A Holtec International Company

Holtec Britain Ltd	HI-2240345
Sponsoring Company	**Document Reference**
0	30 September 2024
Revision No.	**Issue Date**
Report	Non-proprietary
Record Type	**Proprietary Classification**
ISO 9001	No
Quality Class	**Export Control Applicability**

Record Title:

PSR Part B Chapter 14 Safety and Design Basis Accident Analysis

Proprietary Classification

This record does not contain commercial or business sensitive information.

Export Control Status

Export Control restrictions do not apply to this record.

Revision Log

Revision	Description of Changes
0	First Issue to Regulators

Table of Contents

List of Figures

List of Tables

14.1 INTRODUCTION

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

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

Part B Chapter 14 of the PSR presents the Claims, Arguments and intended Evidence (CAE) to demonstrate that the SMR-300 design, and operation are tolerant to faults and that the applicable UK safety targets will be met.

14.1.1 Purpose and Scope

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

This chapter (Part B Chapter 14) links to the overarching claim through Claim 2.1:

Claim 2.1: The nuclear safety assessment identifies plant initiating events and specifies the requirements for safety measures such that safety functions are fulfilled, informs operational and emergency arrangements and demonstrates that risk is tolerable and As Low As Reasonably Practicable (ALARP).

As set out in Chapter A3 [2], Claim 2.1 is further decomposed across several disciplines which are responsible for development of the nuclear safety assessments. This chapter demonstrates that there is a robust methodology for the identification and assessment of fault conditions relevant to the Generic SMR-300 design through satisfying the Chapter Claim 2.1.2.

Claim 2.1.2: The design basis analysis demonstrates that the risk from design basis faults associated with the operation of the generic Holtec SMR-300 are tolerable and As Low As Reasonably Practicable (ALARP).

Further discussion on how the Level 3 claim is broken down into Level 4 claims and how the Level 4 claims are met is provided in subchapter 14.3.

The scope of the chapter (at Rev 0) considers the process to be followed for identification and classification of faults/hazards in totality for the design aligned with UK Relevant Good Practice (RGP) and the relevant Safety Assessment Principles (SAPs) and Technical Assessment Guides (TAGs), referenced where appropriate. The chapter covers the codes and standard associated with hazard identification, classification and assessment, the identification, screening and grouping of initiating events, application of transient and accident computer codes, Design Basis Accident Analysis (UK DBAA) Strategy and the Preliminary Fault Schedule (PFS). Finally, a summary of considerations against the ALARP principle is provided, together with any forward actions or commitments that have arisen.

There are exclusions from the scope of this chapter which are recognised as gaps against UK industry expectation and include:

- Faults external to the reactor which include:
    - Fuel route.
    - Waste systems.
    - Supporting services such as Heating, Ventilation and Air Conditioning (HVAC), air, water etc.
    - Out of core criticality.
    - Specific Spent Fuel Pool (SFP) faults.
    - Specific consideration of Annular Reservoir (AR) faults.
- Comprehensive assessment of internal and external hazards.
- The impact of a dual or multi-unit site in terms of the potential for sharing of support and interfacing facilities and any co-incident activities (e.g. construction of 1 unit while another is being commissioned or operating).
- Consideration of operator related safety function categories and any specific Systems, Structures and Components (SSCs) for accidents related to in-reactor faults or fuel route faults on the basis that the off-site impacts are considered to be more limiting in terms of licensability.
- Human errors as initiators where these relate to supporting specific activities such as maintenance; all operator errors as initiators have been grouped under a single "operator error" IE as a source of spurious actuation rather than as a source of a latent error.

The RP has recognised this gap. As a result, the RP has committed to develop a UK context Preliminary Fault Schedule during (PFS) Step 2.

The intent is to derive a PFS to meet UK context and offer a preliminary identification and categorisation of the associated Safety Function (SF) identification and classification of candidate SSCs that deliver the safety function.

It should be noted that these designations will be preliminary in nature and will be subject to further development and review in line with the maturity of the design.

In terms of the associated fault analysis for the design basis and beyond design basis accidents, the scope of the assessment for Step 2 has been constrained to the analysis that is available from the Deterministic Safety Analysis (US DSA) developed in the US for the Licensing Basis Events (LBEs) as defined above.

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

14.1.2 Assumptions

At the time of preparation of Rev 0 there are no SMR-300 specific US DSA transients results available.

It is assumed that Rev 1 of this chapter will be informed by SMR-300 specific analysis of these transients:

- Large Break Loss of Coolant Accident Analysis.

- Small Break Loss of Coolant Accident Analysis.
- Reactor Coolant Pump Shaft Lock Analysis.
- Main Steam Line Break Accident Analysis.
- Turbine Trip coincident with Loss of Offsite Power Accident Analysis.

Any further assumptions made during the assessment of the above transients will be outlined in Revision 1 of this chapter.

It is assumed relevant international operating experience (OPEX), in particular from Nuclear Regulatory Commission (NRC) and International Atomic Energy Agency (IAEA) supplemented by other Light Water Reactor (LWR) UK GDA projects, will support the further assessment of hazards for SMR-300 including novel design features which remain amendable throughout the OPEX informed approach of the UK DBAA.

14.1.3 Interfaces with other SSEC Chapters

The Safety and Design Basis Accident Analysis chapter interfaces with multiple topic areas across the PSR. Generally, those interfaces comprise specific discipline areas substantiating claims arising from the UK DBAA activities and as such are not specifically detailed here. Other specific interfaces are identified and are described below.

Chapter A1 Introduction [1]: presents an overview of the PSR structure and provides the fundamental purposes of the SSEC.

Chapter A2 General Design and Site Characteristics [3]: presents an overview of the generic design of the SMR-300 presented for the GDA, key safety claims, fundamental design and safety principles and the reference design that it is based upon. This Chapter also outlines which set of codes and standards are used for the design of the SMR-300, which supports the basis for an ALARP Design Process.

Chapter A3 Claims, Arguments and Evidence [2]: presents an overview of the CAE process, this supports the claims presented in subchapter 14.3.

Chapter B15 Beyond Design Basis and Severe Accident Analysis, and Emergency Preparedness [4]: Faults screened as Beyond Design Basis Assessment (BDBA) will be assessed in Chapter B15 [4].

Chapter B16 Probabilistic Safety Assessment [5]: Chapter B16 [5] will provide probabilistic analysis considered for the SMR-300 and will present the assessment results to support these elements of the Probabilistic Safety Assessment (PSA). The PSA will also contribute to the provision of consequence and frequency data that will be provided in the fault and protection schedule.

Chapter B17 Human Factors [6]: Identified Human Factors-related initiating events or human actions will be represented in the UK DBAA. Similarly, claims arising from the UK DBAA on human action/performance will be considered within Chapter B17 [6] of the PSR where required.

Chapter B21 External Hazards [7]: The approach to fault schedule development proposed in this chapter will capture external hazard events identified in Chapter B21 [7].

Chapter B22 Internal Hazards [8]: The approach to fault schedule development proposed in this Chapter will capture internal hazard events identified in Chapter B22 [8].

14.2 DESCRIPTION OF DESIGN BASIS ACCIDENT ANALYSIS

Within this Chapter, US DSA is used to refer to the scope of the US deterministic analysis of the transients and accident events whereas UK DBAA is used to refer to the scope of the analysis used within the UK GDA. For the avoidance of confusion, a clear distinction between the two is presented, as the requirements of US DSA in the US and UK DBAA in the UK have some differences, i.e. satisfying US DSA requirements does not necessarily mean that UK DBAA requirements are satisfied.

14.2.1 Overview of US Approach

In the US context, an initiating event defined in Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications [9] is any event either internal or external to the plant that perturbs the steady state operation of the plant, if operating, thereby initiating an abnormal event, a transient, scenario and potential accident (e.g., a loss of coolant accident (LOCA)). Initiating events trigger sequences of events that challenge plant control and safety systems, the failure of any of which could potentially lead to core damage or large early release.

Identification and Quantification methodologies are used to ascertain (identify) and evaluate (quantify) SMR-300 relevant initiating events within the design basis of the power plant; and to assess if and how initiated scenarios challenge, threaten plant safety. Identifying a consensus consolidated list of initiating events (faults) for a power plant allows developers and licensees to prepare and present safety analyses reports of the plant response to these events, considering all the determined relevant initiating events within that design basis.

Holtec develops a comprehensive Consolidated Faults List (CFL), using a comprehensive engineering evaluation from Defining Initiating Events for Purpose of Probabilistic Safety Assessment [10], PSA Procedures Guide [11], Analysis of Core Damage Frequency From Internal Events: Methodology Guidelines Sec 3 Ref [12], Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process [13] methodology to identify initiating events on both a generic Pressurised Water Reactor (PWR) and plant specific SMR-300 basis (considering unique or novel features). Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995 [14] provides a comprehensive summary of initiating events and estimated frequencies for the United States nuclear industry and noting frequencies from this study have been updated with more current industry data in Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants [15], [13]. These studies comprise the primary sources of industry recognized initiating events used in development of the SMR-300 CFL, as needed to perform safety analyses for Anticipated Operational Occurrence (AOOs), Design Basis Accidents (DBAs) and BDBAs using both US DSA and PSA applied methods and models.

Once initiating events have been identified by considering candidate events from other (PWR) PSAs, along with an SMR-300 plant specific initiating event review, events are selected and screened, and grouped as possible, by identifying an event whose unmitigated consequences effectively bounds a group of initiated events (identifies the worst case amongst of group of events).

An important distinction between US SMR-300 DSA and PSA is that the US DSA safety analyses only credit safety-classified SCCs when evaluating a transient from an initiating event and give no credit or consideration to non-safety systems, active (ac) sources of power or operator actions. PSA safety analysis calculations model and credit non-safety systems and operator actions, with probability of loss of offsite power (LOOP), using deterministic models and/or fault tree analysis, to evaluate initiating event scenarios to calculate likelihood of core damage and radiological release.

In summary, the US DSA is the analysis of the plant response to transients and postulated accidents (or Postulated Initiating Events (PIEs)). US DSA is sometimes also called transient and accident analysis. These analyses – articulated in 14.6 below - determine the limiting conditions of the plant for safety-related systems to protect public health and safety. The plant transients and postulated accidents/PIEs represent a sufficiently broad spectrum of initiating events that has been developed based on over 70 years of experience in the design and operation of light water reactor technologies on the basis of engineering judgements and a combination of deterministic assessment and probabilistic assessment, together with OPEX.

14.2.2 Overview of UK Approach

UK DBAA is the analysis of the accidents that occur within the Design Basis (DB). It is performed deterministically, so it has many similarities with the US DSA (or transient and accident analysis), which is the term used in the US. However, UK DBAA refers to the full scope of fault analysis, not just operational occurrences and 'accidents' within the design basis, (i.e., transients, internal events, internal and external hazards) and is a robust demonstration of the fault tolerance of the facility, and of the effectiveness of its safety measures. The UK approach and licensing requirements are explained further throughout this chapter.

In this chapter, where appropriate, differences between the two approaches are highlighted, described in further detail and subsequently recorded as a Gap to ensure the design, construction, operation and decommissioning of SMR-300 is line with UK licensing requirements.

14.3 DESIGN BASIS ACCIDENT ANALYSIS CLAIMS, ARGUMENTS, EVIDENCE

The primary purpose of a CAE approach is to capture the golden thread of a safety case narrative, in this context, demonstrating how fault studies and analysis are conducted to justify that a high-level or fundamental claim is true. In the context of the generic SMR-300, that is how the Fundamental Purpose of the SSEC (presented in Chapter A1 [1]) is achieved.

