (inside HI-TRAC), in the FHA of the Reactor Auxiliary Building (RAB).
- The HI-TRAC with its MPC is moved from the FHA into containment via the equipment hatch and then into the SFP cask area.
- All fuel assemblies from the reactor core are offloaded to the SFP storage rack.
- New fuel is moved from the HI-TRAC to the SFP storage rack.
- Fuel insert hardware is re-arranged to the required fuel assemblies.
- New, once, and twice-burned fuel assemblies are moved to the reactor core.
- Spent fuel remains in the SFP until the required cooling time for dry storage is achieved. Spent fuel from prior cycles that has reached its required cooling time is moved into the same MPC used to bring new fuel into the SFP and is removed from SFP using the same HI-TRAC.
- The HI-TRAC with its MPC is moved to the FHA.
- The MPC is processed for dry storage inside the HI-TRAC.
- The HI-TRAC is brought to the onsite dry storage facility and transferred into the Underground Maximum Capacity System (UMAX) storage module.

A detailed description of the generic SMR-300 refuelling operations is presented in Part B Chapter 24 [23]. This includes the transfer of new fuel to the reactor, and the transfer of spent fuel to dry storage, that are summarised in the following sub-chapters.

During refuelling, maintenance of equipment inside containment, including inspection of SGE tubes, is performed, as necessary.

9.2.1.5 Abnormal Operations

Abnormal plant conditions in the Plant Overview document [30] align with those AOOs occurring once per reactor lifetime. These are operational processes deviating from normal operation that are expected to occur one or more times during the operating lifetime of the plant This is described in more detail in Part B Chapter 14 Design Basis Analysis (Fault Studies) [15].

If the Main Generator is unavailable the Unit Auxiliary Transformer (UAT) is supplied from the switchyard via back feed of the Main Step-Up Transformer (MSU). If the UAT is unavailable, a bus transfer will be initiated to transfer the loads to the Station Service Transformer (SST), which is fed from the switchyard. In the event of a loss of transmission grid, the main generator can continue to provide power plant loads independent from the grid in Island Mode operation.

The ability to operate the generic SMR-300 in island mode adds an additional layer of reliability during a response to a Loss of Offsite Power (LOOP). This allows the generic SMR-300 to be sited in a wider variety of locations, even where the grid is unreliable, without loss of safety.

For a list of the AOOs relevant to the generic SMR-300, see Part B Chapter 14 Design Basis Analysis (Fault Studies) [15].

9.2.1.6 Fuel Route, Transport and Storage Operations

9.2.1.6.1 Transfer of New Fuel to Reactor

New Fuel Assemblies (NFA) received for refuelling are removed one at a time from the shipping container and moved into the new fuel assembly inspection area of the RAB. After inspection, the accepted new fuel assemblies are stored in the New Fuel Storage Rack (NFSR) in the New Fuel Vault (NFV).

A MPC is placed inside a HI-TRAC transfer cask and brought to the RAB door on a Vertical Cask Transporter (VCT). The HI-TRAC is lowered onto a Low Profile Transporter (LPT) which transports the HI-TRAC into the FHA of the RAB.

The NFV is in the FHA of the RAB. New fuel assemblies are loaded into the HI-TRAC one at a time, using the overhead crane in the RAB. The HI-TRAC is then transported on the LPT through the CS equipment hatch. Inside the CS, the HI-TRAC is flooded with borated water and the Polar Crane lifts the HI-TRAC off the LPT and lowers it into the SFP.

The new fuel from the HI-TRAC is transferred to the Spent Fuel Storage Racks (SFSR) and then is moved into the reactor core using the Fuel Handling Bridge Crane (FHBC) (an alternative option involves transferring the NFAs from the submerged MPC direct to the reactor core using the FHBC). Fuel that will be used for another cycle is returned to the reactor core from the SFSR using the FHBC.

9.2.1.6.2 Transfer of Spent Fuel to Dry Storage

The SMR-300 spent fuel dry storage system is part of Holtec's optimised integrated fuel management system. The generic SMR-300 utilises on-site interim spent fuel storage within the HI-STORM UMAX system, containing an MPC-37 loaded with [REDACTED] spent fuel assemblies.

Consistent with requirements relating to decay heat, burnup, and cooling time, spent fuel can be retrieved from the SFP for dry storage after as little as [REDACTED] of cooling in the SFP. It is expected that dry storage campaigns will commence after the third or fourth refuelling outage (~[REDACTED] years after start of generation), when the discharged spent fuel assemblies of the first cycle will be removed from the SFP and placed into underground dry storage in the HI-STORM UMAX system, which is located at the on-site Interim Spent Fuel Storage Installation (ISFSI). Dry fuel storage campaigns will be undertaken following every subsequent refuelling outage and until all the spent fuel assemblies are placed into dry storage.

Lifting, handling, processing, and transportation equipment is designed to efficiently move spent fuel from the SFP to the UMAX system sited at the on-site ISFSI.

When a dry storage campaign is performed during the refuelling outage, the same HI-TRAC that was used to bring in the new fuel will be used to move spent fuel assemblies out of containment for processing for dry storage. After the new fuel has been removed, and the HI-TRAC is still within the SFP, the spent fuel assemblies are loaded into the HI-TRAC using the FHBC.

A thick stainless-steel lid is placed on the MPC using the polar crane. The HI-TRAC is removed from the SFP using the polar crane and placed on the LPT. The HI-TRAC provides shielding from the spent fuel assemblies and structural protection for the MPC. The thick MPC lid and the water in the MPC also provide shielding.

The HI-TRAC is moved out of the CS the same way it entered and is placed in a dedicated FHA area of the RAB where the spent fuel assemblies and the MPC are prepared for dry storage.

The MPC is drained, dried, backfilled with inert gas and welded shut to provide a pressure vessel boundary as a high integrity containment/confinement barrier for radioactivity on site, during transfer and interim storage within the UMAX system. When complete, the HI-TRAC is moved outside of the RAB the same way it entered.

A VCT then lifts the HI-TRAC off the LPT and carries it to the on-site ISFSI. At the ISFSI, the HI-TRAC is positioned over the HI-STORM UMAX cavity. The bottom hatch of the HI-TRAC is removed and the MPC is lowered into place.

The HI-TRAC is then removed from the area and the HI-STORM UMAX system closure lid is placed over the cavity to complete the dry storage process.

Each HI-STORM UMAX Vertical Ventilated Module (VVM) provides storage of an MPC in the vertical configuration inside a cylindrical cavity located entirely below the top-of-grade of the ISFSI. The VVM, akin to an above ground over-pack, is comprised of a cavity enclosure container and closure lid, as well as interfacing structures.

On-site interim dry storage within the HI-STORM UMAX system is expected to be the storage means for spent fuel, any damaged fuel and non-fuel waste for at least the design life of the SMR-300 reactor.

Based on previous Requesting Parties' GDA submissions for standard PWR fuel with similar characteristics, an interim storage period for spent fuel of 100 years or more is likely to be necessary prior to retrieval for repackaging for disposal in the UK's planned Geological Disposal Facility (GDF).

A detailed description of the generic SMR-300 fuel route, including transport and storage is discussed in Part B Chapter 24 [23].

9.2.1.7 Conduct of Lifting Operations

Heavy loads are not typically lifted within the CS of the SMR-300 during power operations since most heavy loads are associated with refuelling operations (described above in sub-chapter 9.1), and a heavy load drop would not result in a plant trip during normal power operations. Sub-chapter 9.6.1.3 describes the Outage Strategy for SMR-300 [31], which includes lifting and handling routes and equipment.

The conduct of lifting operations will be managed in accordance with the requirements of the SSEC to ensure that risks posed by lifting operations will be ALARP. Lifting operations will be assessed within the safety assessment as outlined within Part B Chapter 22 Internal Hazards [32], and any limits and conditions that are required to ensure that risk is managed ALARP (e.g. plant configurations to ensure appropriate Defence in Depth (DiD), maximum lift masses in accordance with the withstand capability of SSCs). Further information will be presented on this as the SSEC matures.

Within the UK all lifts required within the generic SMR-300 facility and site will comply with the Approved Codes of Practice (ACoP) for Lifting Operations and Lifting Equipment Regulations (LOLER) [33] and Provision and Use of Work Equipment Regulations (PUWER) [34] guidance. The conduct of lifting operations will be defined during the nuclear site licensing phase to ensure that lifting operations are compliant with the limits and conditions of the SSEC.

9.2.2 Key Operational Roles

Key operational roles and the primary responsibilities associated with operation of the SMR-300 in all conditions are described in this section. Information available on operational roles at GDA is largely based on the expected licensed operators, in accordance with NRC definitions. These are identified in the Operating Philosophy Review [24], and summarised below.

9.2.2.1 Reactor Operator

Responsible for monitoring and controlling both units.

9.2.2.2 Senior Reactor Operator

Responsible for monitoring the overall plant state, providing independent checking and approval of selected tasks conducted by the Reactor Operator.

The Senior Reactor Operator (SRO) will be able to monitor the overall plant state and have visibility/oversight of Reactor Operator actions via the read-only mimic displays on the SRO desk and on Large Display Panels (LDP). The SRO will have no control functionality for any systems from the SRO workstation.

9.2.2.3 Shift Manager

The Shift Manager will be responsible for the day-to-day management of the SMR-300 and is expected to be licensed and qualified to perform both SRO and Reactor Operator activities.

The shift manager will be based in an office within or adjacent to the MCR but is not required to be in the MCR at all times. Requirements in relation to their location on site will be dependent on operational mode and condition.

9.2.2.4 Field Support Supervisor

The Field Support Supervisor will provide an interface with the teams local to plant and in the MCR. The Field Support Supervisor is expected to be licensed and qualified to perform both SRO and Reactor Operator activities and provide support to the acting Reactor Operator.

9.2.2.5 Shift Technical Adviser

The Shift Technical Adviser (STA) is responsible for providing independent advice based on their nuclear engineering technical skills and knowledge.

They are expected to advise the operating and supervisory personnel, should unexpected conditions develop. This provides additional, independent, technical and analytical support on actions to terminate or mitigate the consequences of abnormal events or accident conditions.

9.2.3 SSCs Essential to Normal Operations

A UK equivalent categorisation and classification scheme will be identified for the normal operations safety functions of the generic SMR-300.This will identify all generic SMR-300 SSCs that are essential to nuclear safety in normal operations. The approach to the allocation of the UK categorisation and classification scheme is discussed further within Part A Chapter 2 [3].

9.2.4 Conduct of Operations Codes and Standards/Methodologies

This sub-chapter outlines the codes and standards that are relevant for the operational aspects and conduct of operations of the generic SMR-300. The full definition of the conduct of operations, to enable compliance with the UK Licence Conditions (LC), will be developed within the nuclear site licensing phase of the generic SMR-300.

9.2.4.1 SMR-300 Reference Plant Concept of Operation Codes, Standards and Regulations

The SMR-300 conduct of operations is based on the requirements set out in:

- NUREG-0800 Standard Review Plan [35].
- NUREG-0711 Human Factors Engineering Program Review Model [26].
- NUREG/CR-7216 Human Performance Issues Related to the Design and Operation of SMRs [36].
- Nuclear Regulatory Commission. Title 10, Code of Federal Regulations [37].

In addition to the above, the following relevant good practice guidance is available from the IAEA and displayed in Table 2.

Table 2: List of Regulations and International Guidance used for Generic SMR-300 Design Standard

Document/Label	Title
IAEA Specific Safety Guide No. NS-G-70 [38]	Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants
IAEA Specific Safety Guide No. NS-G-72 [39]	The Operating Organization for Nuclear Power Plants
IAEA Specific Safety Guide No. NS-G-74 [40]	Maintenance, Testing, Surveillance, and Inspection in Nuclear Power Plants
IAEA Specific Safety Guide No. NS-G-76 [41]	Conduct of Operations at Nuclear Power Plants

Compliance with NUREG-0711 [26] and NUREG/CR-7216 [36] will be demonstrated within the US Preliminary Safety Assessment Report (PSAR) in support of the Operating License Application (OLA).

Part B Chapter 17 [18] presents how HF consideration has been applied within the GDA stage to demonstrate that the process for HFE applied to the generic SMR-300 is aligned with Office for Nuclear Regulation (ONR) expectations for HF integration in the UK, including a review of the developing operating philosophy and proposed staffing levels. It is recognised that this is based on NUREG-0711, which is based on NRC expectations rather than those of the ONR.

