SAFETY CASE STRUCTURE AND CONTENT

Introduction

A safety case is rarely a single document; it consists of the entirety of the body of evidence presented that demonstrates that the hazards presented by the Nuclear Power Plant (NPP) are adequately controlled and mitigated such that the risk to workers and the public is As Low As Reasonably Practicable (ALARP).

The Office for Nuclear Regulation *(ONR)* Safety Assessment Principles *(SAPs)* use the term 'safety case' to "*encompass the totality of documentation that is developed by the designer, licensee or duty-holder to demonstrate high standards of nuclear safety and radioactive waste management, and any subset of this documentation that is submitted to the ONR*". The SAPs also state that the process for producing the safety case should take into account the needs of end users and that "*A safety case is a logical and hierarchical set of documents that describes risk in terms of the hazards presented by the facility, site and the modes of operation, including potential faults and accidents, and those reasonably practicable measures that need to be implemented to prevent or minimise harm. It takes account of experience from the past, is written in the present, and sets expectations and guidance for the processes that should operate in the future if the hazards are to be controlled successfully. The safety case clearly sets out the trail from safety claims through arguments to evidence*". The ONR's expectations for safety cases is set out in NS-TAST-GD-051.

Safety Case Lifecycle

Development of the NPP design and safety case should be an integrated and iterative process, ensuring lessons are learned and applied before moving to the next stage. For new projects, documents should be completed in step with the design. However, to ensure that the engineering proceeds in a manner that provides confidence that the safety requirements will be met, it is important that a satisfactory safety case is achieved before certain permission hold points (i.e. design, construction, commissioning, operation, and decommissioning). Some areas will need to progress at an early stage (e.g. human factors) to influence the design. It is important that the whole lifecycle of the facility is taken into consideration in all stages; for example decommissioning feasibility should be taken into account during the design stage. The major stages of the NPP lifecycle are shown in Figure 1.

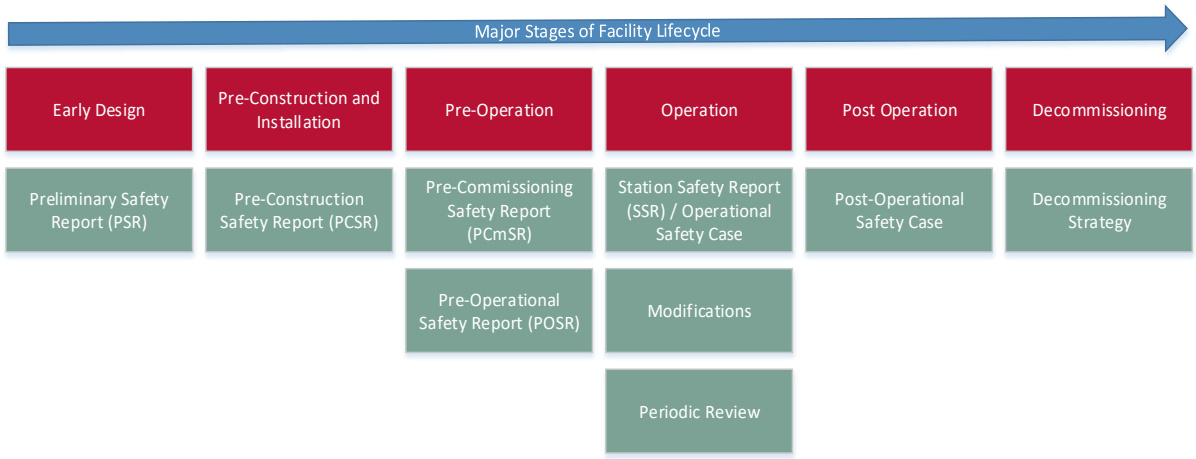

Figure 1: Major Stages of Facility Lifecycle.

Safety Case Structure

There is no definitive guidance on the NPP safety case structure as this will be dictated by factors such as:

- Application type.
- Complexity.
- Organisation structure / requirements.
- Age of the safety case.

At the time of writing the two most developed Nuclear New Build projects in the UK are the construction of a UK European Pressurised Reactor *(EPR)* plant at Hinkley Point C by New Nuclear Build *(NNB)* GenCo and the proposed construction of a UK Advanced Boiling Water Reactor *(ABWR)* at Wylfa in Anglesey by Horizon Nuclear Power *(HNP)*, noting that the latter project has recently been put on hold. Both projects were subjected to the ONR Generic Design Assessment *(GDA)* process (ONR-GDA-GD-006), enabling safety, security and environmental aspects of new UK NPP's to be assessed before applications are made to build at a particular site.

