A Holtec International Company

Holtec Britain Ltd	HI-2240334
Sponsoring Company	**Document Reference**
0	30 September 2024
Revision No.	**Issue Date**
Report	Non-proprietary
Record Type	**Proprietary Classification**
ISO 9001	No
Quality Class	**Export Control Applicability**

Record Title:

PSR Part A Chapter 3 Claims, Arguments and Evidence

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

Table of Contents

List of Figures

3.1 INTRODUCTION

This chapter is an introduction to the Generic SMR-300 Claims, Argument, Evidence (CAE) process. It links the CAE process to the Safety, Security and Environmental Case (SSEC) (comprising the Preliminary Safety Report (PSR), Preliminary Environmental Report (PER) Generic Security Report (GSR) and Preliminary Safeguards Report (PSgR) and will be referenced throughout.

The SSEC and supporting documents have been prepared with the CAE concept in mind; the CAE approach is embedded in the way these documents are structured. Holtec SMR Master Document Submission List (MDSL) [1] contains all substantive documents related to the SSEC and is structured into a tiered hierarchy to reflect the controlling influence of CAE thinking, see PSR Part A Chapter 1 Introduction [2].

This chapter is informed by the Claims, Argument, Evidence Methodology for the Holtec SMR-300 [3] (which provides a literature review of CAE) and is concerned with describing and justifying the CAE approach used for the Generic SMR-300 SSEC.

3.1.1 Purpose

The primary purpose of a CAE approach is to capture the golden thread of a SSEC narrative demonstrating how plant and operational evidence is brought together to justify that a high-level or fundamental claim is true. The fundamental claim, referred to here as the *Fundamental Purpose,* of the Generic SMR-300 SSEC is:

> *"The Generic SMR-300 can be constructed, commissioned, operated, and decommissioned on a generic site in the UK to fulfil the future licensee's legal duties to be safe, secure and protect people and the environment."*

A subsidiary purpose and one of the main drivers for the development of CAE methodology has been a desire to make the complex safety, security (including safeguards) and environmental justification narratives in modern nuclear SSECs more comprehensible and visible.

At this Step 2 Generic Design Assessment (GDA) stage and in line with the expectations of a PSR, the claims architecture has been decomposed to a level which supports demonstration of the fundamental adequacy of the design and the SSEC. The *Claims* presented throughout the SSEC are supported by associated prose (*Arguments*) to connect the claims to the supporting documentation (*Evidence*), which at this early stage is often indicative or not fully mature. Where this is the case, gaps are acknowledged and methodologies and philosophies to address these gaps are presented.

The intent is for the overarching claims architecture to remain consistent for subsequent Tier 1 reports (e.g. to support construction); however, a fully developed CAE decomposition is not currently consistently provided across the SSEC and whilst the *Fundamental Purpose* covers all Structures, Systems and Components (SSCs) and operations in scope of GDA, the CAE route map is not comprehensive in that it has not been decomposed onto all elements and systems of the Generic SMR-300 design. Therefore, it is the intent of PSR Revision 0 to present a snapshot

of the CAE development at the start of Step 2 to provide confidence in its development. The CAE maturity is proportionate to this Step 2 of GDA and to the maturity of the Generic SMR-300 design and SSEC. The CAE route map will be expanded to be comprehensive across the plant design basis in scope of GDA for Revision 1 of the PSR.

This Chapter presents the high-level route map which links the *Claims* made throughout the SSEC to the *Fundamental Purpose*.

3.1.2 Definitions

For this GDA the following definitions are applied:

- **Claims:** A [true / false] statement or assertion with respect to the intent of the Generic SMR-300 SSEC, e.g., *"Risks from external hazards and their combinations are demonstrated to be tolerable and As Low As Reasonably Practicable (ALARP)."*
- **Sub-claims:** A logical decomposition of a "parent" *Claim* into as many levels as required, e.g., *"A comprehensive set of external hazards are identified and screened for assessment."*
- **Arguments:** The reasoning as to why a *Claim* is satisfied, i.e., the bridge between a *Claim* and *Evidence*, e.g., *"External hazards are identified and screened using UK and international relevant good practice and operational experience."*
- **Evidence:** Facts which establish the truth of the *Claim* according to the logic of the *Argument*, e.g., *"Generic Site Envelope Report".*

A master list of definitions and abbreviations relevant to all PSR Chapters can be found in PSR Part A Chapter 2 General Design Aspects and Site Characteristics [4].