9.2.4.2 UK Context and GDA

The generic SMR-300 must be capable of meeting all 36 LCs set out by the ONR within their LC handbook [42] when deployed to a site in the UK. Multiple LCs relate to this PSR Chapter, and a few of the key ones are listed below:

- LC 23 – Operating Rules (OR) [43].
- LC 24 – Operating Instructions [44].
- LC 25 – Operational Records [45].
- LC 26 – Control and Supervision of Operations [46].
- LC 27 – Safety Mechanisms, Devices and Circuits [47].
- LC 28 – Examination, Inspection, Maintenance and Testing [48].
- The ONR Safety Assessment Principles (SAP) from Technical Assessment Guide (TAG)-35 [49]. ONR TAG-35 provides useful guidance relating to Limits and Conditions and OR.

The Limits and Conditions for Nuclear Safety [49] include specific principles for EIMT, including:

- Identification of requirements EMT.1.
- Frequency EMT.2.
- Type-testing EMT.3.
- Validity of equipment qualification EMT.4.
- Procedures EMT.5.
- Reliability claims EMT.6.
- Functional testing EMT.7.
- Continuing reliability following events EMT.8.

SAPs relevant to ageing and degradation include:

- Safe working life EAD.1.
- Lifetime margins EAD.2.
- Periodic measurement of material properties EAD.3.
- Periodic measurement of parameters EAD.4.
- Obsolescence EAD.5.

TAG-09 Examination, Inspection, Maintenance and Testing of items important to Safety [50] provides useful guidance relating to EIMT of items important to safety.

Although the SMR-300 has been designed in line with US NRC Regulatory Requirements, the operational constraints, maintenance, and procedures are likely to remain in line with one another.

The expectations of NUREG-0800 regarding the conduct of operations are that the following topics are addressed:

- Management of the technical support organisation and the operating organisation, including the training and qualification of operators and staff, operational programmes, and administrative procedures.
- Emergency planning.
- Security and cyber-security.
- Operational procedures (see sub-chapter 9.5).
- Maintenance (see sub-chapter 9.6).

The NUREG-0800 expectations that are not subject to claims within this chapter are described below, with reference to the relevant SSEC documentation. Where the UK regulatory requirements are not considered within the conduct of operations developed for the SMR-300 reference plant in accordance with NUREG-0800, these will be identified within the relevant topic areas of the SSEC to support the nuclear site licensing stage.

9.2.4.3 Management of the Technical Support Organisation

Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance [4] presents the approach to the management of the transfer of commitments made within SSEC documentation into the intended operating regime. It also provides an overview of the SSEC development strategy.

The generic SMR-300 will become a notifiable project under CDM 2015 and, as such, will be legally bound to comply with the relevant parts of those regulations. As reported in Part B Chapter 12 Nuclear Site Health and Safety and Conventional Fire Safety [11], Holtec's CDM Strategy [12] has been published, along with the NSHS Safety Management System Report [13], which sets out the means by which the CDM Strategy is to be implemented.

The CDM Strategy and NSHS Safety Management System define the roles of the CDM 2015 Duty Holders. Holtec are clear that they will discharge the duties of Designer, and how that will be done is set out in these documents. Appointment of the other Duty Holders such as Client, Principal Designer and Principal Contractor is expected beyond the GDA stage.

9.2.4.4 Emergency Planning

Emergency preparedness within the ONR SAPs emphasizes the importance of planning and readiness to respond effectively to nuclear emergencies.

To protect the public and the environment from the consequences of a Nuclear Power Plant (NPP) accident, each plant operator/licensee establishes a Severe Accident management programme, which is kept under constant review and development. The main objective of the guidelines used to design such programmes is to utilise any available equipment and ESFs at the NPP to terminate core damage, maintain containment integrity and minimise the release of radioactivity.

Although they are unlikely to be needed, Severe Accident management programmes are a critical part of the DiD concept, which is a hierarchical deployment of different levels of equipment and procedures in a graded approach to protect against a wide variety of incidents, accidents, equipment failures, human errors and events initiated outside the plant.

Part B Chapter 15 Beyond Design Basis and Severe Accident Analysis, and Emergency Preparedness [16] Claim 2.1.3.4 considers accident management and emergency preparedness. The Accident Management Program report [4] supports Part B Chapter 15 [16] at the GDA stage. It is focused on providing guidance and basis for the next step up to the stage where site dependent conditions are considered. The report contains SSCs which are credited with accident prevention, control and management with a link to their detailed description and safety and effectiveness demonstration. ESF operation and effectiveness are highlighted and linked to strategies and procedures which will be needed for a complete Accident Management plan. In addition, some requirements and features of the emergency centre, control room, Post Accident Monitoring System (PAM), etc. are presented.

Part B Chapter 15 [16] shows that the SMR-300 Severe Accident Analysis will provide a framework for the Emergency Operating Procedures (EOP) and Severe Accident Management Guidelines (SAMG) required to be followed by the operators in order to prevent and mitigate Severe Accidents.

9.2.4.5 Security and Cyber Security

The Generic Security Report [51] aims to demonstrate the implementation of the security methodologies developed for the SMR-300 and demonstrate the golden thread from the asset all the way to site security operations. It provides illustrative conceptual security arrangements and expectations on the site licensee. The generic SMR-300 security design will be site specific and will require an assessment against the UK Design Basis Threats, which are outside the scope of the SMR-300 GDA scope of work.

The SMR-300 Conceptual Security Arrangements Report [52] identifies the expectations on the licensee on the security Con Ops for a UK SMR-300. A cyber security risk assessment study is presented within SMR-300 Cyber Security Risk Assessment Study [53].

9.3 OPERATIONAL ASPECTS AND CONDUCT OF OPERATIONS CLAIMS, ARGUMENTS AND EVIDENCE

This chapter presents the operational aspects and conduct of operations focused on demonstrating that the generic SMR-300 design has considered all arrangements to safely manage people and plant for the entire reactor lifecycle, and therefore directly supports Claim 2.3.1.

Claim 2.3.1: Appropriate arrangements to safely manage people and plant during the operation of the generic Holtec SMR-300 are suitably mature.

Claim 2.3.1 has been further decomposed within Part B Chapter 9 to:

- Show that the MCR and RSF will enable the plant to be operated safely in accordance with the limits and conditions derived within the SSEC.
- Provide confidence that the operating limits and conditions of the safety case will be clearly identified within the SSEC and subsequently incorporated into operational documentation.
- Provide confidence that the EIMT requirements will be identified to support the demonstration that the SSCs continue to achieve their safety functional requirements throughout the reactor lifecycle.

This has been undertaken by breaking down Claim 2.3.1 into 3 further claims:

Claim 2.3.1.1 is to provide the holistic demonstration of the design of the MCR and RSF in how they will support safe operation of the generic SMR-300, in accordance with the limits and conditions derived within the SSEC. This includes the design approach, operational procedures, staffing and training of control room operators, hazard tolerance and habitability following defined internal and external hazards.

Claim 2.3.1.2 is an enabling claim to ensure that the SSEC will ultimately derive a set of limits and conditions, and that these limits and conditions of the safety case will be incorporated into operating documentation.

Claim 2.3.1.3 is an enabling claim to ensure that the EIMT requirements will be identified in accordance with UK expectations to support the demonstration that the SSCs continue to achieve their safety functional requirements throughout the reactor lifecycle. The maturity of the supporting design, design substantiation and associated arrangements supporting these claims will develop beyond GDA and will be reflected in future revisions of the SSEC.

Table 3 shows the breakdown of Claim 2.3.1 and identifies in which chapter of this PSR these claims are demonstrated to be met.

Table 3: Claims covered by Part B Chapter 9

Claim No	Claim	Chapter Section
2.3.1.1	The MCR and RSF shall enable the plant to be operated safely in accordance with the limits and conditions of the safety case.	9.4 Main Control Room and Remote Shutdown Facility
2.3.1.2	The limits and conditions of the safety case are clearly identified and will be incorporated into operational documentation.	9.5 Operating Documentation

Claim No	Claim	Chapter Section
2.3.1.3	Examination, Inspection, Maintenance and Testing (EIMT) activities are identified to ensure the SSCs continue to achieve their safety functional requirements throughout operational life.	9.6 Examination, Inspection, Maintenance and Testing

Appendix A provides a full Claims, Arguments and Evidence mapping for Part B Chapter 9, 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.

9.4 MAIN CONTROL ROOM AND REMOTE SHUTDOWN FACILITY

Claim 2.3.1.1: The MCR and RSF shall enable the plant to be operated safely in accordance with the limits and conditions of the safety case.

This sub-chapter presents a description of the overall design of the MCR and RSF to show that they will provide an appropriate means of managing operational activities and delivery of safety functions. This sub-chapter includes a highly cross-cutting set of arguments, which have multiple interfaces and are supported by a significant number of engineering and safety analysis disciplines. MCR and RSF claims and sub-claims will develop in accordance with the SSEC stages beyond GDA.

The following section sets out a number of arguments to support Claim 2.3.1.1, with signposting to interfacing chapters of the safety report where the evidence to support these arguments is being developed (noting that at PSR stage the maturity of this evidence is limited). The arguments are based upon demonstration that each of the systems physically contained within the MCR and RSF and those interfacing systems that directly support them, are appropriate and designed and operated to enable delivery of their relevant safety functions. This includes the need to ensure that hazards and faults with the potential to impact the delivery of these safety functions have been considered and that the MCR and RSF remain habitable to operators.

The design approach for those SSCs which comprise the MCR and RSF are set out in relevant engineering PSR chapters. These individual engineering chapters provide supporting arguments (e.g. adoption of relevant good practice, DiD) to ensure relevant MCR and RSF safety functions can be delivered. The key design decisions for the MCR and RSF will be suitably justified to reduce risks to ALARP.

Future revisions of this chapter will provide a full design description of the MCR and RSF, alongside detailed summaries of the relevant supporting engineering chapters to provide a holistic overview of the MCR and RSF safety case.

Claim 2.3.1.1 has been decomposed into 4 arguments that are presented in specific sub-chapters to address:

- The design approach for the SSCs associated with the MCR and RSF (see sub-chapter 9.4.4).
- Operational procedures, staffing and training (see sub-chapter 9.4.5).
- The identification of hazards and faults with the potential to impact the SSCs located in the MCR and RSF (see sub-chapter 9.4.6)
- MCR and RSF habitability (see sub-chapter 9.4.7)
- In addition, sub-chapter 9.4.1 provides a high-level design description of the MCR and RSF.

9.4.1 Main Control Room Design Description

The SMR-300 MCR is the central location from which all plant operations are coordinated and monitored. It is the principal control station, utilised during both normal and accident conditions to operate the plant safely and maintain it safe.

The MCR houses the I&C equipment including the Human System Interface (HSI) equipment necessary to oversee all plant systems, monitor plant instrumentation, and control plant components for safe operation of both SMR-300 plant units simultaneously. It is designed such that a two-person team (a Reactor Operator and an SRO at separate workstations) is sufficient to operate multiple units. It also contains hardware and software switches to accomplish manual initiation of ESF and reactor trip functions.

The following key functions are provided from the MCR:

- Means to operate SMR-300 and maintain it safe under all conditions.
- Means to manually initiate Reactor Trip and ESF.
- Displays for indication of post-accident monitoring parameters.
- Means for diverse manual initiation of protective actions.
- Functional workstations for plant operations personnel.

[REDACTED], which provides a habitable environment for plant operators during all modes of operation, AOO and Design Basis Accidents (DBA). This is supported by the Main Control Room Habitability System (MCH)[1]. In the event of an accident, the MCR is designed to be utilised for Post-Accident Monitoring.

The MCR and RSF design is presented in the System Design Description for the Main Control Room and Ancillary Stations [54].

The SMR-300 will be operated from the MCR in accordance with Technical Specifications to ensure that the plant is operated within the limits and conditions of the safety case (described further within sub-chapter 9.5.2).

System-level controls within the MCR facilitate simple pump/valve lineup changes and procedure-based automation facilitates startup, shutdown, and mode changes, with operator hold points. Hyperlink-assisted navigation controls aid the operator to access the optimal display for performing the desired operation. Mitsubishi Electric Corporation (MELCO) supply the MCR I&C equipment which is similar to equipment used in NPPs in the US and internationally. There are three main I&C systems within the MCR:

- Plant Control System (PCS).
- Plant Safety System (PSS).
- Diverse Actuation System (DAS).

