# ATTRIBUTES OF A GOOD QUALITY SAFETY CASE

## Background

Before presenting any guidance, tools or techniques that aid the development of good, high quality nuclear safety cases, it is necessary to have a common understanding of what this constitutes. There are a number of existing sources of guidance that discuss the attributes of good quality safety cases. This guidance has been reviewed and consolidated to provide a list of attributes to be used as the basis of the safety case toolkit.

These attributes are presented and discussed in the following sections, with links to relevant aspects of the reviewed material. The guidance, tools and techniques presented in the rest the toolkit is intended to aid organisations in the delivery of high quality safety documentation that satisfies these attributes.

## Key Sources of Information

Various sources of guidance and Operating Experience (*OPEX*) are available which provide examples of both good and bad nuclear safety case practices. These include but are not limited to the following:

- NS-TAST-GD-051 – this presents the guidance for Office for Nuclear Regulation (*ONR*) inspectors on expectations with regard to the structure and content of safety cases for UK nuclear sites produced by the relevant UK licensees.
- Safety Directors Forum – this body consists of nuclear safety leaders from UK licensees. Its purpose is to provide cross-industry guidance on nuclear safety challenges, including safety case production. Right First Time Safety Cases: How to write a useable safety case proposes six principles on which the safety case should be based. These are: **S**uccinct, **H**ome grown, **A**ssessable, **P**roportionate, **E**asy to understand and **D**ocument-lite. 'Right First Time' Safety Cases fundamentally also depend on good **P**reparation (PSHAPED).
- UK Licensee Nuclear Safety Principles – the majority of UK licensees have developed their own set(s) of nuclear safety case principles for application to safety cases on their sites. These capture the intent of the high level principles outlined in international guidance and the ONR Safety Assessment Principles (*SAPs*). The ONR uses its SAPs to assess the safety at existing or proposed nuclear facilities
- UK Licensee Safety Case Guidance and Training – individual UK licensees have their own guidance on the application of their safety management system processes and procedures to produce safety cases of an acceptable quality. To ensure that the processes and guidance are consistently followed and applied, UK licensees typically require that all safety case practitioners – both staff and external consultants – complete approved training.
- International Atomic Energy Agency (*IAEA*) Safety Series – the IAEA has developed and published guidance on a variety of nuclear safety related topics. The guidance produced by the IAEA is used by national regulators and individual UK licensees in the development of their processes and guidance.

- Accident investigations, for example The Nimrod Review led by the Rt Hon. Lord Justice Haddon-Cave and the Ladbroke Grove Rail Inquiry led by Lord Cullen, have identified deficiencies in the production and management of the associated safety documentation.

## Attributes

The following sections present aspirational attributes of a good quality safety case. It is recognised that there is some overlap and potential conflict between some of these attributes. However, consideration of these attributes during the safety case development process will help to improve the quality of safety cases.

### Accessible

To be useful, the safety case needs to be accessible by all relevant users and stakeholders, including external organisations such as the regulator. Production or storage of the safety case in novel or proprietary software that requires specialist UK licences or training should be avoided, as should the unnecessary inclusion of sensitive information resulting in an enhanced security classification.

The safety case should be produced, stored, presented and maintained in a format that makes it readily accessible to all relevant stakeholders. This includes:

- Authors, reviewers and verifiers.
- Internal stakeholders. There are a variety of internal stakeholders that will require access to some or all of the safety case. For example:
    - Operators and Maintainers will require access to the outputs of the safety case such as operation and maintenance procedures, technical specifications and the maintenance schedule. Depending on the individual requirement, this may require both read and write access.
    - Independent Nuclear Safety Assessment. Although not directly involved in the production process, personnel in internal regulatory functions will need access to the full suite of safety case documentation.
- External stakeholders. Safety cases are often produced, modified or independently reviewed by external consultants, and may also be submitted to the regulator. The safety case should therefore be in a form that is easily transmittable outside the organisation of origin. For example, common file types, such as those associated with Microsoft Office programs should be used where practicable. This does not preclude the use of proprietary software to manage the safety case internally, but in this case the output should be easily transferable into a common format.

