HOLTEC BRITAIN

A Holtec International Company

Holtec Britain Ltd	HI-2240345
Sponsoring Company	**Document Reference**
1	23 September 2025
Revision No.	**Issue Date**
Report	Non-proprietary
Record Type	**Proprietary Classification**
ISO 9001	No
Quality Class	**Export Control Applicability**

Record Title:

PSR Part B Chapter 14 Safety/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 to support PSR v0
1	Second issue to Regulators to support PSR v1

Table of Contents

List of Tables

List of Figures

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) 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 Part A Chapter 1 Introduction [1].

The Fundamental Purpose is realised through the Fundamental Objective of the Preliminary Safety Report (PSR). The PSR summarises the safety standards and criteria, safety management and organisation, and the Claims, Arguments and Evidence (CAE) that, using the currently available Evidence, demonstrate the generic SMR-300 design risks to people are likely to be tolerable and As Low as Reasonably Practicable (ALARP).

Part B Chapter 14 presents the 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 Part A Chapter 3 Claims, Arguments and Evidence [2]. This chapter (Part B Chapter 14) links to the overarching claim through the following Level 2 claim:

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 Part A Chapter 3 [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 following Level 3 claim:

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).

This chapter is structured as follows:

- Sub-chapter 14.2 presents further discussion on how the Level 3 claim is broken down into Level 4 claims.
- Sub-chapter 14.3 sets out the overall approach to UK Design Basis Accident Analysis (DBAA) and demonstrates how Level 4 Claim 2.1.2.1 is met.
- Sub-chapter 14.4 covers the identification of plant Initiating Events (IE) and demonstrates how Level 4 Claim 2.1.2.2 is met.
- Sub-chapter 14.5 covers the identification and categorisation of safety functions, performed by appropriately classified safety measures to achieve successful mitigation of all identified design basis faults and demonstrates how Level 4 Claims 2.1.2.3 and 2.1.2.4 are met.

- Sub-chapter 14.6 covers the application and use of United States (US) Transient and Accident analyses and demonstrates how Level 4 Claim 2.1.2.5 is met.
- Sub-chapter 14.7 provides a technical summary of how the claims for this chapter have been achieved, together with a summary of key contributions from this chapter to the overall ALARP position. Sub-chapter 14.7 also discusses any GDA Commitments that have arisen.

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

14.1.2 Exclusions and Limitations

It is noted that the following areas, whilst required to be fully analysed prior to any future deployment of the SMR-300, are less mature at GDA and hence not considered in any significant detail within the scope of Part B Chapter 14:

- Faults external to the reactor which include:
  - Fuel route.
  - Waste systems.
  - Supporting services such as PSR Chapter 14 Design Basis Analysis (Fault Studies) - External reactor fault have been excluded e.g., Fuel route and waste systems (HVAC), air, water, etc.
  - Out of core criticality.
  - Specific consideration of Spent Fuel Pool 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 one unit while another is being commissioned or operating).

It is considered that these omissions are acceptable for the current stage of the SMR-300 design, and any potential design modifications resulting from future work (i.e., beyond GDA timescales) are not foreclosed at this stage.

A limited DBAA has been undertaken to meet UK context based on the Preliminary Fault Schedule (PFS) [4] and offers a preliminary identification and categorisation of the associated Safety Functions (SF) and classification of candidate Structures, Systems and Components (SSC) that deliver the safety function(s). Full details of the analyses for each fault are presented within UK DBAA Summary Report [5]; and a summary of the results is presented within this chapter. It should be noted that these designations are preliminary in nature and will be subject to further development and review in line with the maturity of the design.

14.1.3 Assumptions

Assumptions which relate to this topic have been formally captured in the Commitments, Assumptions and Requirements (CAR) process [6]. Further details of this process are provided in Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance [7].

There are no assumptions raised in relation to Part B Chapter 14.

14.1.4 Interfaces with Other SSEC Chapters

This chapter interfaces with multiple topic areas across the PSR. Generally, the engineering chapters substantiate claims that arise from the UK DBAA; therefore, the full set of interactions is not reproduced here. The key interfaces that link the disciplines are listed below.

- Part B Chapter 1 Reactor Coolant System and Engineered Safety Features (ESF) [8]: Demonstrates that the principal and secondary safety systems deliver the safety functions derived in the UK DBAA.
- Part B Chapter 2 Reactor [9]: Provides the fuel design limits and thermal-mechanical criteria that the transients analysed in this chapter must respect.
- Part B Chapter 4 Instrumentation & Control Systems [10]: Justifies the design, accuracy and response times of the Instrumentation and Control (I&C) that detect IEs and actuate the credited safety systems.
- Part B Chapter 5 Reactor Supporting Facilities [11]: Describes reactor support and auxiliary systems required to maintain operability of safety systems during fault conditions.
- Part B Chapter 6 Electrical Engineering [12]: Presents the electrical support systems, including Class 1E batteries, which ensure the safety systems remain available to perform their safety functions during fault conditions.
- Part B Chapter 15 Beyond Design Basis Accident (BDBA), Severe Accident Analysis, and Emergency Preparedness [13]: Faults screened as beyond design basis analysis are transferred from this chapter to Part B Chapter 15 for further analysis.
- Part B Chapter 16 Probabilistic Safety Assessment (PSA) [14]: Supplies PSA insights and frequency-consequence data that support the fault schedule and confirm categorisation assumptions made in the deterministic analyses.
- Part B Chapter 17 Human Factors (HF) [15]: Identified human failures and Important Human Actions (IHA) will be represented in the UK DBAA as required, and any claims on human action or performance arising from that analysis will be addressed within Part B Chapter 17.
- Part B Chapter 18 Structural Integrity [16]: Substantiates very-high-reliability for components whose failure is identified as intolerable in the deterministic analyses.
- Part B Chapter 21 External Hazards [17]: Provides the external hazard events that feed into the fault and protection schedule developed in this chapter.
- Part B Chapter 22 Internal Hazards [18]: Provides the internal hazard events that feed into the fault and protection schedule developed in this chapter.

14.2 DESIGN BASIS ACCIDENT ANALYSIS CLAIMS, ARGUMENTS AND EVIDENCE

The CAE approach captures the golden thread of the safety-case narrative by showing, through fault studies and analyses, that the high-level claim is valid. For the generic SMR-300, it demonstrates how the Fundamental Purpose of the SSEC set out in Part A Chapter 1 [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 Part A Chapter 3 [2].

This chapter presents the UK DBAA topic for the generic SMR-300 to support the following Level 3 claim:

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 this chapter 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 Deterministic Safety Analysis (DSA) information where appropriate. Table 1 shows the breakdown of Claim 2.1.2 and identifies in which chapter of this PSR these claims are demonstrated to be met to a maturity appropriate for PSR v1. How the sub-claims support the chapter claim is outlined below:

Table 1: Claims Covered by Part B Chapter 14

Claim No.	Claim	Sub-chapter
2.1.2.1	The approach to design basis accident analysis has taken UK relevant good practice into account.	14.3 DBAA Approach
2.1.2.2	A comprehensive set of plant initiating events with the potential to lead to significant radiation exposure or release of radioactive material if unmitigated are identified, screened, and appropriately grouped into design basis faults.	14.4 Fault Identification and Classification
2.1.2.3	Safety functions, categorised by their importance to nuclear safety, are identified for all design basis faults.	14.5 Safety Functions and Safety Measures
2.1.2.4	Safety measures, classified on the basis of their significance in delivering associated safety functions, are identified for all design basis faults and provide sufficient lines of protection based on the fault frequency.	14.5 Safety Functions and Safety Measures
2.1.2.5	Appropriately conservative analysis demonstrates that for all design basis faults, the identified safety measures, in conjunction with operator actions, enable the plant to reach a safe state and ensure that defined acceptance criteria are met.	14.6 Accident Analysis and Modelling

Appendix A provides a full CAE mapping for Part B Chapter 14, which includes any lower-level CAE needed to support the claims in Table 1. This includes identification of evidence available at PSR v1 and aspects for future development of evidence to support these claims beyond PSR v1.

14.3 DBAA APPROACH

This sub-chapter provides the demonstration of the following Level 4 claim:

Claim 2.1.2.1: The approach to design basis accident analysis has taken UK relevant good practice into account.

This sub-chapter supports Claim 2.1.2.1 which is addressed by a single argument:

- The design basis accident analysis for the SMR-300 utilises appropriate methodologies in alignment with national regulatory expectations (A1).

14.3.1 Overview of the US Approach

In the US, the design basis methodology is prescriptive. Title 10 Code of Federal Regulations (CFR) Part 50 [19] establishes the licensing framework and Appendix A lists the General Design Criteria (GDC) that deterministic safety analyses must satisfy. Holtec interprets those criteria for the SMR-300 in HI-2240251, SMR-300 Top-Level Plant Design Requirements [20], which forms part of the Part 50 Safety Analysis Report framework.

A deterministic IE is defined in NUREG-0800, Standard Review Plan, Chapter 15, as any plant event that places the facility in a condition requiring credited safety systems to act in order to meet the acceptance criteria for Anticipated Operational Occurrences (AOO) or postulated accidents. Chapter 15 provides the standard list of transients and accidents that applicants must analyse; licensees add plant-specific events if required, following the guidance in Nuclear Energy Institute (NEI) 97-04 Revised Appendix B: Guidance and Examples for Identifying 10 CFR 50.2 Design Bases [21]. Deterministic safety analyses credit only safety-classified SSCs. Non-safety systems, alternating-current power sources and operator actions are not credited during the first seventy-two hours of any design-basis fault.

In summary, the US DSA evaluates the plant response to the set of transients and postulated accidents defined above and is sometimes termed transient and accident analysis. The selected events span more than 70 years of Light Water Reactor (LWR) design experience, operating experience, and engineering judgement. Sub-chapter 14.5 presents these analyses, which establish the limiting conditions for safety-related systems needed to protect public health and safety. The acceptance criteria presented in sub-chapter 14.6.

14.3.1.1 US Nuclear Regulatory Commission Requirements

The SMR-300 has been designed in accordance with the requirements stipulated in US legislation, specifically 10 CFR Part 50 [19]. Particular attention is drawn to the GDC presented in Appendix A of that Part. These criteria are prescriptive, providing the designer with a mandatory minimum set of requirements that the plant must satisfy.

The US codes and standards and International Atomic Energy Agency (IAEA) guidance that were used to inform the US transient and accident analyses are presented in Table 2.

Table 2: Principal US Codes and Standards and IAEA Guidance

Label	Title
US Codes and Standards	
American National Standards Institute (ANSI)/American Nuclear Society (ANS)-58.14-2011 (R2017)	Safety and Pressure Integrity Classification Criteria for Light Water Reactors [22]
INL/RPT-23-7281	Initiating Event Rates at U.S. Nuclear Power Plants: 2022 Update [23]
NEI 18-04, Revision 1	Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development [24]
NUREG-0800	Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants [25]
NUREG/CR-4483	Reactor Pressure Vessel Failure Probability Following Through-Wall Cracks Due to Pressurized Thermal Shock Events, 1986 [26]
NUREG-0651	Evaluation of Steam Generator Tube Rupture Events, U.S. Nuclear Regulatory Commission, March 1980 [27]
NUREG/CR-5750	Rates of Initiating Events at US Nuclear Power Plants: 1987-1995 with updates [28]
NUREG-6890	Re-evaluation of Station Blackout Risk at Nuclear Power Plants, Analysis of Loss of Offsite Power Events: 1986-2004 [29]
NUREG/CR-6928	Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants with updates [30]
NUREG-1829	Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process [31]
US Nuclear Regulatory Commission (NRC) Regulatory Guide 1.203	Regulatory Guide 1.203: Transient and Accident Analysis Methods [32]
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 [33]
US NRC Regulatory Guide 1.26	Quality Group Classifications and Standards for Water, Steam, and Radioactive Waste-Containing Components of Nuclear Power Plants [34]
IAEA Guidance	
IAEA TECDOC-749	Generic Initiating Events for PSA for WWER Reactors [35]
IAEA TECDOC-719	Defining Initiating Events for Purposes of Probabilistic Safety Assessment [36]
SSR-2/1	Safety of Nuclear Power Plants: Design [37]
SSG-30	Safety Classification of Structures, Systems and Components in Nuclear Power Plants [38]

14.3.2 UK Regulatory Expectations

Argument 2.1.2.1-A1: The design basis accident analysis for the SMR-300 utilises appropriate methodologies in alignment with national regulatory expectations.

Evidence for Argument 2.1.2.1-A1:

- HI-2241279, SMR-300 GDA Safety Assessment Handbook [39] sets out the UK DBAA methodology, cites the Office for Nuclear Regulation (ONR) Safety Assessment Principles (SAP) and related Technical Assessment Guides (TAG), and references IAEA SSR-2/1) [37] and SSG-2 as Relevant Good Practice (RGP) [40].

14.3.2.1 Safety Assessment Principles

The UK ONR operates a goal setting regulatory regime, and regulatory decisions are assessed against the ONR Safety Assessment Principles for Nuclear Facilities [41]. The deterministic analyses presented here are organised so that, in principle, the DBAA can be mapped to the SAPs most directly relevant to design-basis work: fault analysis, Safety Categorisation and Classification, Engineering Key Principles, Designing for Reliability and Reliability Claims. Additional SAP groups including External and Internal Hazards, Reactor Core, Criticality Safety, Safety Systems, Heat Transport Systems, Essential Services, Human Factors and Assurance of Validity of Data and Models are addressed in the specialist engineering chapters, and their findings feed into the fault schedule and safety-function substantiation presented here.

ONR guidance documents and RGP from the IAEA and Western European Nuclear Regulators Association (WENRA) are listed in Table 3. It is noted that ONR guidance provides a framework against which regulatory judgements are made, whereas US NRC guidance offers a structured approach for licence applicants; the UK DBAA draws on both sets of material to demonstrate that the SMR-300 meets UK expectations.