[1] Part A Chapter 2 [3] describes differences relating to the Heating, Ventilation, and Air Conditioning (HVAC) systems interfacing with the MCR due to ongoing development of the US design. For the purpose of GDA the MCH and Control Room Normal Ventilation System are still considered as independent systems, as system design descriptions have not yet matured to reflect any potential changes to the HVAC architecture.

9.4.1.1 Plant Control System

The PCS is the primary operator interface for normal and abnormal plant conditions, providing automatic and manual control of both safety and non-safety functions and components. The PCS presents information relating to prioritised alarms, task-oriented graphic control displays, and computer-based procedures.

The PCS provides displays of plant information and allows the operator to initiate plant control commands from Operational Visual Display Units (O-VDU) located on Operator Consoles within the MCR.

9.4.1.2 Plant Safety System

The PSS monitors all safety plant instrumentation, provides functionality for automatic and manual initiation for reactor trip and ESFs and supports accident monitoring. The PSS is accessed through a dedicated Safety Console situated in the MCR for each reactor unit. From the Safety Console, the Reactor Operator may monitor safety parameters, operate PSS components, and bring the plant to a safe shutdown condition should Operator Consoles be unavailable.

9.4.1.3 Diverse Actuation System

The SMR-300 non-safety DAS provides monitoring, control, and actuation of safety-related and non-safety systems and components required to cope with abnormal plant conditions concurrent with a common cause failure that disables all functions of the PSS.

Controlled from a dedicated Console for each reactor unit in the MCR, adjacent to the Safety Consoles. The DAS can be used to monitor safety instrumentation and control safety components to mitigate DBAs and achieve safe shutdown.

The DAS was originally proposed as a microprocessor technology based on a MELCO product which had similarities with the PSS, such that demonstrating adequate diversity could have proven difficult or impracticable.

A design challenge paper [55] was developed which presented options for a more diverse microprocessor-based DAS, a hardware-based DAS or retaining the existing DAS design. A US design decision paper [56] was then developed and approved to adopt a DAS design based on non-computerised simple hardware technology for the fleet design.

Part B Chapter 4 [7] includes GDA commitment C_C&I_082 for this design modification. Note that as part of the commitment 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.

9.4.2 MCR Layout

Consoles in the MCR provide the HSIs necessary for plant operation, serving as operator workstations, providing process systems indications as well as the controls required to position, run, or apply power to plant components. There is a Console for each on-duty MCR operator which is specialised, based upon their individual role and responsibilities. The layout of Consoles in the MCR is shown below in Figure 1 from the RAB general arrangement [57].

It is noted that finalisation of the layout of the MCR is still under development and will continue beyond GDA.

[REDACTED]

Figure 1: Main Control Room Layout

The primary workstation for the Reactor Operator, the Operator Console, is designed to be a single workstation through which both SMR-300 units may be monitored and controlled. As shown in Figure 1, an Operator Console is provided for each of the two reactor units (55), located side-by-side. A single Console is provided for the SRO (57), directly behind the two Operator Consoles and another Console is also provided directly behind the SRO Console for the STA (58). Consoles and screens are arranged so that the Reactor Operator can, without additional navigation, determine if a protective action has occurred, its completion status, and if a safety channel is inoperable or bypassed.

Key information is also displayed at the SRO and STA Consoles to provide monitoring capability only. The MCR is laid out to ensure that both SRO and STA can easily conduct Reactor Operator supervisory duties, view the status of key parameters and rapidly assess plant safety status.

Separate, dedicated Consoles are provided for interfacing with the PSS and the DAS. A single Safety Console is provided for each unit, located at either side of the Reactor Operator desks (56) containing the HSI for the PSS. The Safety Console is normally unmanned, serving as a backup workstation for the Reactor Operator in the event the Operator Console fails. Also usually unmanned, DAS Consoles (60) are also located adjacent to each Safety Console, serving as a backup in the event of a common cause failure of the PSS.

Auxiliary workstations are also present in the MCR which are not used for plant operation, but provide access to supporting functions within the HSI, such as screen customisation and configuration control. Workspace and equipment are also provided to support administrative tasks including furnishings, printers, and networked computers. Telephones, radios, and a public announcement system are also provided. Relevant workstations from Figure 1 include the following:

[REDACTED]

9.4.2.1 MCR Console Equipment Layout

The layout of equipment on the key MCR Consoles is shown below in Figure 2. The O-VDU are touchscreen monitors that enable operator control of plant components and monitoring of plant parameters from each Operator Console.

The O-VDU are the preferred operation HSI for all normal and abnormal plant conditions. The Safety VDUs (S-VDU) are provided only to accommodate a rare blackout of all non-safety O-VDUs, and the DAS-HSI (D-VDU) is provided only to accommodate a rare Common Cause Failure (CCF) of the PSS. The underlying I&C design is described within Part B Chapter 4 [7].

Two O-VDU monitors are located on each Operator Console, one for each unit, through which various graphical screens may be displayed for monitoring and control.

[REDACTED]

Figure 2: Layout of SMR-300 MCR Console Equipment

Two additional screens are also provided on each Operator Console. Procedures are presented electronically on a Procedure Visual Display Unit (P-VDU) and the status of alarms are presented on a separate Alarm Visual Display Unit (A-VDU). Each screen is integrally mounted on top of a desk section which, in addition to providing workspace for administrative tasks, also houses the cabling and electrical components necessary to power the Operator Console.

The Safety Console is comprised of desk modules with displays embedded in the riser sections. They consist of four spatially dedicated, continuously visible displays, touchscreen panels and two Manual Initiation Switches (MIS) for manual actuation of reactor trip, one for each safety division.

The DAS Console is comprised of a desk module with a single display, hardware and software which are diverse from the Safety Console and the PSS. All required PAM variables are accessible from MCR displays and are uniquely identified.

A LDP is also provided for each of the two units at the front of the MCR (62), positioned for maximum visibility for all personnel, presenting real-time plant data, key parameters and a plant diagram.

The MCR also contains four Master Transfer Switches (MXS) per SMR-300 unit, which are used to transfer plant control between the MCR and RSF.

9.4.3 Remote Shutdown Facility Design Description

The RSF is an alternative location from which both reactor units can be brought to both hot and cold shutdown in the event of the MCR being inaccessible. The facility contains Consoles and displays necessary for plant operation and all the plant indications which are normally accessible from the MCR, including those required to assess plant safety status and for post-accident monitoring. The following key functions are provided from the RSF:

- Provide means to bring the reactor to hot shutdown.
- Provide means to bring reactor to cold shutdown.
- Provide means to transfer plant control between the MCR and RSF.

The RSF is located on the same level of the RAB adjacent to the MCR in an area which is readily accessible from the MCR without placing undue burden upon or delaying reactor operators traversing between the two facilities.

Two fully equipped Operator Consoles are provided within the RSF for access to the PCS system, along with two Safety Consoles for interaction with the PSS. The RSF does not contain DAS Consoles or any associated HSI. The layout of the RSF and both Consoles will be configured in the same manner as their counterparts in the MCR.

The RSF also contains four MXS switches per SMR-300 unit which are used to transfer plant control between the MCR and RSF. To establish RSF control, two of the four MCR MXS switches must be pressed, disabling all MCR HSIs associated with the PSS, PCS, and DAS. Subsequently, two of the four RSF MXS switches are pressed to enable the RSF HSIs for the PSS and PCS within the RSF. The disable and initiate functions are interlocked, so the new location cannot be initiated prior to disabling the current location. Station transfer may be performed in either direction using this process, and the interlock is applied in both cases. During this transfer, the system will continue to function and log the status of the plant.

The RSF contains Consoles and displays necessary for plant operation. One fully equipped Console is provided for the Reactor Operator, and a separate Console provides direct interfacing with the PSS. Visual Display Units (VDU) at both Consoles are configured in the same manner as their counterparts in the MCR. The operator in the RSF has access to all plant indications which are normally accessible from the MCR, including those required to assess plant safety status and for post- accident monitoring.

9.4.4 Main Control Room and Remote Shutdown Facility Design Approach

Argument 2.3.1.1A-1: The design approach for the SSCs associated with the MCR and RSF is appropriate and supports delivery of relevant safety functions.

This sub-chapter identifies the relevant SSEC documents that describe the MCR and RSF design approach. The design approach for the MCR and RSF related SSCs is not considered to be different to any other plant area. The SSEC will derive safety requirements that the MCR and RSF design will be required to demonstrate. At the PSR stage, the design approach to the MCR and RSF is contained within the interfacing PSR chapters.

Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance [4] provides an overarching description of the SMR-300 design process. Signposting is also provided below for the interfacing chapters, where further detail on the design approach for each engineering discipline is provided:

- See Part B Chapter 1 Reactor Coolant System and Engineered Safety Features [58] for the design approach to the habitability related systems within and interfacing with the MCR and RSF.
- See Part B Chapter 4 [7] for the design approach to the I&C systems within and interfacing with the MCR and RSF. It includes GDA commitment C_C&I_082 for a design modification to the DAS. Note that as part of the commitment 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.
- See Part B Chapter 5 [8] for the design approach to the Heating, Ventilation, and Air Conditioning (HVAC) within and interfacing with the MCR and RSF.
- See Part B Chapter 6 [9] for the design approach to the electrical systems within and interfacing with the MCR and RSF.
- See Part B Chapter 10 [10] for designation of Radiologically Controlled Areas (RCA). A radiation zoning system shall be established to classify non-RCA and RCAs according to anticipated personnel occupancy and access restrictions in all areas of the station during normal conditions. The zoning system shall be used to implement radiation protection controls and to direct the movements of personnel or equipment and thereby for use to control personnel exposure. The MCR and RSF are expected to be non-RCAs.
- See Part B Chapter 12 [11] for demonstration of appropriate provisions for safe means of escape and provisions to enable firefighting activities within the RAB design, including the MCR and RSF.
- See Part B Chapter 14 Design Basis Analysis (Fault Studies) [15] for the Design Basis Accident Analysis (DBAA), which identifies safety functions to be performed by the MCR and RSF. The initial UK DBAA highlighted I&C architecture and diversity for design challenge, resulting in a design change to the DAS. This is discussed in sub-chapter 9.4.1.3.
- See Part B Chapter 17 [18] for the design approach to HF for those systems within and interfacing with the MCR and RSF.
- See Part B Chapter 20 [21] for the design approach to the civil structures which house and protect the MCR and RSF.

HF has a key interface with both the design process and associated safety analysis for the MCR and RSF. In addition, HFI is necessary to support the design of procedures and operating documentation, staffing decisions and training to ensure the MCR and RSF provides an appropriate means of managing operational activities.

The following documentation shows the hierarchy of requirements for the MCR and Ancillary Stations. The System Design Description for the MCR and Ancillary Stations defines the design requirements of the MCR and the Ancillary Stations. The System Specification for Monitoring and Operation describes the design basis of the safety and non-safety related HSI system.

- SMR-300 Top Level Plant Design Requirements (which includes both Holtec SMR-300 Objectives and Electric Power Research Institute (EPRI) requirements) [29].
- System Design Description for the Main Control Room and Ancillary Stations [54].
- System Specification for Monitoring and Operation [59].

HF input is required to demonstrate the suitability of workplaces (including the proposed layout of rooms and building footprint) to perform tasks. This will include the MCR and RSF footprint to ensure that the control rooms are sized correctly for the required number of operators.

In future revisions of this chapter, further information will be included under this argument to provide details of the overall MCR and RSF design and how an appropriate balance has been struck between any competing requirements as part of the integrated safety and design process, to ensure that overall design development of the MCR and RSF reduces risks to ALARP. This is likely to include further details on aspects such as:

- Decisions to share MCR and RSF facilities between two units.
- Decisions underpinning the size and layout of the MCR and RSF.
- Decisions around staffing arrangements following completion of the S&Q analysis (see sub-chapter 9.4.5.1).
- Decisions concerning the chosen metrication approach and impact on operational activities in the MCR and RSF. Metrication is discussed within Part A Chapter 2 [3].

It is also noted that Part A Chapter 5 [5] of this PSR considers the holistic risk-reduction process for the generic SMR-300. The process for the assessment of further risk reduction options is presented in Holtec's Design Management Process [60].