The Fundamental Purpose follows a golden thread throughout the SSEC to CAE via the objectives of the PSR, Preliminary Environmental Report (PER) and Generic Security Report (GSR). The overarching SSEC claims are presented in Chapter A3 [2].

This chapter contributes directly to Claim 2.1, which is focused on the demonstration of the identification of hazards/ initiating events and faults and ensuring the risks presented by them are ALARP.

Claim 2.1: The nuclear safety assessment identifies plant initiating events and specifies the requirements for safety measures such that safety functions are fulfilled, informs operational and emergency arrangements and demonstrates that risk is tolerable and As Low As Reasonably Practicable (ALARP).

As set out in Chapter A3 [2], Claim 2.1 is further decomposed across several nuclear safety assessment disciplines which are responsible for development of the nuclear safety assessment. This chapter presents the UK DBAA topic for the generic SMR-300 to support Claim 2.1.2:

Claim 2.1.2: The design basis analysis demonstrates that the risk from design basis faults associated with the operation of the generic Holtec SMR-300 are tolerable and As Low As Reasonably Practicable (ALARP).

Claim 2.1.2 has been further decomposed within Chapter B14 into five Level 4 claims. The decomposition of the chapter claim has been chosen to logically support the building of UK DBAA whilst utilising US DSA information where appropriate. How the sub-claims support the chapter claim is outlined below:

Claim 2.1.2.1 provides demonstration that the overall methodologies used in fault studies, both to identify and analyse design basis faults are appropriate.

Claim 2.1.2.2 applies these appropriate methodologies to identify the PIEs for the SMR-300.

Claim 2.1.2.3 uses best practice methods for the assessment of Transients and Accidents.

Claim 2.1.2.4 uses methods and rules to determine the safety functions and safety measures to provide sufficient lines of protection for the plant.

Claim 2.1.2.5 aims to demonstrate, through deterministic safety assessment undertaken using appropriate methods and assumptions, that the identified functions and features ensure that plant is able to reach a safe state in the event of design basis faults.

Table 1: CAE Chapters

Claim No	Claim	Chapter Section
2.1.2.1	Plant initiating events are identified, and UK DBAA undertaken, using appropriate methodologies.	14.4 Codes, Standards and Methodologies
2.1.2.2	A comprehensive set of plant initiating events are identified, screened and appropriately grouped into design basis faults.	14.5 PIE Identification, Screening & Grouping
2.1.2.3	The assessment of Transients and Accidents shall be undertaken in accordance with best practice analysis methods.	14.6 Application and Use of Transient and Accident Analysis Computer Codes
2.1.2.4	Safety functions and safety measures are identified, categorised and classified based on their importance to nuclear safety for all design basis faults and provide sufficient lines of protection based on the fault frequency and consequence.	14.7 Design Basis Accident Analysis and Preliminary Fault Schedule
2.1.2.5	Analysis demonstrates that for all design basis faults, the identified safety features, in conjunction with operator actions, enable the plant to reach a safe state.	14.7 Design Basis Accident Analysis and Preliminary Fault Schedule

A summary of the current CAE route map for Chapter B14 is provided in Appendix A which is taken from the Generic SMR-300 Overarching SSEC Claim Route map presented in Appendix A of Chapter A3 [2]. A further update on claim decomposition, argument development and evidence maturity will be provided in the subsequent update of the chapter.

14.4 CODES, STANDARDS AND METHODOLOGIES

Claim 2.1.2.1: Plant initiating events are identified, and Design Basis Accident Analysis undertaken, using appropriate methodologies.

This subchapter presents the US standards that were used to inform the US DSA Transient Analysis (TA) and the relevant UK codes used to inform the UK context. Table 2: Principal Regulations, Codes, Standards and Guidance shows the US standards and guides used and Table 3: UK RGP for Design Basis Analysis presents the UK equivalents. Given its significance in influencing the design the use of the General Design Criteria is also briefly introduced.

Table 2: Principal Regulations, Codes, Standards and Guidance

Label	Title
US Codes and Standards	
ANSI/ARANS-58.14-2011 (R2017)	Safety and Pressure Integrity Classification Criteria for Light Water Reactors [16]
10 CFR Part 50 Appendix A	General Design Criteria for Nuclear Power Plants [17]
INL/RPT-23-7281	Initiating Event Rates at U.S. Nuclear Power Plants: 2022 Update. [18]
NEI 18-04, Revision 1.	Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development [19]
NUREG-0800	Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants
NUREG/CR-4483	Reactor Pressure Vessel Failure Probability Following Through-Wall Cracks Due to Pressurized Thermal Shock Events, 1986 [20]
NUREG-0651	Evaluation of Steam Generator Tube Rupture Events, U.S. Nuclear Regulatory Commission, March 1980 [21].
NUREG/CR-5750	Rates of Initiating Events at US Nuclear Power Plants: 1987-1995 with updates. [14]
NUREG-6890	Re-evaluation of Station Blackout Risk at Nuclear Power Plants, Analysis of Loss of Offsite Power Events: 1986-2004 [22]
NUREG/CR-6928	Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants with updates [23]
NUREG-1829	Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process [24]
US NRC Reg Guide 1.203	Regulatory Guide (RG) 1.203: Transient and Accident Analysis Methods [25]
US NRC Reg Guide 1.233	Guidance for a technology-inclusive, risk-informed, and performance-based methodology to inform the licensing basis and content of applications for licences, certifications, and approvals for non-light-water Reactors [26]
US NRC Reg Guide 1.26	Quality Group Classifications and Standards for Water, Steam, and Radioactive Waste-Containing Components of Nuclear Power Plants [27]
IAEA Guidance	
IAEA TECDOC-749	Generic Initiating Events for PSA for WWER Reactors [28]
IAEA TECDOC-719	Defining Initiating Events for Purposes of Probabilistic Safety Assessment [10]
SSR-2/1	Safety of Nuclear Power Plants: Design. [29]
SSG-30	Safety Classification of Structures, Systems and Components in Nuclear Power Plants [30].

14.4.1 NRC Design Requirements

The SMR-300 has been designed against the requirements stipulated within US legislation in particular 10 CFR Part 50 [31]. Particular attention is drawn to the requirements of the General Design Criteria (GDC) presented as Appendix A. The significance of this is that it is prescriptive in that it sets out to the designer a mandatory minimum set of requirements that the plant must achieve. This will become of great significance when the differences between assessment requirements is discussed.

14.4.2 Key ONR Safety Assessment Principles

Key SAPs (see Safety Assessment Principles For Nuclear Facilities [32] – this references Target 4 from the ONR SAPs [32]) have also been identified. These will be used to inform how the UK DBAA methodologies that will be utilised will be developed. The significant SAPs for consideration at this point are identified as:

- FA.1 – FA.9 (Fault Analysis).
- AV.1 – AV.4 (Assurance and Validity of Data Models).
- EKPs (Engineering Key Principles).
- ECSs (Safety Classification and Standards).
- NT (Numerical Targets) – see Chapter A2 [3].

Other ONR guidance documents and RGP from the IAEA and WENRA are shown within Table 3.

Table 3: UK RGP for Design Basis Analysis

Label	Title	Revision
ONR Guidance		
SAPs	Safety Assessment Principles [32]	1
ONR-GDA-GD-006	ONR GDA Guidance to RPs [33]	0
ONR-GDA-GD-007	Nuclear Power Plants Generic Design Assessment Technical Guidance [34]	0
NS-TAST-GD-005	Guidance on the Demonstration of ALARP [35]	11.2
NS-TAST-GD-006	Design Basis Analysis [36]	5.1
NS-TAST-GD-034	Transient Analysis for DBAs in Nuclear Reactors [37]	
NS-TAST-GD-035	Limits And Conditions For Nuclear Safety (Operating Rules) [38]	7
NS-TAST-GD-036	Redundancy, Diversity, Segregation and Layout of Structures, Systems and Components [39]	3
NS-TAST-GD-042	Validation of Computer Codes and Calculation Methods [40]	5.1
NS-TAST-GD-051	The Purpose, Scope, and Content of Safety Cases [41].	4
NS-TAST-GD-094	Categorisation of Safety Functions and Classification of Structures, Systems and Components [42]	2
IAEA Guidance		
SSR-2/1	Safety of Nuclear Power Plants: Design. [29]	1
SSG-2	Deterministic Safety Analysis for Nuclear Power Plants [43]	
SSR-2/2	Safety of Nuclear Power Plants: Commissioning and Operation [44]	1
WENRA Guidance		
-	Safety Reference Levels for Existing Reactors [45]	2021
-	Report on Safety of new Nuclear Power Plant (NPP) [46]	2013
-	WENRA Statement on Safety Objectives for New Nuclear Power Plants [47]	2010

14.4.3 CAE Summary

The argument to support this claim is developed as the relevant codes and standards have been identified to demonstrate that the US DSA will align with international best practice and the UK DBAA analysis will be in line with UK industry expectations by alignment with the SAPs in the absence of project specific requirements.

14.5 PIE IDENTIFICATION, SCREENING & GROUPING

Claim 2.1.2.2: A comprehensive set of plant initiating events are identified, screened and appropriately grouped into design basis faults.

This subchapter sets out the approach that has been applied to date by Holtec International for the following topic areas:

- Identification of relevant PIEs for consideration in the US DSA of the SMR-300.
- Classification of PIEs within the US licensing basis.
- Transients and accidents analysis of PIEs, including the:
    - definition of assessment parameters in accordance with US NRC requirements.
    - transient and accident analysis codes used and their verification and validation.

These areas are expanded in more detail in the subchapters below.

The intent is to utilise, as much as possible, information that has been prepared for the NRC licensing process. The US DSAs, in general, provide a good description of the fault development and provides a judgement of the fault progression against the acceptance criteria which is typically related to fuel characteristics that may lead to a fuel failure and/or core damage or a significant radiological hazard.

14.5.1 Postulated Initiating Event Identification and Grouping for use in Transient Analysis

PIEs are defined as events that lead to AOOs[1] or DBAs within or beyond (BDBAs) the design basis. All PIEs having the potential to lead to a person receiving a significant dose of radiation, or which lead to loss of control and containment of radioactive materials must be identified and classified accordingly.

For the UK DBAA, the PIEs considered for the SMR-300 will ultimately include all foreseeable failures of SSCs of the plant, as well as human failure and possible failures arising from internal and external hazards, whether in full power, low power, or shutdown states, in the reactor, the fuel pool or where sources of radioactivity exist across the twin-unit site (e.g., waste or fuel stores). The path to achieving this is set out in subchapter 14.7.

For the SMR-300, the list of PIEs considered in the US DSA is limited to those events considered to be bounding in terms of off-site public exposures, namely those events with the potential to lead to significant off-site radiological consequences originating from within the reactor plant itself.

The PIEs have been considered relevant if they have the potential to challenge at least one of the fundamental safety functions, namely those high-level safety functions introduced in

[1] The IAEA/NRC descriptor of ‘anticipated operational occurrences’ (AOO) is broadly equivalent to ‘frequent design basis faults’ as used in UK safety cases (initiating event frequency > 1 x 10-3 pa) for which it is expected that analysis is presented to show the effectiveness of independent Level 2 and Level 3 defence in depth safety measures. (ONR)

Chapter A2 [3] (repeated here in Table 4) distilled from the US NRC's Standard Review Plan Branch Technical Position BTP 7-19 [48], IAEA [29] and 10 CFR 50 Chapter 2 [31] .

Table 4: SMR-300 High-Level Functions

Plant Goal	High-Level Function
Ensure Safety	1.1 Control Reactivity
	1.2 Post-Accident Heat Removal
	1.3 Reactor Coolant System Integrity
	1.4 Containment Integrity

In accordance with the ONR SAPs identified in subchapter 14.4, UK DBAA should be performed for all operating phases and all operating modes of the reactor. UK DBAA should also be performed for all events from which may emanate sources of radioactivity outside of the reactor including spent fuel and radioactive waste handling and storage, which meet the relevant consequence and frequency criteria.