Table 3: UK RGP for Design Basis Analysis

Label	Title	Revision
ONR Guidance		
SAPs	ONR Safety Assessment Principles [41]	1
ONR-GDA-GD-006	ONR GDA Guidance to Requesting Parties [42]	0
ONR-GDA-GD-007	Nuclear Power Plants Generic Design Assessment Technical Guidance [43]	0
NS-TAST-GD-005	Guidance on the Demonstration of ALARP [44]	11.2
NS-TAST-GD-006	Design Basis Analysis [45]	5.1
NS-TAST-GD-035	Limits And Conditions for Nuclear Safety (Operating Rules) [46]	7
NS-TAST-GD-036	Redundancy, Diversity, Segregation and Layout of Structures, Systems and Components [47]	3
NS-TAST-GD-042	Validation of Computer Codes and Calculation Methods [48]	5.1
NS-TAST-GD-051	The Purpose, Scope, and Content of Safety Cases [49]	4
NS-TAST-GD-094	Categorisation of Safety Functions and Classification of Structures, Systems and Components [50]	2
IAEA Guidance		
SSR-2/1	Safety of Nuclear Power Plants: Design [37]	1
SSG-2	Deterministic Safety Analysis for Nuclear Power Plants [40]	
SSR-2/2	Safety of Nuclear Power Plants: Commissioning and Operation [51]	1
WENRA Guidance		
-	Safety Reference Levels for Existing Reactors [52]	2021

Label	Title	Revision
-	Report on Safety of new Nuclear Power Plant (NPP) [53]	2013
-	WENRA Statement on Safety Objectives for New Nuclear Power Plants [54]	2010

14.3.2.2 Overview of UK DBAA

Undertaking a DBAA according to the UK regulatory regime involves a rigorous approach to identifying and evaluating potential accidents that occur within the design basis of a nuclear facility (i.e., transients, internal events, internal and external hazards). The primary aim is to ensure that a plant's design is robust enough to prevent or mitigate accidents. In this approach, risk is not quantified, but the adequacy of the design and the suitability and effectiveness of its safety measures are assessed against a specific set of deterministic rules.

Identification of IEs is the first step in a fault sequence. IEs 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. These capture system failures, human errors, and external hazards. For system failures this can be complex failures (involving multiple components) or a single failure (such as the failure of a pump).

Identification and Quantification methodologies are used to ascertain (identify) and evaluate (quantify) SMR-300 relevant IEs within the design basis of the power plant; and to assess if and how initiated scenarios challenge or threaten plant safety. Identifying a complete consolidated list of IEs (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 IEs within that design basis.

Holtec developed an extensive Consolidated Fault List (CFL) [4] using a comprehensive engineering evaluation from Defining Initiating Events for the Purpose of Probabilistic Safety Assessment [36], the PSA Procedures Guide [55], Analysis of Core Damage Frequency from Internal Events: Methodology Guidelines [56] and Estimating Loss-of-Coolant Accident Frequencies through the Elicitation Process [31]. These sources support the identification of IEs for both a generic Pressurised Water Reactor (PWR) and the plant specific SMR-300 basis, including its novel features. Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995 [28] provides a comprehensive summary of IEs and estimated frequencies for the US 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 US Commercial Nuclear Power Plants [30]. These studies comprise the primary sources of industry recognized IEs used in development of the SMR-300 CFL, as needed to perform safety analyses for AOOs, Design Basis Accidents (DBA) and BDBAs using both US DSA and PSA applied methods and models.

After identifying candidate IEs from other PWR PSAs and the SMR-300-specific IE review, the events are selected, screened and, where practicable, grouped by identifying a bounding event whose unmitigated consequences represent the worst case for that group.

For any IE with a frequency above 1E-05 per year the deterministic assessment considers both the initiating event frequency and the predicted unmitigated dose. Where the predicted dose approaches or exceeds the SAP Target 4 Basic Safety Objective (BSO) the analysis shows that, assuming one random failure in the credited safety measures where required by

the safety-function category, doses remain within on-site and off-site limits as illustrated in Figure 1. For example, if a high-frequency fault would give an off-site dose of no more than 1 mSv the function is usually Category C and a single Class 3 SSC may be adequate, provided the risk can be shown to be ALARP.

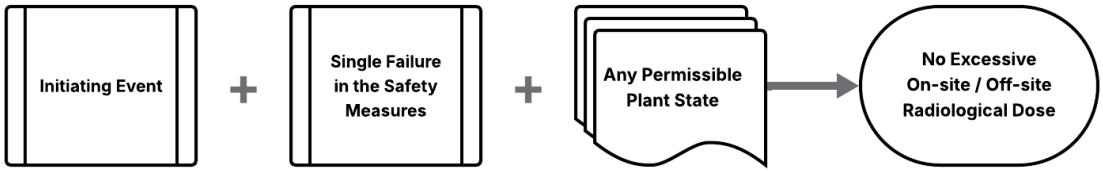

Figure 1: The Basic Principle of UK DBAA

The steps involved in undertaking a UK DBAA are:

1. **Fault Identification:** Identify a comprehensive set of fault sequences and scenarios that can be considered in the design basis of the plant.
2. **Fault Classification:** Classify the faults based on the Initiating Event Frequency (IEF) and potential unmitigated radiological consequences.
3. **Radiological Consequences:** Evaluate the radiological consequences of the accident using established methodologies.
4. **Safety Systems:** Ensure that the design basis includes systems that are adequately redundant, diverse, and fail-safe, and can bring the plant to a safe condition in the event of any DBA.
5. **Control and Mitigation:** Demonstrate that suitable control measures and mitigation systems are in place for each design basis accident, including passive and active systems, emergency shutdown systems, backup power and cooling systems, and Containment Structures (CS) to prevent the release of radioactive materials.
6. **Accident Analysis and Modelling:** Develop models that simulate the plant's response to the IE and fault sequences to demonstrate that Defence in Depth (DiD) is maintained and that no single failure would lead to unacceptable consequences.
7. **ALARP:** Show that all reasonably practicable measures to reduce risks have been identified and implemented.

This structured approach ensures compliance with UK requirements and aligns with international best practices for nuclear safety as given in Specific Safety Guide (SSG) No-2 [40].

A limited UK DBAA has been undertaken to verify the preliminary identification and categorisation of the associated SFs and classification of candidate SSCs that deliver the SF(s). These functions are derived through the hierarchy of High-Level, Plant-Level and Lower-Level SFs, then categorised against the frequency-consequence rules; candidate SSCs are provisionally classified according to the highest category function they support. Full details of the analyses for each fault are presented in UK DBAA Summary Report [5], and a summary of the results is provided in Chapter 14.5.

For Step 1 and 2 of the GDA process, the level of design definition and safety assessment is not sufficient to permit a detailed evaluation of radiological consequences for all faults. Where sufficient data is not available, faults have been assigned into consequence bands given in the UK DBAA Summary Report [5].

14.3.2.3 Deterministic Safety Principles

There needs to be a high level of confidence that identified safety measures will be available to deliver their respective safety functions by incorporation of the following principles:

- Safety measures need to be designed with sufficient integrity and reliability.
- The design should incorporate redundancy to avoid the effects of random failure, and diversity and segregation to avoid the effects of Common Cause Failure (CCF).
- No single random failure anywhere within the safety measures provided to secure a safety function should prevent the performance of that safety function:
    - The design characteristics of any Class 1 SSCs should include single failure tolerance and multiple redundancy.
- Failures consequential upon the initiating fault (for example, SSCs lost to flood water released by a pipe break), and failures expected to occur in combination with the initiating fault arising from a common cause (for example, a loss of power) need to be considered.

The need to invoke these principles is driven by the degree of risk reduction necessary and the mode that the SSC is to be utilised against a given plant state.

The deterministic analyses apply the single failure criterion and the principles of redundancy, diversity, and segregation in accordance with ONR SAPs EDR.4 and EDR.2, respectively. Each fault sequence assumes one random failure in the principal Class 1 safety measures and confirms that a diverse, independent line of protection exists for frequent initiating events. The systematic review of active and passive single failures, and the justification of redundancy and diversity claims, follow the methodology set out in Safety Assessment Handbook [39], which provides the detailed guidance. It should be noted that segregation provisions against internal hazards will be assessed in the forthcoming internal hazards analysis and incorporated in later DBA revisions.

14.3.3 CAE Summary

The material in this sub-chapter substantiates Claim 2.1.2.1 through Argument 2.1.2.1-A1. The SMR-300 GDA Safety Assessment Handbook sets out a UK Design Basis Accident Analysis methodology that derives its rules from the relevant ONR SAPs and TAGs and references IAEA and WENRA guidance as recognised good practice. By adopting that handbook as the governing process, the project has shown that the planned DBAA approach accords with UK regulatory expectations. Claim 2.1.2.1 is therefore demonstrated to the level of maturity appropriate for a PSR.

14.4 FAULT IDENTIFICATION AND CLASSIFICATION

This sub-chapter provides the demonstration of the following Level 4 claim:

Claim 2.1.2.2: A comprehensive set of plant initiating events with the potential to lead to significant radiation exposure or release of radioactive material if unmitigated are identified, screened and appropriately grouped into design basis faults.

This claim pertains to the requirement to demonstrate that an appropriately comprehensive set of design basis faults have been defined. This is to ensure that all potential challenges to nuclear safety arising from faults that meet the stated design basis definition and scope, have been identified for assessment in the safety case.

This sub-chapter supports Claim 2.1.2.2, which has been further decomposed into two arguments:

- The concept, scope, and definition of design basis faults applicable to the SMR-300 are in alignment with appropriate international standards and national regulatory expectations (A1).
- A systematic process of Postulated Initiating Event (PIE) identification, screening and grouping has been followed to derive an appropriately comprehensive and robust set of design basis faults (A2).

This sub-chapter outlines how design-basis faults for the SMR-300 are defined, identified, screened, and grouped. It covers:

- Design basis fault concept and scope which states the definition adopted for a design basis fault, explains the frequency thresholds that bound the scope, and shows alignment with ONR SAPs.
- PIE identification and screening which describes the systematic process that draws on Operating Experience (OPEX), NRC guidance and PSA reference lists, then applies qualitative screening and quantitative frequency cut-offs to exclude non-credible events.

14.4.1 Design Basis Fault Definition

Argument 2.1.2.2-A1: The concept, scope and definition of design basis faults applicable to the SMR-300 are in alignment with appropriate international standards and national regulatory expectations.

Evidence for Argument 2.1.2.2-A1:

- HI-2241279, SMR-300 GDA Safety Assessment Handbook [39] defines design-basis faults using internationally recognised criteria drawn from IAEA SSR-2/1 and ONR SAPs.

14.4.1.1 Fault Definition

Faults within the scope of sub-chapter 14.4 are known as design basis faults. These design basis faults either bound, or correspond to, one or more PIEs that reflect events that can challenge nuclear safety and meet the following definition:

An initiating event that challenges the ability of the plant to perform one or more of the three fundamental safety functions of control of fuel reactivity, fuel heat removal, and confinement of radioactive material such that, if left unmitigated, it would result in unacceptable radiological release due to the failure, or bypass, of one or more containment barriers.

Faults are considered to be within design basis based on their frequency of occurrence. The plant must be designed and operated such that the radiological risk from such faults is tolerable and ALARP.

A PIE can be either a single initiating event or be composed of a “pre-initiating event” occurring in conjunction with other failures or conservatisms. Such “pre-initiating events” are those that degrade operational functions and margins but, if successfully mitigated, do not lead by themselves to operation beyond normal operating conditions. This excludes events that result in deviations of plant conditions from those targeted in normal operations which are not serious enough to meet the definition of a PIE.

PIEs are assumed to arise from:

- Spontaneous failures.
- Spurious actuation by automatic control systems.
- External, internal, or combined hazards.
- Human error.

The process for screening and grouping of PIEs into design basis faults is detailed in sub-section 14.4.2.

14.4.1.2 Design Basis Definition

The set of design basis faults are derived based on the application of frequency of occurrence thresholds that define the Design Basis definition. These are summarised below:

- The set of design basis faults must account for, as a minimum, PIEs with a frequency of occurrence greater than or equal to 1E-05 per reactor year (pry).
- PIEs, or bounding design basis faults, with a frequency of occurrence greater than 1E-03 pry are categorised as “Frequent”. For such faults it must be demonstrated that a diverse means of successful mitigation, in the form of a diverse line of protection, is available in the event of a CCF of one or more SSCs that are claimed as part of the first line of protection.
- Fault sequences, typically comprising of a PIE with subsequent failures, are determined to be within Design Basis if they have a frequency of occurrence greater than or equal to 1E-07 pry.

14.4.1.3 Design Basis Condition Frequency Categories

The Design Basis Condition (DBC) class to be used for the UK DBAA is derived from Part A Chapter 2 [3], ONR SAP Numerical Target 4 [41] (refer to sub-section 14.7.2), and DiD requirements [39].

The DBC classes for the SMR-300 are as follows and presented in Table 4.

- **DBC1 (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, and require assessment under UK DBAA, PSA or Severe Accident Analysis (SAA), depending on their unmitigated consequences.

- **DBC2 (AOO):** An operational process deviating from normal operation that is expected to occur one or more times during the operating lifetime of the plant and requires assessment under UK DBAA, PSA or SAA (depending on the unmitigated consequences).
- **DBC3a (Frequent design basis faults):** 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.
- **DBC3b (Infrequent design basis faults):** 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.
- **DBC4 (Infrequent limiting design basis faults):** 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 per annum 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 (Design Extension Condition):** BDBA faults or events (which may be severe accidents) 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). BDBA faults 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.

  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 100 mSv 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.

Table 4: UK Plant and Design Basis Condition Classes

UK SMR-300 Plant Condition Class	Defence-in-Depth Level	Design Basis Condition Class	UK IEF Range (/y)
Normal Operation	Level 1 – Prevention of abnormal operation and failure by design.	DBC1	IEF > 1
Anticipated Operational Occurrences	Level 2 – Prevention and control of abnormal operation and detection of failures.	DBC2	1 > IEF > 1E-02
Design Basis Accidents – Frequent Faults	Level 3 – Control of faults within the design basis to protect against escalation to an accident.	DBC3a	1E-02 > IEF > 1E-03
Design Basis Accidents – Infrequent Faults	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.	DBC3b	1E-03 > IEF > 1E-04
Design Basis Accidents – Infrequent Limiting Faults		DBC4	1E-04 > IEF > 1E-05
Design Extension Condition (with or without significant core disruption – beyond design basis / severe accidents)		DEC – A (without core damage) DEC – B (core damage)	IEF < 1E-05
Off-Site Emergency (accident with releases requiring implementation of emergency countermeasures)	Level 5 – Mitigation of radiological consequences of significant release of radioactive material.	OSE	N/A
No radiological consequences to exposed groups	N/A	DBC0	Any

14.4.2 PIE Identification, Screening and Grouping

Argument 2.1.2.2-A2: A systematic process of Postulated Initiating Event (PIE) identification, screening and grouping has been followed to derive an appropriately comprehensive and robust set of design basis faults.

Evidence for Argument 2.1.2.2-A2:

- HI-2241323, SMR-300 GDA Preliminary Fault Schedule Report Revision 1 [57] defines and applies the step-by-step process for PIE identification, screening, and grouping.
- HI-2241322, Preliminary Fault Schedule Revision 1 [4] contains the CFL worksheet with assigned IE frequencies and unmitigated consequences, and shows how the screened events are grouped into bounding fault families, thereby demonstrating that a systematic method has produced a comprehensive set of design-basis faults.

The production of a fault schedule is considered RGP in the UK. 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 fault schedule therefore establishes an auditable link between initiating faults considered in the design and requirements to be applied to safety measures.