3.1.3 Interfaces with other PSR Chapters

The CAE route map interfaces with all chapters in the PSR and wider SSEC. Of note, this chapter interfaces with PSR Part A Chapter 1 [2] which introduces the SSEC *Fundamental Purpose*. It also interfaces with the wider SSEC, namely the PER, the GSR and the PSgR.

This chapter will define the overall approach to CAE and describe the methodology being used. The high-level overarching *Claims* presented in this chapter cross-reference to the relevant SSEC chapters where further decomposition of the *Claims* is presented in the appendices of the respective chapter in the form of a table. Demonstration of *Claims* is made in the corresponding chapters.

3.1.4 Assumptions

No assumptions have been made with regards to development of the CAE methodology. Nevertheless, assumptions have been made throughout development of the SSEC that support demonstration of *Claims*. Definition of assumptions in the context of the Generic SMR-300 GDA is presented in PSR Part A Chapter 4 Lifecycle Management of Safety and Quality Assurance (MSQA) [5] Topic-specific assumptions are presented within the respective SSEC chapters and not discussed further here.

3.2 CODES, STANDARDS AND METHODOLOGY

3.2.1 Codes and Standards

Codes and standards related to CAE methodology are sparse and do not necessarily relate specifically to nuclear applications. Nevertheless, the following documentation has been reviewed as part of the development of the CAE route map and is considered to represent a mixture of Relevant Good Practice (RGP) and industry norm:

- Office for Nuclear Regulation (ONR):
  - Safety Assessment Principles (SAPs) for Nuclear Facilities [6].
  - Security Assessment Principles (SyAPs).
  - Technical Assessment Guide (TAG) 51 [7].
- International Atomic Energy Agency (IAEA):
  - Nuclear Energy Series No. NP-T-3.27 Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants [8].
- Best Available Techniques (BAT) for the Management of the Generation and Disposal of Radioactive Wastes Good Practice Guide [9].
- Industry practice:
  - Claims Arguments Evidence – Information, studies and research results on CAE [10].
  - Understanding, assessing and justifying I&C systems using Claims, Arguments and Evidence [11].
  - Using Structured Assurance Case Approach to Analyse Security and Reliability of Critical Infrastructures [12].
- Previous GDA submissions:
  - Rolls Royce SMR Step 1 PSR [13].
  - CGN UK HPR1000 Step 4 PCSR GDA Project Pre-Construction Safety Report, Chapter 1 [14].

Further New Nuclear Power Plants: generic Design Assessment Technical Guidance [15] has been reviewed to understand lessons learnt from previous GDAs with regards to topic area approach to CAE.

Whilst a CAE approach is not prescribed by the ONR, TAG 51 [7] states, *"CAE can be useful for for planning a safety case because it can describe the purpose and requirements of evidence that has yet to be produced".* To this end and recognising the maturity of the design and SSEC at this Revision 0 of the PSR, it is expected that gaps will be identified through the proposed CAE route map.