However, UK DBAA refers to the full scope of fault analysis, not limited to faults from operational occurrences and 'accidents' within the design basis, but including transients, and faults initiated by internal events, internal and external hazards etc. UK DBAA is a robust demonstration of the fault tolerance of the facility, and of the effectiveness of its safety measures. Accordingly, the starting point for UK DBAA is always a comprehensive list of initiating events that feed into the PIEs. The UK DBAA provided for the generic SMR-300 must demonstrate that a systematic and comprehensive identification of all faults and hazards has been performed. There is gap with respect to the fault identification for the generic SMR-300 design not fulfilling the UK expectations in compliance with ONR TAG GD 006 and SAP FA.2. This will be addressed by undertaking a systematic and comprehensive walkdown of the SMR-300 design coupled with a review of the relevant NUREG/IAEA reports, PWR (and other GDA) safety analysis reports, fault schedules and PIE lists in applicable PWR and SMR safety submissions. This will be achieved in a series of hazard and fault identification workshops in order to derive a comprehensive initiating event and PIE schedule for all operating states of the reactor, including relevant external and internal hazards and all interfacing activities within the NPP that have the potential to present a radiological hazard.

During Step 2, it is intended to present a limited set of safety analyses for several PIEs identified in Table 5 , and to supplement them with additional initiating events analyses, as practical, to provide confidence in the SMR-300 (the US reference plant) protection systems. In order to ensure completeness of the hazard and fault identification process, the PIEs considered for the SMR-300 design will need to include all foreseeable failures of duty systems and SSCs of the plant, as well as human failures and possible failures arising from internal and external hazards, whether in full power, low power or shutdown states, in the reactor, the fuel pool, fuel handling system, waste operations or some other activity containing sources.

During GDA Step 2, a Hazard and Fault Identification and Study Report will be developed, which will present the results of the hazard and fault identification studies carried out in accordance with the strategy and will provide the basis for development of the PFS. This document will also present the proposed structure and format of the PFS to be applied in the structure and content for future safety reports.

Although the Holtec SMR is a unique design, it is a PWR that uses similar materials and SSCs to the existing global PWR fleet. Therefore, the PIEs identified for traditional PWRs have been used to guide the identification of PIEs for the reference design. Other PWR and SMR plant designs that have been approved by the US NRC with inherent passive safety features are also used to help guide the identification process, i.e., the Preliminary Safety Analysis Reports (PSARs) of Westinghouse's AP1000 [49] and NuScale's SMR [50].

PIEs are grouped into specific fault groups to compare their effects, safety limits and protection or mitigation strategies on a common basis according to the groups identified in NUREG 0800 Standard Review Plan (Chapter 15). These comparisons can help identify limiting PIEs for detailed analysis and eliminate non-limiting PIEs from further consideration in the deterministic analysis. The following fault groups were identified for the SMR-300 US DSA based on US NRC regulatory guidance:

1. Increase in heat removal by the secondary system.
2. Decrease in heat removal by the secondary system.
3. Decrease in Reactor Coolant System (RCS) flow rate.
4. Reactivity and power distribution anomalies.
5. Increase in reactor coolant inventory.
6. Decrease in reactor coolant inventory.
7. Radioactive release from a subsystem or component.
8. Anticipated Transient Without Scram (ATWS).

The deterministic list of PIEs that have been identified as being applicable to the SMR-300 are defined in Table 5 taken from SMR-300 Initiating Event Identification and Classification [51].

The PIEs have been considered relevant if they have the potential to challenge at least one of the fundamental safety functions, namely those high-level safety functions introduced in Chapter A2 [3] (repeated here in Table 4) distilled from the US NRC [48], IAEA [29] and 10 CFR 50 Chapter 2 [31] .

At present, these analyses are scheduled to be completed but are not yet available. It is expected that during Step 2 SMR-300 TA will complete the following:

- Large Break Loss of Coolant Accident Analysis.
- Small Break Loss of Coolant Accident Analysis.
- Reactor Coolant Pump Shaft Lock Analysis.
- Main Steam Line Break Accident Analysis.
- Turbine Trip coincident with Loss of Offsite Power Accident Analysis.

Table 5: PIEs and Fault Grouping for the SMR-300 from US DSA

Postulated Initiating Event	Licensing Basis Event Classification	Rationale/Basis for Inclusion
Increase in Heat Removal by the Secondary System		
Decrease in feedwater temperature	AOO	(REDACTED)
Increase in feedwater flow	AOO	
Increase in steam flow	AOO	(REDACTED)
Inadvertent operation of steam generator safety valve	AOO	(REDACTED)
Steam piping failures inside and outside of containment	DBA	(REDACTED)
Inadvertent operation of PDH	AOO	(REDACTED)
Inadvertent operation of SDH	AOO	(REDACTED)
Decrease in Heat Removal by the Secondary System		

Postulated Initiating Event	Licensing Basis Event Classification	Rationale/Basis for Inclusion
Loss of external load	AOO	(REDACTED)
Turbine trip	AOO	(REDACTED)
Loss of condenser vacuum	AOO	
Closure of Main Steam Safety Valves (MSIVs)	AOO	(REDACTED)
Loss of Alternating Current (AC) power to station auxiliaries	AOO	(REDACTED)
Loss of normal feedwater flow	AOO	(REDACTED)
Feedwater line breaks inside and outside containment	DBA	(REDACTED)
SDH Tube Rupture	DBA	(REDACTED)
Decrease in RCS Flow Rate		
Partial loss of RCS flow	AOO	(REDACTED)
Total loss of RCS flow	AOO	
Reactor Coolant Pump (RCP) rotor seizure (locked rotor)	AOO	(REDACTED)
RCP shaft break	AOO	(REDACTED)
Reactivity and Power Distribution Anomalies		
Uncontrolled Rod Control Cluster Assembly (RCCA) withdrawal from a subcritical or low-power startup condition	AOO	(REDACTED)
Uncontrolled RCCA withdrawal at power	AOO	
RCCA misoperation	AOO	(REDACTED)
Inadvertent decrease in RCS boron concentration	AOO	(REDACTED)
Inadvertent loading and operation of a fuel assembly	AOO	(REDACTED)
Spectrum of rod ejection accidents	DBA	(REDACTED)
Increase in Reactor Coolant Inventory		
Inadvertent operation of the Passive Core Cooling System (PCCS)	AOO	(REDACTED)
Chemical Volume and Control System (CVC) malfunction	AOO	(REDACTED)
Decrease in Reactor Coolant Inventory		
Inadvertent opening of a pressuriser safety valve or Automatic Depressurisation System (ADS) valve	AOO	(REDACTED)
Failure of small lines carrying RCS coolant outside containment	AOO	(REDACTED)
Steam generator tube rupture (SGTR)	DBA	(REDACTED)
Loss of coolant accidents	DBA	(REDACTED)
Radioactive Release from a Subsystem or Component		
Postulated radioactive releases due to liquid-containing tank failures	DBA	(REDACTED)
Fuel handling accidents	DBA	(REDACTED)
Spent fuel cask drop accidents	DBA	(REDACTED)
Anticipated Transient Without Scram (ATWS)		
Anticipated Transient Without Scram (ATWS)	BDBA	(REDACTED)

14.5.2 Licensing Basis Event Classification

The identification and classification of groups of PIEs/fault groups is an important process that serves as the foundation for the US DSA and transient and accident analysis. The identification and classification of fault groups provides the bases for determining the adequacy of the evaluation models per Steps 1 and 2 of the US NRC RG 1.203 [25].

In addition to the event classifications within Appendix A to 10 CFR Part 50 - General Design Criteria for Nuclear Power Plants [52] (or plant states in SSR 2/1 [29]), Holtec have also considered the application of the risk-informed performance-based guidance defined within NEI 18-04 [19] in support of US NRC RG 1.233 [26]. Note that this NEI document is for non-light water reactors but describes a systematic approach that is not technology-dependent, so is an appropriate supplement to standard PWR event classification. Noting that the Holtec fault group classification is referred to as the licensing basis event classification.

The identified licensing basis event classifications considered in the design of the SMR-300 are defined as follows.

- Normal Operation (NO): Operation within specified operational limits and conditions. For a nuclear power plant, this includes startup, power operation, shutdown, maintenance, testing and refuelling. These events will occur more frequently than once in the lifetime of the plant.
- AOO: A condition of normal operation which is expected to occur one or more times during the life of the nuclear power unit. NUREG-0800, Chapter 15 [53] refers to AOOs as incidents of moderate frequency (i.e., events that are expected to occur several times during the plant's lifetime) and infrequent events (i.e., events that may occur during the lifetime of the plant).
- DBA: A postulated accident that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to ensure public health and safety. DBAs are unanticipated occurrences; they are postulated to occur but not expected to occur during the life of the nuclear plant unit.
- BDBA: BDBAs are rare event sequences of AOOs or DBAs that include a failure or failures of the single-failure proof plant safety systems. BDBAs are analysed to fully understand the capability of the plant design. These events are not expected to occur during the life of the plant and are beyond the scope of what a nuclear plant must be designed and built to withstand.
- Design Extension Condition (DEC): A subset of BDBAs that are not considered for DBAs, but that are considered in the design process of the facility in accordance with best-estimate methodology to keep releases of radioactive material within acceptable limits. Design extension conditions could include severe accident conditions.

The licensing basis event frequency thresholds resulting from these definitions are summarised within Table 6.

Table 6: Holtec SMR Frequency Thresholds

Frequency Type	US Frequency Threshold
AOO	> 1×10^{-2} / plant-year
DBA	< 1×10^{-2} / plant-year and > 1×10^{-4} / plant-year
BDBA	< 1×10^{-4} / plant-year

In addition to the frequency of occurrence of these events, there are also transient and accident analysis acceptance criteria linked to the licensing basis event classification. Within the US DSA, these acceptance criteria are used to confirm the licensing basis event classification once the transient and accident analysis has been undertaken.

How the above classifications will be aligned to the UK context to support the production of UK DBAA is explained further in subchapter 14.7.2.

14.5.3 CAE Summary

The argument to support Claim 2.1.2.2 is that, whilst yet to be completed, the above methodology outlines the steps required to identify, screen and group initiating events in order to achieve the claim. It is expected that during Step 2, the SMR-300 TA will complete analysis of several specific initiating events providing confidence in achieving the claim. The FS strategy has also stated that an additional number of fault assessments will be undertaken to provide further confidence in the design and to demonstrate the adequacy of the FS strategy.

14.6 APPLICATION AND USE OF TRANSIENT AND ACCIDENT ANALYSIS COMPUTER CODES

Claim 2.1.2.3: The assessment of Transients and Accidents shall be undertaken in accordance with best practice analysis methods.

The purpose of this subchapter is to provide an overview of the approach taken to perform US DSA by Holtec International (HI) to meet NRC regulatory requirements. This is significant as it is stated in the assumptions that there is no SMR-300 data available but it is assumed that a limited number of analyses will be undertaken and completed within Step 2 that can support later issues of this chapter. Therefore, an understanding of how the HI TA is prepared and how it can be used to inform the UK DBAA is required.

The US DSA of the SMR-300 is the analysis of the plant response to transients and postulated accidents (or PIEs). US DSA is sometimes also called transient and accident analysis. These analyses determine the limiting conditions of the plant for safety-related systems to protect public health and safety. The plant transients and postulated accidents/PIEs represent a broad spectrum of initiating events that has been developed based on over 70 years of US fleet operating experience in the design and operation of light water reactor technologies on the basis of engineering judgements and a combination of deterministic assessment and probabilistic assessment, together with OPEX.

