|  |
| --- |
| ONR GUIDE |
| **THE PURPOSE, SCOPE, AND CONTENT OF SAFETY CASES** |
| **Document Type:** | Nuclear Safety Technical Assessment Guide |
| **Unique Document ID and Revision No:** | NS-TAST-GD-051 Issue 7.1 |
| **Date Issued:** | December 2022 | **Review Date:** | December 2024 |
| **Prepared by:** |  | Inspector (Nuclear Safety) |
| **Approved by:** |  | Professional Lead |
| **Record Reference:** | CM9 Folder 1.9.3.996. (2020/284313) |
| **Revision commentary:** | Rev 6: This revision includes:* general restructuring/reformatting to provide greater clarity
* review against modern relevant good practice
* visual aids summarising typical content and structure, and lifecycle of a safety case
* expanded explanation of claims, arguments and evidence
* inclusion of reference to defence in depth in the safety case

Rev 7: Updated Review PeriodIssue: 7.1: Minor update to remove extant URLs from the document to mitigate potential configuration control issues arising because of changes to third-party web domains. |

**TABLE OF CONTENTS**

[1. INTRODUCTION 2](#_Toc24441119)

[2. PURPOSE AND SCOPE (Of THIS GUIDE) 2](#_Toc24441120)

[3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION 3](#_Toc24441121)

[4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED 4](#_Toc24441122)

[5. ADVICE TO INSPECTORS 5](#_Toc24441123)

[6. REFERENCES 21](#_Toc24441124)

[7. GLOSSARY AND ABBREVIATIONS 22](#_Toc24441125)

[APPENDIX 1: COMMON PROBLEMS WITH SAFETY CASES 24](#_Toc24441126)

[APPENDIX 2: NIMROD REVIEW - SAFETY CASE SHORTCOMINGS & TRAPS 27](#_Toc24441127)

[APPENDIX 3: GUIDANCE ON THE RELATIONSHIP BETWEEN STAGES OF A NUCLEAR FACILITY LIFE-CYCLE AND THE ASSOCIATED SAFETY CASES 30](#_Toc24441128)

[APPENDIX 4. CLAIMS ARGUMENTS EVIDENCE STRUCTURES WITHIN THE SAFETY CASE 37](#_Toc24441129)

1. INTRODUCTION

ONR has established its Safety Assessment Principles (SAPs) [1] for use by ONR inspectors when assessing safety cases for nuclear facilities/activities. The principles presented in the SAPs are supported by a suite of guides to further assist ONR’s inspectors in their technical assessment work in support of making regulatory judgements and decisions.

This technical assessment guide (TAG) for ONR inspectors is on the purpose, scope and content of safety cases. The SAPs use the term ‘safety case’ “*to encompass the totality of the documentation developed by a 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 Office for Nuclear Regulation (ONR)*”. For the purposes of this guidance, the term dutyholder shall be used to refer to any organisation with responsibility for a safety case.

The previous update of this TAG ensured compatibility with the 2014 major revision of the SAPs. This revision provides greater clarity of guidance to inspectors, and includes:

* general restructuring/reformatting to provide greater clarity and alignment with the SAPs;
* a review against current relevant good practice;
* use of visual aids summarising typical content and structure and lifecycle of a safety case;
* expanded explanation of expectations with regard to claims, arguments and evidence, with an example approach and structure given in a new appendix; and
* reference to implementation of the defence in depth concept in safety cases.
1. PURPOSE AND SCOPE (Of THIS GUIDE)

The purpose of this document is to provide ONR inspectors with broad guidance to support exercising of their regulatory judgement on safety cases for controlling nuclear and radiological[[1]](#footnote-1) hazards. It sets out the purpose of safety cases for nuclear facilities and activities and expectations on how they are used, on their overall qualities, on how they may be structured and on what information they should contain. Guidance in the main body of the report is supplemented by information in appendices on specific topic areas.

The scope covers safety cases for the different phases in the lifecycle of facilities, e.g. design, construction, commissioning, operation, decommissioning. Guidance is given to inspectors on the aspects that should be addressed in safety cases for the different phases of operation.

The guide does not address the following in depth:

* arrangements for the production and modification of safety cases (including checking and review) and the implementation of these arrangements, SAP SC.1, SC.2 (see guidance in NS-INSP-GD-014 [4]);
* periodic reviews of safety cases (guidance given in NS-TAST-GD-050 [3], NS-INSP-GD-015 [5]);
* specifics of operations/activities that safety cases cover (other than reference to supporting documentation);
* detail of environmental and non-nuclear safety issues that dutyholders may discuss in safety cases.