9.4.5 MCR and RSF Procedures and Staffing

Argument 2.3.1.1A-2: Operational procedures, staffing and training will ensure that the MCR and RSF is operated in accordance with the assumptions and requirements of the safety assessment.

This sub-chapter outlines that an appropriate approach is being used to develop operational arrangements (operating procedures, staffing and qualification requirements of plant personnel), to ensure activities conducted from the MCR and RSF can safely be carried out. This is supported by:

- Operating Philosophy Review [24].
- HFE PMP [25].

The SMR-300 will be operated from the MCR in accordance with Technical Specifications to ensure that the plant is operated within the limits and conditions of the safety case.

Development of operating documentation and Technical Specifications is addressed further in Claim 2.3.1.2.

The systematic S&Q analysis generated as part of the HFE PMP [25] is described in sub-chapter 9.4.5.1. The first iteration of the S&Q review, which will include a summary of key roles and responsibilities for SMR-300, will be available towards the end of 2025 to support the NRC Construction Permit Application (CPA) to the NRC. This will coincide with the end of GDA Step 2 and be complete prior to the beginning of the Pre-Construction Site Specific SSEC (PC-SS-SSEC) produced in the UK. This will support the demonstration that staffing and training will ensure that the MCR and RSF is operated in accordance with the assumptions and requirements of the safety assessment. This is considered to be an appropriate maturity for a PSR.

9.4.5.1 Staffing and Qualification

Information available relating to staffing levels for the SMR-300 focuses predominantly on licensed operators located in the MCR at GDA. The staffing levels are identified in the Operating Philosophy Review [26].

The SMR-300 MCR is designed to accommodate NRC regulations for the minimum number of operators expected within a single control room for a multi-unit reactor, outlined in 10 CFR 50.54 [37]. However, the SMR-300 design philosophy emphasises automation, intuitive controls to reduce operator burden and the use of passive safety features to reduce reliance on the operator. It is therefore expected that a corresponding decrease in overall workload will be achieved, and that minimum staffing can be reduced.

[REDACTED]

The first iteration of the S&Q review, which will include a summary of key roles and responsibilities for SMR-300, will be available towards the end of 2025 to support the CPA to the NRC. This will coincide with the end of GDA Step 2 and be complete prior to the beginning of the PC-SS-SSEC produced in the UK.

The staffing and qualification requirements for other plant personnel will be defined and demonstrated fully in the nuclear site licensing phase in accordance with LCs 10 [61], 12 [62] and 36 [63] by the licensee.

9.4.6 MCR and RSF Hazard Tolerance

Argument 2.3.1.1A-3: Hazards and faults with the potential to impact the SSCs located in the MCR and RSF are identified and safety functions are appropriately incorporated in the design.

The safety analysis approach for the MCR and RSF is not considered to be different to any other plant area. A UK DBAA will be undertaken within Part B Chapters 14 (Fault Studies), 21 (External Hazards) and 22 (Internal Hazards). This will define the full set of SSEC safety functional requirements. The safety functions identified from the UK DBAA will be used to inform the MCR and RSF design development during detailed design. Part B Chapter 17 (Human Factors) presents the approach and analysis that will ultimately demonstrate that where measures to protect SSCs located in the MCR and RSF are human based, any human actions can be appropriately carried out.

This sub-chapter provides cross referencing to the relevant interfacing chapters that will ultimately demonstrate the MCR and RSF hazard tolerance, to demonstrate that the hazards and faults with the potential to impact the SSCs located in the MCR and RSF are identified and safety functions to protect and mitigate these are incorporated in the design (noting that at PSR stage the maturity of any evidence is limited). This is supported by:

- Part B Chapter 14 Design Basis Analysis (Fault Studies) [15].
- Part B Chapter 21 External Hazards [64].
- Part B Chapter 22 Internal Hazards [32].
- Part B Chapter 17 Human Factors [18].

Part B Chapter 14 Design Basis Analysis (Fault Studies) [15] provides the approach and analysis that will ultimately demonstrate that the MCR and RSF will remain available in the event of relevant faults. If required, safety functions for hazard tolerance will be identified. A summary of this analysis will be provided upon completion of the UK DBAA; however, it is anticipated that all hazards with the potential to impact the SSCs within the MCR and RSF will be assessed within Part B Chapters 21 and 22 for external and internal hazards. These are described further below.

Part B Chapter 21 External Hazards [64] identifies the fundamental derived acceptance criteria which are inherent within the generic SMR-300 design for design basis and beyond design basis external hazards within the development of the GDA Reference Design. It presents the approach and analysis that will be undertaken in support of deployment of the generic SMR-300 on a generic site. This will identify all relevant safety functional requirements on SSCs in the MCR and RSF to ensure that they remain available, to mitigate the consequences of external hazards (including combinations of hazards and extreme external hazards).

See Part B Chapter 22 Internal Hazards [32] for the approach and analysis to demonstrate that SSCs in the MCR and RSF remain available, to prevent or mitigate the consequences of internal hazards. This is in support of an argument that the individual building/area/room assessments for Internal Hazards support the claim that the plant can reach a safe shutdown state for all Internal Hazard Design Basis Events (DBE). Work is planned beyond PSR on a MCR Internal Hazards Assessment.

Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance [4] provides an overarching description of the generic SMR-300 design process. Any need for greater substantiation against UK DBAA requirements will be subject to the process for the assessment of further risk reduction options presented in Holtec's Design Management Process [60]. The ALARP Design Process [65] provides further detail of how the current US design process interfaces with the requirement to demonstrate compliance with the ALARP principle and highlights options to strengthen this interface. Further details will be set out in the UK GDA project quality arrangements, provided as part of the submission.

Future versions of this chapter will present the key ALARP considerations and/or design decisions for the MCR and RSF to demonstrate that the MCR and RSF will be suitably justified to reduce risks to ALARP. These will ultimately reside within the relevant engineering chapters that are cross referenced from this chapter.

9.4.7 MCR and RSF Habitability

Argument 2.3.1.1A-4: Impacts to the habitability of the MCR and RSF are identified, and safety measures are in place to ensure habitability is maintained.

The Control Room Normal Ventilation System (CRV) provides supply and extract ventilation to the MCR during all modes of operation. Continuous positive pressure is maintained to prevent entry of contaminated, un-conditioned and un-filtered air.

The MCH is designed to provide adequate radiation protection for 72 hours following the Maximum Hypothetical Accident (MHA) Loss-of-Coolant Accident (LOCA) and provide instrumentation and control to maintain the plant in a safe condition under accident conditions [66]. The MCH is made up of individual systems that create an environment that is safe and comfortable for human occupancy, allowing required operations to continue during both normal and abnormal conditions.

This sub-chapter provides an overview of the habitability of the MCR, that it will be ensured for all required faults and hazards, and transfer to the RSF is available should the MCR become uninhabitable (e.g. in the event of fire within the MCR). Signposting is also provided below for the interfacing chapters, where further detail is provided (noting that at PSR stage the maturity of any evidence is limited).

See Part B Chapter 1 Reactor Coolant System and Engineered Safety Features [58] for the MCH which provides an environment that is safe and comfortable for human occupancy in the MCR by maintaining temperature, pressure, and humidity in the MCR.

Part B Chapter 5 [8] describes the HVAC design interfacing with the MCR and RSF. The SMR-300 design is based upon the principle of a passive design which does not rely on active HVAC to ensure cooling in fault conditions. A GDA commitment (C_Mech_028) has been raised in Part B Chapter 19 [20] to ensure that the HVAC design interfacing with the MCR and RSF supports the SSEC requirements and meets UK RGP.

Part B Chapter 14 Design Basis Analysis (Fault Studies) [15] provides the approach and analysis that will ultimately demonstrate that the MCR and RSF will remain available in the event of relevant faults. A summary of this analysis will be provided upon completion of the UK DBAA. The initial UK DBAA was performed for the PSR scope, no reactor faults have placed cooling related safety functions on the HVAC systems for mitigation. A GDA commitment (C_Faul_103) has been raised in Part B Chapter 14 [15], to complete the UK DBAA and ensure a holistic and comprehensive safety assessment to appropriately address UK expectations.

It is anticipated that all hazards affecting the habitability of the MCR and RSF will be assessed within Part B Chapters 21 and 22 for external and internal hazards, and habitability in the event of a radiological release in Part B Chapter 10. These are described further below.

- Part B Chapter 21 External Hazards [64] identifies the fundamental derived acceptance criteria which are inherent within the generic SMR-300 design for design basis and beyond design basis External Hazards within the development of the GDA Reference Design. It presents the approach and analysis that will be undertaken in support of the deployment of the generic SMR-300 on a generic site. This will identify all relevant safety functional requirements on the MCR and RSF to remain habitable following external hazards (for example, seismic), including combinations of hazards and extreme external hazards.

- Part B Chapter 22 Internal Hazards [32] for the approach and analysis to demonstrate that SSCs in the MCR and RSF remain available, to prevent or mitigate the consequences of internal hazards (for example, extreme heat). This is in support of an argument that the individual building/area/room assessments for Internal Hazards support the claim that the plant can reach a safe shutdown state for all Internal Hazard DBEs. Work is planned beyond PSR on a MCR Internal Hazards Assessment to support the demonstration that the MCR and RSF will remain available in the event of relevant internal hazards.
- See Part B Chapter 10 Radiological Protection [10] for the approach and analysis to demonstrate that the MCR and RSF is not rendered uninhabitable in the event of radiological releases following an accident.

Part B Chapter 15 Beyond Design Basis and Severe Accident Analysis, and Emergency Preparedness [16] will ultimately present the approach and analysis to demonstrate that the MCR and RSF will remain available in the event of severe accidents and identify where transfer to the RSF will occur, should the MCR become uninhabitable. This will be part of the overall accident management and emergency preparedness development for the generic SMR-300.

The SSEC will identify the full set of habitability requirements that the MCR and RSF will be required to deliver to enable safe operation of the generic SMR-300. Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance [4] provides an overarching description of the generic SMR-300 design process. Any potential design improvements identified against habitability requirements will be subject to the process for the assessment of further risk reduction options presented in Holtec's Design Management Procedure [60]. The ALARP Design Process [65] provides further detail of how the current US design process interfaces with the requirement to demonstrate compliance with the ALARP principle and highlights options to strengthen this interface. Further details will be set out in the UK GDA project quality arrangements, provided as part of the submission.

Future versions of this chapter will present the key ALARP considerations and/or design decisions for the MCR and RSF to demonstrate that the habitability of the MCR and RSF will be suitably justified to reduce risks to ALARP. These will ultimately reside within the relevant engineering chapters that are cross referenced from this chapter. This is supported by:

- Part B Chapter 14 Design Basis Analysis (Fault Studies) [15].
- Part B Chapter 21 External Hazards [64].
- Part B Chapter 22 Internal Hazards [32].
- Part B Chapter 1 Reactor Coolant System and Engineered Safety Features [58].
- System Design Description for Main Control Room Habitability System [67].
- Part B Chapter 10 Radiological Protection [10].
- Part B Chapter 15 Beyond Design Basis and Severe Accident Analysis, and Emergency Preparedness [16].

9.4.8 CAE Summary

A fundamental design philosophy of the SMR-300 is to minimise human actions and once passive features are initiated, to require a very low level of human intervention.

The design approach for the MCR and RSF related SSCs is not considered to be different to any other plant area. The SSEC will derive safety requirements that the MCR and RSF design will be required to demonstrate. At the PSR stage, the design approach to the MCR and RSF is contained within the identified interfacing PSR chapters. Future revisions of this chapter will include a summary of the key design aspects of SSCs within the MCR and RSF. The initial UK DBAA [15] highlighted I&C architecture and diversity for design challenge, resulting in a DAS design modification. Note that as part of the commitment 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. This demonstrates the integrated design and safety approach. This is identified as a GDA commitment in Part B Chapter 4 [7].

The SMR-300 will be operated from the MCR in accordance with Technical Specifications to ensure that the plant is operated within the limits and conditions of the safety case.

The first iteration of the S&Q review, which will include a summary of key roles and responsibilities for SMR-300, will be available towards the end of 2025 to support the NRC CPA to the NRC. This will coincide with the end of GDA Step 2 and be complete prior to the beginning of the PC-SS-SSEC produced in the UK. This will support the demonstration that staffing and training will ensure that the MCR and RSF is operated in accordance with the assumptions and requirements of the safety assessment. This is considered to be an appropriate maturity for a PSR.