A PFS [4] has been produced to support PSR Revision 1 documents and the development of the PFS in support of the GDA Step 2 process for the SMR-300 has been in two stages:

- **Stage 1:** Revision 0 which was focussed on ‘in-reactor’ design basis faults and a limited set of DEC events.
- **Stage 2:** Revision 1 which covers ‘in-reactor’ design basis faults, additional DEC events, a preliminary set of external hazards, the CFL, and initial consideration of internal hazards.

The PFS has been informed by a limited (OPEX-based) fault and Hazard Identification (HAZID) study which has examined international and relevant PWR projects (including other GDA projects) and any novel or unique features of the SMR-300 design in order to identify a credible and complete set of faults. This list of faults, numbering over 450 individual sequences covering DBCs and DECs, together with severe accident scenarios has been recorded in the CFL which will provide the “live” file for the development of the PFS.

The CFL has been included as a separate sheet within Revision 1 of the PFS [4]. The intention is that the CFL will continue to be developed and updated as the SMR-300 design and safety analysis matures.

14.4.2.1 Consolidated Fault List

14.4.2.1.1 Fault and HAZID Process

In order to develop an initial PFS for the SMR-300, a fault and HAZID study process has been undertaken [4]. The first stage of this process was the development of a CFL, which presents the results of all the fault identification studies carried out and provides the basis for the set of relevant faults assessed through the PFS.

The CFL is based on a combination of sources, including:

- The use of RGP, OPEX and the application of HAZID techniques, based on the following data:
  - NUREG/CR-5750 – Rates of Initiating Events at US Nuclear Power Plants: 1987-1995 with updates [28].
  - NUREG/CR-6928 – Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants with updates [30].
  - IAEA TECDOC-749/R – Generic Initiating Events for PSA for WWER Reactors [35].
  - IAEA TECDOC-719 – Defining Initiating Events for Purposes of Probabilistic Safety Assessment [36].
  - Westinghouse AP-1000 UK Pre-Construction Safety Report (PCSR) Fault Schedule [58].
  - EDF European Pressurised Reactor (EPR) PCSR Fault and Protection Schedule [59].
  - China General Nuclear (CGN) HPR-1000 PCSR [60].
- Additional fault identification studies, including:
  - Failure Modes and Effects Analysis (FMEA).
  - Hazard and Operability (HAZOP).
  - Master Logic Diagrams.

The CFL identifies PIEs, their preliminary IEF, not based on SMR-300 specific PSA results, and their preliminary unmitigated radiological consequences.

14.4.2.1.2 CFL Content

The CFL is provided as a dedicated worksheet in the PFS spreadsheet [4]. It collates the preliminary set of PIEs identified from OPEX, NRC and IAEA guidance, previous UK GDA projects and SMR-300 design reviews. For each event, the sheet records the initiating-event frequency band, an estimate of the unmitigated radiological consequences and qualitative screening notes. These data underpin the screening and bounding exercise that generates the preliminary fault lists on the subsequent PFS worksheets covering in-reactor, ex-reactor, DEC, and external-hazard faults; the worksheet headings are summarised in Safety Assessment Handbook [39] and explained in detail in PFS Report [57].

14.4.2.1.3 Preliminary Fault Schedule

The PFS [4] identifies bounding fault groups and which PIEs each one bounds, the group IEF, the unmitigated radiological consequences of the bounding PIE in the group, the safety function(s) and safety categories required for each fault, the duty systems which have to fail for the fault to progress, the principal safety systems claimed for fault mitigation, the diverse safety systems claimed for fault mitigation (where required), any additional notes around other systems that may provide further DiD (although not claimed), and any essential support systems and potential CCFs. The content of PFS for each heading is presented in Safety Assessment Handbook [39], with supplementary detail in PFS Report [57].

Comprehensive analyses of ‘ex-reactor’ faults (including Fuel Storage and Transport Route, Radioactive Waste Management and HVAC) and internal hazards are not included in Revision 1 of the PFS, since formal HAZID work is limited at this stage due to the lack of maturity of the design. However, a limited set of External Hazards faults and a Fuel Storage and Transport Route fault have been included, and consideration has been given as to how internal hazard initiating events will be incorporated into a future revision of the fault schedule (refer to PFS

Report [57] for further details). Hence, beyond GDA timescales, the fault analysis will continue to develop in line with the developing maturity of the SMR-300 design. Fault studies will be planned for all 'ex-reactor' fault groups (i.e., internal hazards, external hazards, fuel route / handling, waste management, and HVAC related faults) and all DEC events in accordance with the identified methodologies. The fault schedule will be updated accordingly and a full summary provided in the PCSR.

14.4.3 CAE Summary

It has been demonstrated that the requirements of Claim 2.1.2.2 are only partially met. The provided methodology for identifying, screening, and grouping design basis faults aligns with international and national expectations. The CFL and PFS concentrate on in-reactor faults and a limited set of external and DEC events, reflecting the maturity of the design data available when the schedule was assembled. Several equipment areas, together with fuel-route and radioactive-waste faults, remain to be captured. Commitment C_Faul_103 requires the fault schedule programme to be completed after GDA Step 2, deriving every PIE with an unmitigated consequence above 0.1 mSv and confirming the associated safety measures. Future DBAA studies that implement this Commitment will extend the schedule, allowing full demonstration that a comprehensive, systematically derived set of design-basis faults has been achieved.

14.5 SAFETY FUNCTIONS AND SAFETY MEASURES

This sub-chapter provides the demonstration of the following Level 4 claims:

Claim 2.1.2.3: Safety functions, categorised by their importance to nuclear safety, are identified for all design basis faults.

Claim 2.1.2.4: Safety measures, classified based on their significance in delivering associated safety functions, are identified for all design basis faults and provide sufficient lines of protection based on the fault frequency.

These claims pertain to the requirement to demonstrate that all the necessary categorised safety functions have been identified and are performed by appropriately classified SSCs to achieve successful mitigation of all identified design basis faults.

This sub-chapter supports Claim 2.1.2.3, which has been further decomposed into two arguments:

- All the necessary safety functions have been identified through the application of the safety function hierarchy i.e., High-Level Safety Functions (HLSF), Plant Level Safety Functions (PLSF) and Lower-Level Safety Functions (LLSF) (A1).
- All identified safety functions have been appropriately categorised based on the fault frequency and unmitigated radiological consequences (A2).

This sub-chapter supports Claim 2.1.2.4, which has been further decomposed into two arguments:

- All the safety measures required to perform the necessary safety functions have been identified (A1).
- All identified safety measures have been appropriately classified based on the categorisation of the safety function(s) they perform and the line(s) of protection in which they are claimed (A2).

This sub-chapter outlines the derivation and application of safety functions and safety measures for the SMR-300 design. It covers:

- Identification of safety functions, showing how the HLSF, PLSF and LLSF hierarchy is applied to every bounding fault.
- Preliminary categorisation of those safety functions using frequency and consequence criteria defined in Safety Assessment Handbook [39].
- Identification of the duty, principal and diverse SSCs that deliver each safety function.
- Preliminary classification of those SSCs, based on the category of the safety function they perform and their importance in the line of protection.
- Demonstration, for each design-basis fault, that all necessary mitigating safety functions have been identified and categorised, and that the plant design includes safety systems capable of delivering those functions, with each SSC assigned an appropriate provisional UK class.

It should be noted that the PFS links the fault-identification work in sub-chapter 14.4 with the analyses presented here. The spreadsheet version of the PFS [4] assigns a LLSF to every initiating event and records the associated safety systems, while the accompanying PFS report [57] describes the methodology and sets out the IEF bands, safety-function categories and provisional UK classes. These data together with UK DBAA Summary Report [5] form the baseline for the evidence cited in sub-sections 14.5.1 to 14.5.4 and will be updated as further DBAA studies are completed.

14.5.1 Identification of Safety Functions

Argument 2.1.2.3-A1: All the necessary safety functions have been identified through the application of the safety function hierarchy i.e., High-Level Safety Functions (HLSFs), Plant Level Safety Functions (PLSFs) and Lower-Level Safety Functions (LLSFs).

Evidence for Argument 2.1.2.3-A1:

- HI-2241577, SMR-300 GDA UK DBAA Summary Report Revision 0 [5] applies the safety-function hierarchy and lists the resulting Lower-Level Safety Functions for each bounding fault.
- HI-2241323, Preliminary Fault Schedule Revision 1 [4] maps each bounding fault to the relevant Top-Level and L1 Safety-Function Requirements for both primary and, where applicable, secondary lines of protection, showing that multiple safety functions are allocated where necessary.

A safety function is a specific purpose or objective that must be accomplished in the interests of safety and be specified or described with minimal reference to the physical means of achieving it:

- Safety functions that are needed during the normal operation of a facility usually relate to Levels 1 and 2 of the DiD hierarchy.
- Safety functions that are needed in response to a fault or accident condition usually relate to Levels 3 to 5 of the DiD hierarchy.

It should be noted that no operator actions are credited within the deterministic safety analysis of the SMR-300. All safety functions identified through the hierarchy are intended to be delivered by passive engineered systems without reliance on human intervention during the first 72 hours following a fault. Part B Chapter 17 [15] and the Human Reliability Assessment (HRA) Step 2 Position Statement [61] confirm that no Important Human Actions are claimed in the deterministic assessment.

To assist with the derivation of safety functions, a hierarchical structure has been created as shown in Figure 2.

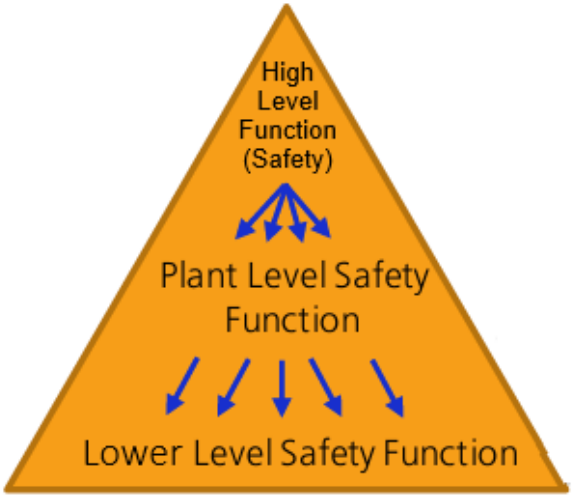

Figure 2: Hierarchy of Safety Functions

At the highest level are the Holtec International HLSFs (which are derived from the three fundamental safety functions identified in Requirement 4 of IAEA Specific Safety Report 2/1 [37] (i.e., control of reactivity, removal of heat from the reactor, and confinement[1] of radioactive material). In addition, a further high level safety function described as 'Other' can be used to capture cross cutting elements. Such cross-cutting elements include support to safety functions such as monitoring of plant operation and controlling environmental conditions within the plant. More details can be found in the UK DBAA Summary Report [5]

These HLSFs are broken down into PLSFs [5]. PLSFs provide high level objectives that collectively satisfy the HLSFs. The PLSFs define the specific safety requirement or objective at a high level and do not refer to a physical means of achieving the functional and performance requirements. In order to provide a list of safety functions at an appropriate level of detail, the PLSFs are broken down further into LLSFs. An LLSF combines the objective of the PLSF with a level of defence in depth to convey the physical means of achieving the functional requirement. These HLSFs, PLSFs and LLSFs are set out in the UK DBAA Summary Report [5].

The UK DBAA applies the safety function hierarchy to each identified fault, while the PFS records the HLSFs and LLSFs requirements for identified faults that must be met by the primary and secondary (where required) lines of protection. Each design-basis fault is linked to the complete set of safety functions it demands. Hence all necessary safety functions have been systematically derived and assigned across the design-basis fault set.

14.5.2 Categorisation of Safety Functions

Argument 2.1.2.3-A2: All identified safety functions have been appropriately categorised based on the fault frequency and unmitigated radiological consequences.

[1] 'Confinement' typically refers to preventing the escape of radioactive material to the environment, whereas 'containment' is associated with the physical means by which this is achieved.

Evidence for Argument 2.1.2.3-A2:

- HI-2241577, SMR-300 GDA UK DBAA Summary Report Revision 0 [5] assigns Safety-Function Categories to the LLSFs, in accordance with ONR SAP frequency-and-consequence criteria, claimed for the six bounding faults analysed.
- HI-2241323, SMR-300 GDA Preliminary Fault Schedule Report Revision 1 [57] explains how these categories are recorded in the PFS worksheets through the Safety Function Category column together with the IEF bands that support the categorisation.

The categorisation of safety functions (LLSFs) and the subsequent classification of relevant SSCs are integrated with the hazard and fault assessments; they are an extension of the fault-study methodology, support redundancy and diversity requirements, and demonstrate DiD.

Safety function categorisation is the process by which safety functions are categorised based on their significance regarding nuclear safety. The suggested scheme makes use of the three categories recommended in ONR SAP ECS.1 [41]:

- **Category A:** Safety functions that play a principal role in ensuring nuclear safety in that they are associated with the removal of intolerable radiological risks from design basis faults, either by prevention of the risks or reduction of the risks to broadly acceptable levels.
- **Category B:** Safety functions that make a significant contribution to nuclear safety in that they are associated with the removal of radiological risks outside the design basis by either preventing the risks or reducing the risks to broadly acceptable levels for foreseeable events and beyond design basis faults, which are identified in fault studies. Functions whose failure would lead to a demand on a Category A safety function are also categorised as B.
- **Category C:** safety functions that do not fall into either of Categories A or B. They are mainly associated with the support of Category A or B safety functions or identified from ALARP or Best Available Techniques (BAT) analyses.

14.5.2.1 Initial Safety Function Categorisation

The first step involves the assignment of an initial expectation of a safety function category using a process driven mainly by the design basis analysis. The two most important factors in this determination are:

a) The consequences (potential unmitigated radiological doses) should the safety function not be performed.
b) The likelihood with which a demand is placed upon the safety function.

Based on the information presented above, safety function categories have been assigned as shown in Table 5.

Table 5: Assignment of Safety Function Categories

IEF Class (Design Basis Condition)		Threshold for the Severity of the Consequences relevant to the Safety Function Category		
		Category A	Category B	Category C
Frequent design basis faults (DBC2 and DBC3a)	Off-Site	>1 mSv	0.1 – 1 mSv	<0.1 mSv
	On-Site	>200 mSv	2 – 200 mSv	<2 mSv
	Off-Site	>10 mSv	0.1 – 10 mSv	<0.1 mSv

IEF Class (Design Basis Condition)		Threshold for the Severity of the Consequences relevant to the Safety Function Category		
		Category A	Category B	Category C
Infrequent design basis faults (DBC3b)	On-Site	>500 mSv	2 – 500 mSv	<2 mSv
Limiting design basis faults (DBC4)	Off-Site	>100 mSv	1 – 100 mSv	< 1 mSv
	On-Site	>500 mSv	20 – 500 mSv	<20 mSv
Design Extension Conditions (DEC-A and DEC-B)	Off-Site	N/A	>100 mSv	<100 mSv
	On-Site	N/A	N/A	All dose ranges

Additional information on the derivation of safety functions is given in Appendix B. A summary of the LLSFs identified for each of the faults considered in the initial UK DBAA is presented in the UK DBAA Summary Report [5]. It is noted that the safety function category is the highest claim made on it on each line of defence in any design basis fault.