The guide does not prescribe the actual content or level of detail that needs to be addressed in safety cases. These are a matter for the dutyholder to determine taking into account the hazards and the specifics of each safety case. ONR’s expectations for specific topic areas are set out in its suite of TAGs.

This TAG contains guidance to advise and inform ONR staff in the exercise of their regulatory judgment. Although the guide has been developed for ONR’s own use, it indicates to dutyholder and other stakeholders the standards that ONR expects to be met in safety cases.

1. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

**Nuclear Site Licence Conditions**

The regulatory basis for this guide encompasses a number of licence conditions. LC23 (Operating Rules), specifically 23(1), requires a licensee to produce an adequate safety case in respect of any operation that may affect safety. LC19 (Construction or Installation of New Facility), LC20 (Modification to Design of Facility under Construction), LC21 (Commissioning), LC22 (Modification or Experiment on Existing Facility) and LC35 Decommissioning) all require ‘adequate documentation to justify safety’ within the context of the specific condition. LC14 (Safety Documentation) and LC15 (Periodic Review) require a licensee to make and implement adequate arrangements for the production of safety cases and for the periodic review and reassessment of safety cases.

Licence conditions apply where a nuclear site licence is granted to a licensee. In some instances ONR will assess safety cases where no licence has been granted (eg Generic Design Assessment (GDA) of new facilities); in such situations the same broad principles for safety case assessment are applied.

**Other Relevant Legislation**

In addition to the nuclear site licence condition requirements, safety documentation may be required under other legislation enforced by the ONR (eg IRR, REPPIR, MHSAW, COMAH, HSWA[[2]](#footnote-2)) or to meet the legal requirements enforced by other regulators (e.g. Environment Agency, Natural Resources Wales, Scottish Environment Protection Agency). As appropriate, dutyholders may cross reference within a safety case to supporting information contained in other safety documentation.

Sections 2 and 3 of the HSW Act 1974 require the employer to reduce the risks to employees and other persons, so far as is reasonably practicable (SFAIRP). Therefore it is a fundamental requirement that the safety case should demonstrate how nuclear risks are reduced so far as is reasonably practicable; also referred to as demonstrating risks have been reduced to levels “As Low As Reasonably Practicable” (ALARP).

1. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED

**SAPs**

The SAPs [1] provide a framework to guide regulatory decision-making in the nuclear permissioning process. The SAPs include a section on the Regulatory Assessment of Safety Cases (paras 79–113) with principles SC.1 – SC.8. These principles encompass: safety case processes (SC.1 and SC.2); safety case characteristics (SC.3 to SC.6); and safety case management (SC.7 and SC.8). SAP ST.5 and ST.6 extend these principles to take account of other hazardous facilities on or off the site, and interactions between facilities on multi-facility sites. As identified in the Application of the SAPs and the Regulatory Assessment of Safety Cases sections of the SAPs, during safety case assessment inspectors should use the principles proportionately, commensurate with the radiological hazards presented.

Other SAPs that are relevant in the production and implementation phases of safety cases include the principles on Leadership and Management for Safety (paras 53–78 of [1]). These SAPs cover the aspects of safety culture, resources, competences, the use of contractors, decision making and the effectiveness of managing, auditing, reviewing and being a learning organisation. These attributes are fundamental to the successful production, implementation and maintenance of safety cases.

The SAPs contain further specialised principles relating to particular topic areas which feed into, and form part of the overall safety case (e.g. engineering key principles and fault analysis). As these principles are wide ranging, and application will vary depending on the type and extent of hazards on a particular facility, the supporting guidance documents are not listed here but are available on the ONR website www.onr.org.uk/operational/index.htm.

**WENRA Reactor Safety Reference Levels**

The objective of the Western European Nuclear Regulators Association (WENRA) is to develop a common approach to nuclear safety in Europe by comparing national approaches to the application of IAEA safety standards. Their Safety Reference Levels (SRLs), which are primarily based on the IAEA safety standards, represent good practices in the WENRA member states and represent a consensus view of the main requirements to be applied to ensure nuclear safety. In particular, ONR’s policy is that the WENRA SRLs developed for civil nuclear reactors, waste and spent fuel storage, and radioactive waste treatment and conditioning [6] are considered to be UK relevant good practice (see section 4 of [7]).

