CLAIMS, ARGUMENTS AND EVIDENCE

Introduction

In order to build and operate a Nuclear Power Plant (*NPP*) in the UK, the operator is required to obtain licences and permissions from a number of different bodies. These bodies include planning authorities, environmental regulators, and, importantly in the context of a nuclear safety case, the Office for Nuclear Regulation *(ONR)* which is responsible for granting a nuclear site licence. This is a legal document, issued for the full life cycle of the facility.

While the safety case is a mandatory regulatory requirement, its primary purpose is to enable the operator of a nuclear facility or process to satisfy themselves that:

- They have considered all the potential risks associated with the activities on their site;
- They have implemented suitable and sufficient measures to mitigate the risk of radiological consequences to their staff and the public to a level that is As Low As Reasonably Practicable *(ALARP)*.

The safety case is an operational document, or suite of documents, and is the tool for communicating to operators and other stakeholders how the safety of the plant is maintained during normal operations and foreseeable fault conditions.

Historically, safety cases were presented as unstructured prose. This approach made the safety arguments difficult to follow, especially given the volume of documentation that makes up a site safety case. The progression of safety case principles and guidance, such as those provided in the ONR Safety Assessment Principles (SAPs), has meant that a structured safety case demonstrates compliance with regulatory expectations, and communicates the safety case to all other stakeholders more easily. The application of a structured safety case improves the link between the safety Claims, Arguments and Evidence (CAE).

Purpose

The purpose of CAE is to improve the clarity and accessibility of the safety case, and there are many different ways in which it can be applied. For example, at a very high level where the claims and arguments relate directly to how the Nuclear Safety Principles (*NSPs*) will be delivered and the fundamental safety functions ensured, or all the way down to claims on individual systems, sub-systems or components. The appropriate level of usage varies by application depending on the type and complexity of the plant or system being considered. CAE is a structured approach which aids the visibility, review and assessment of safety case documentation. The key terms can be defined as follows.

- **Claim**: A high-level assertion or statement.
- **Argument**: Supports the claim and provides the link to the supporting evidence. It also allows the supporting justification to be broken up to aid visibility.
- **Evidence**: Facts and judgements that support the applicable argument(s).

In order for the CAE structure to be effective the claims must be set at an appropriate level which then allows appropriate arguments and evidence to be developed.

UK Regulatory Context

The ONR do not prescribe to licensees how they should produce their safety cases or what they should look like. It is the responsibility of individual licensees to develop their own safety management system detailing the processes and procedures through which they will ensure nuclear safety on their site is maintained. The ONR review and agree these arrangements and regulate licensees against them. It is understood that for the new nuclear plant, particularly in the area of Control and Instrumentation (*C&I*), the ONR is keen for licensees to develop CAE structures that show how the design meets the fundamental principles against which safety will be judged, e.g. ONR SAPs and associated Technical Assessment Guides (*TAGs*).

Structure

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

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

Modern safety cases are generally based around a pyramidal structure, such as that shown in Figure 1, 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 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.