14.5.3 Identification of SSCs

Argument 2.1.2.4-A1: All the safety measures required to perform the necessary safety functions have been identified.

Evidence for Argument 2.1.2.4-A1:

- HI-2241577, SMR-300 GDA UK DBAA Summary Report Revision 0 [5] identifies SSCs that deliver the required safety functions for each fault.
- HI-2241322, Preliminary Fault Schedule Revision 1 [4] lists, for each initiating event, either the principal safety system or the inherent safety characteristic that delivers the required safety functions for the first line of protection and, where applicable, the secondary safety system or inherent safety characteristic that delivers the required safety functions for the second line, thereby providing traceability between the fault list and the credited safety measures.

Safety functions can be provided by engineered means (i.e., SSCs) or operator actions (i.e., Human Based Safety Claims). However, operator action is not credited within the first 72 hours of any DBA within the SMR-300 design; therefore, no operator related safety functions or associated SSCs are claimed for in-reactor or fuel-route faults as introduced in section 14.5.1.

The aim of deterministic safety analysis is to demonstrate that there are adequate lines of protection based on the frequency of a fault. Figure 3 shows that the design intent is to mitigate each fault sequence to a frequency of 1E-07 even though the design-basis limit for specifying initiating events is 1E-05. Faults with an initiating frequency ≤ 1E-03 pry require only a first line of protection; faults occurring more frequently than this threshold also require a diverse line, together known as the main line of defence. The reliability targets are a failure probability no greater than 1E-04 for the first line and 1E-02 for the diverse line, giving the combined protection needed to achieve the 1E-07 pry sequence goal.

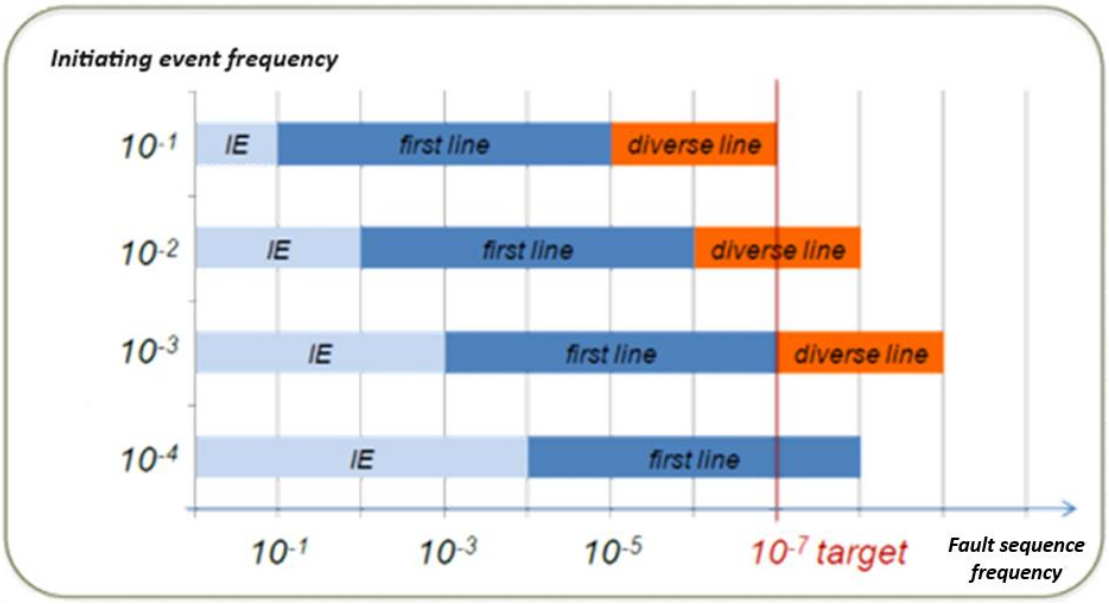

Figure 3: Outline of Where Diverse Lines of Protection are Required

To show how the frequency argument is applied in practice, a Small Break Loss of Coolant Accident (SBLOCA) can be used as an example. An SBLOCA is considered to be not large enough to discharge decay heat by the break flow alone, so the fully passive engineered systems design must depressurise the Reactor Coolant System (RCS) and inject make-up. Initial analyses indicate that SBLOCA is a frequent fault, therefore the safety demonstration must provide both a principal and a diverse line of defence. The worst-case unmitigated consequence for SBLOCA is currently assessed to lie in consequence band C (public dose between 1 mSv and 10 mSv). On this basis the principal safety functions are the control of reactivity (Safety-Function Category A) and removal of heat from the reactor (Safety-Function Category A). The principal line uses the Plant Safety System (PSS) as the actuation platform, one Automatic Depressurisation System (ADS) Stage 1 train, Primary Decay Heat Removal System (PDH) and a Passive Core Makeup Water System (PCM) accumulator to depressurise the RCS, inject make-up and remove decay heat. The diverse core cooling line assumes a CCF in the PSS and therefore credits the Diverse Actuation System (DAS) to initiate ADS Stage 2, Secondary Decay Heat Removal System (SDH) and an independent PCM train. Holtec is assessing a design option to implement the DAS using analogue technology [62] with, which provides inherent diversity from the PSS digital systems and remains unaffected by the common-cause failures. It should also be noted that the DAS is currently a non-safety-related system; however, plans are in place to upgrade its safety classification to meet the diversity requirements of both the NRC and ONR. A third analysis branch addresses diverse reactor shutdown by postulating that the control rods do not insert; here the PSS still functions but two ADS Stage 1 trains, ADS Stage 2 and a PCM injection train provide sub-criticality and heat removal. In every branch the Passive Containment Heat Removal System (PCH) maintains long-term cooling. Full justification of the diverse lines will be completed once the DBAA programme and supporting deterministic safety analyses are finalised beyond GDA Step 2. The quantitative evaluations will then be presented in the PCSR.

The fault analysis process for the SMR-300 has been configured to demonstrate that UK context has been adequately addressed. 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 faults selected for inclusion in the initial UK DBAA are listed in Table 6, noting these are based on 'In-Reactor' faults identified in Revision 0 of the PFS [4].

Table 6: Faults Selected for the Initial UK DBAA

No	Fault Title	Where Covered
1	Turbine Trip coincident with a Loss of Offsite Power (TTLOOP).	Appendix B of [5]
2	Steam Generator Tube Rupture (single tube).	Appendix C of [5]
3	Medium sized break LOCA (75-150 mm inside diameter).	Appendix D of [5]
4	Steam system line break (intermediate or large) (inside containment).	Appendix E of [5]
5	Long-term Loss of Offsite Power (LOOP) in excess of 72 hours.	Appendix F of [5]
6	Anticipated Transient Without Scram (ATWS) involving a TTLOOP event – failure to insert control rods.	Appendix G of [5]

These faults cover a representative range of DBAs and have been specifically selected for the following reasons:

1. To provide confidence of the necessary skills and competence to conduct a full UK DBAA and understand the fundamental construct of a UK DBAA, including the application of categorisation of safety functions and classification of SSCs.
2. To provide confidence that the transient and accident analyses that have been conducted against the US NRC context contain adequate detail to be able to draw likely meaningful comparisons against the requirements of the UK regulatory framework and support a UK DBAA.
3. To provide confidence that the novel aspects of the design that have been included within scope (notably the AR, Passive Core Cooling System (PCC) and Passive Containment Heat Removal System (PCH)) are likely to meet UK expectations and therefore likely to be licensed within the UK.
4. To propose candidate Operating Rules (OR) and the methodology for deriving the Safe Operating Envelope (SOE) for the safe operation of the SMR-300 plant, as derived via the new discrete analyses.

It should also be noted that because all other reactor fault families are also mitigated by the same passive safety systems, resolving the Design Challenges identified in sub-section 14.5.5 is expected to bound any similar issues that may arise when the full UK DBAA is completed after Step 2. A summary of the PFS entries for the faults considered in the initial UK DBAA is presented in Table 7.

Table 7: Summary of the PFS Entries for Faults Considered in the Initial UK DBAA

Fault Group	PIE / Fault	Bounding Plant State	IEF Range (/y)	DBC Class	Unmitigated Radiological Consequences	
					On-Site	Off-Site
Trips	TTLOOP	PS-1	1 > IEF > 1E-02	DBC2	>200 mSv	>1 mSv
Steam Generator Tube Rupture (SGTR) / Heat Exchanger (HX) Faults	Steam generator tube rupture (single tube)	PS-1	1E-02 > IEF > 1E-03	DBC3a	>100 mSv	>1 mSv
RCS Inventory Decrease (LOCA Related)	Medium sized break LOCA (75-150 mm inside diameter)	PS-1	1E-03 > IEF > 1E-04	DBC3b	>500 mSv	>100 mSv
Increased Heat Removal	Steam system line break (intermediate or large) inside containment)	PS-1 / PS-2	1E-03 > IEF > 1E-04	DBC3b	>500 mSv	>100 mSv
Loss of Services	LOOP greater than 72 hours	PS-4	1E-04 > IEF > 1E-05	DBC4	<20 mSv	<1 mSv
ATWS	ATWS by rods failure to insert – TTLOOP	PS-1	<1E-05	DEC-A	>500 mSv	>100 mSv

Full details of the analyses for each fault are presented within the relevant Appendix of [5]. A brief summary of the safety measures for each of the six faults considered in the initial UK DBAA [5] is presented below. It is noted that, for the following assessments, only the safety classified systems are claimed (as defined in the US). Any non-safety systems that would normally help to mitigate the fault are ignored for the purposes of the analysis as described in SMR-300 Structures, Systems and Component Classification [63].

14.5.3.1 Turbine Trip coincident with a Loss of Offsite Power

A TTLOOP fault is a significant event that triggers a complex sequence of responses from the PSS. The fault sequence progression involves various mechanical, electrical, and safety systems that respond to maintain plant safety. A TTLOOP is analysed because a grid disturbance can follow a turbine trip and, conversely, any LOOP produces an immediate reactor trip. The event therefore combines two highly credible challenges: the sudden removal of the secondary heat sink and the loss of all alternating-current supplies. The turbine trip and simultaneous loss of off-site power isolate the steam pathway, shut down feedwater and other auxiliary systems, and cause the reactor coolant and secondary pressures to rise. With the secondary heat sink lost, main steam and primary pressures rise until the PSS receives the high secondary pressure signal that actuates PDH and SDH. Their actuation signal in turn generates the reactor trip signal, inserting all control rods. Around the trip point both Pressuriser Safety Valves (PSV) and Main Steam Safety Valves (MSSV) lift briefly to relieve the transient peak, then reseat. PDH and SDH remain in service and the RCS cools and depressurises. The PCM accumulators inject highly borated water once their set-point is reached, keeping the core sub-critical. If Alternating Current (AC) power is still unavailable after 24 hours, ADS Stage 1 and then Stage 2 actuate to further depressurise the RCS and open the Passive Core Makeup Water Tank (PCMWT) gravity-feed line for direct injection into the Reactor Pressure Vessel (RPV). During PCMWT injection the tank is aligned with the

Spent Fuel Pool, establishing a long-term passive recirculation cooling that maintains core submergence and a stable shutdown condition for at least 72 hours.

All SSCs claimed to mitigate the TTLOOP fault are reliant upon the PSS and the Direct Current (DC) Power Distribution System (DCE) to perform their safety function(s). LLSFs relevant to the TTLOOP fault have been identified and appropriately categorised; SSCs that mitigate the TTLOOP fault have been identified and appropriately classified. Details are provided in the UK DBAA Summary Report [5].

14.5.3.2 Steam Generator Tube Rupture (single tube)

A SGTR fault is a significant event that triggers a complex sequence of responses from the PSS. The fault sequence progression involves various mechanical, electrical, and safety systems that respond to maintain plant safety. Following the double-ended tube break, the plant trips on low pressuriser pressure, isolates feed and let-down, and issues a S-signal that stops the Reactor Coolant Pumps (RCP) and initiates PDH and SDH. The RCS cools and depressurises while ADS Stages 1 and 2 open and borated water from accumulators (then PCMWT) is injected, after which the core remains submerged, and the plant is cooled passively for at least 72 hours.

All SSCs claimed to mitigate the SGTR fault are reliant upon the PSS and DCE to perform their safety function(s). Safety functions relevant to the SGTR fault have been identified and appropriately categorised; SSCs that mitigate this fault have been identified and appropriately classified. Details are provided in the UK DBAA Summary Report [5].

14.5.3.3 Medium Break LOCA (75-150 mm inner diameter)

A Medium Break LOCA (MBLOCA) fault is a significant event that triggers a complex sequence of responses from the PSS. The fault sequence progression involves various mechanical, electrical, and safety systems that respond to maintain plant safety. Following the double-ended break in a Direct Vessel Injection (DVI) line, pressuriser pressure falls, the reactor trips and an S-signal isolates secondary systems and stops the RCPs. PDH and SDH start to remove decay heat while ADS Stages 1 and 2 open and highly borated water from the intact accumulator, then the PCMWT, is injected through the unbroken DVI line. The RCS cools, the core remains submerged, and the plant enters passive long-term recirculation cooling that can be sustained for at least 72 hours.

All SSCs claimed to mitigate the MBLOCA fault are reliant upon the PSS and DCE to perform their safety function(s). Safety functions relevant to the MBLOCA fault have been identified and appropriately categorised; SSCs that mitigate this fault have been identified and appropriately classified. Details are provided in the UK DBAA Summary Report [5].

14.5.3.4 Main Steam Line Break (inside containment)

A Main Steam Line Break (MSLB) fault is a significant event that triggers a complex sequence of responses from the PSS. The fault sequence progression involves various mechanical, electrical, and safety systems that respond to maintain plant safety. Following a double-ended main steam line break inside containment, the rapid secondary side depressurisation cools the RCS and raises reactor power until the PSS trips the reactor on high power, inserts the control rods and issues a S-signal that shuts the main steam isolation valve, isolates feedwater and trips the RCPs. Containment pressure and temperature reach their peak; on generation of the S-Signal the PDH return valves automatically open, commencing passive decay-heat removal through PDH and depressurising the RCS. As cooling continues, highly borated water from the accumulators is injected to maintain core sub-criticality. The plant then enters passive recirculation cooling and remains in a safe, stable condition for at least seventy-two hours.