Safety cases are directly addressed in WENRA’s report on reactor SRLs for existing reactors Issue N “Contents and updating of safety analysis report (SAR)” [6]. This states that the licensee shall provide a SAR to demonstrate that the plant fulfils relevant safety requirements and use it as the basis for continuous support for safe operation and for assessing the safety implications of changes to the facility or to operating practices. This Issue N appendix provides some useful guidance and has been taken into account in this TAG.

**IAEA Safety Standards**

IAEA General Safety Requirements, GSR Part 4, 2009, “Safety Assessment for Facilities and Activities” [8] states that safety assessments[[3]](#footnote-3) are to be undertaken as a means of evaluating compliance with safety requirements (and thereby the application of the IAEA fundamental safety principles) for all facilities and activities and to determine the measures that need to be taken to ensure safety. The safety assessments are to be carried out and documented by the organisation responsible for operating the facility or conducting the activity; they are to be independently verified and are to be submitted to the regulatory body when required as part of the licensing or authorisation process. Guidance on the format and content of the safety assessments for facilities provided in the related IAEA safety guides (eg [9] and [10]) has informed this guidance.

Further IAEA Specific Safety Requirements (SSRs) provide guidance on management of safety for specific facilities/activities which will inform the safety case; for example:

* safety of nuclear fuel cycle facilities, SSR-4 [11];
* safety of nuclear power plants: design, SSR-2/1 (Rev 1) [12]; and,
* safety of nuclear power plants: commissioning and operation, SSR2/2 (Rev 1) [13].
1. ADVICE TO INSPECTORS

**Definition of a Nuclear Safety Case**

The nuclear safety case is a term used to encompass the totality of the documentation developed by a designer, licensee or dutyholder to demonstrate high standards of nuclear (including radiological) safety and radioactive waste management. This approach in UK regulation differs from many overseas regulatory regimes, and further guidance for non-UK parties is given in [15].

The nuclear safety case provides the information required to allow the UK’s safety standards to be maintained. Paragraph 86 in the SAPs [1] states 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’.*

LC23 requires the licensee to produce an adequate safety case to demonstrate the safety of any operation that may affect safety. The term ‘nuclear safety case’ may be used in reference to a site, a facility, part of a facility, a modification to a facility or to the operations within a facility, or to one or more significant issues. ONR expects that where multiple safety cases are provided to demonstrate the safety of the licensee’s operations the interfaces between these documents are clear and the totality of the documentation provides a holistic demonstration of safety across the overall undertaking.

The dutyholder may wish to produce holistic safety cases in which both nuclear safety and non-nuclear safety risks are considered in an overall demonstration that risks are reduced ALARP. This guidance applies specifically to nuclear safety aspects; therefore the term ‘nuclear safety case’ is shortened to safety case herein.

**The Purpose of a Safety Case**

The primary purpose of a safety case is to provide the dutyholder (or intended dutyholder) with the information required to enable safe management of the facility or activity in question across its lifecycle, and to reduce risks to ALARP (paragraphs 111-112 of SAPs [1]).

The safety case should be understandable and useable, and clearly owned by those with direct responsibility for safety. It should communicate a clear and comprehensive argument to its users that a facility can be operated or that an activity can be undertaken safely. It should demonstrate appropriate defence in depth in design, that the associated risk and hazards have been assessed, the appropriate limits and conditions have been defined and adequate safety measures have been identified. Further detail on the content and structure of the safety case is given later in this section.

The implementable requirements of the safety case (e.g. limits and conditions necessary in the interest of safety; safety measures; examination, inspection maintenance and testing regimes for engineering measures; claims on human action) must be properly implemented so that the facility can be operated and maintained in a safe manner, and so that radiological risks are managed to reduce them to ALARP (SAP SC.6 [1]). When assessing safety cases inspectors, should seek assurance that the licensee has identified all implementable requirements and that these have been captured in such a way that their implementation can be tracked onto plant as part of safety case implementation.

**Stages of a Facility’s Lifecycle (SAP SC.3)**

SAP SC.3 states “*For each lifecycle stage, control of the hazard should be demonstrated by a valid safety case that takes into account the implications from previous stages and for future stages*”.