The safety analysis approach for the MCR and RSF is not considered to be different to any other plant area. A UK DBAA will be undertaken within Part B Chapters 14 (Fault Studies), 21 (External Hazards) and 22 (Internal Hazards). This will define the full set of SSEC safety functional requirements, including habitability requirements. Any need for greater substantiation against UK DBAA requirements will be subject to the process for the assessment of further risk reduction options presented in Holtec's Design Management Process [60] during detailed design post-GDA. The initial UK DBAA has been performed at PSR and for the identified scope, no reactor faults have placed cooling related safety functions on the HVAC systems for mitigation. A GDA commitment (C_Faul_103) has been raised in Part B Chapter 14 [15] to complete the UK DBAA and ensure a holistic and comprehensive safety assessment to appropriately address UK expectations. A GDA commitment has been raised in Part B Chapter 5 [8] to ensure that the HVAC design interfacing with the MCR and RSF supports the SSEC requirements and meets UK RGP.

Future versions of this chapter will present the key ALARP considerations and/or design decisions for the MCR and RSF to demonstrate that the MCR and RSF will be suitably justified to reduce risks to ALARP.

9.5 OPERATING DOCUMENTATION

Claim 2.3.1.2: The limits and conditions of the safety case are clearly identified and will be incorporated into operational documentation.

Claim 2.3.1.2 has been decomposed into 2 arguments to address the derivation OR (limits and conditions) within the SSEC in accordance with RGP, and to support the nuclear site licensing phase to inform the production of operating documentation in the form of Technical Specifications.

9.5.1 Operating Limits and Conditions

Argument 2.3.1.2A-1: The SSEC will enable the derivation of ORs (limits and conditions) during the nuclear site licensing phase to inform the production of the Technical Specifications.

Once a site has been chosen for the first UK generic SMR-300, a site-specific SMR-300 design and PC-SS-SSEC will be developed which will meet the specific site characteristics. It is envisaged that this will be concurrent with the development of the licensee organisation who will take responsibility for and lead the delivery of the SSEC, with Holtec providing support as designer.

The safety management during the operation of the plant will be the responsibility of the licensee within the operating organisation. Operating limits and conditions are required to ensure the plant is operated safely at all times. Implementation of these limits and conditions on a Nuclear Licensed Site is captured by procedural arrangements responding to the 36 standard LCs that are attached to every Nuclear Site Licence (NSL).

The operational limits and conditions defining normal operations should be derived from the SSEC and are OR for the purposes of compliance with LC 23. There are many other detailed requirements applying to nuclear sites, but these are not directly relevant to the GDA process. During GDA, the safety case ownership role rests with the Requesting Party.

ORs link the safety case analysis and assumptions with actual operational limits and conditions in force at the facility. The SSEC will enable the derivation of ORs (limits and conditions) in accordance with ONR TAG-35 [49] during the nuclear site licensing phase, resulting in operating limits and conditions, to inform the production of the Technical Specifications for the purposes of compliance with LC 23. The SSEC will be expected to be developed beyond this GDA to determine the ORs required for safe operation that form the operating envelope for the generic SMR-300.

The completed PC-SS-SSEC will reflect the completed detailed design and agreed operational approach required by the licensee and provide a robust substantiation of the claims underpinned by a CAE trail. The fault assessment will be demonstrably fully comprehensive, with a clear definition of the limits and conditions and engineered and operational safety measures required to ensure safety during normal, abnormal and design basis conditions. DiD provisions, including the emergency arrangements, will be adequately mature so there is confidence these can be reliably implemented. Operating limits and conditions are subject to plant-specific development and on-going maintenance throughout the whole plant lifetime. The whole set of the operating documentation relies on the design requirements and the licensee's experience and practice and will be finalised in the nuclear site licensing phase.

Assumptions and other parts of the safety case, such as Severe Accident Analysis, are also sources that will inform the definition of ORs. The development of the SSEC beyond the GDA stage will inform the development of these ORs.

The Holtec SMR-300 GDA Through-Life Safety, Security and Environmental Case Strategy [68] presents a staged SSEC development strategy where each stage of the SSEC development builds on information from the previous stage and looks forward to subsequent stages. This is broadly consistent with the staged approach to safety case submissions within ONR TAG-051 [69].

The completed PC-SS-SSEC will reflect the completed detailed design and agreed operational approach required by the licensee and provide a robust substantiation of the claims underpinned by a CAE trail. The fault assessment will be demonstrably fully comprehensive, with a clear definition of the limits and conditions and engineered and operational safety measures required to ensure safety during normal, abnormal and design basis conditions. DiD provisions, including the emergency arrangements, will be adequately mature so there is confidence these can be reliably implemented.

This sub-chapter outlines the derivation of OR within the SSEC to enable and inform the production of the Technical Specifications for the purpose of demonstrating compliance with LC 23, ensuring the plant is safely operated at all times. This will be done during the nuclear site licensing phase. At the GDA stage, this is by providing references to where certain types of limits and conditions will ultimately be presented across the SSEC. The SSEC will identify limits and conditions in the following areas:

- Part B Chapter 10 Radiological Protection [10] will define the limits and conditions derived from RP analysis (e.g. zoning, restriction of access).
- Design Basis Analysis (Fault Studies), Internal and External Hazards (Part B Chapters 14 [15], 21 [64] and 22 [32]) will determine the limits of normal operation, the safe envelope of operation, safety settings, design basis limits and (in conjunction with the engineering analysis) safety limits. They will also inform the required availability of safety measures; and provide significant insight against the expectations of the DiD framework. Part B Chapter 14 [15] identifies candidate ORs linked to faults with unmitigated radiological consequences that exceed 20 mSv to a worker (on site), or 1 mSv to the public (off-site) for the faults assessed within the initial UK DBAA. A GDA commitment (C_Faul_103) has been raised in Part B Chapter 14 [15] to complete the UK DBAA beyond GDA Step 2.
- Part B Chapter 15 Beyond Design Basis and Severe Accident Analysis, and Emergency Preparedness [16] will derive limits and conditions required by the Beyond Design Basis and Severe Accident Analysis.
- Engineering substantiation of ESFs (Part B Chapters 1 [58], 2 [6], 4 [7], 5 [8], 6 [9], 13 [14]) will inform the determination of the limits of normal operation and the safe envelope of operation, provide limits on operation to prevent fault initiation or escalation; ensure design assumptions and intent are met; set conditions on appropriate plant and equipment configurations; specify the timing of maintenance and testing activities; cater for plant ageing and corrosion effects; and set ORs relating to

equipment qualification. Part B Chapter 18 [19] will identify limits and conditions associated with structural integrity requirements.

- Part B Chapter 23 [22] will derive limits and conditions from chemistry studies (e.g. chemical Technical Specifications). Preliminary chemistry limits and conditions have been defined at PSR (informed by what are likely to be control parameters for SMR-300).
- Part B Chapter 16 Probabilistic Safety Assessment [17] will inform EIMT related ORs and proof testing intervals, and also determining ORs governing the availability of safety measures for deriving time-based ORs, those relating to allowed substitution periods and the unavailability of safety measures, so that any periods of elevated risk may be suitably justified by the licensee and be a key input to holistic reviews of ORs.

9.5.2 Operating Procedures

Argument 2.3.1.2A-2: Operating procedures will be developed during the nuclear site licensing phase utilising the limits and conditions derived by the SSEC.

Operating procedures are important to plant safety. They support and guide personnel to interact with plant systems and respond to plant-related events under different conditions. These procedures form an essential part of the administrative safety measures. Modern power stations adopt a Technical Specification approach to ORs, whereby limits and conditions include specific time periods so that non-compliance is only deemed to have occurred when the limit has been exceeded for longer than a prescribed time, or on a specific number of times within a given time period.

Technical Specifications for the US Reference SMR-300 Plant CPA will be developed in accordance with 10 CFR 50.34(a)(5) [28]. Technical Specifications do not need to be fully developed in accordance with 10 CFR 50.36 until the OLA.

The SMR-300 Technical Specifications produced in support of the OLA can be used to inform the development of operating documentation by the licensee in accordance with LCs 23 [43], 24 [44] and 25 [45] during the nuclear site licensing phase. The Technical Specifications for the generic SMR-300 will be based upon the limits and conditions derived by the PC-SS-SSEC, as described in sub-chapter 9.5.1. The PC-SS-SSEC will include information on how operational philosophies will inform procedural development, particularly when details of the future duty holder/licensee arrangements are known.

9.5.3 CAE Summary

The SSEC will enable the derivation of ORs (limits and conditions) in accordance with ONR TAG-35 [49] during the nuclear site licensing phase. A site-specific SMR-300 design and PC-SS-SSEC will be developed which will reflect the completed detailed design and agreed operational approach required by the licensee, with a clear definition of the limits and conditions required to ensure safety during normal, abnormal and design basis conditions. DiD provisions, including the emergency arrangements, will be adequately mature so there is confidence these can be reliably implemented.

Operating procedures will be developed during the nuclear site licensing phase utilising the limits and conditions derived by the SSEC and is the responsibility of the licensee. The Technical Specifications for the generic SMR-300 will be based upon the limits and conditions derived by the PC-SS-SSEC. The PC-SS-SSEC will include information on how operational philosophies will inform procedural development, particularly when details of the future duty holder/licensee arrangements are known.

Technical Specifications will be developed for the US Reference SMR-300 CPA in accordance with 10 CFR 50.34(a)(5) [28]. Technical Specifications do not need to be fully developed in accordance with 10 CFR 50.36 until the OLA. The SMR-300 Technical Specifications produced in support of the OLA can be used to inform the development of operating documentation by the licensee in accordance with LCs 23 [43], 24 [44] and 25 [45] during the nuclear site licensing phase.

9.6 EXAMINATION, INSPECTION, MAINTENANCE AND TESTING

Claim 2.3.1.3: Examination, Inspection, Maintenance and Testing (EIMT) activities are identified to ensure the SSCs continue to achieve their safety functional requirements throughout operational life.

EIMT is required to maintain the availability of SSCs during the service life by monitoring degradation with the aim of minimising or preventing failures. If failures do occur, maintenance activities shall be conducted to restore the capability of failed SSC to their required functionality.

The generic SMR-300 is designed so that the need for maintenance is minimised. For example, the pressuriser design eliminates the need for power-operated relief valves, reducing the chances of RCS leakage and meaning there is no need for maintenance of these valves. However, it is important that preventative and corrective measures are put in place to detect and mitigate the degradation of functioning SSCs or to restore a failed SSC to an acceptable level of performance. This means mechanisms to specify and plan appropriate measures, and enabling measures being in place for accessing SSCs (e.g., hatches, ladders etc.) to allow maintenance activities to be carried out when required.

The SMR-300 and its design management arrangements have been developed to ensure that effective EIMT will be delivered, ensuring that appropriate activities to support EIMT are included, that the schedule for these activities is appropriate for SSCs to continue to deliver their design basis, that there is sufficient space to conduct these activities, and that the inspection methods incorporated can identify degradation of SMR-300 SSCs.

These features of the SMR-300 combine to ensure that the EIMT regime used is fit for purpose and ensures that SMR-300 safety features continue to deliver plant safety.

These aspects are undertaken by the licensee during the nuclear site licensing phase.

The EIMT programme will be delivered by suitably qualified staff, which will be ensured by Quality Assurance (QA) processes that are beyond the scope of fundamental assessment. For this reason, the training, qualification and QA processes related to human actions supporting the EIMT programme are not explored in PSR Revision 1.

This sub-chapter outlines the EIMT activities, planning and arrangements that are relevant for the generic SMR-300 at the GDA stage. It is important to ensure that the following is defined to ensure that the SSCs continue to achieve their safety functional requirements throughout the operational life:

- That the approach to EIMT is embedded within the design process to ensure that it can be conducted, as required.
- That EIMT requirements are identified by the SSEC, taking due consideration of design life, reliability, ageing and degradation.

Claim 2.3.1.3 has been decomposed into four arguments. EIMT in design development is considered in the first two arguments, for the identification of EIMT requirements and inclusion within the maintenance schedule (see sub-chapter 9.6.1), and that there is sufficient space provision within the generic SMR-300 plant arrangement such that EIMT can be conducted (see sub-chapter 9.6.2). EIMT in operations is considered in the second two arguments, regarding the appropriate scheduling of maintenance, that EIMT will be optimised such that it will be scheduled to identify degradation sufficiently early (see sub-chapter 9.6.3), and that appropriate inspection methods will be provisioned to adequately identify degradation of SSCs (see sub-chapter 9.6.4).