All SSCs claimed to mitigate the MSLB fault are reliant upon the PSS and DCE to perform their safety function(s). Safety functions relevant to the MSLB fault have been identified and appropriately categorised; SSCs that mitigate this fault have been identified and appropriately classified. Details are provided in the UK DBAA Summary Report [5].

14.5.3.5 LOOP greater than 72 hours

A long-term LOOP fault is a significant event that triggers a complex sequence of responses from the PSS. The fault sequence progression involves various mechanical, electrical, and safety systems that respond to maintain plant safety.

Following a LOOP, the main feedwater, pressuriser heaters and sprays and Chemical and Volume Control System (CVC) are all isolated. The RCPs coast down and the PSS trips the reactor on low RCS flow. A turbine trip is initiated upon receipt of a reactor trip signal generated the PSS, at which point the Turbine Governor Valve (TGV) fails closed. Loss of the normal heat sink causes RCS and steam generator pressures to rise until high main steam pressure actuates PDH and SDH. These passive systems remove decay heat and depressurise the RCS. Highly borated water from the accumulators, once their set-point is reached, keeps the core sub-critical and submerged. If AC power remains unavailable 24 hours after the event, or earlier if a S-Signal with low pressuriser level, ADS Stage 1 and then Stage 2 actuate, further depressurising the RCS and allowing gravity injection from the PCMWT into the RPV. The plant then transitions to passive recirculation cooling and remains in a stable state for at least 72 hours beyond which the reactor stays shut down until AC power is restored.

All SSCs claimed to mitigate the long-term LOOP fault are reliant upon the PSS and DCE to perform their safety function(s). Safety functions relevant to the long-term LOOP fault have been identified and appropriately categorised; SSCs that mitigate this fault have been identified and appropriately classified. Details are provided in the UK DBAA Summary Report [5].

14.5.3.6 ATWS Involving a TTLOOP Event – Failure to Insert Control Rods

An ATWS + TTLOOP fault is one of the "worst case" accidents that triggers a complex sequence of responses from the PSS. The fault sequence progression involves various mechanical, electrical, and safety systems that respond to maintain plant safety. A turbine trip with simultaneous LOOP isolates steam flow, pressuriser spray and heaters, shuts feedwater, and lets the RCPs coast down. The rapid rise in RCS and steam generator pressure is detected, and PDH and SDH start to remove heat, but the control rods fail to insert. Pressuriser pressure continues to climb until the high pressure set point is reached and PSVs open to relieve excess pressure from the primary circuit by discharging steam into PCMWT. After which PDH and SDH, supported by negative Doppler and moderator-temperature reactivity feedback, cool and depressurise the RCS to a low power steady state. As secondary side pressure falls, a S-signal isolates the Main Steam System (MSS). If AC power is not restored within 24 hours, this will actuate Stage 1 ADS which works in conjunction with PCM to reduce RCS pressure in two stages to allow passive injection of borated water into the RCS for reactivity control via the accumulators, and then PCMWT injection (via ADS Stage 2). The core becomes sub-critical, decay heat is removed passively, and the plant remains in a safe, stable condition for at least 72 hours.

All SSCs claimed to mitigate the ATWS + TTLOOP fault are reliant upon the PSS and DCE to perform their safety function(s). Safety functions relevant to the ATWS + TTLOOP fault have been identified and appropriately categorised, and SSCs that mitigate the ATWS + TTLOOP fault have been identified and appropriately classified. Details are provided in the UK DBAA Summary Report [5].

14.5.4 Classification of SSCs

Argument 2.1.2.4-A2: All identified safety measures have been assigned an equivalent UK classification based on the categorisation of the safety function(s) they perform and the line(s) of protection in which they are claimed.

Evidence for Argument 2.1.2.4-A2:

- HI-2241577, SMR-300 GDA UK DBAA Summary Report Revision 0 [5] allocates provisional UK safety classes to the identified safety measures using the classification rules set out in the Safety Assessment Handbook [39].
- HI-2241323, SMR-300 GDA Preliminary Fault Schedule Report Revision 1 [4] describes how the PFS captures the line of protection and the status against design-basis targets for every SSC with information that underpins the provisional class assignments.

The US NRC classifies SSCs according to their safety-related functions. This functional approach, set out in Regulatory Guide 1.26 [34] and 10 CFR 50 Section 55a 'Codes and Standards' subparts (c), (d), and (e) [19], is applied in the SMR-300 classification methodology [63] This approach ensures that the intended safety functions are preserved while allowing design flexibility. Further details of the US approach are provided in Part A Chapter 2 [3]. The engineering chapters of the PSR align with Design Reference Point (DRP) [64], which reflect the output of the US Classification methodology.

The approach adopted for UK deployment is centred around demonstrating equivalency between the SMR-300 design, and UK categorisation and classification expectations. This is achieved through the application of formal safety assessment techniques, which are consistent with UK context expectations. These safety assessment techniques are developed to identify a comprehensive set of UK aligned safety functions and safety measures, and to demonstrate that radiological risks are tolerable and ALARP. This formal UK aligned safety assessment has commenced during GDA Step 2, through the development of a PFS and a limited set of DBAA.

The categorisation and classification expectations which are derived from this UK aligned assessment, can then be compared with the existing SMR-300 design and its corresponding US categorisation and classification. Work has commenced via relevant safety analysis and engineering disciplines, to demonstrate equivalency between the US and UK expectations and confirm that for all aspects, the SMR-300 design meets UK expectations. Where equivalency is at risk of not being demonstrable, then this may lead to a UK design challenge, potentially resulting in a modification to the design or requiring supplemental safety justification to demonstrate the current design reduces risks to ALARP. This equivalency demonstration is still in progress and is discussed further throughout PSR v1 Part B chapters. UK Design Challenges identified to date are reported in sub-chapter 14.5.6 and a dedicated GDA Commitment (C_Faul_103) is identified to complete the safety assessment work beyond Step 2.

SSC classification is the process by which SSCs are classified based on their significance in delivering associated safety functions. The suggested scheme makes use of the three classifications recommended in ONR SAP ECS.2 [41]:

- **Class 1:** Any SSC that forms a principal means of fulfilling a Category A safety function.
- **Class 2:** Any SSC that makes a significant contribution to fulfilling a Category A safety function or forms a principal means of ensuring a Category B safety function.

- **Class 3:** Any other SSC contributing to a categorised safety function.

It follows that any SSC claimed in the safety case as the first line means of delivering a Category A safety function must be Class 1. From this basic understanding, it also follows that SSCs claimed as secondary or diverse means of delivering a Category A safety function must be at least Class 2, as must the first line means claimed as delivering Category B safety functions.

The class of an SSC is fundamentally linked with its reliability. Performance targets associated with each SSC class are shown in Table 8. The Probability of Failure on Demand (PFD) is considered for systems operating in the low-demand mode; the frequency of a dangerous Failure per Year (PFY) is considered for systems operating in the high demand and continuous modes Failure Frequencies (FF).

Table 8: Performance Targets Linked to SSC Classification

SSC Class	PFY	PFD
Class 1	1E-03 ≥ FF ≥ 1E-05	1E-03 ≥ PFD ≥ 1E-05
Class 2	1E-02 ≥ FF > 1E-03	1E-02 ≥ PFD > 1E-03
Class 3	1E-01 ≥ FF > 1E-02	1E-01 ≥ PFD > 1E-02

Design requirements for redundancy, diversity, segregation and separation, single failure tolerance, reliability expectations, etc. should all follow from the designated classification.

The requirement to categorise safety functions and classify SSCs (and operator actions where such actions are credited in the safety case) is a fundamental aspect of design-basis analysis and applies across all levels of defence in depth, except for certain Level 5 provisions that are fulfilled by emergency arrangements rather than safety functions.

14.5.4.1 Initial SSC classification

The key factors in the initial assignment are:

a) Categorisation of a safety function(s) to be performed by the SSC.
b) The probability that the item will be called upon to perform them.

This is interpreted as the prominence of the SSC in the delivery of the safety function:

- For SSCs delivering preventative functions, as part of the normal operation of the plant, then it is likely that these will be in continuous or frequent demand. They should initially be considered as a principal means of delivering the safety function.
- For SSCs delivering protective or mitigative functions, in response to a fault or accident condition, then the principal / significant / other means usually relates to their position in the hierarchy of defence in depth and, often, but by no means always, to the order in which the SSCs respond to the progression of a fault (i.e., first / second / third).

There are no fixed requirements as to the number of safety systems required to deliver a safety function:

- A single SSC may contribute to the delivery of several safety functions; its class should be determined by the highest category function that it is intended to deliver.
- It is a regulatory expectation that Class 1 and Class 2 SSCs will feature within the safety measures identified for design basis faults. If two means of providing a safety function are identified, then one of these should be identified as the principal means.

The main expectation for the safety system or SSC classification is that it is based on the safety function category that needs to be delivered by the system and its relative importance in delivering that safety function. This permits the classification process to include principal and secondary (or back-up) safety systems as part of the DiD provision (refer to Table 9).

Table 9: Initial Classification of SSCs

Safety Function Category	SSC Classifications		
	Principal Means	Secondary Means	Other Means
Category A	Class 1	Class 2	Class 3
Category B	Class 2	Class 3	Class 3 (if needed)
Category C	Class 3	Class 3 (if appropriate)	Class 3 (if appropriate)

The details of the SSCs claimed against each of the faults considered in the initial UK DBAA is presented in the UK DBAA Summary Report [5]. The preliminary safety class shown corresponds to the highest class assigned at this entire-system level. Component level classifications will be produced as the fault schedule is refined under Commitment C_Faul_103.

It is noted that the actuation of the Class 1 and Class 2 SSCs claimed in the mitigation of the faults are dependent on the PSS without reliance on operator intervention. Hence, the boundary of each SSC must be extended to include the PSS. Furthermore, since DCE supplies power to all the safety-classified valves associated with the Class 1 and 2 SSCs claimed in the mitigation of the faults, the boundary of each SSC must be extended to include DCE.

14.5.5 Potential Risks Identified Against UK Expectations

As discussed in Section 14.5.4, the approach adopted for UK deployment is centred around demonstrating equivalency between the SMR-300 design, and UK categorisation and classification expectations. Early in GDA Step 2, an overarching Design Challenge Paper [DC 03][2] [65] was produced on the subject of the approach to categorisation and classification, single failure criteria and diversity. This concluded that in addition to limited DBAA work to support the GDA process, a more comprehensive UK aligned safety assessment should be conducted subsequent to GDA. The commitment to undertake this work is captured as GDA Commitment C_Faul_103.

C_Faul_103: *Holtec commit to ensuring that the repurposing of the US safety analyses undertaken for the Palisades SMR-300 design also considers and undertakes, as necessary, supplemental safety assessment to appropriately address UK expectations and good practice. This supplemental assessment should incorporate the full scope UK SMR-300 design and will be targeted to ensure a holistic and comprehensive approach across the recognised safety assessment disciplines. Future UK SSEC is therefore expected, as a minimum, to encompass:*

- *Completion of the identification of PIEs, within the full scope UK SMR-300 design.*
- *Harmonisation between this initiating event list for use in both deterministic and probabilistic assessments.*

[2] References in the form [DC NN] denote individual Design Challenge Papers, where “NN” is the unique paper number.

- *Extension of the scope of PSA to assess the SMR-300 design and operation to Level 3 PSA; this will include all sources of radionuclide release and operations (such as the Spent Fuel Pool) and all potential initiating events (e.g.,Internal Hazards, External hazards).*
- *Development of a UK-aligned set of design basis faults.*
- *An updated UK Fault and Protection Schedule, which covers all design basis faults for the SMR-300.*
- *UK DBAA studies to:*
    - *Identify UK aligned expectations for safety function categorisation and SSC classification for each bounding fault.*
    - *Demonstrate, supported by appropriately verified and validated UK DBAA, that the design can safely mitigate all design basis faults.*
    - *Undertake supporting radiological consequence analysis to demonstrate the residual risks are tolerable and ALARP.*
- *UK-aligned Severe Accident studies, informed by the PSA and DBAA, to ensure that the facility can be brought into a long-term safe, stable state.*
- *Incorporate Human Factor Engineering analysis (including Human Reliability Analysis) throughout DBAA / PSA / SAA.*

Several potential risks against UK expectations have been identified in the initial UK DBAA [5]. Where the associated design risk is significant, it is escalated as a Design Challenge and managed through the Design Adaptation Committee in accordance with the Design Management Process [66]. Design Challenges may be accompanied by preliminary optioneering or may flag the need for more detailed studies once supporting safety justification, including radiological-consequence assessments, are available. Consequently, final resolution of Design Challenges is often linked to progression of C_Faul_103. The key safety significant risks against UK expectations, identified by the initial DBAA work, are discussed in further detail below.

[REDACTED]

Refer to sub-section 14.7.2.3 or further details of the Design Challenges being led by the fault studies workstream. Other risks identified from the initial UK DBAA work are being tracked as normal business through progression of the fault studies workstream beyond GDA Step 2.

14.5.6 Candidate Safety Functional Requirements and Operating Rules

14.5.6.1 Safety Functional Requirements

Safety Functional Requirements (SFR) have been derived from the LLSFs and the performance requirements of the SSCs examined in the initial UK DBAA; they are recorded in the DBAA Summary Report [5]. The current list relates only to the six representative in-reactor faults studied during GDA Step 2, so it is not yet comprehensive. Once the full DBAA programme is complete, a complete schedule of SFRs will be produced for all design-basis faults, and an engineering schedule will confirm that the SMR-300 systems design, substantiated in the relevant systems chapters can deliver each SFR. The interim SFR list can be found in the UK DBAA Summary Report [5].

14.5.6.2 Operating Rules

ONR SAP SC.6 [41] defines the expectation for a safety case to identify operating limits and conditions to ensure that a facility is kept in a safe condition, and that the safety case justifies how any requirements will be implemented effectively.

ONR SAP FA.9 [41] identifies the following types of limits and conditions, and suggests that these should be derived from the DBAA:

1. Performance requirements and safety settings for safety systems and safety-related equipment.
2. Conditions governing permitted plant configurations and the availability of safety systems and safety-related equipment.
3. The SOE for the facility.

These limits and conditions, also known as ORs, are conditions that are required for safe plant operation and specify the minimum performance standards and configuration requirements for equipment critical to nuclear safety. They are written for operators so that compliance can be clearly demonstrated, and any non-compliance readily identified. A complete set of ORs therefore define a SOE for an operator to implement, with the envelope being as close to routine operations as reasonably practicable.

Candidate ORs have been identified and linked to faults with unmitigated radiological consequences that exceed 20 mSv to a worker (on-site), or 1 mSv to the public (off-site). Where applicable, limits have been proposed for the following parameters:

- RCS pressure-boundary pressure.
- MSS pressure-boundary pressure.
- Peak clad temperature.
- Avoidance of reactor-core overheating.
- Containment heat-removal capability.
- Water level in the PCMWT.
- Water level in the Annular Reservoir.