The lifecycle of a facility from conception through to decommissioning can be divided into defined stages requiring consideration. The strategy and basis for safety at each stage should be defined early in the evolution of the safety case. The safety case for each stage should demonstrate the safety of that stage, be forward looking and contain sufficient detail to give confidence that the safety intent for all subsequent stages, including decommissioning, will be achieved. Any constraints imposed on subsequent stages (including key assumptions to carry forward) should be identified in the safety case.

Examples of key stages in the lifecycle for a facility, the associated safety cases and their particular purpose are shown in Appendix 3. Para 99 in the SAPs states “*The specific scope, content and depth of information provided at each stage will vary, and should be commensurate with the nature of the particular stage and interrelationships with other stages. For example, in the early stages (e.g. design concept) the safety case will be more a statement of future intent, claims and principles, whereas a safety case for an operational stage needs to contain far more detail, evidence and analysis*”. Each new stage is expected to utilise information from the previous stage and build on it as appropriate. Similarly, the case should be forward looking such that the impact of the design/operation decisions on future activities is given proportionate consideration, with appropriate level of confidence that any claims can be supported by evidence. For licensed sites, safety case evolution may be aligned with site arrangements under Licence Conditions 19 - 22. Additional guidance for new reactor assessment is given under ONR’s GDA technical guidance [15] and in [23], which considers licensing of nuclear installations more broadly.

In practice the sub-division of the stages of safety case evolution may be dependent on a number of factors including the nature of the facility in question, precedent, regulatory expectations and dutyholder requirements. The various illustrative stages listed in Appendix 3 result from significant steps in facility definition, though a particular facility or operation may not require all safety case stages. This is particularly so for the Early Design stage, which may not require a Preliminary Safety Case, for example for projects with short time scales or of an established design.

The dutyholder will need to decide whether or not it is appropriate to produce a separate safety case for each stage of the facility lifecycle, or whether to produce combined safety cases for multiple stages. It is expected that the dutyholder will have agreed with ONR a schedule of submissions in support of permissioning particular activities [23, 24], which may be aligned to key safety case stages. For complex installations, sub-division of the stages may be beneficial; for example a safety case for construction may be divided into civil construction and facility installation stages, or radiological non-active and active commissioning stages. All safety cases must have a clear scope in terms of the permission being sought for the stage they justify. For combined documents, the scope and permission requested must be commensurate with the stages being combined. For some facilities, initial commissioning with non-active materials prior to introduction of active materials is the normal approach; however, the extent to which this can be done may vary for different facilities; for example, extensive commissioning on non-active feed materials is common on fuel processing facilities.

Supplementary documents will often be added to the safety case to cover an activity at a point in time. For example;

1. as a method statement to demonstrate that the integrity of facility will be maintained and quality assured during construction and installation work, or
2. a justification to demonstrate the safety of a temporary facility modification by defining and substantiating, for a limited period of time, operations which are outside the normal envelope prescribed by existing rules and instructions. Such modifications should be managed under the Licensee’s LC22 arrangements.

Development of a safety case should be an iterative process and ensure that lessons are learned and applied before going forward to the next stage. For new projects, documents should ideally 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 stages in the project commence (i.e. design, construction, commissioning, operation, and decommissioning). Some areas will need to progress at an early stage to influence and balance the design (e.g. human factors).

It is important that the whole lifecycle of the facility is taken into consideration in all stages. For example, decommissioning feasibility and associated safety and waste management issues should have been considered to an adequate extent in all previous lifecycle stages. A detailed decommissioning safety analysis may not be practicable in the early life of a facility, but an outline strategy demonstrating how decommissioning and waste management have been considered within the design evolution is expected.

**The Content and Structure of a Safety Case**

ONR does not prescribe the format of safety cases and the documents that make up the safety case; however there are regulatory expectations as to what the safety case should address. SAP SC.4 expects that “*A safety case should be accurate, objective and demonstrably complete for its intended purpose*”. Paragraphs 100-102 in the SAPs [1] give guidance to inspectors on what should be covered by the safety case:

*‘100. A safety case should:*

*(a) explicitly set out the argument for why risks are ALARP; and*

*(b) link the information necessary to show that risks are ALARP, and what will be needed to ensure that this can be maintained over the period for which the safety case is valid;*

*(c) support claims and arguments with appropriate evidence, and with experiment and/or analysis that validates performance assumptions;*

*(d) accurately and realistically reflect the proposed activity, facility and its structures, systems and components;*

*(e) identify all the limits and conditions necessary in the interests of safety (operating rules); and*