9.6.1 Identification of EIMT Requirements

Argument 2.3.1.3A-1: Appropriate operational activities have been incorporated into the maintenance schedule of the plant to support the EIMT programme.

This sub-chapter summarises the processes and planned work to ensure that EIMT requirements will be identified and incorporated into the operating schedule of the generic SMR-300. As part of the development of the SMR-300, there are several routes by which EIMT requirements are incorporated into the operating schedule of the plant. These are described further in sub-chapters 9.6.1.1 to 9.6.1.4.

The extensive Operating Experience (OPEX) and RGP associated with Pressurised LWRs have shaped the development of American Society of Mechanical Engineers (ASME) design codes, NRC regulations, and EPRI guidance. As these standards underpin the SMR-300 design requirements, there is confidence that the design processes and associated management arrangements will identify the appropriate operational activities within the maintenance schedule to support the EIMT programme. The ASME design codes, NRC regulations and EPRI guidance also gives confidence that the SMR-300 design will adequately account for key degradation and ageing mechanisms.

This is supported by:

- SMR-300 Design Standard for Grouping and Separation [70].
- SMR-300 System Design Project Plan [71].
- Outage Strategy for SMR-300 [31].

While the approach to degradation and ageing is generally sufficient for a two-step GDA, it highlights a difference in regulatory expectations between the US and the UK.

Additional work may be required after the GDA phase, in parallel with the development of the UK-specific DBAA (fault studies and hazard assessments) (see Part B Chapter 14 [15]). This work would focus on further evaluating degradation and ageing mechanisms to ensure that all relevant factors are adequately captured to support general substantiation. Particular attention will be needed for novel aspects of the SMR-300 design that are important to safety, such as the use of an Annular Reservoir (AR), which may not be fully addressed by existing OPEX and RGP for Pressurised LWRs. Furthermore, certain UK policy requirements related to higher reliability components (see Part B Chapter 18 [19]) will necessitate a more systematic demonstration of how degradation and ageing are managed. This includes using appropriate techniques for both Pre-Service and In-Service Inspection in accordance with UK RGP.

GDA commitment C_MSQA_109 is identified in Part A Chapter 4 [4] to develop an ageing and degradation strategy to verify SMR-300 arrangements and activities for degradation management in the UK context. Target for resolution: Issue of Long Lead Item and SSC procurement specification.

9.6.1.1 OPEX Presented in Formal Guidance

Requirements from guidance produced by the US NRC and EPRI, such as the Guideline for the Management of Materials Issues [72] and the Steam Generator Program Guidelines [73] are incorporated into SSC designs, including requirements on operating and maintenance cycles.

These requirements are represented by SMR Design Standards, including the SMR Design Standard for Grouping and Separation [70].

9.6.1.2 OPEX Incorporated into SSC Specifications

As per the SMR-300 System Design Project Plan [71] as the design of SSCs progresses, Holtec will gather input from suppliers on various aspects, including system maintenance schedule requirements. Maintenance requirements for significant SSCs inform the Outage Strategy for SMR-300 [31], and detailed in maintenance plans.

9.6.1.3 Outage Strategy

The Outage Strategy for SMR-300 [31] documents the high-level plant outage execution strategy, including maintenance schedules, maintenance activity schedules, lifting and handling routes, lifting and handling equipment.

Insights from previous design reviews and operational experiences are utilised to shape outage strategy. The document compiles observations, design impacts, and recommended changes for various components (e.g., heat exchangers, pumps, and integrated head assemblies) to enhance safety, ease maintenance, and ensure efficient outage execution.

Detailed tables list maintenance periodicities for major components over a 15-year period (across 10 outages). This planning ensures that inspection and maintenance activities are integrated into the outage schedule without significantly impacting the overall project timeline.

The strategy provides a structured approach to managing refuelling outages by combining detailed sequencing and lessons learned from operational experience to ensure minimal outage duration and optimised equipment reliability.

9.6.1.4 US and UK Regulatory Expectation Differences

For the US context, EIMT is intrinsically embedded into the design procedure, and most of the pre-cursor work to inform this (degradation and ageing mechanisms, derivation from nuclear safety classifications etc.) is captured in the prescriptive requirements and design features that the design adopts. Therefore, the demonstration of how the fundamental mechanism and how EIMT is provisioned to address them would not be obvious when viewed from the UK regulatory context.

The methodology used to identify ageing and degradation mechanism inputs, ultimately shaping EIMT activity, differs from UK practice. The US context depends upon, and takes credit from, the prescriptive requirements of NRC guidance, compliance with relevant design codes (primarily ASME Subsection XI [74]), and the incorporation of elements from the EPRI Utility Requirements Document (URD) to inform how SSCs are designed and thus what mechanisms are captured in the SMR-300 requirements.

This is generally an implicitly integrated step within the design management process rather than underpinned by a stand-alone strategy. These represent the best source of RGP due the large amount of OPEX that this guidance is formulated upon. Holtec International is also an active member of the Nuclear Energy Institute (NEI) embedding a proactive industry led management of degradation issues. Because of the embedment of RGP into requirements, it is likely that the majority (if not all) of the appropriate considerations will be captured, upon which through-life management will be built upon.

An example of this is detailed in Part B Chapter 23 [22] that illustrates the cascade from RGP sources to ensure a culture of recognising and managing degradation.

In the UK, there is an expectation that ageing and degradation has been systematically understood, particular to the design, and therefore the resultant management activities and decisions in the design can be shown to specifically manage these mechanisms (concurrent with considerations like material and environmental choices).

The extensive OPEX and RGP associated with Pressurised LWRs have shaped the development of ASME design codes, NRC regulations, and EPRI guidance. As these standards underpin the SMR-300 design requirements, there is confidence that the design processes and associated management arrangements adequately account for key degradation and ageing mechanisms. While this approach is generally sufficient for a two-step GDA, it highlights a difference in regulatory expectations between the US and the UK.

Additional work may be required after the GDA phase, in parallel with the development of the UK-specific DBAA (fault studies and hazard assessments) (see Part B Chapter 14 [15]). This work would focus on further evaluating degradation and ageing mechanisms to ensure that all relevant factors are adequately captured to support general substantiation. Particular attention will be needed for novel aspects of the SMR-300 design that are important to safety, such as the use of an AR, which may not be fully addressed by existing OPEX and RGP for Pressurised LWRs. Furthermore, certain UK policy requirements related to higher reliability components (see Part B Chapter 18 [19]) will necessitate a more systematic demonstration of how degradation and ageing are managed. This includes using appropriate techniques for both Pre-Service and In-Service Inspection in accordance with UK RGP.

GDA commitment C_MSQA_109 is identified in Part A Chapter 4 [4] to develop an ageing and degradation strategy to verify SMR-300 arrangements and activities for degradation management in the UK context. Target for resolution: Issue of Long Lead Item and SSC procurement specification.

9.6.2 Design for EIMT Access

Argument 2.3.1.3A-2: The plant arrangement allocates sufficient space to enable the EIMT programme and reduce risks ALARP.

Several processes and standards within Holtec International govern and ensure that space is allocated in the design of the plant to achieve a considered balance of optimisation factoring in EIMT and other topics and limitations. Constructability, Operability, Maintainability and Safety (COMS) reviews undertaken in detailed design will provide the formal inter-disciplinary optioneering of the layout, which will ensure adequate provision for EIMT access, such that the required EIMT can be undertaken on the relevant SSCs. This is supported by:

- SMR-300 Top Level Plant Requirements [29].
- Design Standard for Human Factors: Maintenance, Inspection and Testing [75].
- SMR-300 Design Configuration Control [76].
- SMR-300 SmartPlant Standards [77].
- SMR-300 System Design Project Plan [71].

Space allocation is an ongoing task through the SMR-300 development. Part A Chapter 2 [3] describes how the key design requirements have influenced the high level architecture of the SMR-300 plant layout, identifying some key examples, and the processes and design considerations that will influence the continuous development of the plant layout beyond GDA through detailed design.

Several processes and standards within Holtec International govern and ensure that space is allocated in the design of the plant to achieve a considered balance of optimisation factoring in EIMT and other topics and limitations:

- SMR-300 Top Level Plant Requirements [29], for example the provision of adequate access space for maintenance, testing, operation, and component removal or replacement necessary to achieve plant design life is a specific design requirement.
- HF guidance as set out in SMR-160 Design Standard for Human Factors: Maintenance, Inspection and Testing [75]. These HF design standards then inform the requirements to produce the relevant general arrangement drawings by the civil engineering team.
- SMR-300 Design Configuration Control [76].
- SMR-300 SmartPlant Standards [77].
- Interdisciplinary SSC Design Reviews, as discussed in the SMR-300 System Design Project Plan [71].
    - These are recorded in the supporting documents related to SSCs, such as specifications and System Design Descriptions (SDD).
- Currently envisioned for detailed design (SMR-300 System Design Project Plan [71]), after the initial isometrics etc. are produced (i.e., at Revision 0).
    - Stress analysis work will be conducted, which will then incorporate new layout changes due to flexibility calculations, pipe supports and other design developments.
    - After this process, COMS reviews provide the formal inter-disciplinary optioneering of the layout.
- The Outage Strategy [31] provides analysis on operations required for EIMT and refuelling. Lifting paths, laydown space allocation, capturing access requirements and work sequencing. While operations and EIMT feedback is already considered in the Nuclear Quality Assurance (NQA-1) design process, the outputs from the Outage Strategy will further inform detailed design as maintenance requirements are assessed in greater detail, and provide requirements, recommendations and optimisations for the SMR-300 layout.
- SSC specifications and engagement with equipment suppliers identifies spatial requirements for EIMT. Examples of these requirements include maintenance access space, equipment laydown area and equipment handling space.

The Holtec CDM Strategy [12] sets out a series of actions that are foreseen to be necessary in readiness for the design phases to ensure UK health and safety compliance. The Safety Management System Report [13] sets out how these will be implemented. These actions are related to bringing Holtec's health and safety arrangements and the SMR-300's design processes in line with UK requirements. Holtec are currently undergoing early-stage collaboration to explore how this may be implemented in readiness for the design phases. This will contribute to the Design Safety Management Plan, set out in the Safety Management System Report [13]. This is discussed in greater detail in Part B Chapter 12 [11].

SMR-300 design control is described in further detail in Part A Chapter 4 Lifecycle Management [4], which includes layout consideration and additional interim design reviews, including COMS reviews, which may be convened if identified in the Design Quality Plans (including HF assessments). Application of this in the design phase and throughout the SMR-300's lifecycle will ensure that sufficient and safe space and access is allocated to enable EIMT. Other conventional safety risks related to EIMT will be eliminated or reduced, So Far As Is Reasonably Practicable (SFAIRP). This will be captured through design risk reviews considering the lifecycle of SSCs.

9.6.3 EIMT Scheduling

Argument 2.3.1.3A-3: EIMT activities are scheduled and managed to identify degradation sufficiently early for risk control measures to be implemented (i.e., protection and mitigation measures).

This sub-chapter identifies that processes are in place to capture the detailed EIMT requirements and ensure that the scheduling of EIMT will be optimised to identify degradation sufficiently early for risk control measures to be implemented. This will develop as the design evolves beyond GDA, through detailed design and into the Licensing process, and is supported by:

- Outage Strategy for SMR-300 [31].
- SMR-300 System Design Project Plan [71].

The Outage Strategy for SMR-300 [31] identifies major EIMT activity schedules, including inspection of major equipment. The schedule is produced using OPEX (including EPRI guidance) and SSC supplier guidance, as outlined in the design processes outlined in this sub-chapter. The inspection activities are regular and provide indication of degradation and can be actioned by protection and mitigation where degradation is found. The outage strategy captures much of the periodicity plans for major SSCs, as the main starting point to optimise EIMT as development progresses.

The development of SSCs and their specifications includes producing maintenance manuals which will be used to inform more detailed interim maintenance schedules.