The fault specific candidate ORs and their supporting justification are recorded in the UK DBAA Summary Report [5]. These provisional limits will be refined and incorporated into a complete SOE as the DBAA programme progresses.

Although ORs are not expected to be subject to HRA, as operator action is not credited within the first 72 hours of any DBA, the integration of HF remains important. As part of our broader Human Factors Engineering (HFE) any operational tasks relevant to maintaining the SOE will be captured in the operational task schedule described in the Step 2 Summary of Claims on Users report [67]. If any operator actions are identified as having a primary safety role, they will be tracked within the OTS and assessed through the HRA process, in line with the HRA strategy to be developed under Part B Chapter 17 Commitment C_Huma_003. This linkage is also reflected in Commitment C_Faul_103.

14.5.7 CAE Summary

The current PFS and the initial DBAA work provide only partial coverage of the SMR-300 fault spectrum, therefore Claims 2.1.2.3 and 2.1.2.4 cannot yet be fully demonstrated. A level of maturity appropriate for a PSR has nevertheless been achieved for the following reasons.

- The PFS gives the initial listing of reactor-fault families and assigns provisional safety functions and preliminary SSC classes to each, establishing a structured basis for subsequent deterministic analysis. It is however recognised that for a considerable number of reactor faults, the initial UK categorisation and classification within the PFS are yet to be confirmed by associated DBAA.
- Targeted DBAA studies have been completed for a set of representative in-reactor faults. These assessments demonstrate that the claimed safety systems meet the deterministic acceptance criteria for those faults and identify potential risks, all of which have been raised as Design Challenges or captured as GDA Commitments for resolution after Step 2.
- The SMR-300 relies predominantly on the same passive systems to mitigate the majority of reactor faults. Resolving the Design Challenges already identified is therefore expected to bound the issues likely to arise when the remaining reactor faults are assessed in future DBAA work.
- Fuel route faults and radioactive waste faults are yet to be considered in significant detail either in the PFS or the DBAA. However, this is considered to be a reasonable position to support a fundamental design assessment.

On this basis Claims 2.1.2.3 and 2.1.2.4 are considered to be met to a level commensurate with a PSR, subject to the completion of the outstanding Design Challenges and GDA Commitments.

14.6 ACCIDENT ANALYSIS AND MODELLING

This sub-chapter provides the demonstration of the following Level 4 claim:

Claim 2.1.2.5: Appropriately conservative analysis demonstrates that for all design basis faults, the identified safety measures, in conjunction with operator actions, enable the plant to reach a safe state and ensure that defined acceptance criteria are met.

This claim addresses the requirement to demonstrate that for all design basis faults the consequences are tolerable. This is primarily achieved through the continued confinement of radioactive material by the claimed containment barriers (i.e., fuel cladding, reactor coolant pressure boundary and containment structure). The demonstration of tolerability is made through the application and use of US DSA transient analysis.

This sub-chapter supports Claim 2.1.2.5, which has been further decomposed into three arguments:

- Acceptance criteria have been defined such that compliance with them enables this to be demonstrated (A1).
- The transient and accident analysis for the SMR-300 utilises methodologies defined as best practice within the US regulatory environment as required by the US Nuclear Regulatory Commission (NRC) (A2).
- Additional analyses have been performed to underpin the demonstration of ALARP within a UK context (A3).

This sub-chapter outlines how DSA confirms that the SMR-300 satisfies its acceptance criteria. It covers:

- Definition of acceptance criteria that set thermal-hydraulic, structural-integrity and radiological limits and show alignment with ONR SAP numerical targets.
- Performance of transient and accident analyses using US best-practice codes and models and presentation of the principal results.
- Supplementary UK analyses and Commitments that support the ALARP demonstration and capture forward work.

14.6.1 Acceptance Criteria

Argument 2.1.2.5-A1: Acceptance criteria are defined such that meeting them demonstrates adequate levels of safety.

Evidence for Argument 2.1.2.5-A1:

- HI-2240235, SMR-300 Acceptance Criteria for Deterministic Safety Analysis Revision 2 [68] defines thermal-hydraulic, structural-integrity and radiological criteria for AOOs and DBAs.

The acceptance criteria for the SMR-300 are linked to the classification of the licensing basis event (i.e., AOOs, DBAs, and BDBAs identified in SMR-300 Acceptance Criteria for Deterministic Safety Analysis Revision 2 [68]). Details on the BDBA acceptance criteria are included in Part B Chapter 15 [13]. These criteria are, in general, underpinned by a

comprehensive suite of transient analysis. The general acceptance criteria for AOOs and DBAs are provided below, and additional fuel specific criteria for both event classes are given in SMR-300 GDA Fuel Design Criteria and Limits report [69].

14.6.1.1 AOO Acceptance Criteria

The following are the specific acceptance criteria for AOOs:

- Pressure in the reactor coolant and MSSs shall be maintained below 110% of the design values in accordance with the American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code [70].
- Specified Acceptable Fuel Design Limits (SAFDL) are not exceeded. The SAFDLs used to demonstrate fuel integrity are:
    - Fuel cladding integrity shall be maintained by ensuring that the minimum Departure from Nucleate Boiling Ratio (DNBR) remains above the 95/95 DNBR limit.[3]
    - Fuel Centreline Melt (FCM) temperature is not exceeded.
    - Transient Clad Strain (TCS) limit is not exceeded.
- 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.

It is noted that the AOO acceptance criteria are more onerous than the DBA acceptance criteria introduced below.

14.6.1.2 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 [71].
- 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 [19] also apply:
    - The calculated maximum fuel element cladding temperature shall not exceed 2200 °F (or 1204 °C).

[3] A Departure from Nucleate Boiling (DNB) is the point at which the heat transfer from a fuel rod rapidly decreases due to the insulating effect of a steam blanket that forms on the surface of the rod when the temperature continues to increase. The 95/95 limit corresponds to a 95% probability at the 95% confidence level that DNB will not occur.

- 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.
- The calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed for an extended period of time after successful Emergency Core Cooling System (ECC) initiation.

A complete list of acceptance criteria can be found in [68].

14.6.2 Application and Use of US Transient and Accident Analysis

Argument 2.1.2.5-A2: The transient and accident analysis for the SMR-300 utilises methodologies defined as best practice within the US regulatory environment as required by the US Nuclear Regulatory Commission (NRC).

Evidence for Argument 2.1.2.5-A2:

- HI-2240980, SMR-300 Transient Analysis for the Generic Design Assessment Revision 0 [72] documents limiting transients calculated with NRC-approved codes and demonstrates compliance with the acceptance criteria.
- HI-2241556, SMR-300 Codes Verification and Validation Summary Report Revision 0 [73] summarises the verification and validation evidence that supports the analysis codes.
- HI-2250047, SMR-300 RELAP5-3D Verification and Validation Plan Revision 0 [74] sets out the ongoing plan for code-specific verification and validation.

14.6.2.1 Methodology

Transient and accident analyses have been performed, in accordance with US NRC regulatory requirements, to show that the operation of the SMR-300 does not pose an unacceptable risk or consequences, with DBAs assessed using a conservative deterministic methodology and AOOs assessed using a best estimate methodology. The main objective of the transient and accident analysis 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 4. 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 the applicable acceptance criterion until the plant can be considered to have met the safe shutdown condition.

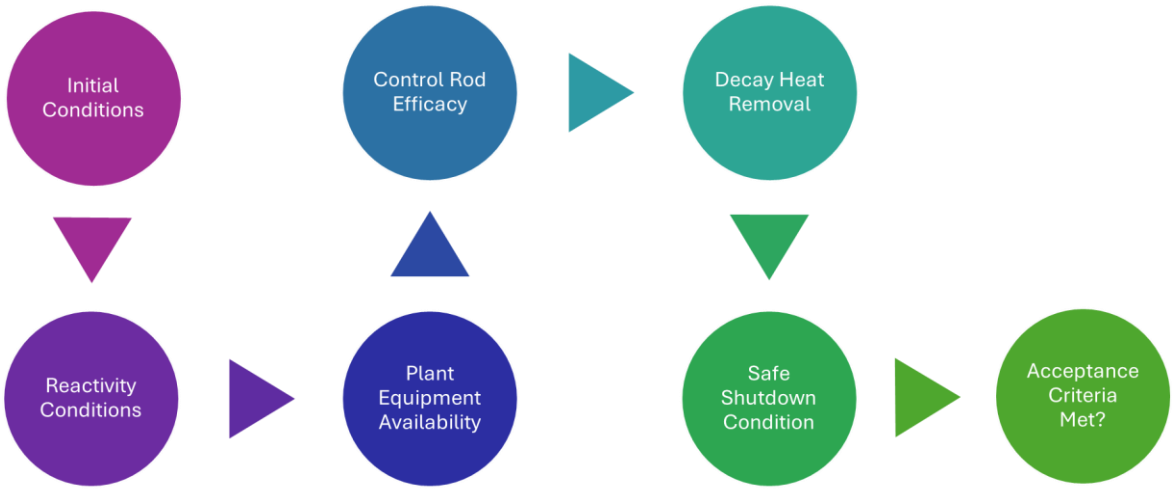

Figure 4: US Transient and Accident Analysis Methodology

To date, a wider programme of deterministic analyses is in progress including additional DBA work that will also support the forthcoming US licensing application for the Palisades deployment, and the following representative transient and accident analyses have been undertaken for the support of ongoing UK DBAA through SMR-300 Transient Analysis for the Generic Design Assessment [72]:

- MSLB, involving a rupture of one of the main steam lines inside containment at full power resulting in an overcooling event.
- Inadvertent actuation of the PDH, involving the sudden inadvertent actuation at full operating power resulting in an overcooling event.
- Inadvertent actuation of the SDH, involving the sudden inadvertent actuation at full operating power resulting in an overcooling event.
- TTLOOP involving a sudden turbine trip at full power without the availability of off-site power resulting in an overheating event.
- Large Break Loss of Coolant Accident (LBLOCA), involving a Double-Ended Guillotine (DEG) rupture of one of the cold leg pipes at full power resulting in a rapid reduction in coolant inventory.
- SBLOCA, involving a DEG rupture of one of the DVI lines at full power.
- ATWS involving a TTLOOP event followed by the failure to insert the control rods to achieve shutdown.

14.6.2.2 Use of Computer Codes

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

- System thermal hydraulics analysis using RELAP5-3D.
- Core thermal hydraulics analysis using COBRA-FLX.
- Containment analysis using GOTHIC.
- Core physics modelling utilising CASMO5, CMSLINK5, SIMULATE5 and SIMULATE-3K.
- Radiological consequences using RADTRAD.
- Source term modelling using SCALE / ORIGEN and MCNP.

- Atmospheric dispersion using ARCON2.0.

A description of these codes is provided in Appendix C.

Regulatory Guide 1.203 [32] sets out the US NRC's expectations for developing and assessing an Evaluation Model (EM) for transient and accident analyses. The guidance requires definition of the EM scope and requirements, assembly of an assessment base of relevant experimental data, development of the calculational framework, demonstration of adequacy through bottom-up and top-down assessments, and application of quality-assurance and documentation controls.

For the SMR-300 the RELAP5-3D code will be qualified following the Evaluation Model Development and Assessment Process (EMDAP) described in [32]. This plan covers requirement definition, scaling analysis, selection of Separate and Integral Effects Tests, model development, validation, uncertainty assessment and documentation. Equivalent EMDAP plans for the remaining analysis codes will be produced as the design matures beyond GDA; a full summary will be provided in the PCSR. The remaining analysis codes already have existing US NRC approved topical reports. It is planned to leverage these approvals and demonstrate the applicability of each code, with any necessary model adjustments, to the SMR-300 design during the ongoing validation programme.

SMR-300 Codes Verification and Validation Summary Report [73] summarises several key references which demonstrate RGP for the development and use of safety-critical computer codes. ONR SAPs AV.1 to AV.8 [41] were used as a basis of comparison between regulatory best practice and quality guidance from NRC (i.e., Regulatory Guide 1.203 [32]) and Holtec documentation (i.e., Holtec Standard Procedure - Computer Programs [75], and Holtec Quality Procedure - Test Control [76]). The details from this assessment are given in the SMR-300 Codes Verification and Validation Summary Report [73].

The US transient and accident analyses have provided a useful source of information which has been aligned and utilised (where appropriate) during the development of the initial UK DBAA. The detail output from the US transient and accident analyses used to inform the UK DBAA is presented in the UK DBAA Summary Report [5].

14.6.3 Risks Identified Against UK Expectations

Several potential risks in the transient analyses when assessed against UK expectations have been identified from the initial UK DBAA [5]. The commitment to undertake this work is captured as part of C_Faul_103, regarding the need to demonstrate, supported by appropriately verified and validated UK DBAA, that the design can safely mitigate all design basis faults.

[REDACTED]

14.6.4 Additional Analyses

Argument 2.1.2.5-A3: Additional analyses have been performed to underpin the demonstration of ALARP within a UK context.

Evidence for Argument 2.1.2.5-A3:

- HI-2241577, SMR-300 GDA UK DBAA Summary Report Revision 0 [5] presents supplementary deterministic studies that support the ALARP demonstration.
- GDA Commitment C_Faul_103 records the requirement to a gap analysis and any further analyses necessary to finalise the ALARP case.

A gap analysis is required to identify any additional analyses required to underpin the demonstration of ALARP within a UK context. This is to be captured within GDA Commitment C_Faul_103. More details are presented in sub-section 14.7.2.

14.6.5 CAE Summary

It has been demonstrated that the requirements for Claim 2.1.2.5 have been partially met. Acceptance criteria consistent with UK and US guidance have been defined, and initial transient and accident analyses, performed with NRC best-practice methods, show compliance with those criteria. It would not generally be expected to have a comprehensive set of DSA results to support a PSR. The maturity of the DSA will continue to progress post GDA Step 2 to verify and validate the design and inform the SMR-300 design development where margins are challenged. This iterative approach between the safety analysis and ongoing design development, is discussed further in Part A Chapter 4 [7]. Code verification and validation activities and supplementary UK analyses will continue to be progressed as part of GDA Commitment C_Faul_003 will complete the ALARP demonstration in a future revision of the safety case.

14.7 CHAPTER SUMMARY AND CONTRIBUTION TO ALARP

This sub-chapter provides an overall summary and conclusion of the Design Basis Analysis (Fault Studies) chapter and how this chapter contributes to the overall demonstration of ALARP for the generic SMR-300.

Part A Chapter 5 Summary of ALARP and SSEC [77] sets out the overall approach for demonstration of ALARP and how contributions from individual chapters are consolidated. This sub-chapter therefore consists of the following elements:

- Technical Summary.
- ALARP Summary:
  - Demonstration of Relevant RGP.
  - Evaluation of Risk and Demonstration Against Risk Targets.
  - Options Considered to Reduce Risk.
- GDA Commitments.
- Conclusion.