*(f) identify any other requirements necessary to meet or maintain the safety case such as surveillance, maintenance and inspection.*

*101. To achieve these, a safety case should:*

*(a) identify the facility’s hazards by a thorough and systematic process;*

*(b) identify the failure modes of the plant or equipment by a thorough and systematic fault and fault sequence identification process;*

*(c) demonstrate that the facility conforms to relevant good engineering practice and sound safety principles. (For example, a nuclear facility should be designed against a set of deterministic engineering rules, such as design codes and standards, using the concept of ‘defence in depth’ and with adequate safety margins.) Instances where good practice has not been met should be identified and a demonstration provided to justify why these are considered to grossly disproportionate;*

*(d) provide sufficient information to demonstrate that engineering rules have been applied in an appropriate manner. (For example, it should be clearly demonstrated that all structures, systems and components have been designed, constructed, commissioned, operated and maintained in such a way as to enable them to fulfil their safety functions for their projected lifetimes.);*

*(e) analyse normal operations and show that resultant doses of ionising radiation, to both members of the workforce and the public are, and will continue to be, within regulatory limits and ALARP;*

*(f) analyse identified faults and severe accidents, using complementary fault analysis methods to demonstrate that risks are ALARP;*

*(g) demonstrate that radioactive waste management and decommissioning have been addressed in an appropriate manner; and*

*(h) provide the basis for the safe management of people, plant and processes. (For example, the safety case should address management and staffing levels, training requirements, maintenance requirements, operating and maintenance instructions, and contingency and emergency instructions).*

*Further guidance on these topics is set out in the relevant section(s) of these principles.*

*102. To demonstrate that risks have been reduced to ALARP, the safety case should:*

*(a) identify and document all the options considered for risk prevention or reduction;*

*(b) provide evidence justifying the criteria used in decision making or option selection;*

*(c) justify the options chosen in terms of meeting relevant good practice, and discard any options as being either less effective than the chosen option(s) or grossly disproportionate.’*

*Content of a safety case*

The content of a safety case will vary between different dutyholders and different applications. This section aims to give guidance on what is the typical content included in most dutyholder safety cases and therefore inform what we would typically expect. The extent to which each section is considered will vary, based on the scope of the safety case (see sub-section below). Figure 1 below presents an overview of the types of information, analysis and substantiation that might be considered within a typical safety case for a nuclear licensed site (although terminology for each aspect will vary between dutyholders). The scope of elements shown and their interaction is illustrative and not intended to be exhaustive or representative of safety cases for all facilities. For example, in this case the fault analysis includes deterministic, probabilistic and severe accident conditions to support demonstration of risk management and consideration of different levels of defence in depth (discussed later in paragraph 5.41).



***Figure 1*** *– Example diagrammatic representation of the content of a safety case*

The safety case should provide relevant design information, such as site layout and plant/facility design, and explicitly identify the structures, systems and components (SSCs) required in the interest of safety. Further, the safety case should define the operational philosophy of the site to ensure that they align with the safety assessment that supports its operation. The safety case should explicitly justify why the design meets the requirements of the assessment, typically using design substantiation documentation. Further guidance on the expectation for design justification can be found in relevant ONR SAPs and TAGs on engineering, and organisational, human factors and QA. Given the broad range of different TAGs which impact upon the safety case these are not listed in full here; inspectors should consult the ONR intranet/internet for the most up to date listing of guidance.

Safety assessment or analysis is performed to identify the potential radiological consequences and the operations/faults/hazards that can lead to them. The analysis should aim to identify that suitable and sufficient protection is in place. A fault schedule (or equivalent document) should be used to summarise the faults in safety case, with a clear link to safety measures (SAPs para 407 and FA.8). A fault schedule will typically identify the following detail as a minimum, but additional information can be included to add further benefit and clarity to the case:

* Design basis initiating events considered in the safety case.
* Initiating event frequencies.
* Unmitigated and unprotected consequences.
* Safety functions to be delivered including reactivity control, cooling and containment.
* Safety measures to deliver the safety functions (SSCs plus any human actions).

The safety case should also consider radiological waste and ultimately redundant equipment/structures that will result from operations; therefore assessment should be carried out to ensure that its production is prevented or minimised as far as reasonably practicable (SAP RW.2), that it can be appropriately controlled and managed in a way which reduces risks ALARP. Further guidance on the expectation for assessment can be found in the ONR TAGs suites on accident analysis, radiological protection and nuclear liabilities regulation.