3.2.2 Principles

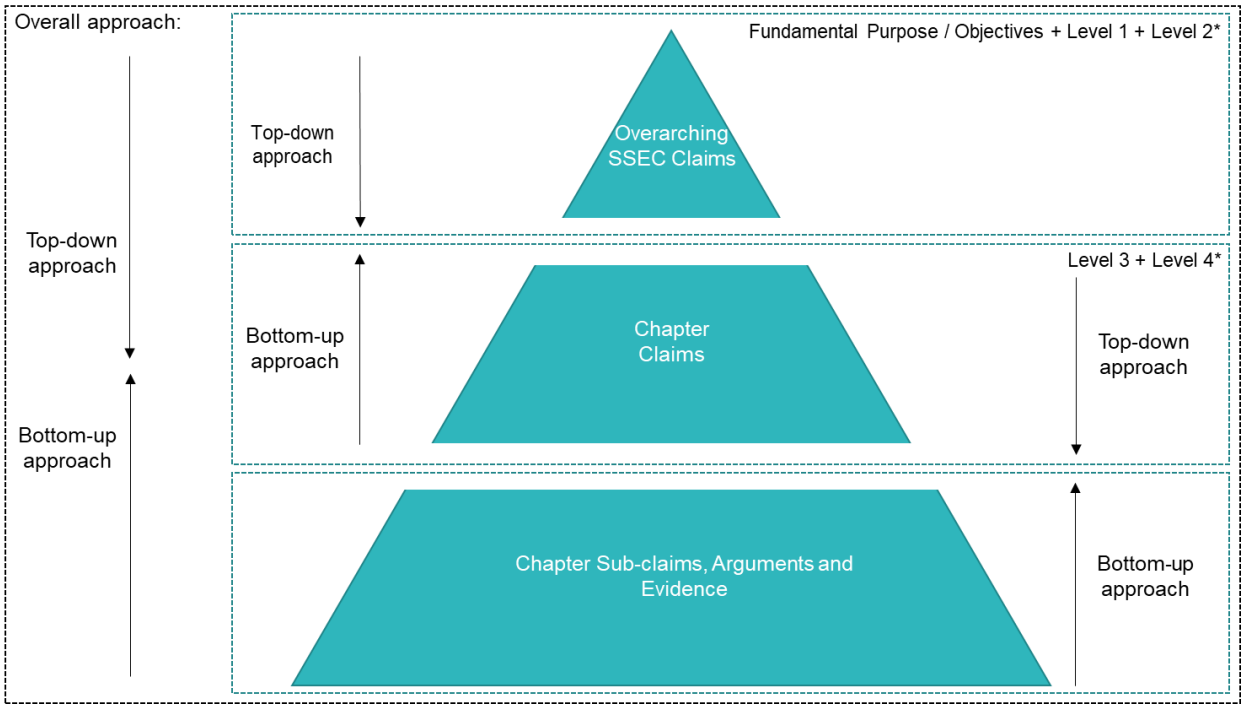
The following principles are applied to the development of the CAE route map specifically for the Generic SMR-300; their intent is to codify what constitutes an adequate CAE approach:

- **Principle 1**: *Claims*, *Arguments* and *Evidence* that are linked in a CAE tree form a golden thread. Each route through the tree from the highest-level *Claim* to the lowest level *Evidence* forms a separate partial golden thread.
- **Principle 2**: *Claims* are organised into a hierarchy from high level general statements about a plant quality to lower level increasingly specific statements about that quality.
    - The intent of high-level *Claims* is that they express the highest-level qualities expected by the public, regulators, etc.
    - The intent of low-level *Claims* is that they can be unambiguously linked to specific plant *Evidence* for support.
- **Principle 3**: An *Argument* should be used to demonstrate why a particular *Claim* decomposition has been used unless it is self-evident from the context of its use. Multiple *Arguments* should be avoided to support each *Claim* decomposition. If the decomposition is complex, then single *Arguments* should separate successive levels of sub-ordinate *Claims*. The following approaches suggested in industry practice [10] are used to decompose *Claims*:
    - Refine (into more specific and precise terminology)
    - Substitute (with different but equivalent claims)
    - Divide (into lower-level constituents)
    - Calculate (based on contributing values)
    - Terminate (with *Evidence*).
- **Principle 4**: It should be clear how an item of *Evidence* supports the *Claim* it reports to. *Evidence* should be related to relevant observable facts, or to analysis of factual data (see industry practice [10]).
- **Principle 5:** Where *Evidence* is not available to support a *Claim* at this step in GDA, a gap will be acknowledged (with appropriate justification of why claim maturity is acceptable) and methodologies and philosophies to address these gaps proposed. Further details on how such gaps are managed is provided in PSR Part A Chapter 4 [5].