14.6.1 Use of US DSA Transient Analysis

The SMR-300 has been designed against the GDC. This therefore also sets the limit of the scope for US DSA transient analysis that needs to be performed to satisfy NRC expectations for licensing. In general, US DSA is required to demonstrate the following:

- The ability of the plant to operate safely without risk to the health and safety of the public.
- Selected plant features are designed to mitigate the consequences of postulated transients and accidents.
- The integrity of the three radiological barriers is maintained during an event, i.e.:
    - Reactor Coolant Pressure Boundary (RCPB).
    - Fuel Cladding.
    - Containment Structure (CS).

The US DSA utilises a variety of computer codes to develop and understand plant responses which include detailed examinations of:

- Thermal hydraulic analysis using RELAP 5 – 3D.
- Sub channel analysis using COBRA-FLX.
- Containment Analysis using GOTHIC.
- Core Physics modelling utilising CASMO5, CMSLINK5, SIMULATE5 and SIMULATE-3K.
- Radiological Consequences of TA (to be performed).
- Source Term Modelling.

A description of these codes is provided in Appendix B

The difference in scope of the US DSA to UK DBAA in a UK context is significant. The expectations for a UK DBAA usually require an analysis of all initiating events, as outlined in subchapter 14.5, which have the capability to generate a radiological consequence to a worker and / or public receptor. It is also used to inform the Design Basis (DB) for the plant. Whilst this type of analysis is also performed deterministically, there are many similarities with the US DSA approach. Correspondingly there are also differences. Significantly, the UK DBAA scope is not defined by regulation (as in the US) but derived by a robust Hazard Identification (HAZID) of the plant in all operating modes whilst satisfying the ALARP principle which will be satisfied by the production of a PFS.

Additionally, within a UK context the UK DBAA is the primary mechanism for the identification of SSCs that are important to maintain the safe operation of the plant. NRC have issued extensive Regulatory Guidance (RG) [RG1.26 [27]] on the definition of SSCs which due to the application of the GDCs takes a different approach to the UK context.

The strategic aim of this chapter is to utilise as much US DSA data as possible. Care is required to ensure that the context is utilised correctly. In general, the HI US DSA data is a transient analysis and this limits how it is used to satisfy UK DBAA requirements.

14.6.2 Assessment of Transients and Accidents

The integrity of the three radiological barriers (the fuel cladding, the reactor coolant pressure boundary, and the containment structure) prevents or limits the release of radioactivity from the reactor. These barriers act independently to prevent or limit the release of radioactive material during PIEs and the exposure to an individual. The source term for radiological exposure will be determined based on the results of the analysis, the effects of the event on the fuel, the reactor coolant pressure boundary, and the containment.

The main objective of the transient and accident analysis performed within the US DSA is to evaluate the ability of the plant to operate without undue hazard to the health and safety of the public. In the transient and accident analysis, the complete event sequence is modelled; from the initial conditions to the safe, stabilised condition, as shown in Figure 1. The analyses are performed with conservative assumptions about initial conditions and plant equipment availability with application of the single failure criterion, non-safety system response, and modelling parameters that produces the most limiting results for each figure of merit of each acceptance criteria until the plant can be considered to have met the safe shutdown condition. The effects of the SPF are also considered for the removal of decay heat from the Containment Enclosure Structure (CES). There are a number of key assumptions and characteristics that must be assumed before the results can be determined to meet the acceptance criteria established by the US NRC.

Figure 1: Transient and Accident Analysis Methodology for the US DSA (US)

14.6.3 Acceptance Criteria

The transient and accident analysis acceptance criteria are linked to the classification of the licensing basis event (AOO, DBA, BDBA) identified in subchapter 14.5.2. Detail on BDBA acceptance criteria is included in PSR Part B Chapter 15 BDBA, Severe Accidents Analysis and Emergency Preparedness [4]. These criteria are, in general, underpinned by a comprehensive suite of transient analysis. A gap analysis will be required at a future date in order to identify and additional analyses required to underpin the demonstration of ALARP within a UK context.

14.6.3.1 AOO Acceptance Criteria

The following are the specific acceptance criteria for AOOs:

- Pressure in the reactor coolant and main steam systems shall be maintained below 110 percent of the design values in accordance with the American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code [54].
- Fuel cladding integrity shall be maintained by ensuring that the minimum Departure from Nucleate Boiling Ratio (DNBR) remains above the 95/95 DNBR limit.
- An AOO should not generate a postulated accident without other faults occurring independently or result in a consequential loss of function of the RCS or reactor containment barriers.

14.6.3.2 DBA Acceptance Criteria

Unlike an AOO, a DBA could result in sufficient damage to preclude resumption of plant operation. The following are the specific acceptance criteria for DBAs under the US NRC regulatory regime:

- Pressure in the RCS and main steam system should be maintained below acceptable design limits, considering potential brittle as well as ductile failures.
- Fuel cladding integrity will be maintained if the minimum DNBR remains above the 95/95 DNBR limit. If the minimum DNBR does not meet this limit, then the fuel is assumed to have failed.
- The release of radioactive material shall not result in offsite doses in excess of the guidelines in 10 CFR Part 100 – Reactor Site Criteria [55].
- A postulated accident shall not, by itself, cause a consequential loss of required functions of systems needed to cope with the fault, including those of the RCS and reactor containment system.
- For LOCAs, the following acceptance criteria from 10 CFR 50.46 [31] also apply:
    - The calculated maximum fuel element cladding temperature shall not exceed 2200 °F (or 1204°C).
    - The calculated total oxidation of the cladding shall nowhere exceed 0.17 times the total cladding thickness before oxidation.
    - The calculated total amount of hydrogen generated from the chemical reaction of the cladding with water or steam shall not exceed 0.01 times the hypothetical amount that would be generated if all the metal in the cladding cylinders surrounding the fuel, excluding the cladding surrounding the plenum volume, were to react.
    - Calculated changes in core geometry shall be such that the core remains amenable to cooling.

After any calculated successful initial operation of the Emergency Core Cooling System (ECCS), the calculated core temperature shall be maintained at a low value and decay heat shall be removed for the extended period of time required by the long-lived radioactivity remaining in the core.

14.6.4 CAE Summary

The argument to support Claim 2.1.2.3 is that, whilst yet to be completed, the above methods of computation utilise US best practice as required by the NRC. During Step 2, the SMR-300 TA will complete analysis of several specific initiating events providing confidence in achieving the claim and ensuring UK requirements are met. A gap analysis will be required at a future date in order to identify and additional analyses required to underpin the demonstration of ALARP within a UK context.

14.7 DESIGN BASIS ACCIDENT ANALYSIS

Claim 2.1.2.4: Safety functions and safety measures are identified, categorised and classified based on their importance to nuclear safety for all design basis faults and provide sufficient lines of protection based on the fault frequency and consequence.

Claim 2.1.2.5: Analysis demonstrates that for all design basis faults, the identified safety features, in conjunction with operator actions, enable the plant to reach a safe state.

The aim of the UK DBAA approach for the GDA is to outline the philosophies and approaches to be followed to protect against credible faults, such that risks are reduced to ALARP. As described above, this automatically implies that initiating event frequencies, unmitigated consequences, and the reliability of safety measures are considered. A safety function categorisation and classification process, consistent with UK expectations, will be applied so that each technical topic area can then demonstrate that the associated functional requirements can be met through the ongoing production of UK DBAA. This will then determine whether additional measures may be required, whether there is sufficient Defence in Depth (DiD) and ultimately, and if and how the generic SMR-300 reduces risks to levels that are tolerable and ALARP. In addition, a limited set of US DSAs for the SMR-300 will be developed during step 2. This will be supplemented by a set of UK context UK DBAA to cover the sub-set of faults.

14.7.1 Development of the UK DBAA

In order to meet the requirements for UK context, as defined by the ONR, it is necessary to ensure that the SAPs relevant to the safety analysis approach are met, in particular:

- Fault analysis should be carried out comprising suitable and sufficient design basis analysis, probabilistic safety analysis and severe accident analysis to demonstrate that risks are ALARP – FA.1.
- Fault analysis should identify all initiating faults having the potential to lead to any person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement. – FA.2.
- Fault sequences should be developed from the initiating faults and their potential consequences analysed – FA.3.
- Design basis analysis should be carried out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety measures – FA.4.
- The safety case should list all initiating faults that are included within the design basis analysis of the facility – FA.5.
- For each initiating fault within the design basis, the relevant design basis fault sequences should be identified – FA.6.
- Analysis of design basis fault sequences should use appropriate tools and techniques, and be performed on a conservative basis to demonstrate that consequences are ALARP – FA.7.
- DBA should provide a clear and auditable linking of initiating faults, fault sequences and safety measures – FA.8.

- The design basis analysis should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions - FA.9.
- The safety function(s) to be delivered within the facility should be identified by a structured analysis – EKP.4.
- Safety measures should be identified to deliver the required safety function(s) – EKP.5.
- The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be identified and then categorised based on their significance with regard to safety – ECS.1.
- Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety – ECS.2.

The demonstration that these key principles have been met will require the fault analysis process for the SMR-300 to be configured in order to demonstrate that UK context has been adequately addressed. As a result, the strategy to be adopted for the fault analysis topic area during Step 2 of the GDA process, including how the ALARP principle will be applied, has been described below. This will be commenced in Step 2 with the PSR V1 providing a demonstration of how the design will meet the requirements of ALARP in certain critical design and operating features with the full ALARP demonstration, supported by a full and complete deterministic and probabilistic safety analysis, as applicable to the SMR-300, provided in the (Pre Construction Safety Report) PCSR for the site-specific stage. The fault analysis process will, therefore, develop over the period of the GDA and the site specific application and will be fully described in the HB Safety Assessment Handbook which will be produced in Step 2.

The approach to UK DBAA that will be laid out below is well known to the UK and will consist of the following steps:

Fault analysis will cover the following areas:

- Hazard and fault identification (in plant faults, internal and external hazards).
- Fault screening, grouping and bounding.
- Fault sequence modelling and development.
- Plant condition classes and the estimation of IE/PIE frequencies.
- Radiological consequence analysis methods.
- Fault analysis (DBA, PSA, SAA), defining the applicability of the UK DBAA, PSA and SAA.
- Safety function definition and categorisation and definition of performance (safety functional) requirements.
- Designation and classification of duty and safety structures, systems and components and their implications (including inherent technical characteristics, passive and active systems).
- Definition of key safety parameters and operating limits and conditions.
- Substantiation of safety claims (including V&V requirements for inherent technical characteristics and passive safety systems).
- Structure and content of PFS.
- Structure and content of preliminary engineering schedule.
- ALARP assessment (normal operations and accidents).

The UK DBAA will be informed by the US DSA which forms the basis for the PSAR for the SMR-300, which will be constructed in accordance with the requirements set out by the US NRC. These requirements have been established based on over 70 years of relevant experience in the design, safety justification and safe operation of light water reactors. Within this approach, the safety analysis examines a set of reference faults which are considered to be representative and bounding for the reactor plant in terms of the potential to place demands on systems in order to deliver the fundamental nuclear safety functions of:

- Control of reactivity.
- Removal of heat from the reactor and from the fuel store.
- Confinement of radioactive substances, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

It should be noted that in the UK, the confinement function is often separated into a confinement function to protect against release or redistribution of radioactive material and a shielding related function to protect against the effects of direct radiation exposures. This has been captured in the UK context PFS in the 'Other' safety function. An integral output to drive this process is the development of the PFS.