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

14.7.1 Technical Summary

Part B Chapter 14 aims to demonstrate the following Level 3 claim to a maturity appropriate for a PSR:

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 into five Level 4 claims which have been demonstrated throughout this chapter. This chapter explains:

- The approach, strategy, and methodology for production of a UK DBAA utilising US DSA input (Claim 2.1.2.1):
  - Relevant codes and standards have been identified to demonstrate that the UK DBAA analysis aligns with UK industry expectations by alignment with the ONR SAPs (in the absence of project-specific requirements).
- The approach, strategy, and methodology for production of a PFS (Claim 2.1.2.2):
  - A structured and systematic process has been applied to identify, screen and group a provisional set of design-basis faults. Benchmarking against a published UK PWR safety case provides confidence that the current list is adequate for the current design maturity. The fault schedule will be extended and confirmed in later GDA steps to ensure full coverage.
- The approach to categorisation of safety functions and classification of SSCs reflects the limited yet targeted scope of DBAA completed to date:
  - The PFS establishes the first structured list of reactor fault families and, for those already assessed, identifies the safety functions needed for successful mitigation and assigns provisional categories to each (Claim 2.1.2.3). Adequate lines of protection have been demonstrated for these faults and identified

uncertainties or potential shortfalls have been escalated as Design Challenges or GDA Commitments for progression beyond GDA Step 2.
    - The same analyses confirm that the passive safety systems embodied in the current design provide the principal SSCs required to deliver those functions, and these SSCs have been provisionally classified (Claim 2.1.2.4). Because most remaining reactor faults will rely on the same passive systems, resolving the Design Challenges identified so far is expected to bound similar issues that may arise when the full DBAA portfolio is completed after Step 2.
- The assessment of accidents and transients has established acceptance criteria and applied recognised US analysis codes to representative operating modes, using limiting single failures and conservative initial conditions in line with modern standards. This scope supports Claim 2.1.2.5 for the events already analysed, the need for further studies to complete the portfolio and finalise the ALARP demonstration has been captured in GDA Commitment C_Faul_103.

Throughout this chapter and in support of all claims, the appropriate methodology in accordance with RGP and UK licensing requirements have been identified. The US DSA provides a substantial source of information and has been utilised in the development of the initial UK DBAA undertaken on a limited number of initiating events. The identified gaps will be addressed in subsequent licensing phases if the SMR-300 proceeds beyond GDA.

14.7.2 ALARP Summary

14.7.2.1 Demonstration of RGP

The SMR-300 basis of design has been developed in accordance with US codes and standards and takes due cognisance of good practice (including OPEX) adopted in the US and elsewhere (e.g. Electric Power Research Institute (EPRI), NEI, IAEA). Part A Chapter 2 [3] presents the overall approach to the assessment of the generic SMR-300 design against UK codes and standards.

The principal codes and standards are identified within sub-chapter 0. Table 3 contains the RGP considered for design basis analysis. This is based on:

- Existing practices adopted on UK nuclear licensed sites.
- Application in earlier and successful GDA submissions.
- Recognition as RGP by ONR SAPs and TAGs.

The UK DBAA provides insights for use in the design of the safety measures used to provide the significant safety functions to meet relevant risk targets. In the UK context, there is an additional requirement that the risk from faults to the public, workforce and environment should be ALARP. 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.

The UK DBAA is therefore a crucial part of the demonstration that risks are ALARP:

- Sub-chapter 14.4 shows that Holtec follows RGP by using a functional approach to identify a set of safety functions to provide all necessary levels of DiD against a limited set of potential faults.

- Sub-chapter 14.5 demonstrates that the safety functions are categorised based on importance to safety with suitably classified SSCs allocated to provide these safety functions.

These contributions are subject to the correct substantiation of requirements and implementation of safety management arrangements.

14.7.2.2 Evaluation of Risk and Demonstration Against Risk Targets

The numerical targets against which the demonstration of ALARP is considered can be found in Part A Chapter 2 [3]. The UK DBAA identifies SSCs, which through the defined safety functions, 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 ONR SAP Numerical Targets 1-3 [41].
- By achieving their safety classification as a duty system or a protection system, where claimed, they will contribute to the achievement of accident risk, ONR SAP Numerical Targets 4-9 [41].

The evaluation of the normal operations and accident risks against Targets 1-9 is summarised in Part A Chapter 5 [77].

ONR SAP Numerical Target 4 for design basis analysis represents criteria for assessing the safety of a facility's design and operations for faults that could have significant radiological consequences. They are based on initiating fault frequencies and so take no account of the reliability of the claimed safety measures. Instead, they place the focus on the effectiveness of the safety measures in addressing the fault's consequences (effective dose).

ONR SAP Numerical Target 4 sets Basic Safety Levels (BSL) and BSOs for on-site and off-site dose. Detailed UK consequence calculations that would allow formal comparison with these targets have not yet been completed, so compliance cannot be demonstrated at this stage. Preliminary US analyses and the passive design of the SMR-300 provide confidence that doses will fall below the Target 4 limits and are likely to approach the objectives once fully assessed. The required UK consequence assessments are programmed under a GDA Commitment and will be reported in a future revision of the safety case.

It is a regulatory expectation that design basis techniques are applied to fault sequences with frequencies down to 1E-07 per annum – this is known as the design basis fault sequence cut-off frequency. Refer to the UK DBAA Summary Report [5] for a summary of the IEF and unmitigated radiological consequences of each fault considered in the initial UK DBAA.

Detailed radiological consequence assessments are not yet available to support PSR v1. During development of the PFS, unmitigated consequences were conservatively estimated using engineering judgement and data from comparable PWR events. These estimates assign indicative dose bands to each fault and confirm that the credited lines of protection are sufficient to meet ONR SAPs Numerical Target 4. Further information on the conservative approach is provided in the PFS Report [57]. Comprehensive radiological consequence analyses will be completed for each design basis fault beyond GDA timescales and reported in the PCSR.

14.7.2.3 Options Considered to Reduce Risk

Where appropriate, optioneering has been undertaken to determine optimal design solutions, consistent with the ALARP principle. The process for the assessment of risk reduction options is presented in Design Management Process [66].

Design Challenges have been raised to further progress the prospective risks (refer to sub-section 14.5.5) identified in the initial UK DBAA. Given the cross-cutting nature of the fault studies scope, a considerable number of Design Challenges interface with the ongoing fault studies work and GDA Commitment C_Faul_103. These Design Challenges are listed below, with reference to the current PSR chapter where more information is presented.

- I&C Architecture [DC 01] – Part B Chapter 4 [10].
- Diverse Means of Shutdown [DC 04] – Part B Chapter 1 [8].
- Mechanical SSC Classification [DC 05] – Part B Chapter 19 [78].
- Single Failure Criterion in Passive Safety Systems [DC 12] – Part B Chapter 14.
- HVAC Architecture, Design Codes and Design Basis [DC 13] – Part B Chapter 5 [11].
- Valve Diversity and Motor Operated Valves [DC 25] – Part B Chapter 19 [78].

A summary of the relevant Design Challenges being led by the Fault Studies workstream is presented below.

14.7.2.3.1 Differences in the Application of Categorisation and Classification [DC 03]

[REDACTED]

14.7.2.3.2 Single Failure Criterion in Passive Safety Systems [DC 12]

[REDACTED]

14.7.3 GDA Commitments

Holtec recognise that differences exist between US and UK requirements, with regards to the scope and extensiveness of the safety assessment applied to the SMR-300 design. The Preliminary Safety Analysis Report for the Palisades SMR-300 design will reference safety analyses that will be repurposed for any future UK SSEC.

The following GDA Commitment is therefore identified in this chapter of the PSR:

C_Faul_103: *Holtec commit to ensuring that the repurposing of the US safety analyses undertaken for the Palisades SMR-300 design also considers and undertakes, as necessary, supplemental safety assessment to appropriately address UK expectations and good practice. This supplemental assessment should incorporate the full scope UK SMR-300 design and will be targeted to ensure a holistic and comprehensive approach across the recognised safety assessment disciplines. Future UK SSEC is therefore expected, as a minimum, to encompass:*

- *Completion of the identification of PIEs, within the full scope UK SMR-300 design.*
- *Harmonization between this initiating event list for use in both deterministic and probabilistic assessments.*
- *Extension of the scope of PSA to assess the SMR-300 design and operation to Level 3 PSA; this will include all sources of radionuclide release and operations (such as the*

Spent Fuel Pool) and all potential initiating events (e.g.,Internal Hazards, External hazards).

- *Development of a UK-aligned set of design basis faults.*
- *An updated UK Fault and Protection Schedule, which covers all design basis faults for the SMR-300.*
- *UK DBAA studies to:*
  - *Identify UK aligned expectations for safety function categorisation and SSC classification for each bounding fault.*
  - *Demonstrate, supported by appropriately verified and validated UK DBAA, that the design can safety mitigate all design basis faults.*
  - *Undertake supporting radiological consequence analysis to demonstrate the residual risks are tolerable and ALARP.*
- *UK-aligned Severe Accident studies, informed by the PSA and DBAA, to ensure that the facility can be brought into a long-term safe, stable state.*
- *Incorporate Human Factor Engineering analysis (including Human Reliability Analysis) throughout DBAA / PSA / SAA.*

14.7.4 Conclusion

Part B Chapter 14 presents the fault studies approach undertaken and presents the CFL and PFS. It identifies the relevant claims, arguments and currently available evidence that form the basis of the safety case for the fault studies topic to a maturity appropriate for a PSR. It also summarises the approach to design basis accident analysis in the UK context and the extent to how this has been applied for GDA Step 2.

The conclusion of this chapter of the PSR is that:

- The chapter claims identified have been met to a maturity appropriate for a PSR, noting the associated Design Challenges and GDA Commitments which have been raised. As the design and safety case continue to be developed, further evidence will be provided to substantiate these claims.
- 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.
- Design basis provisions have been assessed by analysing several selected bounding faults that have informed safety categorisation of claimed safety measures, with consequent requirements for redundancy, diversity, and segregation. The analyses have also informed performance requirements, so that the safety measures can meet the deterministic success criteria relevant to the plant state that needs to be achieved following a postulated fault. The analysis undertaken so far provides confidence that the selected design basis faults can be adequately protected with margin to the acceptance criteria. Any potential shortfalls as a result of the analyses to date have been captured as Design Challenges and GDA Commitments.

Beyond GDA timescales, the scope of the deterministic analysis will be widened to cover all fault scenarios and all modes of operation. Safety measures will be identified in a more detailed manner for faults in areas other than the reactor and at-power operation, including for shutdown modes, for the Spent Fuel Pool, for fuel handling activities and for waste treatment and storage. Radiological consequence analysis for fault sequences will also be undertaken

and evaluated against relevant acceptance criteria. At PCSR maturity, the documentation created at the PSR stage will be expanded upon to have a fully developed set of design basis faults, whereby all credible 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 UK Fault and Protection Schedule to capture this information.

Based on the preliminary evidence currently available, there is confidence that the design of the SMR-300 is on an appropriate trajectory to demonstrate that there will be sufficient DiD provided by the safety measures against all fault sequences identified at this stage to deliver the Holtec International HLSFs.

14.8 REFERENCES

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

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

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

[4] Holtec Britain, “HI-2241322, Preliminary Fault Schedule,” Revision 1, May 2025.

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

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

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

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

[9] Holtec Britain, “HI-2240776, Holtec SMR GDA PSR Part B Chapter 2 Reactor [UK Exp Ctrl],” Revision 1, July 2025.

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

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

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

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

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

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

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

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

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

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

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

[21] United States Nuclear Regulatory Commission, “NEI 97-04, Revised Appendix B, Guidance and Examples for Identifying 10 CFR 50.2 Design Bases,” November 2002.

[22] American National Standards Institute & American Nuclear Society, “ANSI/ANS-58.14-2011 (R2017) Safety And Pressure Integrity Classification Criteria For Light Water Reactors,” January 2017.

[23] Idaho National Laboratory, “INL/RPT-23-72818, Initiating Event Rates at US NPP, 2022 Update,” June 2023.

[24] Nuclear Energy Institute, “NEI 18-04, Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development,” Revision 1, August 2019.

[25] United States Nuclear Regulatory Commission, “NUREG-0800, Chapter 15, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Transient and Accident Analysis,” Revision 3, March 2007.

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

[27] United States Nuclear Regulatory Commission, “NUREG-0651, Evaluation of Steam Generator Tube Rupture Events,” March 1980.

[28] United States Nuclear Regulatory Commission, “NUREG/CR-5750, Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995,” February 1999.

[29] United States Nuclear Regulatory Commission, “NUREG/CR-6890, Reevaluation of Station Blackout Risk at Nuclear Power Plants,” December 2005.

[30] United States Nuclear Regulatory Commission, “NUREG/CR-6928, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants,” February 2007 (2017 update).

[31] United States Nuclear Regulatory Commission, “NUREG-1829, Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process,” April 2008.

[32] United States Nuclear Regulatory Commission, “Regulatory Guide 1.203, Transient and Accident Analysis Methods,” December 2005.

[33] United States Nuclear Regulatory Commission, “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.

[34] United States Nuclear Regulatory Commission, “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.

[35] International Atomic Energy Agency, “IAEA-TECDOC-749, Generic Initiating Events for Psa for WWER Reactors,” 1994.

[36] International Atomic Energy Agency, “IAEA-TECDOC-719, Defining Initiating Events for Purpose of Probabilistic Safety Assessment,” 1993.

[37] International Atomic Energy Agency, Specific Safety Requirements No. SSR-2/1, Safety of Nuclear Power Plants: Design, Revision 1, 2016.

[38] International Atomic Energy Agency, “Specific Safety Guide SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants,” 2014.

[39] Holtec Britain, “HI-2250210, SMR-300 GDA Safety Assessment Handbook,” Revision 1, June 2025.

[40] International Atomic Energy Agency, “Specific Safety Guide No. SSG-2, Deterministic Safety Analysis for Nuclear Power Plants,” Revision 1, 2019.

[41] Office for Nuclear Regulation, “Safety Assessment Principles For Nuclear Facilities,” Revision 1, January 2020.

[42] Office for Nuclear Regulation, “ONR-GDA-GD-006, New Nuclear Power Plants: Generc Design Assessment Guidance to Requesting Parties,” Revision 0, October 2019.

[43] Office for Nuclear Regulation, “ONR-GDA-GD-007, New Nuclear Power Plants: Generic Design Assessment Technical Guidance,” Revision 0, May 2019.

[44] Office for Nuclear Regulation, “NS-TAST-GD-005, Guidance on the Demonstration of ALARP,” Revision 11.2, June 2023.

[45] Office for Nuclear Regulation, “NS-TAST-GD-006, Design Basis Analysis,” Issue 5.1, December 2022.