3.2.3 Methodology

CAE implementation in nuclear safety cases is traditionally presented as a tree-like representation in a top-down bifurcating (or branching) structure, starting with a single high-level or *Fundamental Purpose* and working down to multiple examples of *Evidence* to support that single claim. This basic morphology has been adopted for the Generic SMR-300. Figure 1 presents the overall high-level approach to decomposition of the *Fundamental Purpose.*

A primary top-down approach from the *Fundamental Purpose* is applied to identify appropriate *Sub-claims* where evidence is readily producible and understood. A secondary bottom-up approach is applied whereby the extent of the claims are validated against any available evidence produced, or planned to be produced, during GDA when following established codes, standards or other RGP, noting that documentation exists for the SMR-160 design with some documents being updated for Generic SMR-300 during this GDA.



*Note: Claim "levels" are approximate with some variation throughout the CAE route map.

Figure 1: High-level CAE approach

3.2.4 Decomposition

The SSEC Fundamental Purpose can be achieved as a product of the PSR Objective, PER Objective, the GSR Objective and the PSgR Objective (detailed in PSR Part A Chapter 1 [2]). The PSR Objective together with the PER Objective, the GSR Objective and the PSgR Objective then diverge to the individual overarching *Claims*, which have *Sub-claims*, *Arguments* and *Evidence* trails in the respective chapters of each report that forms the SSEC. This is visualised in a simple hierarchy in Figure 2.

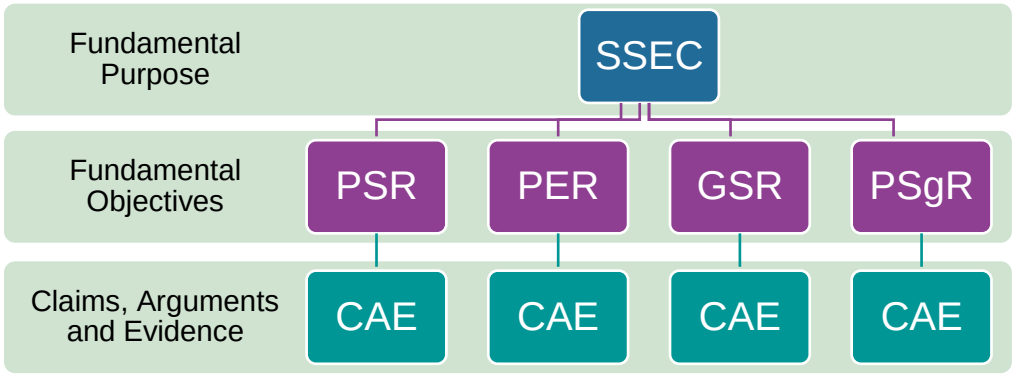


Figure 2: The Fundamental Purpose, Objective and CAE Hierarchy

Further decomposition of the *Fundamental Objectives* takes inspiration from systems development process lifecycle. A "V-model" has been used to derive claims throughout the SSEC development lifecycle. The V-model applies to all areas of the SSEC but it is illustrated here for nuclear safety.

As per Figure 3 the SSEC development process lifecycle has been divided into the following phases:

- **Safety Analysis:** This is where the safety requirements and system architecture are defined and detailed, and demonstration that the design reduces risk to a level which is tolerable and ALARP.
- **Design:** This is where the SSCs that form the design are developed to ensure they meet the relevant safety requirements and appropriate codes and standards adopted to ensure risks are reduced to ALARP.
- **Construct, install and commission:** This is where the overall design is verified and validated against the requirements placed on the systems / processes.
- **Operation:** Operational arrangements are developed to ensure the operation of the plant remains within with the identified the limits and conditions This includes ongoing maintenance of the as installed design so that substantiation of requirements remains verified and valid and safety performance is maintained.
- **Decommission:** This is where the operational activities are no longer undertaken and the plant is decommissioned. Consideration should be given in the preceding phases as to the requirements and subsequent design for future decommissioning.

This is broadly consistent with that presented in the Categorisation of Safety Functions and Classification of Structures, Systems and Components [16].