A key activity for the GDA is the production of a strategy for development of the fault analysis topic area. This strategy will explain:

- How the current (US DSA) licensing basis events within the SMR-300 based on NRC guidance have been developed and what the evidence is for their derivation as the bounding set of reference faults.
- How international OPEX (NRC and IAEA supplemented by other LWR UK GDA projects) will be brought together in Subject Matter Expert (SME) workshops to identify a set of Initiating Events that cover a complete set (entire plant design basis) PIEs for (UK DBAA) analysis, addressing all relevant aspects of the nuclear power plant and its operating states, including highlighting specific faults which have been eliminated by the SMR-300 design.
- How the identification of potential faults and hazards associated with novel or unique aspects of the SMR-300 design will be undertaken.
- How individual PIEs will be assigned a frequency band and unmitigated consequence and, subsequently a safety function category (including the process for safety function categorisation).
- How the requirements for safety systems to deliver categorised safety function(s) are addressed within the design, including the classification of such systems.
- How the output of the process will be documented in a PFS across the entire plant design basis, to then be used by the technical topic areas in the PSR, the PCSR and the subsequent stages.

14.7.2 Licensing Basis Event and Design Basis Alignment

UK DBAA is an essential component of the wider demonstration that is needed in a UK safety case to show that a facility is fault tolerant of the 'accidents' that occur within the design basis (i.e., transients, internal events, internal and external hazards), that it has adequate DiD, and with a robust demonstration of the fault tolerance of the facility and of the effectiveness of its safety measures.

The Design Basis Condition (DBC) class to be used for the generic SMR-300 is derived from Chapter A2 [3] Target 4 (ONR SAP [32] Target 4), the US Licensing basis events (subchapter 14.5.2 and Table 6) and the DiD requirements.

The DBC classes for the UK SMR-300 are as follows and presented in Table 7:

- **DBC1 (Normal Operation):** Operation within specified operational limits and conditions. For a nuclear power plant, this includes startup, power operation, shutdown, maintenance, testing and refuelling. These events will occur more frequently than once in the lifetime of the plant, and require assessment under UK DBAA, PSA or SAA (depending on their unmitigated consequences). The equivalent US licensing basis event classification is NO.
- **DBC2 (AOO):** A condition of normal operation that is expected to occur one or more times during the life of the plant and requires assessment under UK DBAA, PSA or SAA (depending on the unmitigated consequences). The equivalent US licensing basis event classification is AOO.
- **DBC3a (Frequent DBAs):** A postulated accident that a nuclear facility must be designed and built to withstand by provision of adequate safety measures. DBC3a covers those faults or events occurring more frequently than once in a thousand years and which require assessment under UK DBAA, PSA or SAA (depending on their unmitigated consequences). DBAs are unanticipated occurrences; they are postulated to occur but not expected to occur during the life of the plant. The equivalent US licensing basis event classification is DBA.
- **DBC3b (Infrequent DBAs):** A postulated accident that a nuclear facility must be designed and built to withstand by provision of adequate safety measures. DBC3b covers those faults or events occurring less frequently than once in a thousand years and requires assessment under UK DBAA, PSA or SAA (depending on the unmitigated consequences). DBAs are unanticipated occurrences; they are postulated to occur but not expected to occur during the life of the plant. The equivalent US licensing basis event classification is DBA.
- **DBC4 (Infrequent Faults with Failure of First Line of Defence):** Rare events or faults that are usually referred to as design limiting conditions within the design basis i.e. conditions which are not expected to occur (including failures involving the first line of defence) but are postulated because their consequences could include the potential release of significant amounts of radioactive material: they are the most extreme conditions which must be considered in the design and they represent limiting cases. DBC4 covers those faults or events occurring less frequently than once in ten thousand years and requires assessment under UK DBAA, PSA or SAA (depending on their unmitigated consequences). The equivalent US licensing basis event classification is BDBA. Expected to occur with a frequency >1E-05 pa and they represent the most significant difference between the US and UK approach i.e. they are in the UK design basis but are BDBA for the US.
- **DEC:** BDBA faults or events (which may be severe accidents) are not considered for DBAs, but that are considered in the design process of the facility where significant core damage may occur in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. DECs cover those faults or events occurring less frequently than once in a hundred thousand years and require assessment under UK DBAA, PSA or SAA (depending on the unmitigated consequences). BDBAs are analysed to fully understand the capability of the plant

design. These events are not expected to occur during the life of the plant and are beyond the scope of what a nuclear plant must be designed and built to withstand. The equivalent US licensing basis event classification is BDBA. DEC events are placed in two classes:

- **DEC-A:** Complex sequences which involve failures beyond those considered in the UK DBAA or sequences following more severe initiating events than those considered in the UK DBAA or sequences following more severe initiating events than those considered in the UK DBAA but with additional protection measures that prevent core damage.
- **DEC-B:** Sequences in which the protection systems designed to prevent core or spent fuel damage fail and core or spent fuel damage does occur.

- **Off-Site Emergency (OSE)**: A category of accident with off-site releases requiring implementation of emergency countermeasures. OSE covers those faults or events with potential unmitigated radiological consequences above 100mSv off site. OSE requires assessment under SAA only.
- **DBC0:** Faults or events with radiological consequences to exposed groups below the applicable limits. These faults or events do not require assessment under UK DBAA, PSA or SAA, but may be considered elsewhere in the SSEC. There is no equivalent US licensing basis event classification to this DBC class.

Note that the UK DBC are not assigned a consequence band – the applicability and use of UK DBAA, PSA and SAA for unmitigated radiological consequences to the exposed groups will be derived in the Safety Assessment Handbook. The unmitigated radiological consequences will also be applied in the categorisation of safety functions in accordance with ONR TAG 94 [42] – see subchapter 14.7.

Table 7: UK Plant and Design Basis Condition Classes

<table>
<tr><th>US SMR-300 Frequency Threshold</th><th>UK SMR-300 Plant Condition Class</th><th>DiD Level</th><th>Design Basis Condition Class</th><th>UK IEF Range (/y)</th></tr>
<tr><td>>1/plant year</td><td>Normal Operations</td><td>Level 1 - Prevention of abnormal operation and failure by design</td><td>DBC1</td><td>IEF>1</td></tr>
<tr><td>> 1E-02 / plant-year</td><td>Anticipated Operational Occurrences</td><td>Level 2 - Prevention and control of abnormal operation and detection of failures.</td><td>DBC2</td><td>1>IEF>1E-02</td></tr>
<tr><td>< 1E-02 / plant-year and > 1E-04 / plant-year</td><td>Design Basis Accidents - Frequent Faults</td><td>Level 3 - Control of faults within the design basis to protect against escalation to an accident.</td><td>DBC3a</td><td>1E-02>IEF>1E-03</td></tr>
<tr><td rowspan="2">< 1E-02 / plant-year and > 1E-04 / plant-year</td><td>Design Basis Accidents - Infrequent Faults</td><td rowspan="3">Level 3 - Control of faults within the design basis to protect against escalation to an accident.
Level 4 – Control of severe plant conditions in which the design basis may be exceeded, including protection against further fault escalation and mitigation of the consequences of severe accidents</td><td>DBC3b</td><td>1E-03>IEF>1E-04</td></tr>
<tr><td>Design Basis Accidents - Infrequent Faults with failure of first line of defence</td><td>DBC4</td><td>1E-04>IEF>1E-05</td></tr>
<tr><td rowspan="3"><1E-04 / plant year</td><td>Design Extension Condition (with or without significant core disruption – beyond design basis / severe accidents)</td><td>DEC</td><td>IEF<1E-05</td></tr>
<tr><td>Off Site Emergency (accident with releases requiring implementation of emergency countermeasures)</td><td>Level 5 – Mitigation of radiological consequences of significant release of radioactive material</td><td>OSE</td><td>N/A</td></tr>
<tr><td>No radiological consequences to exposed groups</td><td>N/A</td><td>DB0</td><td>Any</td></tr>
</table>

14.7.3 UK DBAA Methodologies

US methods used are considered best practice for reactor accidents, as the RGs (particularly RG 1.183 Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors [56] and RG 1.203 [25]) are the international standards for calculating releases from reactor accidents.

However, it is recognised that the measures of success in the UK are different – namely the calculation of unmitigated doses and the consideration of on-site exposures as well as off-site exposures. Furthermore, a justification for normal operations and fault conditions is expected to comply with the numerical targets. Chapter A2 [3] introduces the UK numerical targets that will be applied to the generic SMR-300 (which are equivalent to ONR SAPs [32] NT.1 to NT.9).

Assumptions made during the US DSA will need to be validated for the UK DBAA and then extrapolated to give the effective doses to the exposed groups of concern to demonstrate that risks are ALARP. For example, the UK DBAA may depend explicitly or implicitly on a number of limits and conditions, which are important to the safety case.

Limits and conditions fall into three main groups:

- Limits and conditions that identify the initial conditions for transient analysis.
- Limits and conditions that are assumed for the operation of SSCs important for safety.
- Limits and conditions imposed by the analysis to limit effective doses either to the public or to the workforce.

There is a gap with respect to the methodologies and approaches to be adopted for the calculation of unmitigated doses and consideration of on-site exposures as well as off-site exposures to be defined for the generic SMR-300. There is also a gap with respect to the assumptions, methodologies, and approaches to be adopted for the development of the fault analysis, which must be defined for the generic SMR-300, particularly where they differ from the US DSA approach. These will be addressed through the development of a Safety Assessment Handbook representing the methodologies and approaches to be adopted for the development of the fault analysis which will be produced. This document will be focused on the requirements and methods to be applied to PSR development and will include how the approach will then be developed for the future PCSR in order to demonstrate that the risks from the calculated exposures are ALARP.

Fault analysis will cover the following areas:

- Hazard and fault identification (in plant faults, internal and external hazards).
- Fault screening, grouping and bounding.
- Fault sequence modelling and development.
- Plant condition classes and the estimation of IE/PIE frequencies.
- Radiological consequence analysis methods.
- Fault analysis (DBA, PSA, SAA), defining the applicability of the UK DBAA, PSA and SAA.
- Safety function definition and categorisation and definition of performance (safety functional) requirements.

- Designation and classification of duty and safety structures, systems and components and their implications (including inherent technical characteristics, passive and active systems).
- Definition of key safety parameters and operating limits and conditions.
- Substantiation of safety claims (including V&V requirements for inherent technical characteristics and passive safety systems).
- Structure and content of PFS.
- Structure and content of preliminary engineering schedule.
- ALARP assessment (normal operations and accidents).

This document will primarily focus on the requirements and methods to be applied during PSR development but will identify how the approach will then be developed for future PCSRs.

14.7.4 Safety Function Alignment, Safety Function Categorisation and SSC Classification

In order to address a gap in the alignment between safety importance of engineered systems and the associated quality requirements for the design, analysis, manufacture, test, inspection and certification of such systems, the NRC developed a quality classification system in the 1970s to provide licensees with guidance. This was intended to assist licensees in meeting the requirements set out in GDC 1, namely that related to quality standards and records. The resulting RG 1.26 [27] sets out this guidance which comprises four distinct quality (for safety) groups, as applicable to PWRs, groups A-D. This is expanded on in Chapter A2 [3].

It is acknowledged in Chapter A2 [3] that there will be a need to align the fundamental safety functions and SMR-300 high-level safety functions (Table 4) to include the faults and hazards outside of the reactor building. In addition, Chapter A2 [3] identifies that a UK-specific approach to safety function categorisation and safety system classification is required to demonstrate completeness in terms of UK context.

The safety function categorisation and safety system classification process identified in the Safety Assessment Handbook will be used to inform design teams during Step 2 for them to consider whether the associated functional requirements can be met, whether additional measures may be required, whether there is sufficient DiD and as necessary, input to any ALARP considerations. No formal analysis of SSC substantiation is anticipated within the PSR stage.