The frequency of inspection to manage ageing and degradation is determined in different ways depending on the component and degradation mechanisms. Ageing Management is primarily identified and managed through compliance with ASME Boiler and Pressure Vessel Code Section III and XI requirements. Other sources include Generic Ageing Lessons Learned for Subsequent Licence Renewal (GALL-SLR) Report, NUREG-2191 Volumes 1 and 2 [78] and EPRI sources which are captured in SSC requirements. It is an expectation in the US that prospective licensees consider the design implications of needing to comply with ageing management programmes beyond the initial licensing period of 40 years. In the SMR-300 System Design Project Plan [71] these considerations are expected to be captured in operations/maintenance insights, fed by Process Flow Diagrams and component performance calculations. Detailed plans are formed from this to optimise maintenance that will be captured and defined in the maintenance plans produced during detailed design.

UK expectations in regard to the structural integrity of higher reliability components (covered in Part B Chapter 18 [19]) may introduce differing EIMT frequencies for the UK for certain components that fall under this scope due to the "beyond code" nature of the methodology.

Part A Chapter 4 Lifecycle Management [4] describes the SMR-300 design arrangements, including design lifecycle management, inputs, interfaces and record keeping that are in place to deliver a safe and secure UK SMR-300. This will ultimately include the implementation of the provisions and requirements listed in the SMR QA management (including EIMT requirements as an output of the SSEC).

9.6.4 Inspection Methods

Argument 2.3.1.3A-4: Inspection methods incorporated into the SMR-300 design are suitable to identify degradation of the SMR-300 SSCs.

This sub-chapter shows that equipment suppliers are required to prepare inspection and testing plans for all equipment, with requirements for field testing and inspection plans and procedures. Holtec maintain authority over these procedures and can challenge, modify, accept in full or reject these plans and procedures. UK specific context regarding higher reliability components may specify additional or differing arrangements for qualified inspections that will be developed following the Technical Advisory Group on the Structural Integrity (TAGSI) approach which will be fully defined post-GDA. Specification of personnel that will be involved in EIMT operations and their qualification is out of scope of GDA and will be addressed at a later stage of the licensing process. This is supported by:

- Structural Integrity Principles and Methodology [67].

The SMR-300 is designed with a fundamental principle of using established technology and methods guided by OPEX from a well understood operating fleet in the US, and this OPEX is collated in guidance from EPRI and the US NRC (via Regulatory Guidance documents), ASME design codes as well as incorporating guidance from equipment suppliers. This OPEX identifies the likely degradation rates of equipment and informs the maintenance schedule of SMR-300 SSCs.

Equipment suppliers are required to prepare inspection and testing plans for all equipment, with requirements for field testing and inspection plans and procedures. Holtec maintain authority over these procedures and can challenge, modify, accept in full or reject these plans and procedures.

UK specific context regarding higher reliability components may specify additional or differing arrangements for qualified inspections that will be developed following the TAGSI approach. This process is identified and discussed in Part B Chapter 18 Structural Integrity [19] and the supporting document Structural Integrity Principles and Methodology [67].

Specification of personnel that will be involved in EIMT operations and their qualification is out of scope of GDA at this time and will be addressed at a later stage of the licensing process.

9.6.5 CAE Summary

The EIMT position of SMR-300 shows that processes and mechanisms exist for the capture of appropriate EIMT operations. The generic SMR-300 design retains the ability to accommodate EIMT operations within the spatial design, chronologically schedule to be effective, and deploy the appropriate techniques and methods in these operations.

Much of the work required to fully detail these arguments will occur as SMR-300 progresses through the preliminary and detailed design phases. Considering the baseline design is still around the concept phase, the arguments and the evidence presented are indicative of the Holtec International processes and are adequately mature. These processes provide a route to progress EIMT provisions through detailed design.

There is a distinction to be made between “nuclear” EIMT/ageing and degradation management (which is in GDA scope), and the “conventional” EIMT and general plant maintenance plan (which would be the responsibility of the licensee). The former begins in earlier design phases to ensure that the design incorporates the appropriate considerations that relate to nuclear safety. Which leads into a difference between regulatory expectation between the US and UK expectations.

The extensive OPEX and RGP associated with Pressurised LWRs have shaped the development of ASME design codes, NRC regulations, and EPRI guidance. As these standards underpin the SMR-300 design requirements, there is confidence that the design processes and associated management arrangements adequately account for key degradation and ageing mechanisms.

While this approach is generally sufficient for a two-step GDA, it highlights a difference in regulatory expectations between the US and the UK. Additional work may be required after the GDA phase, in parallel with the development of the UK-specific DBAA. This work would focus on further evaluating degradation and ageing mechanisms to ensure that all relevant factors are adequately captured to support general substantiation. Furthermore, certain UK policy requirements related to higher reliability components will necessitate a more systematic demonstration of how degradation and ageing are managed. This includes using appropriate techniques for both Pre-Service and In-Service Inspection in accordance with UK RGP.

As such there may be a need for further work post-GDA, alongside the maturation of UK DBAA to further assess degradation and ageing to ensure that all considerations are captured adequately. GDA commitment C_MSQA_109 is identified in Part A Chapter 4 [4] to develop an ageing and degradation strategy to verify SMR-300 arrangements and activities for degradation management in the UK context.

9.7 CHAPTER SUMMARY AND CONTRIBUTION TO ALARP

This sub-chapter provides an overall summary and conclusion of the Description of Operational Aspects and Conduct of Operations chapter and how this chapter contributes to the overall demonstration of ALARP for the generic SMR-300. Part A Chapter 5 [5] sets out the overall approach for demonstration of ALARP and how contributions from individual chapters are consolidated.

This sub-chapter therefore consists of the following elements:

- Technical Summary;
- ALARP Summary
    - Demonstration of Relevant 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.

9.7.1 Technical Summary

Part B Chapter 9 aims to demonstrate the following Level 3 claim to a maturity appropriate for a PSR:

Claim 2.3.1: Appropriate arrangements to safely manage people and plant during the operation of the generic SMR-300 are suitably mature.

Claim 2.3.1 has been decomposed into three further claims:

Claim 2.3.1.1 is to provide the holistic demonstration of the design of the MCR and RSF in how they will support safe operation of the generic SMR-300, in accordance with the limits and conditions derived within the SSEC. This includes the design approach, operational procedures, staffing and training, hazard tolerance and habitability following defined internal and external hazards.

The fundamental design philosophy of the SMR-300 is to minimise human actions and once passive features are initiated, to require a very low level of human intervention. At the PSR stage, the design approach to the MCR and RSF is contained within the identified interfacing PSR chapters. The integrated design and safety approach is demonstrated to a level considered appropriate for a PSR through the initial UK DBAA and other topic areas, where GDA commitments are raised across the SSEC in:

- Part B Chapter 4 [7] where a DAS design change has been identified to enhance the I&C architecture and diversity.
- Part B Chapter 5 [8] to ensure that the HVAC design interfacing with the MCR and RSF supports the SSEC requirements and meets UK RGP.

The expected SMR-300 minimum staffing levels are provided. The first iteration of the S&Q review will include a summary of key roles and responsibilities for SMR-300 and be available to support the NRC CPA to the NRC. This will coincide with the end of GDA Step 2 and be complete prior to the beginning of the PC-SS-SSEC produced in the UK. This will support the demonstration that staffing and training will ensure that the MCR and RSF is operated in accordance with the assumptions and requirements of the safety assessment and considered to be an appropriate maturity for a PSR.

Claim 2.3.1.2 is an enabling claim to ensure that the SSEC will ultimately derive a set of limits and conditions, and that these limits and conditions of the safety case will be incorporated into operating documentation.

The SSEC will enable the derivation of ORs (limits and conditions) in accordance with ONR TAG-35 [49] during the nuclear site licensing phase. A site-specific SMR-300 design and PC-SS-SSEC will be developed which will reflect the completed detailed design and agreed operational approach required by the licensee. Operating procedures will be developed during the nuclear site licensing phase utilising the limits and conditions derived by the SSEC. The Technical Specifications for the generic SMR-300 will be based upon the limits and conditions derived by the PC-SS-SSEC. The PC-SS-SSEC will include information on how operational philosophies will inform procedural development, particularly when details of the future duty holder/licensee arrangements are known. Technical Specifications will be developed for the US Reference SMR-300 CPA in accordance with 10 CFR 50.34(a)(5) [28] and do not need to be fully developed in accordance with 10 CFR 50.36 until the OLA. The SMR-300 Technical Specifications produced in support of the OLA can be used to inform the development of operating documentation by the licensee in accordance with LCs 23 [43], 24 [44] and 25 [45].

Claim 2.3.1.3 is an enabling claim to ensure that the EIMT requirements will be identified in accordance with UK expectations to support the demonstration that the SSCs continue to achieve their safety functional requirements throughout the reactor lifecycle.

The EIMT position of SMR-300 shows that processes and mechanisms exist for the capture of appropriate EIMT operations. The generic SMR-300 design retains the ability to accommodate EIMT operations within the spatial design, chronologically schedule to be effective, and deploy the appropriate techniques and methods in these operations. These processes and mechanisms will continue through detailed design.

A difference between US and UK regulatory expectations has been identified for the identification of degradation and ageing mechanisms of concern. The extensive OPEX and RGP associated with Pressurised LWRs have shaped the development of ASME design codes, NRC regulations, and EPRI guidance. As these standards underpin the SMR-300 design requirements, there is confidence that the design processes and associated management arrangements adequately account for key degradation and ageing mechanisms. This approach is considered generally sufficient for a two-step GDA, however there may be a need for further work post-GDA, alongside the maturation of UK DBAA to further assess degradation and ageing to ensure that all considerations are captured adequately. A GDA commitment is identified in Part A Chapter 4 [4] to develop an ageing and degradation strategy to verify SMR-300 arrangements and activities for degradation management in the UK context.

Claim 2.3.1 is considered met at a maturity to be expected at the PSR stage.

The maturity of the supporting design, design substantiation and associated arrangements supporting these claims will develop beyond GDA and will be reflected in future revisions of the SSEC.

9.7.2 ALARP Summary

Part A Chapter 5 [5] presents the totality of the generic SMR-300 design against the ALARP principles. This section presents the ALARP considerations specific to this topic area. The methodology for this is discussed in Part A Chapter 5 [5] and consists of two main elements:

- Design complies with RGP.
- Options to reduce the risk have been identified and implemented where the effort to do so is not grossly disproportionate to the benefit that would be realised.

The following sub-chapters present the ALARP considerations for the Operational Aspects and Conduct of Operations.

9.7.2.1 Demonstration of RGP

The RGP codes and standards for the conduct of operations has been identified throughout this chapter. By considering this at an early stage, the conduct of operations is likely to result in an operational programme that can be demonstrated to be ALARP.

A holistic summary of the MCR and RSF is presented within this chapter, that will increase in detail following completion of detailed design. It is shown within this summary that the design process will ensure that SSCs within the MCR and RSF are appropriately designed and substantiated, to deliver their relevant safety functions. Detailed information demonstrating RGP is contained within the identified supporting PSR chapters and not repeated herein.

9.7.2.2 Evaluation of Risk and Demonstration Against Risk Targets

The numerical targets against which the demonstration of ALARP is considered can be found in Part A Chapter 2 [3].

The Conduct of Operations does influence the potential normal operation exposures and therefore provides a key input into the demonstration of Numerical Targets 1 to 3, however the evaluation of this, and any potential improvements or optimisations are presented within Part B Chapter 10 [10].

The evaluation of the normal operations and accident risks against Targets 1-9 is summarised in Part A Chapter 5.

9.7.2.3 Options Considered to Reduce Risk

The process for the assessment of risk reduction options is presented in Holtec's Design Management Process [60]. Part A Chapter 5 [5] considers the holistic risk-reduction process for the generic SMR-300.

The Conduct of Operations does influence the potential normal operation exposures, however the evaluation of this, and any potential improvements or optimisations are presented within Part B Chapter 10 [10].

Design modification to the DAS has been identified at PSR to meet UK DBAA requirements as a means to reduce risk. This is demonstration of the integrated design and safety approach in support of Claim 2.3.1.1. The GDA commitment is referred to in sub-chapter 9.7.3.

The scheduling of EIMT will ultimately be optimised to ensure risks are reduced ALARP. As the design progresses, considerations will be given to balance EIMT periodicities for maintaining the demonstration of SSEC claims and the management of degradation and ageing, versus potential implications on dose uptake. This is normal design practice that will ultimately be managed by the licensee. A GDA commitment in Part A Chapter 4 [4] to develop and ageing and degradation strategy is referred to in 9.7.3.