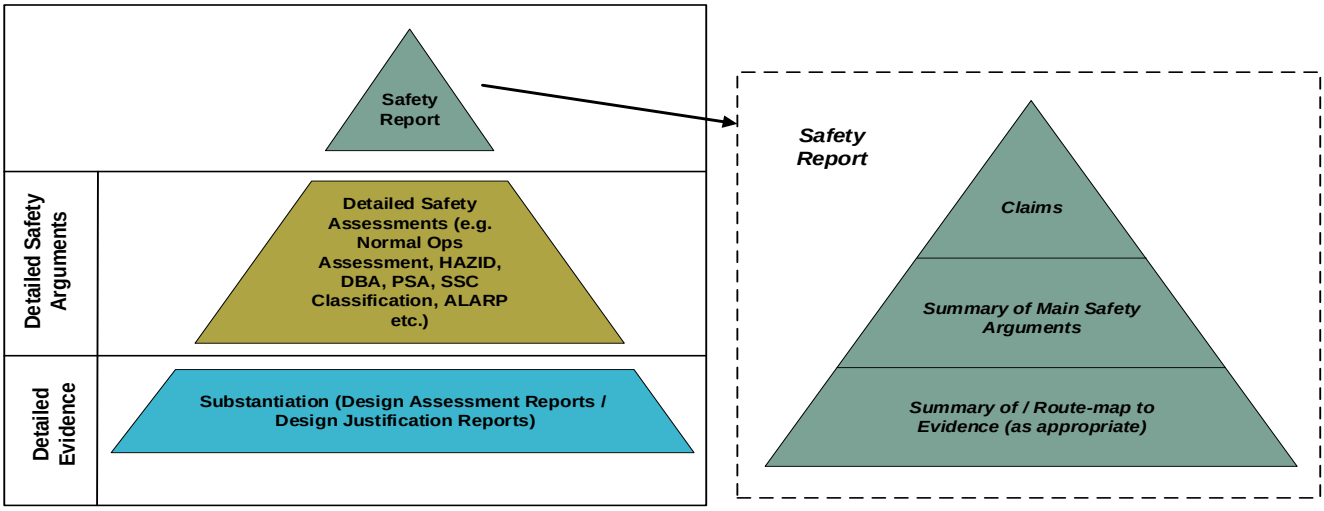

Figure 1: Modern Safety Case Structure.

Claims, Arguments and Evidence

All safety cases seek to demonstrate a high-level claim that 'the proposed activities are safe', and justify this claim by providing supporting information. Safety cases have always been based on CAE even if this has tended to be implicit within the text of the safety case. More recently there has been a move towards explicitly structuring the safety case around a set of defined claims as to why the risk associated with the plant or process in question is ALARP, supported by relevant arguments and evidence to substantiate the claims. Benefits of the CAE approach vary depending on the application being considered, with CAE often better suited to applications like C&I systems rather than claims on human action. However, CAE can be used to provide clear and auditable links from what the plant, processes and people claim to do to maintain safety and why, down to supporting analysis and other evidence that demonstrates the relevant requirements can be met, with the required reliability and integrity. A high-level CAE structure example is shown in Figure 2.

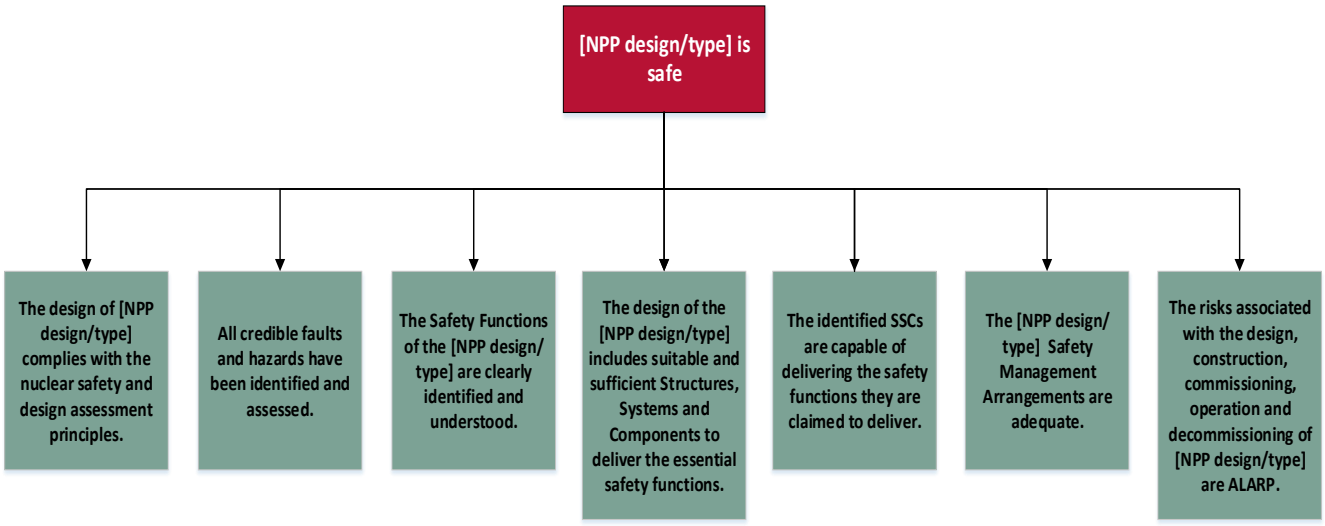

Figure 2: High-Level CAE Structure.