Modern safety cases are generally based around a pyramidal structure, such as that shown in Figure 2, with the safety report (which many people refer to incorrectly as the safety case) presenting the claims and high-level arguments, with appropriate signposts to the detailed arguments and evidence presented in the supporting analysis and design substantiation. The level of detail increases down the pyramid from the top level safety report to the low level technical calculations and analysis reports. The aim is to avoid unnecessary updates to the safety report(s) (which have a significant process burden) as a result of minor changes to design details and analysis that do not directly impact on the Claims Arguments Evidence *(CAE)* or basis of the safety case. This layered approach to structuring the safety case is considered current best practice and has been implemented in modifications and updates to safety cases for existing generation and as the basis of new build safety cases being produced for UK EPR and UK ABWR.

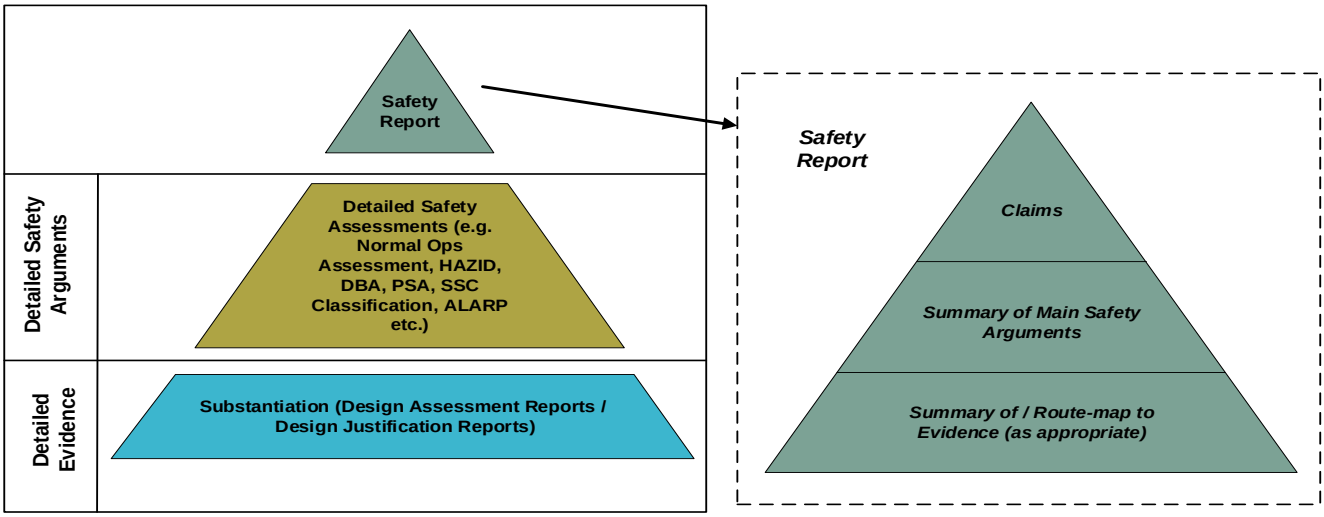

Figure 2: Modern Safety Case Structure.

For their GDA Pre-Construction Safety Report *(PCSR)* submissions both NNB GenCo and HNP have adopted a safety case chapter structure similar to that shown in Figure 3.

Figure 3: Safety Case Chapter Structure.

The early development of NPP design and safety case structure can be mapped through a number of research topics. Topics of particular importance to the early development of the safety case include the following: GDA Roadmap, Fundamental Nuclear Safety Principles, Fault Schedule, Engineering Schedule, Safety Case Data Set and Safety Case Process Diagram.

The detailed structure and presentation of the NPP suite of documentation includes, but is not limited to, detailed guidance that underpins the safety case, system descriptions and fault assessments that cannot be explicitly defined. The main point of note is that the structure and content of all documentation should provide a 'golden thread' from the safety reports through to detailed fault assessment and supporting evidence.

Additional Information & Guidance

- ONR, NS-TAST-GD-051, The Purpose, Scope, and Content of Safety Cases, December 2019.
- ONR, ONR-GDA-GD-006, New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties, October 2019.
- ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition Revision 1 (January 2020)