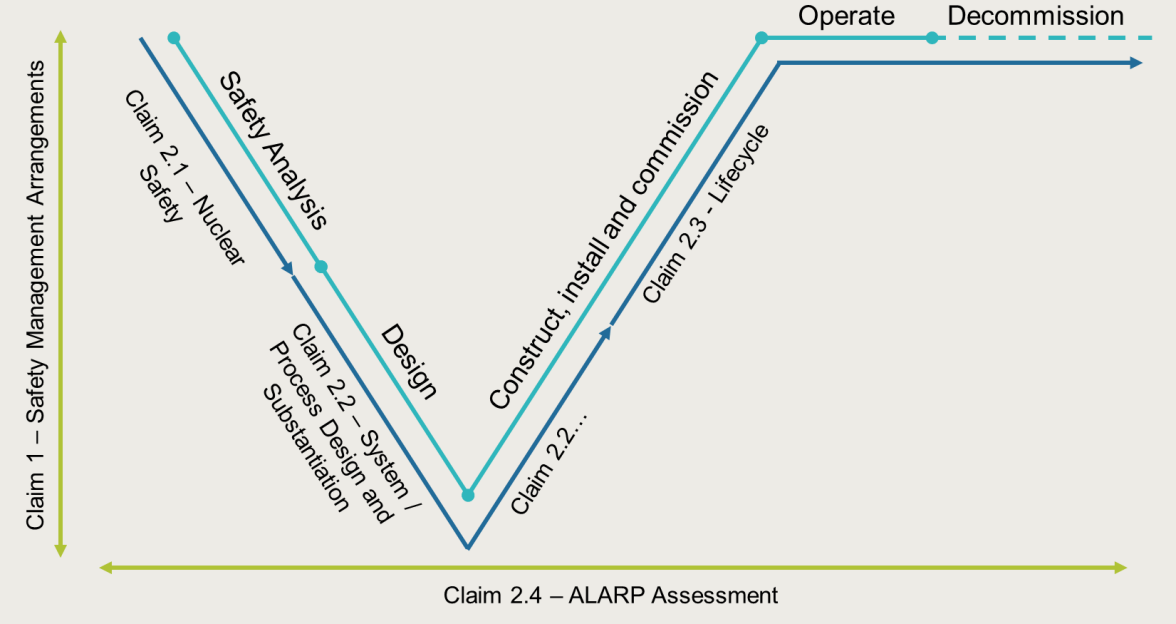


Figure 3: CAE "V-model"

3.2.5 Notation

A simple multilevel sequential numbering system has been applied. For example, *Claim 2.1* is the 1st claim under *Claim 2* and subsequently *Claim 2.1.3* is the 3rd claim under *Claim 2.1*. Note that as per Principle 3 (see Subchapter 3.2.2), *Claims* are decomposed as necessary into *Sub-claims*. As such, there is no significance as to the "level" of *Claim*, e.g., a level 3 *Claim* could in principle contain the same level of detail as a level 5 *Claim*. Numbering of Arguments and Evidence will be undertaken as the CAE route map is further expanded to be comprehensive in future safety reports beyond the scope of the GDA process.

3.3 CAE TRAIL

3.3.1 Overarching SSEC Claims

The resultant overarching SSEC Claim route map to relevant SSEC chapters is presented in Appendix A.

3.3.2 Chapter Claims

This chapter links out to the relevant SSEC chapters that satisfy the “Overarching SSEC Claims” and the *Fundamental Purpose*. Chapter *Claims* have been further decomposed (where necessary). Further rationale for decomposition to Chapter Claims in the Generic SMR-300 CAE Model [17] along with the entire CAE route map.

Each chapter defines how the high-level *Claims* are linked to that chapter so that the *Evidence* provided within can be argued to support these *Claims*. Some *Claims* will be supported entirely from *Evidence* within a single chapter, but many will require support from multiple chapters. Chapters have been structured to highlight the *Claims* narrative with cross-references to *Arguments* and *Evidence* explicitly included.

It is recognised that there are several elements / topics covered in the SSEC for Nuclear Power Plants (NPPs) that are cross-cutting in nature and therefore may result in chapter *Claims* under multiple areas of the “Overarching SSEC Claims”. Where this is the case, this has been clearly articulated within the main body of the chapter.

For example, it can be considered as a “science” or “safety analysis” discipline on the basis that exposure assessments are required to drive design requirements. Alternatively, radiological protection can be considered as an “engineering” or “systems-based” discipline with respect to shielding or containment design to meet requirements identified during the safety analysis. This is demonstrated in the CAE Model (see Appendix A) with Radiological Protection claims being presented under both Claim 2.1 (Nuclear Safety) and Claim 2.2 (System / Process Design and Substantiation).