The progression of safety case principles and guidance has meant that a structured safety case demonstrates compliance with regulatory expectations, and communicates the safety case to stakeholders more easily.

The UK Advanced Boiling Water Reactor *(ABWR)* Generic Design Assessment *(GDA)* Pre-Construction Safety Report *(PCSR)*, and follow-on site-specific PCSR, adopted a CAE structure for the systems areas. While the PCSR for the UK European Pressurised Reactor (*EPR*) was not produced in an explicit CAE format, the licensee has recognised the potential benefits of CAE and has considered the feasibility of implementing CAE in the Pre-Commissioning Safety Report (*PCmSR*) or the operational safety case for Hinkley Point C. This may be influenced by the fact that even though the ONR is not prescriptive about the form or structure of the safety case provided for assessment, it is noted in GDA guidance that the CAE approach is commonly used to structure the safety case in the nuclear industry and elsewhere. The ONR's expectations for safety cases is set out in NS-TAST-GD-051 whilst ONR-GDA-GD-006 provides details on the GDA process.

The relationships between the head document, system sub-chapters and fault schedule are shown in **Figure 3** highlighting the interrelatedness of key safety case documents. This high level structure could be applied to support the development of a CAE structure.

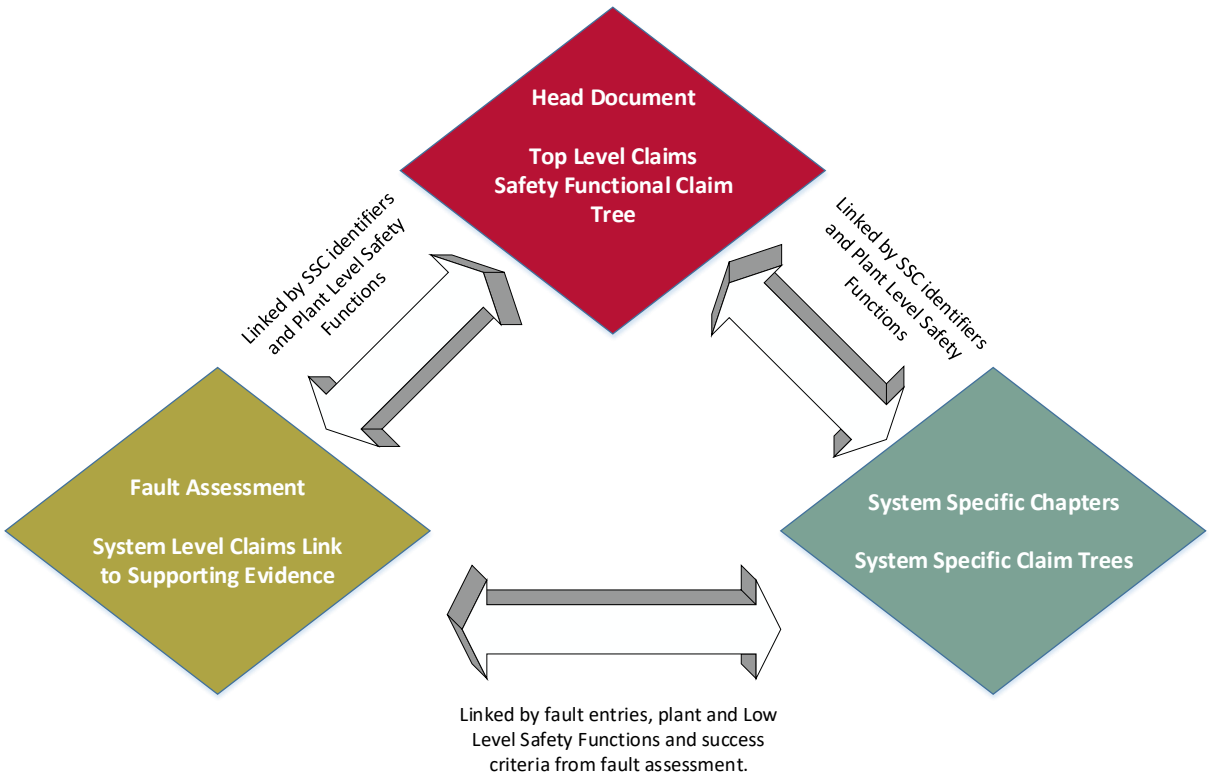

Figure 3: Safety Case Document Relationships.

Benefits and Pitfalls

It is recognised that adoption of a more formal CAE approach does generally make new safety cases easier to understand at the proposal stage, and provides a more effective way for those not directly involved in the production of the safety case to pick up and assimilate the information at a later date. It is therefore considered that CAE is generally accepted as representing good practice in safety case production within the UK nuclear industry. However, while CAE can help with the visibility and transparency of the safety case, there are limitations and potential pitfalls associated with its application as discussed in Table 1.

CAE Benefits	CAE Pitfalls
Easy to follow The CAE structure providing a simple, structured representation of the safety case.	**Claims may be defined at the wrong level** If there is a one to one relationship between claims and arguments it is likely that the claims have been specified at too low a level. Similarly if there are only one or two claims that each have a significant number of overlapping arguments then they are likely at too high a level.

CAE Benefits	CAE Pitfalls