The requirement for accessibility needs to be balanced with the need for robust configuration control.

### Affordable

The balance between cost and benefit is inherent in the As Low as Reasonably Practicable (*ALARP*) principle that is the cornerstone of the UK Regulatory framework and safety case development.

While justification of increases in risk for commercial gain – so-called reverse ALARP – is not generally acceptable, commercial impacts need to be considered in the decision-making process. The cost of

producing the safety case is a commercial attribute which should be balanced against the safety benefits accruing from the safety case.

### Auditable

Safety cases inevitably involve decisions, judgements, and assumptions. OPEX has shown that if the basis of these is not adequately captured and accessible, maintenance or future modification of the safety case can be much more difficult and costly than necessary.

For example, the calculations underpinning key design parameters and performance requirements are not always directly referenced within safety case deliverables, or can be easily located using references from the safety case. Even if such calculations can be found, unless the assumptions and uncertainties are clearly identified, future modifications can be difficult.

Suitably Qualified and Experienced Persons (*SQEP*) judgements present another potential challenge. Judgements by key individuals based on their knowledge and experience are often fundamental to the safety case, however, given the specialist nature of these judgements it can be difficult to adequately capture and communicate their basis in the safety case so they can be fully understood in the future, including any potential restrictions and limitations, by others.

Adequately capturing the basis of the decisions, judgements and assumptions that underpin the safety case is therefore an essential aspect of high quality safety cases.

### Clear, Consistent and Intelligible

All of the identified sources of good practice agree that safety cases should be produced in clear, intelligible language that can be easily understood by all stakeholders. Obscure or overly complicated language should be avoided as they can make the safety case difficult to understand, resulting in it being misinterpreted or ignored.

The ability to convey complex technical arguments in simple language is one of the key skills of a safety case author. The safety case is a not vehicle to demonstrate the author's intelligence; it should communicate the necessary information in as simple and unambiguous a way as possible.

### Concise, Succinct and Proportionate

There is a common perception that safety cases are large, cumbersome and unwieldy, and that their quality is measured in volume. In the Nimrod accident investigation Haddon-Cave observed that safety cases and reports are often too long, bureaucratic, repetitive, and comprise impenetrable detail and documentation.

It is unavoidable that the safety case for something as complex as a nuclear reactor will consist of a significant amount of supporting text, drawings, diagrams, and calculations. To be useful a safety case should communicate the risks associated with the plant or process under consideration as simply and succinctly as possible, and detail how these are adequately mitigated.

The size and complexity of the safety case is dependent on a number of factors, including:

- The complexity of the process or application.

- The novelty.
- The risk.

Good quality safety cases successfully communicate complex technical problems clearly and concisely, and identify and focus on the areas of real risk and how these will be managed. There will always be time, budget and resource pressures so intelligent and proportionate application of resource to the areas of greatest risk, novelty and complexity is essential to maximise the benefit from the safety case.

The faults with the most significant consequences do not necessarily require the greatest coverage in the safety case, as these may already be well understood and there may be existing industry best practice for dealing with them.

## Demonstrably Complete

Safety cases tend to focus on demonstrating that suitable and sufficient measures are in place to deal with identified faults and hazards, and the importance of demonstrating completeness can sometimes be lost.

Providing confidence that all reasonably foreseeable deviations from safe operation are identified and have been assessed and suitable structures, systems and components implemented where necessary is one of the key aims of the safety case.

This should include links to the engineering substantiation of the chosen design solution, as well as evidence of the consideration of alternative designs or approaches. Any areas of uncertainty should also be identified.

The safety case should present a comprehensive assessment of the risks associated with the plant, process or activity being considered, and demonstrate that suitable and sufficient measures are in place to adequately manage them during the period for which it is to remain valid. This should include links to the engineering substantiation of the chosen design solution as well as evidence of the consideration of alternative designs or approaches. Any areas of uncertainty should also be identified.