14.7.5 Preliminary Fault Schedule

A fault schedule is a UK-specific way of presenting the fault sequences and showing the golden thread from event identification to safety measure justification and sits alongside the CAE hierarchy of the safety case. The ONR considers a comprehensive fault schedule to be a vital part of any safety case and is often the place of entry for a safety case professional or operator into the detailed analysis or safety case discussion. For GDA, a complete fault schedule is a very useful vehicle for the RP to demonstrate to ONR the completeness and coherence of the safety case and the robustness of the design and it is a regulatory expectation of the GDA that the fault analysis scope will be presented in a fault schedule (ONR-GDA-GD-007 [34]). However, fault schedules are not widely used or understood by overseas reactor vendors and, as it is not required for the US design. A PFS that captures the UK DBAA approach and shows the golden thread through the PSR will need to be produced in accordance with the methodology to be outlined in the Fault Studies Strategy.

A PFS will be derived based on relevant PWR OPEX, other GDA projects, and examination of any novel or unique features of the SMR-300 design which will then be used to signpost to the relevant technical topic areas. This document will present the PFS as applicable to Step 2 as a comprehensive list of relevant identifiable initiating faults which could lead, either directly or in combination with other failures, to a radiological consequence. It will detail the IE/PIE frequency band (i.e., the plant condition class) and the estimated unmitigated radiological consequences with each PIE. It will provide a listing of the safety functions relevant to each fault, their category and the corresponding SSC(s) designed to prevent or mitigate the consequence, together with the SCC(s) preliminary classifications. The equivalent safety system classifications from the US process (Holtec SMR Safety Classifications A-F) will also be presented and any differences explained.

The PFS will then provide the “handshake” element of the transition to the technical topic areas for assessment and resolution of the claims and demands that the safety analysis places on the design in terms of the number, type, quality and performance of safety structures, systems and components and any necessary human factors considerations. Through the provision of the PFS, and other documents, should novel areas or areas warranting further consideration arise, additional interfaces/documentation may be required (this could either be part of GDA documentation or for future design phases). For any such issues, they shall be dealt with on a case-by-case basis involving the required topic areas and stakeholders.

At PCSR maturity, the documentation created at the PSR stage will be expanded upon to have a fully developed set of faults, such that all credible faults have been identified for the SMR-300 and have been recorded in the PFS.

Within the PFS, the information in Table 8 will be provided.

Table 8: Preliminary Fault Schedule Content

Heading	Content
Fault ID and Fault Ref	Discrete Identification Number is provided for each fault entry. Separate faults may be identified for the same initiating event occurring during different operating mode(s), or in different locations within the plant where unique consequences may result. The Fault Ref column serves to provide references or IDs for the fault in HAZID studies or references for traceability of the fault elsewhere where it is discussed in more detail.

Heading	Content
Initiating Event (Fault and Consequences)	A brief description of each initiating fault and the unmitigated consequences of the fault progressions are given. The fault consequence column provides a description of the state of the plant following the initiating fault. The information in this column does not provide details of how the fault is mitigated, which is provided in the following columns.
Consequences	Description of unmitigated consequences including challenge to structures and barriers
Reactor Operating Modes Affected	This column indicates the reactor operational Modes impacted (PS1 to PS6) where the fault is applicable. Different Modes of operation may be pertinent to different faults.
Safety Function	This column provides the fundamental safety function challenged by the initiating event.
Initiating Event Frequency (PCC)	This column provides the initiating event frequency (DBC/DEC class) information for the fault and the event classification.
Radiological Impact / Consequence Bands	This set of columns is intended to provide information on dose bands for both On-Site and Off-Site for comparison against Chapter A2 [3] Target 4 [32] (SAP NT.4).
Safety Function Category	This column provides information on the preliminary categorisation of the safety functions (Cat A-C).
Duty System	This set of columns is intended to provide information on the detail of duty (NO/DBC1) system which fails, the DiD level 1 or 2 (preventative) associated with the duty system and System Design Descriptions (SDD) reference for the system. This will also include the preliminary classification of the duty safety systems(s) based on the IEF claim.
Principal Safety System	This set of columns is intended to provide information on the detail of the principal safety systems in place. This includes information on the lower level safety function to be delivered e.g. short term cooling and the DiD level (2,3, or 4) associated with the system. This will also include information on signal/actuation (the means of detection/activation for the system) and the action taken in response (i.e. automatic or operator), the preliminary classification of the safety systems based on the safety function category and its relative importance in the delivery of the specific safety function and the details of the SDD. The minimum number of trains required to deliver the safety function will be provided. The preliminary US quality or safety classification (NRC) and the reliability/probability of failure on demand (PFD) claim will also be included.
Secondary and Supporting Safety Systems	This set of columns is intended to provide information on the secondary and supporting safety systems in place. This includes information on the lower level safety function to be delivered e.g. short term and long term cooling, information on signal/actuation (the means of detection/activation for the system and action taken in response i.e. automatic or operator), the DiD level (2, 3, or 4) associated with the system and the preliminary classification of the safety systems based on the safety function category and its relative importance in the delivery of the specific safety function. The details of the SDD, minimum number trains required to deliver the safety function and the PFD will be provided. Detail on the preliminary US quality or safety classification (NRC) will also be included.
Status vs Design Basis Targets (T4)	This column will provide discussion on whether the claimed safety systems can meet T4 targets and how i.e. through frequency, consequence or residual risk reduction.
Additional Defence-in-Depth Provisions	This column will provide a list of any additional safety systems not claimed in DBA but that will contribute to PSA/SAA as part of DiD.
Essential Support Systems	This column will provide information on any essential support systems e.g. containment functions, power cooling water requirements, human resource etc.
Potential Common Mode or Cause Failure	This column will provide detail on any potential common mode or cause failure which may impact on the delivery of the safety functions.
Comments	This column will provide cross references to supporting analysis or discussion including reference to the engineering schedule for details relevant to each claimed system. Clarifications, nuances, exceptions, and any additional detail not contained within the other columns are included in this column.

14.7.6 Extent of Fault Analysis for PSR Revision 1

The extent of the deterministic safety assessment available to support PSR Revision 1 will be limited. The aim is that the analysis in the US produced US DSAs will be used to provide exemplars within the PSR; the extent will be limited in that it will be limited to the LBEs required by the NRC. Hence, the fault analysis at PSR Revision 1 (i.e. UK DBAA equivalent) will aim to provide confidence in the strategy and proposed approach.

Hence, to prove confidence in the strategy for fault analysis, several representative events have been chosen and will be subjected to the full methodology to demonstrate that it is effective and to provide a benchmark against which to draw comparisons against the Quality Classes defined by RG 1.26 and presented within Annex B.

The following faults have been chosen for this demonstration. They have been selected on the basis of two fault groups which are chosen from the LBEs and a further four faults from the early identification work streams to develop the PFS. The intention is to also use a spread of fault types to demonstrate the approach. The proposed faults are:

1. A DEC-A fault involving a DBC2 or DBC3a fault (e.g. failure of auxiliary lines carrying outside containment) coupled with an AR failure – selected as a demonstration of the deterministic approach to be applied to DEC faults and to assess a novel design feature (PFS fault).
2. Steam generator tube rupture – selected as DBC3a fault (LBE and PFS fault).
3. Turbine trip (DBC2) including coincident with a LOOP (LBE and PFS fault).
4. Increased heat removal fault requiring activation of passive decay heat removal (PDH, SDH) e.g. large or intermediate main steam line break – selected as DBC3b or DBC4 fault (PFS fault).
5. Small break LOCA – selected as DBC3 fault (LBE and PFS fault).
6. Long term LOOP in excess of 72 hours – selected as DBC2 fault (LBE and PFS fault).

For each of the faults identified for development, the output will be based on the following outline structure and content:

- Fault Title (e.g. small break LOCA).
- Description of fault - summary of PFS entry with some information on IEs e.g. mechanical failure of valve, spurious actuation (I&C failure or operator error) and relevant plant state, DBC class and SFC category.
- Acceptance criteria - statement of relevant acceptance criteria for DBC class & fault.
- Detection and action - means of detection of fault transient and initiation of action.
- Safety functions - list of safety functions impacted by fault and functions required to be achieved to reach controlled and safe state (e.g. reactor trip actuated on “pressure drop of SG high 0” signal, turbine trip and isolation of the full load main feedwater lines on all SGs actuated on receipt of reactor trip signal, ASDS actuated by “SG pressure high 1” signal).
- Event Sequences - summary of how event progresses from fault to controlled state and safe state (including what each of those states actually is).
- Single Failure Considerations - assessment of single failure criterion and any common cause failures.

- Analysis - summary of analysis assumptions, extent of deterministic analysis undertaken (or due to be performed), applicable codes & models, results of analysis (if available or when they are expected to be available e.g. PCSR stage).
- Mitigated Radiological Consequences - presentation of mitigated consequences.
- Conclusions - summary of conclusion of analysis.

In some cases, the SMR-300 US DSA will be able to be applied directly and will provide the analysis, arguments and evidence necessary. In certain other cases, there will not be a full US DSA available; in such cases, the demonstration fault analysis will include as much information as is available and will set out the scope of work which is required to be completed.

14.7.7 CAE Summary

The argument to support Claim 2.1.2.4 is that, whilst yet to be completed, the above methodology aligns with UK best practice for production of a UK DBAA. The US developed US DSA will provide a substantial source of information and will be aligned and utilised where appropriate during the UK DBAA development. A clear method for the identification, categorisation and classification of Safety Functions and Safety Measures is understood and will be developed in more detail through the production of Safety Assessment Handbook.

The argument to support Claim 2.1.2.5 is that whilst yet to be completed, described within is a methodology to enable the completion of Claim 2.1.2.5 via the generation of the PFS. The evidence will be generated within Step 2 by assessment of a limited number of faults providing confidence in the PFS methodologies to be applied to all faults.

14.8 CHAPTER SUMMARY AND CONTRIBUTION TO ALARP

This sub-chapter provides an overall summary and conclusion of the Safety and Design Basis Accident Analysis Chapter and how this Chapter contributes to the overall demonstration of ALARP for the generic SMR-300. PSR Part A Chapter 5 Summary of ALARP [57] sets out the overall approach for demonstration of ALARP and how contributions from individual chapters are consolidated.

This subchapter therefore consists of the following elements:

- Technical Summary
- ALARP Summary
    - Review against Relevant RGP
    - Demonstration Against Risk Targets
        - Evaluation of Risk
    - Risk Reduction Options
    - GDA Commitments and Forward Actions
- Conclusion

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

14.8.1 Technical Summary

As set out in Chapter A3 [2], this chapter presents the UK DBAA topic for the generic SMR-300 to support Claim 2.1.2:

Claim 2.1.2: The design basis analysis demonstrates that the risk from design basis faults associated with the operation of the generic Holtec SMR-300 are tolerable and As Low As Reasonably Practicable (ALARP).