Future versions of this chapter will present the key ALARP considerations and/or design decisions for the MCR and RSF to demonstrate that the MCR and RSF will be suitably justified to reduce risks to ALARP. These will ultimately reside within the relevant engineering chapters that are cross referenced from this chapter.

9.7.3 GDA Commitments

At Revision 1 there are no GDA commitments identified for Part B Chapter 9, Description of Operational Aspects and Conduct of Operations. However, there are GDA commitments that are raised across the SSEC that do affect the claims within this chapter:

Part B Chapter 4 [7] includes GDA commitment C_C&I_082 for a design modification to the DAS. Note that as part of the commitment 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.

A GDA commitment (C_Faul_103) has been raised in Part B Chapter 14 [15] to complete the UK DBAA and ensure a holistic and comprehensive safety assessment to appropriately address UK expectations.

A GDA commitment (C_Mech_028) has been raised in Part B Chapter 19 [20] to ensure that the HVAC design interfacing with the MCR and RSF supports the SSEC requirements and meets UK RGP.

GDA commitment (C_MSQA_109) is identified in Part A Chapter 4 [4] to develop an ageing and degradation strategy to verify SMR-300 arrangements and activities for degradation management in the UK context. Target for resolution: Issue of Long Lead Item and SSC procurement specification. This supports the ultimate demonstration of Claim 2.3.1.3.

GDA commitments have been formally captured in the Commitments, Assumptions and Requirements process [79]. Further details of this process are provided in Part A Chapter 4 [4].

9.7.4 Conclusion

The conclusion of this chapter of the PSR is that:

- The chapter claims identified have been met to a maturity aligned with a PSR. Further claims, arguments and evidence will be presented in due course as the design develops.

- This chapter outlines the approach to plant operations and the undertaking of operations. These cannot be outlined in full at the GDA stage, as they are developed by the licensee in the site licensing phase, based on their specific operating requirements, experience and practice.
- The MCR is designed to provide a habitable area from which to safely operate the reactor. The RSF is a control station which serves as a backup to the MCR, should it be inoperable or require evacuation. The SSEC requirements for the MCR and RSF will be developed further in accordance with completion of the UK DBAA, which will also identify the required habitability requirements. These will be confirmed during detailed design, and any potential MCR or RSF design changes will be subject to Holtec's Design Management Process [60] during detailed design post-GDA.
- The expected SMR-300 minimum staffing levels are provided that will be underpinned by the systematic S&Q analysis generated as part of the HFE PMP [25].
- The SSEC will enable the derivation of ORs (limits and conditions) in accordance with ONR TAG-35 [47] during the nuclear site licensing phase. A site-specific SMR-300 design and PC-SS-SSEC will be developed which will reflect the completed detailed design and agreed operational approach required by the licensee. Technical Specifications will be developed for the US Reference SMR-300, which could be used to inform the development of operating documentation by the licensee in accordance with LCs 23 [43], 24 [44] and 25 [45].
- The generic SMR-300 EIMT position at GDA shows that processes exist for the capture of appropriate mechanisms and drivers and therefore the appropriate EIMT operations. The generic SMR-300 design retains the ability to accommodate EIMT operations within the spatial design, the ability to schedule them to be effective, and deploy the appropriate techniques and methods in these operations. An ageing and degradation strategy to verify SMR-300 arrangements and activities for degradation management in the UK context will be produced post-GDA.
- Operational aspects and conduct of operations constitute safety case implementation and as such, is largely undertaken by the licensee following the PC-SS-SSEC stage. It will therefore be fully developed within the nuclear site licensing phase of the generic SMR-300 and not within the GDA process.

9.8 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-2240335, Holtec SMR GDA PSR Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance," Revision 1, July 2025.

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

[6] Holtec Britain, "HI-2240776, Holtec SMR GDA PSR Part B Chapter 2 Reactor," Revision 1, July 2025.

[7] Holtec Britain, "HI-2240338, Holtec SMR GDA PSR Part B Chapter 4 Control and Instrumentation Systems," Revision 1, July 2025.

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

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

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

[11] 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.

[12] Holtec Britain, "HI-2241088, Holtec Britain CDM Strategy," Revision 0, November 2024.

[13] Holtec Britain, "HI-2241089, Holtec Nuclear Site Health and Safety Management System Report," Revision 0, January 2025.

[14] Holtec Britain, "HI-2240344, Holtec SMR GDA PSR Part B Chapter 13 Radioactive Waste Management," Revision 1, July 2025.

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

[16] Holtec Britain, "HI-2240346, Holtec SMR GDA PSR Part B Chapter 15 BDBA, Severe Accidents Analysis and Emergency Preparedness," Revision 1, July 2025.

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

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

[19] Holtec Britain, "HI-2240349, Holtec SMR GDA PSR Part B Chapter 18 Structural Integrity," Revision 1, July 2025.

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

[21] Holtec Britain, "HI-2240357, Holtec SMR GDA PSR Part B Chapter 20 Civil Engineering," Revision 1, July 2025.

[22] Holtec Britain, "HI-2240352, Holtec SMR GDA PSR Part B Chapter 23 Reactor Chemistry," Revision 1, July 2025.

[23] Holtec Britain, "HI-2240353, Holtec SMR GDA PSR Part B Chapter 24 Fuel Transport and Storage," Revision 1, July 2025.

[24] Holtec Britain, "HI-2240731, Operating Philosophy Review," Revision 0, March 2025.

[25] Holtec International, "HPP-160-1014, SMR-160 Human Factors Engineering Program Management Plan," Revision 2, January 2023.

[26] United States Nuclear Regulatory Commission, "NUREG-0711, Human Factors Engineering Program Review Model," Revision 3, 2012.

[27] International Atomic Energy Agency, "IAEA Nuclear Safety and Security Glossary," 2022 Edition.

[28] United States Nuclear Regulatory Commission, "Regulation 10 CFR Part 50 - DOMESTIC LICENSING OF PRODUCTION AND UTILIZATION FACILITIES".

[29] Holtec International, "HI-2240251, SMR-300 Top Level Plant Design Requirements," Revision 2, January 2025.

[30] Holtec Britain, "HI-2240077, SMR-300 Plant Overview," Revision 1, April 2024.

[31] Holtec Britain, "HI-2250400, Outage Strategy for SMR-300," Revision 0, 2025.

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

[33] Health and Safety Executive, "Lifting Operations and Lifting Equipment Regulations (LOLER) 1998: Open Learning Guidance," 2008.

[34] Health and Safety Executive, "Provision and Use of Work Equipment Regulations 1998 (PUWER)," Second Edition, 2008.

[35] United States Nuclear Regulatory Commission, "NUREG-0800, Chapter 13 Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition — Conduct of Operations," July 2023.

[36] United States Nuclear Regulatory Commission, "NUREG CR-7216, Human Performance Issues Related to the Design and Operation of SMRs," January 2012.

[37] United States Nuclear Regulatory Commission, "Title 10, Code of Federal Regulations".

[38] International Atomic Energy Agency, "IAEA: Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants. Specific Safety Guide No. SSG-70," Revision 1, 2022.

[39] International Atomic Energy Agency, "IAEA: The Operating Organization for Nuclear Power Plants. Specific Safety Guide No. SSG-72," Revision 1, 2022.

[40] International Atomic Energy Agency, "IAEA: Maintenance, Testing, Surveillance and Inspection in Nuclear Power Plants. Specific Safety Guide No. SSG-74," Revision 1, 2022.

[41] International Atomic Energy Agency, "IAEA: Conduct of Operations at Nuclear Power Plants. Specific Safety Guide No. SSG-76," Revision 1, 2022.

[42] Office for Nuclear Regulation, "Licence Condition Handbook," February 2017.

[43] Office for Nuclear Regulation, "NS-INSP-GD-023, LC 23 - Operating Rules," Issue 7, May 2024.

[44] Office for Nuclear Regulation, "NS-INSP-GD-024, LC 24 - Operating Instructions," Issue 7, May 2024.

[45] Office for Nuclear Regulation, "NS-INSP-GD-025, LC 25 - Operating Records," Issue 7.2, April 2024.

[46] Office for Nuclear Regulation, "NS-INSP-GD-026, LC 26 - Control and Supervision of Operations," Issue 6.1, October 2024.

[47] Office for Nuclear Regulation, "NS-INSP-GD-027, LC 27 - Safety Mechanisms, Devices and Circuits," Issue 6, December 2019.

[48] Office for Nuclear Regulation, "NS-INSP-GD-028, LC 28 - Examination, Inspection, Maintenance and Testing (EIMT)," Issue 9, July 2024.

[49] Office for Nuclear Regulation, "NS-TAST-GD-035, Limits and Conditions for Nuclear Safety (Operating Rules)," Issue 7, March 2023.

[50] Office for Nuclear Regulation, "NS-TAST-GD-009, Examination, Inspection, Maintenance and Testing of items important to Safety," Issue 7, November 2023.

[51] Holtec Britain, "HI-2240878, SMR-300 Generic Security Report for the Generic Design Assessment," Revision 0, June 2025.

[52] Holtec Britain, "HI-2240877, SMR-300 Conceptual Security Arrangements Report," Revision 0, 2025.

[53] Holtec Britain, "HI-2240876, SMR-300 Cyber Security Risk Assessment Study," Revision 0, 2025.

[54] Holtec International, "HI-2240457, System Design Description for the Main Control Room and Ancillary Stations," Revision 0, June 2024.

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

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

[57] Holtec International, "DWG_15299, General Arrangement of Reactor Auxiliary Building for SMR-300," Revision 3, 2024.

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

[59] Holtec International, "HI-2220303, System Specification for Monitoring and Operation," Revision 1, February 2024.

[60] Holtec Britain, "HPP-3295-0017, Design Management Process," Revision 1, 2024.

[61] Office for Nuclear Regulation, "ONR NS-INSP-GD-010, LC 10 - Training," Issue 4, December 2022.

[62] Office for Nuclear Regulation, "NS-INSP-GD-012, LC 12 - Duly authorised and other suitably qualified and experienced persons," Issue 4, December 2022.

[63] Office for Nuclear Regulation, "NS-INSP-GD-036, LC 36 - Organisational Capability," Issue 1, March 2021.

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

[65] Holtec Britain, "HI-2240125, ALARP Design Process," Revision 1, May 2024.

[66] Holtec International, "HI-2146060, System Design Description for Main Control Room Habitability System," Revision 0, November 2021.

[67] Holtec Britain, "HI-2241237, Structural Integrity Principles and Methodology," Revision 0, 2025.

[68] Holtec Britain, "HI-2241455, Holtec SMR-300 Through-Life Safety, Security and Environmental Case (SSEC) Strategy," Revision 0, December 2024.

[69] Office for Nuclear Regulation, "NS-TAST-GD-051, The Purpose, Scope, and Content of Safety Cases," Issue 7.1, December 2022.

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

[71] Holtec International, "HI-2250198, System Design Project Plan," Revision 0, March 2025.

[72] Nuclear Energy Institute, "NEI 03-08, Guideline For The Management Of Materials Issues," February 2017, Revision 3.

[73] Nuclear Energy Institute, "NEI 97-06 Steam Generator Program Guidelines," January 2011, Revision 3 .

[74] American Society of Mechanical Engineers, "Boiler and Pressure Vessel Code, Section XI – Rules for Inservice Inspection of Nuclear Power Plant Components," 2023 & 2021.

[75] Holtec International, "HPP-160-3016, SMR-160 Design Standard for Human Factors: Maintenance, Inspection, and Testing," Revision 0, June 2018.

[76] Holtec International, "HPP-8002-1010, SMR-300 Design Control," Revision 1, May 2025.

[77] Holtec International, "HPP-8002-0008, SmartPlant Standards," Revision 0, October 2024.

[78] United States Nuclear Regulatory Commission, “NUREG-2191, Generic Aging Lessons Learned for Subsequent License Renewal (GALL-SLR) Report – Final Report,” Revision 0, Volume 2, July 2017.

[79] Holtec Britain, “HPP-3295-0013, Holtec SMR-300 Generic Design Assessment Capturing and Managing Commitments, Assumptions and Requirements,” Revision 1, January 2025.

9.9 LIST OF APPENDICES

Appendix A PSR Part B Chapter 9 CAE Route Map

Table 4: PSR Part B Chapter 9 CAE Route Map

[REDACTED]