## Evidential

Claims and arguments presented in the safety case should be supported by appropriate evidence in the form of assessment, analyses, design information and other data to underpin any:

- Assumptions, including sensitivity.
- Claims on integrity or performance of engineered features supported by arguments and evidence.
- Justification of the relevance of any claimed OPEX.
- Verification and validation of codes and methodologies used in the substantiation.

The requirement to provide appropriate evidence may seem obvious but historically there have been examples of safety case judgements being made in the absence of supporting evidence, on the basis that evidence would be subsequently produced. When this did not happen, a gap was subsequently left in the safety case. In some instances the fact that the evidence was not pre-existing was not clearly communicated in the original safety case, and subsequent safety cases assumed that the judgment had been suitably underpinned, thus perpetuating the problem.

## Living and Maintainable

The safety case reports a point in time in the lifecycle of a plant or process. However, the configuration of plant may evolve and develop as a result of ageing or degradation mechanisms, modifications, OPEX etc., and the understanding of the associated risks, or standards and expectations will rarely remain unchanged during the lifetime of the plant or safety case. The safety case must therefore be a living document, or set of documents, which continues to reflect the plant configuration throughout all stages of the plant lifecycle. It must not be 'shelf-ware' that is produced and then forgotten about.

To enable the safety case to be maintained and ensure that it remains representative of the actual plant state at all stages in the plant lifecycle, it needs to be produced and stored in a way that allows it to be easily updated and maintained with adequate processes in place to control any changes or modifications.

Current practice is generally to use a document control system to control the configuration of the suite of documentation that constitutes the safety case, in combination with a robust modification control process. While the safety case documentation, and configuration management systems and processes are generally software based, the safety case documents are generally 'dumb' in that they are standalone documents and not fully integrated with the design information supporting analysis and evidence.

Electronic safety cases that utilise software solutions to fully integrate the safety case with the design and substantiation, thereby offering greater flexibility and ease of update and maintenance, have been successfully implemented in other industries and are considered to represent the future of safety case production in the nuclear industry.

The options for implementing the safety case electronically in the nuclear industry have been considered separately in the guidance titled Electronic Safety Cases.

## Representative

It is a common criticism that safety cases are produced by safety case specialists without hands-on experience of the plant or process in question, being based solely on other documentation.

It is essential that the safety case reflects the actual plant and processes and is not just based on a paper analysis e.g. the actual plant configuration, state and dimensions should be physically confirmed where possible and not read from other documentation. It also essential that SQEPs with appropriate plant knowledge, such as operators and maintenance staff, are involved in the development and review of the safety case to ensure that it reflects the reality of the plant and operations.

For new builds, unless there is a mock-up, training facility or similar plant already operating, it will not be possible to physically visit the plant. However, modern tools such as virtual reality enable virtual walk-downs to be conducted prior to any construction work being commenced, and it is strongly recommended that such tools are utilised in the design of new plant to ensure that the safety case team fully understand the plant layout and interactions. These tools are also extremely useful for educating other stakeholders such as regulators.

### Valid

Similar to the demonstration of completeness discussed above, restrictions and limitations on the validity of the safety case are often poorly communicated.

There will likely be a number of limitations on the validity of a particular safety case, and these must clearly understood so that it can be identified when any of them are close to being breached or already have been.

Limitations on validity may include:

- Time.
- Plant availability.
- Material types / quantities.
- Staffing levels.

## Additional Information & Guidance

- ONR, NS-TAST-GD-051, The Purpose, Scope, and Content of Safety Cases, December 2019.
- UK Nuclear Safety Case Forum Guide, Right First Time Safety Cases: How to write a useable safety case, March 2014.
- ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition.
- The Nimrod Review: An Independent Review into the Broader Issues Surrounding the Loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006 by Charles Haddon-Cave QC, October 2009.
- Ladbroke Grove Rail Inquiry by the Rt Hon Lord Cullen PC, 2001.