Claim 2.1.2 has been further decomposed within Chapter B14 into five Level 4 claims which have been demonstrated throughout this chapter. This chapter explains:

- The CAE that are relevant for the UK DBAA of the generic SMR-300.
- The codes and standards that demonstrate UK RGP for the generic SMR-300 undergoing GDA. **(Claim 2.1.2.1)**
- The US DSA undertaken for the SMR-300 provides a useful input into the development of the UK DBAA, and can be considered to represent RGP transient analysis for PWRs for the reasons set out below:
    - Safety functions have been defined for the reactor consistent with the US NRC [48] and 10 CFR 50 Chapter 2 [31] .
    - The initial list of bounding PIEs in Table 56 has been produced, consistent with the guidance provided by NUREG-0800, Chapter 15 [53]. It has been informed by engineering judgements by suitably qualified and experienced engineers via a combination of deterministic assessment and probabilistic assessment, together with OPEX from the PWR fleet. **(Claim 2.1.2.2)**
- The assessment of accidents and transients including acceptance criteria and analysis methodologies for all operating modes of the reactor, including limiting single failures and conservative operating conditions, to ensure that the assessment of transients and

accidents is carried out according to industry good practice and modern standards. **(Claim 2.1.2.3)**
- The approach, strategy and methodology for production of a UK DBAA utilising US DSA input. **(Claim 2.1.2.4)**
- The approach, strategy and methodology for productions of a PFS. **(Claim 2.1.2.5)**

Throughout this chapter and in support of all claims, the appropriate methodology in accordance with RGP and UK licensing requirements have been identified. It is acknowledged that the US DSA provides a substantial source of information but does not meet UK licensing requirements. Whilst information from the US DSA will be utilised in the development of the UK DBAA, gaps have been identified and will be addressed. In order to provide confidence in this approach, during Step 2, the SMR-300 TA will complete analysis of several specific initiating events ensuring UK requirements are met for safety analysis and the ALARP principle is demonstrated.

14.8.2 ALARP Summary

14.8.2.1 Review against RGP

In the UK, meeting the design basis and probabilistic targets alone is not sufficient to demonstrate that the plant is adequately safe. There is the additional requirement that the risk must be demonstrated to be ALARP.

The DB assessment and PSA provide insights for use in the design of the safety measures used to provide the significant safety functions to meet DB and probabilistic targets. It is an additional requirement in the UK that the risks from faults to the public, workforce and environment should be ALARP. As part of the assessment of each fault, an assessment is made of other measures that might be claimed to decrease the risk from the fault. Whether or not these measures are claimed is based on whether to do so would be considered reasonably practicable.

The ALARP assessment determines if there are any reasonably practicable means to further reduce the risk from individual faults, including the identification of SSCs for DiD and in the safety case as a whole. As a result of the ALARP assessment, other SSCs may be identified as providing DiD or reducing risk in other ways.

In future, this section will present the most significant nuclear safety risks associated with the SSCs within the scope of this chapter, a high-level overview of how the ALARP principle has been applied for UK DBAA and how this contributes to the overall ALARP argument for the generic SMR-300. The UK DBAA is a crucial part of the demonstration that those risks are ALARP.

The ALARP considerations will follow the approach discussed in Chapter A5 [57] and will consider:

- completeness of hazard identification.
- adequate DiD and diversity in the design.
- the margins to acceptance criteria not being met.

14.8.2.2 Demonstration Against Risk Targets

The numerical targets against which the demonstration ALARP is considered can be found in Chapter A2 [3]. The UK DBAA will identify SSCs, which through the defined safety functions, will contribute to the demonstration of ALARP by comparison against the risk targets in two ways:

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

Risks above the Basic Safety Limit (BSL) are not acceptable. Risks below the BSL require a demonstration of ALARP proportionate to the level of risk. The Basic Safety Objective (BSO) represents the modern safety standards and expectations against which the UK Generic SMR-300 will be assessed.

14.8.2.2.1.1 Evaluation of Risk

At this time, the evaluation of the normal operations and accident risks against Targets 1-9 of the SAPs [32] has not been presented. This information will be presented in later versions of this PSR Chapter, PSR Part B Chapter 9 Conduct of Operations [58] for normal operations, Chapter B15 [4], and PSR Part B Chapter 16 Probabilistic Safety Analysis [5] for accident conditions.

14.8.2.3 Risk Reduction Options

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

Revision 1 of this PSR, will summarise those option evaluations, and briefly explore if other risk reduction options have or could be considered and either:

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

The process for the assessment of risk reduction options is presented in Generic Design Assessment Reference Design Process and GDA Prospective Design Change Register [59]. Chapter A5 [57] considers the holistic risk-reduction process for the Generic SMR-300.

14.8.2.4 GDA Commitments and Forward Actions

Forward Actions have been collated and arranged via the process described in PSR Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance [60]. Chapter A5 [57] describes the contribution of the forward actions to the ALARP argument.

14.8.3 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.
- Methodologies to identify, screen and group PIEs have been recognised to align with UK licensing requirements.
- Methodologies for transient and accident analysis in accordance with best practice whilst appropriately utilising US DSA data are understood.
- Methodologies for identification, categorisation and classification of safety functions and safety measures whilst ensuring sufficient DiD have been identified.
- Demonstration that the strategy and methodology are likely to result in an assessment that reduces risks to ALARP.
- Identification of Forward Action Plan for future activities for developments beyond PSR stage. It is expected that this includes the further assessment of the SMR-300 design as further design basis details become available to ensure that any additional faults have been identified and their fault sequences developed such that suitable and sufficient safety measures are identified. The outputs of this work will result in an updated Fault and Engineering/ SSC Schedule to capture this information.

The UK DBAA considerations in this chapter will culminate in a conclusion of the adequacy of the design with respect to UK DBAA criteria. At PCSR maturity, the documentation created at PSR stage will be expanded upon to have a fully developed set of faults such that all credible faults have been identified and assessed for the SMR-300 and have been recorded in the PFS.

14.9 REFERENCES

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

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

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

[4] Holtec Britain, "HI-2240346, Holtec SMR GDA PSR Part B Chapter 15 BDBA, Severe Accidents Analysis and Emergency Preparedness," Revision 0, August 2024.

[5] Holtec Britain, "HI-2240347, Holtec SMR GDA PSR Part B Chapter 16 Probabilistic Safety Assessment," Revision 0, August 2024.

[6] Holtec Britain, "HI-2240348, Holtec SMR GDA PSR Part B Chapter 17 Human Factors," Revision 0, August 2024.

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

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

[9] American Society of Mechanical Engineers, "Addenda to ASME/ANS RA-S-2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," ASME/ANS RA-Sb-2013..

[10] "IAEA, Defining Initiating Events for Purpose of Probabilistic Safety Assessment, IAEA-TECDOC-719, IAEA, Vienna (1993)".

[11] NUREG/CR-2300, PSA Procedures Guide, January 1983..

[12] NUREG/CR-4550, Analysis of Core Damage Frequency From Internal Events: Methodology Guidelines, September 1987..

[13] NUREG-1829, Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process, 04/2008..

[14] NUREG/CR-5750, Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995, 02/1999..

[15] NUREG/CR-6928, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, 02/2007 as updated through 2017 on NRC Website https://nrcoe.inl.gov/resultsdb Initiating Events Data through 2017.

[16] “ANSI/ANS-58.14-2011 (R2017) Safety And Pressure Integrity Classification Criteria For Light Water Reactors”.

[17] United States Nuclear Regulatory Commission, NRC Regulations Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criteria for Nuclear Power Plants.

[18] I. N. Labratory, “INL/RPT-23-72818, Initiating Event Rates at US NPP, 2022 Update,” June 2023.

[19] Nuclear Energy Institute (NEI), “Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development,” NEI 18-04, Revision 1.

[20] “NUREG/CR-4483, “Reactor Pressure Vessel Failure Probability Following Through-Wall Cracks Due to Pressurized Thermal Shock Events,” 1986”.

[21] “NUREG-0651, “Evaluation of Steam Generator Tube Rupture Events, U.S. Nuclear Regulatory Commission,” March 1980”.

[22] “NUREG/CR-6890, "Reevaluation of Station Blackout Risk at Nuclear Power Plants," December 2005”.

[23] “NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," February 2007”.

[24] “NUREG-1829, “Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process,” April 2008”.

[25] US NRC, “Regulatory Guide 1.203, Transient and Accident Analysis Methods,” December 2005.

[26] US NRC, “Regulatory Guide 1.233, Guidance for a technology-inclusive, risk-informed, and performance-based methodology to inform the licensing basis and content of applications for licences, certifications, and approvals for non-light-water reactors, Revision 0,” June 2020.

[27] US NRC, “Regulatory Guide 1.26, Quality Group Classifications and Standards for Water, Steam, and Radioactive Waste-Containing Components of Nuclear Power Plants, Revision 6,” December 2021.

[28] "IAEA, Generic Initiating Events for Psa for WWER Reactors, IAEA-TECDOC-749, IAEA, Vienna (1994)".

[29] IAEA, Safety of Nuclear Power Plants: Design. Specific Safety Requirements No. SSR-2/1, Revision 1, 2016.

[30] IAEA, "Specific Safety Guide SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants," 2014.

[31] US NRC, "Regulation 10 CFR Part 50 - DOMESTIC LICENSING OF PRODUCTION AND UTILIZATION FACILITIES".

[32] ONR, Safety Assessment Principles For Nuclear Facilities, Revision 1, January 2020.

[33] ONR, ONR-GDA-GD-006, New Nuclear Power Plants: Generc Design Assessment Guidance to Requesting Parties, Revision 0, October 2019.

[34] ONR, ONR-GDA-GD-007, New Nuclear Power Plants: Generic Design Assessment Technical Guidance, Revision 0, May 2019.

[35] ONR: NS-TAST-GD-005 Guidance on the Demonstration of ALARP, Revision 11.2, June 2023.

[36] Office for Nuclear Regulation, "NS-TAST-GD-006, Design Basis Analysis, Issue 5.1".

[37] " NS-TAST-GD-034 ONR Technical Assessment Guides (Transient Analysis for DBAs in Nuclear Reactors)".

[38] "NS-TAST-GD-035 ONR Technical Assessment Guide (TAG) Limits and Conditions for Nuclear Safety (Operating Rules)".

[39] ONR: NS-TAST-GD-036, Diversity, Redundancy, Segregation and Layout of Mechanical Plant, Revision 3, November 2023.

[40] "NS-TAST-GD-04 Nuclear Safety Technical Assessment Guide - Validation of Computer Codes and Calculation Methods".

[41] ONR: NS-TAST-GD-051, The Purpose, Scope and Content of Safety Cases, Revision 4, December 2022.

[42] ONR, "ONR-TAG NS-TAST-GD-094, "Categorisation of Safety Functions and Classification of Structures, Systems and Components, Revision 2," 2019.

[43] IAEA: Deterministic Safety Analysis for Nuclear Power Plants, No. SSG-2, Revision 1, 2019.

[44] IAEA: Safety of Nuclear Power Plants: Commissioning and Operation Specific Safety Requirements No. SSR-2/2 (Rev.1). IAEA. Vienna. 2016.

[45] WENRA, Safety Reference Levels for Existing Reactors, February 2021.

[46] WENRA: Report on Safety of new NPP designs, March 2013.

[47] WENRA: WENRA Statement on Safety Objectives for New Nuclear Power Plants, November 2010.

[48] US NRC, "NUREG -0800 Standard Review Plan BTP 7-19, Guidance for Evalution of Defense in Depth and Diversity to Address Common Cause Failure Due to Latent Design Effects in Digital Safety Systems', Revision 8," January 2021.

[49] Westinghouse Electric Company, "Westinghouse Design Control Document - Tier 2 - Chapter 15 - Accident Analyses," Revision 19, June 2011.

[50] NuScale Power LLC, "Chapter 15: Transient and Accident Analyses," Revision 5, July 2020.

[51] Holtec International, "HI-2240626, SMR-300 Initiating Event Identification and Classification," 2024.

[52] United States Nuclear Regulatory Commission, "Appendix A to Part 50 - General Design Criteria for Nuclear Power Plants".

[53] US Nuclear Regulatory Commission, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Transient and Accident Analysis," NUREG-0800, Chapter 15.

[54] ASME, Boiler and Pressure Vessel Code, Section III-Rules for Construction of Nuclear Facility Components, 2022.

[55] US NRC, "10 CFR PART 100—REACTOR SITE CRITERIA," 2015.

[56] "RG 1.183, Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors" (Rev. 0, July 2000)".