Easier to assess, agree and implement The clarity of the CAE structure makes it more straightforward to assess whether the arguments and evidence are sufficient to support the claim, and also confirm that the actual configuration of the plant reflects the claims made in the safety case.	**Over emphasis on 'word-smithing'** The key to good CAE is clear and concise claims and arguments. It should normally be possible to define a claim or argument in a single sentence.
Structures thinking The CAE approach encourages individuals to consider whether suitable and sufficient arguments and evidence can be provided before making a claim. This reduces the potential for claims being made that cannot be substantiated.	**Claims are too narrow** This can result in too many claims (see above) and may also result in gaps in the safety case.
Sets the high-level strategy for the safety case Identifying the claims and preliminary supporting arguments and evidence early in the development process defines the structure and strategy of the safety case.	**Claims are too wide** If a claim is overly broad or generic then it becomes difficult to determine whether the supporting arguments and evidence are suitable and sufficient.
Enables required evidence to be scoped Early definition of claims and arguments allows the required evidence to be identified and scoped early in the project. As a lot of evidence takes the form of detailed assessment and analysis the lead time to produce it can be significant and therefore early scoping is essential.	**"Reinventing the wheel"** It can be tempting to try and do things differently, resulting in the requirement to generate new arguments and supporting evidence. Care needs to be taken when re-using existing CAE as it may be difficult to identify any subtle differences between the applications and gaps in the CAE.

Table 1: CAE Benefits and Pitfalls

Presentation of CAE

CAE can be presented in a number of forms including diagrammatically, tabulated or simply as structured prose. The presentation of the CAE structure can be developed top-down from the high-level CAE structure shown above, and will ultimately cascade down to the system-specific information. In any case with the modern safety case approach, whereby functional requirements including faults and hazards are specified and clearly identified, the presentation of all claims made on systems, sub-systems and components are more easily identified. The safety case is more structured in the specification of requirements from the fault schedule through to system-specific documentation.

Modern safety cases benefit from improved identification of functional requirements, but are also challenged by the complexity of design and volume of information. Structuring the safety case in CAE may provide a solution to managing the complexity of the safety case, depending on whether it is fully or partially implemented.

Additional Information & Guidance

- ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition Revision 1 (January 2020)
- 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.