[46] Office for Nuclear Regulation, “NS-TAST-GD-035, ONR Technical Assessment Guide (TAG) Limits and Conditions for Nuclear Safety (Operating Rules),” Revision 7, March 2023.

[47] Office for Nuclear Regulation, “NS-TAST-GD-036, Diversity, Redundancy, Segregation and Layout of Mechanical Plant,” Revision 3, November 2023.

[48] Office for Nuclear Regulation, “NS-TAST-GD-04, Nuclear Safety Technical Assessment Guide - Validation of Computer Codes and Calculation Methods,” Revision 8, April 2023.

[49] Office for Nuclear Regulation, “NS-TAST-GD-051, The Purpose, Scope and Content of Safety Cases,” Revision 4, December 2022.

[50] Office for Nuclear Regulation, “ONR-TAG NS-TAST-GD-094, Categorisation of Safety Functions and Classification of Structures, Systems and Components,” Revision 2, 2019.

[51] International Atomic Energy Agency, “Specific Safety Requirements No. SSR-2/2, Safety of Nuclear Power Plants: Commissioning and Operation,” Revision 1, 2016.

[52] Western European Nuclear Regulators' Association, “Safety Reference Levels for Existing Reactors,” February 2021.

[53] Western European Nuclear Regulators' Association, “Report on Safety of new NPP designs,” March 2013.

[54] Western European Nuclear Regulators' Association, “WENRA Statement on Safety Objectives for New Nuclear Power Plants,” November 2010.

[55] United States Nuclear Regulatory Commission, “NUREG/CR-2300, PSA Procedures Guide,” January 1983.

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

[57] Holtec Britain, “HI-2241323, Preliminary Fault Schedule Report,” Revision 1, May 2025.

[58] Westinghouse, “UKP-GW-GL-793NP, AP-1000 Pre-Construction Safety Report,” Revision 1, January 2016.

[59] EDF, “UK EPR - The Pre-Construction Safety Report (PCSR),” [Online]. Available: https://www.edfenergy.com/energy/nuclear-new-build-projects/hinkley-point-c/reactor/uk-epr-generic-design-assessment.

[60] General Nuclear Systems Ltd, “HPR/GDA/PCSR/0001, Pre-Construction Safety Report,” Revision 0, 2018.

[61] Holtec Britain, “HI-2240725, Human Reliability Assessment Step 2 Position Statement,” Revision 0, January 2025.

[62] Holtec Britain, “HI-2240612, UK SMR-300 GDA Design Challenge - I&C Architecture [DC 01],” Revision 0, May 2025.

[63] Holtec International, “HPP-8002-0012, SMR-300 Structures, Systems and Component Classification,” Revision 0, February 2025.

[64] Holtec Britain, “HI-2240648, GDA Design Reference Point,” Revision 2, May 2025.

[65] Holtec Britain, “HI-2241290, UK SMR-300 GDA Design Challenge - Differences in the application of Categorisation and Classification principles between US and UK licensing regimes and associated risks to the SMR-300 design [DC 03],” Revision 0, December 2024.

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

[67] Holtec Britain, “HI-2240727, Summary of Claims Placed on System Users for SMR-300,” Revision 0, May 2025.

[68] Holtec International, “HI-2240235, SMR-300 Acceptance Criteria for Deterministic Safety Analysis,” Revision 2, August 2024.

[69] Holtec Britain, “HI-2241327, Holtec SMR-300 GDA Fuel Design Criteria and Limits [UK Exp Ctrl],” Revision 1, May 2025.

[70] American Society of Mechanical Engineers, “Boiler and Pressure Vessel Code, Section III-Rules for Construction of Nuclear Facility Components,” 2022.

[71] United States Nuclear Regulatory Commission, “10 CFR PART 100—REACTOR SITE CRITERIA,” 2015.

[72] Holtec International, “HI-2240980, SMR-300 Transient Analysis for the Generic Design Assessment,” Revision 0, September 2024.

[73] Holtec Britain, “HI-2241556, SMR-300 Codes Verification and Validation Summary Report,” Revision 0, December 2024.

[74] Holtec International, “HI-2250047, SMR-300 RELAP5-3D Verification and Validation Plan,” Revision 0, January 2025.

[75] Holtec International, “HSP-101101, Computer Programs,” Revision 3, February 2023.

[76] Holtec International, “HQP-11.0, Holtec Quality Procedure - Test Control,” Revision 25, October 2018.

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

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

[79] United States Nuclear Regulatory Commission, “Regulatory Guide 1.194, ATMOSPHERIC RELATIVE CONCENTRATIONS FOR CONTROL ROOM RADIOLOGICAL HABITABILITY ASSESSMENTS AT NUCLEAR POWER PLANTS,” June 2003.

[80] United States Nuclear Regulatory Commission, “Regulatory Guide 1.249, USE OF ARCON METHODOLOGY FOR CALCULATION OF ACCIDENT-RELATED OFFSITE ATMOSPHERIC DISPERSION,” Revision 0, 2022.

14.9 LIST OF APPENDICES

Appendix A PSR Part B Chapter 14 CAE Route Map

Table 10: PSR Part B Chapter 14 CAE Route Map

[REDACTED]

Appendix B Derivation of Safety Functions

Note: The list of LLSFs is not exhaustive and will be developed as additional faults are subjected to a full UK DBAA.

Table 11: List of Safety Functions

High Level Function (Safety)	Plant Level Safety Function (PLSF)	Lower-Level Safety Function (LLSF)
1.1: Control Reactivity / Shutdown	1.1.1: Reactor Trip	Shutdown the reactor and maintain core sub-criticality by rapid negative reactivity insertion.
	1.1.2: RCS Boron Concentration	Maintain core reactivity control by controlling boron concentration – slow variation.
		Prevent uncontrolled positive reactivity insertion in the core by ensuring minimum boron concentration of water injected into the RCS.
1.2: Post-Accident Heat Removal	1.2.1: Core Decay Heat Removal	Remove heat from the core to the reactor coolant and transfer heat from the reactor coolant to the ultimate heat sink.
	1.2.2: Maintain Coolant Inventory	Ensure sufficient RCS inventory for core cooling.
		Prevention of RCS leakage through the RCP seals.
		Prevention of RCS drainage through auxiliary lines.
		RCS Pressurizer level control.
	1.2.3: Spent Fuel Decay Heat Removal	Remove heat from the fuel bundle(s) in the Spent Fuel Pool.
1.3: Reactor Coolant System Integrity	1.3.1: Reactor Coolant Pressure Boundary Isolation	Ensure confinement of radioactive material by the reactor coolant pressure boundary.
	1.3.2: RCS Pressure Control	Maintain integrity of the reactor coolant pressure boundary.
1.4: Containment Integrity	1.4.1: Containment Isolation	Ensure confinement of radioactive material by the reactor containment structure and containment isolation valves.
		Limitation of mass / energy release inside containment.
		Limit the release of radioactive waste and airborne radioactive material.
	1.4.2: Containment Pressure and Temperature Control	Remove heat from containment and transfer this heat to the ultimate heat sink.
1.5: Other	1.5.1:Component Protection	Prevent or limit the consequences of failure of a component or structure whose failure would cause the impairment of a safety function.
	1.5.2: Plant Protection	Maintain, monitor, and control environmental conditions within the plant for the operation of safety systems.

High Level Function (Safety)	Plant Level Safety Function (PLSF)	Lower-Level Safety Function (LLSF)
	1.5.3: Operator Protection	Maintain, monitor, and control environmental conditions within the plant for the habitability of personnel necessary to allow performance of operations important to safety.
		Provide suitable means of protecting operators from the effects of direct radiation exposure.

Appendix C Use of Modelling Codes in US Transient and Accident Analysis

This appendix outlines the suite of computer programs applied in the transient analysis for the SMR-300 and explains how they are linked to demonstrate that the acceptance criteria set in sub-section 14.6.1 are satisfied. The analytical workflow proceeds through four main stages:

- **System thermal-hydraulics:** The transient or accident is first modelled with RELAP5-3D, which calculates RCS and MSS pressures, flows and temperatures and confirms compliance with the pressure, temperature, and LOCA limits
- **Core thermal-hydraulics:** Time-dependent boundary conditions from RELAP5-3D are transferred to COBRA-FLX, which evaluates the DNBR and FCM temperature. If COBRA-FLX predicts any fuel failure, then the resulting source term in the RCS is considered.
- **Containment response:** Mass and energy releases predicted by RELAP5-3D form the input to GOTHIC, which determines containment pressure and temperature histories and assesses passive containment-cooling performance. Where a containment bypass path exists, GOTHIC provides release data to the dose-assessment codes.
- **Core physics:** The CMS5 suite (CASMO5, CMSLINK5, SIMULATE5 and SIMULATE-3K) generates lattice data, steady-state power distributions and transient power histories for the thermal-hydraulic models.
- **Source term:** SCALE, with its TRITON and ORIGAMI modules, produces isotopic inventories and time-dependent release fractions for input to the dose codes.
- Atmospheric dispersion: ARCON calculates atmospheric dispersion factors for on-site and off-site locations.
- **Dose assessment:** RADTRAD determines Total Effective Dose Equivalent (TEDE) using the SCALE source term and ARCON dispersion factors, while MCNP adds direct-shine and sky-shine dose components to the MCR result.

The following sub-sections describe the computer codes for each of these steps.

System Thermal-Hydraulics Code

RELAP5-3D:

RELAP5-3D is the system thermal-hydraulics code used to predict RCS behaviour during AOOs and DBAs. Developed by Idaho National Laboratory for the US Department of Energy, it is an industry standard best estimate tool that models heat transfer, fluid flow, steam generation and ESFs operation. The code represents the coupled response of the core, primary loop, and secondary systems, and can simulate events such as ATWS, loss of off-site power, loss of feedwater and loss of flow. Control, turbine, condenser and feedwater components are included to the extent needed for accurate transient and accident modelling.

Core Thermal-Hydraulics Code

COBRA-FLX:

COBRA-FLX is the core thermal-hydraulics code used to calculate coolant conditions in every fuel assembly subchannel during steady state and transient operation. Derived from the COBRA-TF (Coolant Boiling in Rod Arrays - Two Fluid) family, the code was originally developed at Pacific Northwest Laboratory and has since been enhanced by several organisations for LWR analysis.

COBRA-FLX employs a two-fluid, three-field model that tracks liquid film, liquid droplets, and vapour, and it solves nine conservation equations in either sub-channel or full three-dimensional Cartesian form. The SMR-300 analysis uses COBRA-FLX to process boundary conditions from RELAP5-3D, determine DNBR and FCM, and identify any fuel damage that would affect the radiological source term.

Containment Analysis Code

GOTHIC:

GOTHIC is the containment thermal-hydraulics code used to predict pressure and temperature behaviour following high energy line breaks. Mass and energy release data from RELAP5-3D are imported, and GOTHIC solves the mass, momentum, and energy conservation equations for multicomponent, multiphase flow to calculate the containment response. The GOTHIC code also models the PCH to analyse the heat transfer capabilities and the time required to depressurise containment. Developed by Numerical Advisory Solutions, GOTHIC is widely applied for design, licensing and operating analysis of nuclear plant containments and is accepted for determining peak pressure and temperature in DBAs such as LOCAs and MSLBs inside the containment.

Core Physics Codes

The core-physics calculations for the SMR-300 use the CMS5 code suite (CASMO5, CMSLINK5, SIMULATE5 and SIMULATE-3K) developed by Studsvik Scandpower.

- CASMO5 is a lattice-physics code that models PWR fuel assemblies with 586-group neutron data and 18-group gamma data from the ENDF/B-VII library. Its principal output is a set of multigroup cross-sections, discontinuity factors and control rod worth data for core level simulations.
- CMSLINK5 converts the CASMO5 card-image files into a binary nuclear-data library for use by the nodal simulators. 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 is a three dimensional steady state nodal code that solves the multigroup diffusion (or optional simplified P3) equations with isotopic tracking for 50 nuclides. It produces the power distribution and reactivity feedback used by the thermal-hydraulics models.
- SIMULATE-3K extends SIMULATE5 to transient kinetics, coupling time-dependent neutron diffusion with detailed thermal-hydraulic feedback on the same spatial mesh. Transient power histories generated by SIMULATE-3K can be fed to RELAP5-3D for system analysis.

The CMS5 suite therefore provides consistent lattice data, steady-state core conditions and time-dependent power histories for the integrated transient and accident analysis

Source Term Code

SCALE with TRITON and ORIGAMI Modules:

For source terms calculations, SCALE simulation suite is used. SCALE is a multi-application code system with tools for reactor physics, criticality safety, radiation shielding, and spent fuel characterization for a range of nuclear systems. SCALE is developed and maintained by Oak Ridge National Laboratory.

The radiological consequences analyses use two of the SCALE code computational modules, TRITON, and ORIGAMI. TRITON is used as a control module for transport and depletion calculations which is also used to prepare problem and exposure-dependent multigroup cross-sections. TRITON utilizes these cross-sections to perform 2D deterministic transport calculations. TRITON then initiates ORIGAMI for depletion calculations. ORIGAMI performs ORIGEN burnup calculations for each of the specified power regions to obtain the spatial distribution of isotopes in the burned fuel. The process repeats until the simulation reaches its end time.

Atmospheric Dispersion Code

ARCON:

ARCON is used to calculate on-site and off-site atmospheric dispersion factors for DBAs. The code follows the methods endorsed in Regulatory Guide 1.194 [79] and 1.249 [80]. It retains the dispersion algorithms of ARCON96 while providing an updated user interface. ARCON implements a building wake model that treats ground level, building vent, elevated and diffuse release modes, and it processes hour-by-hour meteorological data with sector averaging to capture directional dependence. For longer transport distances the program applies a straight-line Gaussian diffusion model, producing atmospheric dispersion factors that are transferred to RADTRAD for dose assessment.

Dose Assessment Codes

RADTRAD:

RADTRAD calculates TEDE at the exclusion area boundary, low population zone outer boundary, main control room and technical support centre. Inputs are the release fractions and timing from SCALE source-term analysis and the atmospheric dispersion factors produced by ARCON. The code tracks radionuclide transport through building pathways, filters and ventilation streams, accounting for decay and daughter in growth as material moves between compartments and to the environment. Retention within each pathway is recorded so that the inventory at every receptor can be determined throughout the event.

MCNP:

MCNP supplements RADTRAD by evaluating direct-shine and sky-shine dose components to control room occupants. The Monte Carlo model represents the containment, shield walls, ventilation ducts and filter housings in full three-dimensional detail and transports photons (and, if required, neutrons or electrons) using continuous energy cross section data. The calculation includes effects such as incoherent and coherent scattering, fluorescent emission,

bremsstrahlung, and annihilation gamma rays, providing a fixed-source dose rate that is added to the airborne contribution from RADTRAD.