[57] Holtec Britain, "HI-2240336, Holtec SMR GDA PSR Part A Chapter 5 Summary of ALARP," Revision 0, August 2024.

[58] Holtec Britain, "HI-2240340, Holtec SMR GDA PSR Part B Chapter 9 Conduct of Operations," Revision 0, August 2024.

[59] Holtec Britain, “HPP-3295-0017, Holtec SMR-300 Generic Design Assessment Reference Design Process and GDA Prospective Design Change Register,” Revision 1, TBC.

[60] Holtec Britain, “HI-2240335, Holtec SMR GDA PSR Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance,” Revision 0, August 2024.

[61] “RG 1.157, "Best-Estimate Calculations of Emergency Core Cooling System Performance” (Rev. 0, May 1989)”.

[62] US NRC, “Regulatory Guide 1.145, Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants,” February 1993.

14.10 LIST OF APPENDICES

Appendix A CAE Route Map

Table 9: Chapter B14 CAE Route Map

Overarching SSEC Claim	Chapter Claim/s	Chapter Sub Claim	Chapter Section
Claim 2.1 – Nuclear Safety **The nuclear safety assessment identifies plant initiating events and specifies the requirements for safety measures such that safety functions are fulfilled, informs operational and emergency arrangements and demonstrates that risk is tolerable and As Low As Reasonably Practicable (ALARP).**	**Claim 2.1.2** The design basis analysis demonstrates that the risk from design basis faults associated with the operation of the generic Holtec SMR-3300 are tolerable and As Low As Reasonably Practicable (ALARP).	**Subclaim 2.1.2.1** Plant initiating events are identified, and Design Basis Accident Analysis undertaken, using appropriate methodologies.	14.4 Codes and Standards
		Subclaim 2.1.2.2 A comprehensive set of plant initiating events are identified, screened and appropriately grouped into design basis faults.	14.5 PIE Identification, Screening & Grouping
		Subclaim 2.1.2.3 The assessment of Transients and Accidents shall be undertaken in accordance with best practice analysis methods.	14.6 Application and Use of Transient and Accident Analysis Computer Codes
		Subclaim 2.1.2.4 Safety functions and safety measures are identified, categorised, and classified based on their importance to nuclear safety for all design basis faults and provide sufficient lines of protection based on the fault frequency and consequence.	14.7 Design Basis Accident Analysis and Preliminary Fault Schedule
		Subclaim 2.1.2.5 Analysis demonstrates that for all design basis faults, the identified safety features, in conjunction with operator actions, enable the plant to reach a safe state.	14.7 Design Basis Accident Analysis and Preliminary Fault Schedule

Appendix B Use of Modelling Codes in Transient Analysis

This appendix summarises the computer programs that are used in the transient analysis and the methodologies used for demonstrating the established acceptance criteria have been met. There are three main steps:

Thermal hydraulic analysis:

- The transient and accident analysis calculations start with thermal hydraulic analysis using the RELAP5-3D code. The RELAP5-3D calculations determine whether the acceptance criteria for RCS and Main Steam System (MSS) pressure, as well as the LOCA acceptance criteria are satisfied.

Subchannel analysis:

- The outputs from RELAP5-3D will be used as input to the subchannel analysis code COBRA-FLX to determine whether the acceptance criteria for DNBR and Fuel Centreline Melt (FCM) temperature are satisfied. If COBRA-FLX predicts any fuel failure, then the resulting source term in the RCS is considered.

Containment Analysis:

GOTHIC is used to determine the mass and energy release into containment from events such as a LOCA or Main Steam Line Break (MSLB). These events do not challenge pressure and temperature design limits of the containment. As a result, any releases outside containment are calculated using the maximum allowable containment leakage rate.

Containment bypass events consider the design basis source term in the primary and secondary coolant, as appropriate, so that the resultant radiological consequences off-site can be calculated.

The following subchapters describe the methodology and computer codes for each of these steps. Once the point of release and the specific characteristics have been determined, the radiological consequences can be calculated.

Thermal Hydraulic Analysis Methodology

RELAP5-3D

RELAP5-3D is the system thermal-hydraulics code used for predicting the RCS performance during an accident analysis. The code was developed by Idaho National Laboratory (INL), sponsored by the U.S. Department of Energy (DOE). This tool is used for calculating many complex integrated phenomena such as the heat transfer to the RCS, fluid flow through the coolant loop, steam generation, and the ESFs processes among other phenomena. It is an industry standard computer code used in best-estimate transient simulation of light water reactor coolant systems during postulated accidents.

The code models the coupled behaviour of the RCS and the core for accidents and operational transients such as ATWS, LOOP, loss of feedwater, and loss of flow. A generic modelling approach is used that permits simulating a variety of thermal hydraulic systems. Control system and secondary system components are included to permit modelling of plant controls, turbines, condensers, and secondary feedwater systems to the extent necessary for accurate modelling of each transient and accident.

Modelling Parameters

As part of the Limit of Operating Envelope (LOE) approach, modelling parameters are generally assigned to their best estimate values. Biases and uncertainties associated with the modelling parameters are reviewed and identified. At this time, a code assessment of RELAP5-3D versus testing data specific to the SMR-300 has not been performed. Therefore, the biases and uncertainties of the modelling parameters are not accounted for. A more detailed analysis of modelling parameter biases and uncertainties will be implemented later.

Although biases and uncertainties of the RELAP5-3D model are not accounted for at this time, sensitivities may be performed on some modelling options. For example, events that involve a pipe rupture may perform sensitivities on the critical flow model.

Traditionally, the biases and uncertainties associated with the modelling parameters of a computer code are accounted for first. However, since biases and uncertainties are not accounted for at this time, sensitivities of any model options are performed after the combination of LOE conditions, single failures, and non-safety systems operation that produce the most limiting results have been determined. The basis for performing the modelling option sensitivities last is to ensure that they are applied conservatively. For example, without computer code validation, it is not known whether a modelling option sensitivity is conservative for one LOE condition but not another.

Initial Conditions

The LOE analysis approach is based on a conservative application of key operating parameters. Parameters related to safety system performance are conservatively set at their safe operating limits while key modelling parameters are set at their best estimate values. The relevant modelling parameters set at their best estimate values are also consistent with the guidance in RG 1.157 [61]. It should be recognised that the LOE analysis approach assumes an unlikely occurrence of a plant configuration where key systems and components are simultaneously operating at their safe operating limits. The LOE approach results in conservative and bounding results.

Subchannel Analysis Methodology

COBRA-FLX

The computer code, COBRA-FLX, is the primary computational tool to thermal-hydraulically analyse the fluid conditions in core subchannels under steady-state or transient conditions. COBRA-FLX is derived from the COBRA family of codes and based on COBRA-TF (Coolant Boiling in Rod Arrays – Two Fluid).

COBRA-FLX is a Thermal/Hydraulic (T/H) simulation code designed for LWR vessel analysis. It uses a two-fluid, three-field (i.e., liquid film, fluid drops, and vapor) modelling approach. Both sub-channel and 3D Cartesian forms of nine conservation equations are available for LWR modelling. The code was originally developed by Pacific Northwest Laboratory in 1980 and had been used and modified by several institutions over the last few decades.

Core Physics Codes

The core physics codes suite, described below, are developed by Studsvik Scandpower, Inc.

CASMO5: A state of the art lattice physics code for modelling PWR and Boiling Water Reactor (BWR) fuel. The code uses 586 group neutron data and 18 group gamma data from ENDF/B-VII nuclear data library. The 18 group gamma data is suitable for gamma sensitive in-core detector modelling and gamma energy deposition calculations. One of the principal purposes of CASMO5 is to generate Multigroup cross sections, discontinuity factors, and control rod depletion data for use in the advanced core simulator SIMULATE5 code.

CASMO5: A state of the art lattice physics code for modelling PWR and Boiling Water Reactor (BWR) fuel. The code uses 586 group neutron data and 18 group gamma data from ENDF/B-VII nuclear data library. The 18 group gamma data is suitable for gamma sensitive in-core detector modelling and gamma energy deposition calculations. One of the principal purposes of CASMO5 is to generate Multigroup cross sections, discontinuity factors, and control rod depletion data for use in the advanced core simulator SIMULATE5CMSLINK5: A utility or linking code that processes CASMO5 card image files into a binary formatted nuclear data library for use by SIMULATE5/SIMULATE-3K. CMSLINK5 code collects the following data from CASMO5 card image files:

- Multigroup macroscopic/microscopic nodal cross sections.
- Multigroup submesh macroscopic cross sections.
- Detector data.
- Pin power reconstruction data.
- Kinetics data.
- Isotopics data.
- Spontaneous fission data.

SIMULATE5: A diffusion code that solves the multigroup diffusion or, optionally the simplified P3 transport equations. Cross sections are described by a hybrid microscopic-macroscopic model that includes 50 isotopes (17 actinides and 30+ fission products and burnable absorbers). It is a 3-D, steady state, multi-group nodal code for analysis of both PWRs and BWRs.

SIMULATE-3K: A transient analysis code that models the nuclear core of commercial PWR and BWR are using three-dimensional diffusion theory. Detailed thermal-hydraulic feedback is modelled on the same mesh as the nuclear model.

Modelling Parameters

As part of the LOE approach, modelling parameters are generally assigned to their best estimate values. Biases and uncertainties associated with the modelling parameters are reviewed and identified. At this time, a code assessment of COBRA-FLX versus testing data specific to the SMR-300 has not been performed. Therefore, the biases and uncertainties of the modelling parameters are not accounted for. A more detailed analysis of modelling parameter biases and uncertainties will be implemented later.

Initial Conditions

Framatome's COBRA-FLX subchannel model receives time dependent boundary conditions from the RELAP5-3D transient run. These boundary conditions include core exit pressure, core flow, core inlet temperature, and total reactor power.

Since the RELAP5-3D model does not model individual fuel assemblies, but rather groups of common fuel assemblies in channels, the channel flow from RELAP5-3D must be converted into a single fuel assembly flow. To calculate an individual assembly flow for COBRA-FLX, the RELAP5-3D channel flow is divided by the number of fuel assemblies represented in the channel. The reactor power from RELAP5-3D must be converted for COBRA-FLX as well. The radial peaking factors for each RELAP5-3D channel must be converted to a linear heat rate based on the initial core power before the transient initiates.

The linear heat rate in COBRA-FLX is used to calculate the initial power. To model the change in power during the transient, the normalised core power with respect to time is input to COBRA-FLX. The power should be normalized based on the initial power prior to transient initiation.

Containment Analysis Methodology

GOTHIC is a thermal hydraulic code that predicts the containment pressure and temperature response to a high energy line break inside containment. For a high energy line break, RELAP5-3D will predict the mass and energy released from the break. The mass and energy release will then be used as input into GOTHIC to predict the containment pressure and temperature response. The GOTHIC code also models the PCH system to analyse the heat transfer capabilities and the time required to depressurise containment.

GOTHIC

Numerical Advisory Solutions' GOTHIC is a versatile, general-purpose thermal-hydraulics code that solves the conservation equations for mass, momentum, and energy for multicomponent, multi-phase compressible flow in lumped parameter and/or multi-dimensional geometries. Typical applications include the design, licensing, safety and operating analysis of nuclear power plant systems, containments, and confinement buildings. GOTHIC can be used in licensing for predicting peak pressure and temperature response in containment for DBAs, including LOCAs and main steam line breaks inside containment.

Source Terms

Core Isotopic Inventory

The isotopic inventories of fuel assemblies are calculated. Isotopic concentrations are based on the detailed geometry of a fuel assembly, rated power plus uncertainty, maximum assembly average exposure, and a range of U-235 enrichments. The isotopic inventory is calculated at several time steps in the fuel cycle.