Despite this, only *Claims* and *Sub-claims* (where necessary) have been presented for Revision 0 of this PSR. The CAE route map will be expanded to be comprehensive across the plant design basis in scope of GDA for Revision 1 of the PSR with the intention to provide *Arguments* and *Evidence* (where appropriate and available). As previously noted, *Claims* are decomposed as necessary into *Sub-claims*.

3.3.3 Mapping against Engineering Design Principles

An exercise will be undertaken during Step 2 of the GDA in which the Generic SMR-300 Engineering Design Principles (EDPs) will be mapped against the CAE route map, thereby demonstrating that they have been applied during the development of the design and SSEC. Currently, only outline EDPs have been presented in PSR Part A Chapter 2 [4].

3.3.4 Gaps Identified

As alluded to in TAG 51 [7] and mentioned previously, CAE is useful in identifying gaps in the SSEC and subsequently provide context as to the purpose and requirements of evidence that has yet to be produced. Where gaps are identified in specific chapters, forward actions and/or commitments will be raised in the respective chapters to address these. Forward Actions have been collated and are managed via the process described in PSR Chapter A4 [5].

3.4 SUMMARY, FORWARD ACTIONS & COMMITMENTS

This chapter of the SSEC introduces the *Claims*, *Arguments*, *Evidence* approach to be used for the Generic SMR-300 and presents the high-level route map that links the *Claims* throughout the SSEC to the *Fundamental Purpose*.

A systematic approach has been used for top-down decomposition of *Claims* which considers the entire development process lifecycle. The approach taken is consistent with UK nuclear industry RGP and draws on learning from previous GDA submissions. A secondary bottom-up approach has been used to ensure that the resulting *Claims* are comprehensive and reflect all aspects of an NPP.

Nevertheless, the CAE route map at this Revision 0 of the PSR only provides a snapshot of the development so far which is proportionate to the maturity of the Generic SMR-300 design and SSEC. The CAE route map will be expanded at Revision 1 to be comprehensive across the plant design basis in scope of GDA including Arguments as far as practicable for Chapter Claims / Subclaims and identification of Evidence where available.

3.5 REFERENCES

[1] Holtec Britain, “Holtec SMR Master Document Submission List for the Generic Design Assessment,” Revision 0, May 2024.

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

[3] Holtec Britain, “HI-2240670: Claims, Argument, Evidence Methodology for the Holtec SMR-300 Project,” Revision A, May 2024.

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

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

[6] ONR, “Safety Assessment Principles for Nuclear Facilities,” 2014 Edition, Rev. 1 (2020).

[7] ONR, “NS-TAST-GD-051: The Purpose, Scope, and Content of Safety Cases,” Issue 7.1, 2022.

[8] IAEA, “Nuclear Energy Series No. NP-T-3.27: Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants,” 2018.

[9] Nuclear Industry Safety Directors Forum, “Best Available Techniques (BAT) for the Management of the Generation and Disposal of Radioactive Wastes Good Practice Guide,” Issue 1, December 2010.

[10] CAE Framework, “Claims Arguments Evidence – Information, studies and research results on CAE,” CAE Framework, [Online]. Available: claimsargumentsevidence.org.

[11] S. Guerra, “Understanding, assessing and justifying I&C systems using Claims, Arguments and Evidence”.

[12] N. K. et al, “Using Structured Assurance Case Approach to Analyse Security and Reliability of Critical Infrastructures,” *Computer Safety, Reliability, and Security. Lecture Notes in Computer Science,* vol. 9338, 2014.

[13] RR SMR, “E3S Case PSR Chapter 1: Introduction,” 2023.

[14] General Nuclear System Ltd,, “UK HPR1000 GDA Project Pre-Construction Safety Report, Chapter 1,” Ver. 1.

[15] ONR, “ONR-GDA-GD-007: New Nuclear Power Plants: generic Design Assessment Technical Guidance,” Revision 0, May 2019.

[16] ONR, “NS-TAST-GD-094: Categorisation of Safety Functions and Classification of Structures, Systems and Components,” Revision 2, July 2019.

[17] Holtec Britain, “HI-2241013: CAE Model,” Revision 0, August 2024.

3.6 LIST OF APPENDICES

Appendix A Overarching SSEC Claims

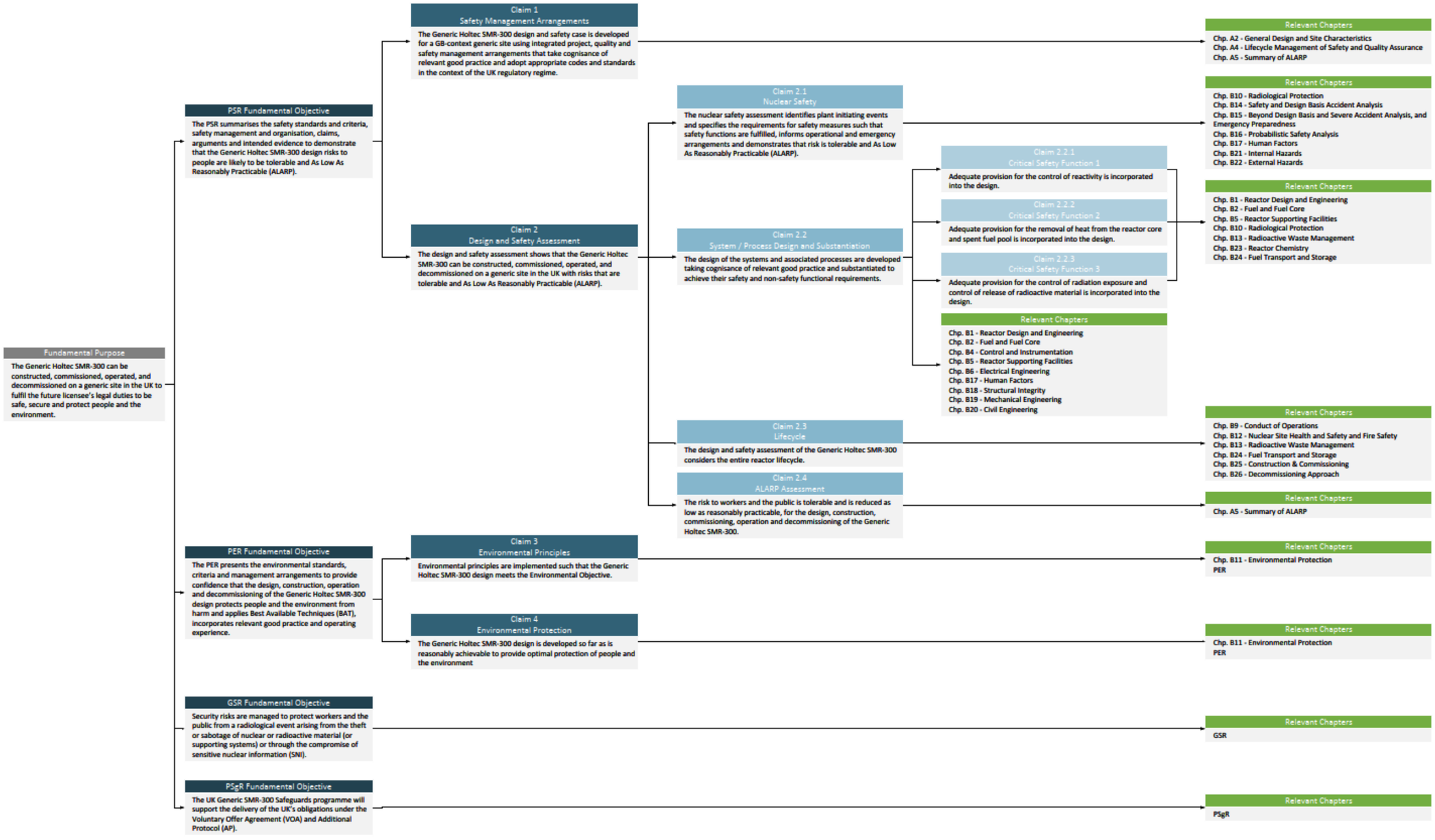


Figure 4: Generic SMR-300 Overarching SSEC Claim Route Map