There are many influencing factors that need to be considered in the management of nuclear safety such as security, conventional health and safety and asset protection.  These factors should be fully incorporated within design and operational decisions using a balanced approach to ensure synergies are optimised and any conflict effectively resolved.  The safety case should articulate how these factors will influence design and safety and justify how management of any resultant nuclear safety risks have been reduced ALARP.  Interaction between safety and security assessment is discussed in paragraphs 39-41 and 32-34 of SAPs and SyAPs[[4]](#footnote-4) respectively.

The methods used by different dutyholders for the safety case to demonstrate that risks are ALARP vary widely. Foremost, the inspector should consider whether the safety case demonstrates compliance with relevant regulations, codes, standards, specifications and other relevant good practice. ONR uses numerical targets to aid judgements when considering whether radiological hazards are being adequately controlled and risks are reduced ALARP. Further guidance on application of these targets and the expectation for ALARP can be found in the ONR TAG on demonstration of ALARP [7].

The safety case should demonstrate how nuclear risks are reduced ALARP within the context of the dutyholder’s undertaking. There may also be additional constraints outside of the dutyholder’s immediate control which could influence nuclear safety, such as strategic factors (eg Government policy, consideration of vulnerable groups, risk in an area outside of the dutyholder’s control) and strategic imperatives. Claims related to these factors can sometimes appear in safety cases under the banner of ‘group/global ALARP’, ‘programme ALARP’, ‘holistic ALARP’ or ‘dynamic ALARP’. Dutyholders use these terms to try and capture prioritisation, strategic factors and/or wider national factors. Whilst this is understandable, it can lead to a lack of clarity as many of these factors normally lie outside the scope of the Health and Safety at Work etc Act 1974 (and dutyholders’ undertakings) and therefore ought not to feature in an ALARP case. While such factors should not form part of the dutyholder’s ALARP justification, these factors can inform our regulatory decisions and it is helpful if dutyholders, where relevant, identify them explicitly and separately from their ALARP considerations. If the level of risk has not been reduced ALARP, relevant dutyholder and strategic factors can be taken into account by ONR in our regulatory decisions. Ref [19] provides a summary of ONR’s risk informed decision making processes and the influence of strategic factors and imperatives in forming a regulatory judgement.

The safety case should explicitly identify all of the requirements of the safety case in a clearly defined form (SAP SC.6). These will notably include all of the limits and conditions required in the interest of safety (LC23(1) - further guidance on this aspect is provided in ONR’s TAG on limits and conditions [17]) and the operational instructions that implement the limits and conditions (also known as Operating Rules). An engineering schedule (or similar document) may be useful to capture the required SSCs and associated maintenance requirements. Examples of implementable requirements are given in Figure 1; the inspector should seek assurance that all such requirements are captured in way to ensure that their implementation can be tracked onto plant as part of safety case implementation.

The safety case, safety case processes and the site management arrangements will have to interact to ensure that the safety case undergoes appropriate due process and can be effectively implemented. Therefore it is expected that the content, format and outputs of the safety case should be written to work within the dutyholder’s management arrangements (including using dutyholder’s terminology).

*Scope of the safety case*

LC23 (1) requires that “the licensee shall, in respect of any operation that may affect safety, produce an adequate safety case to demonstrate the safety of that operation”. The safety case should be clear in its definition of scope of operations, plant operating modes, plant boundaries and interactions/interfaces and lifecycle assumptions. If the site/overall safety case is broken down to cover different operations, the dutyholder should be explicit about the scope of each of its safety cases and the interfaces to other safety cases/processes, i.e. what does the safety case cover (e.g. new site/facility, facility extension, modification, boundaries and interactions, decommissioning). The dutyholder should able to demonstrate that the totality of all its site safety cases covers all site operations that may affect safety, and demonstrate consistency in the underpinning assumptions.

The safety case should also be explicit about the time period for which the safety case is valid for. For example, some safety cases might only be valid for short term modifications or operations, while others will be valid for the life of the facility.

*Safety case reasoning*

Paragraph 86 of the SAPs indicates ONR’s expectation that the safety case should clearly set out the trail from safety claims, through arguments, to evidence. At a high level, these can be explained as follows:

* Claims (or assertions) are statements that can be shown to be true (or false) with appropriate confidence. Once complete, a satisfactory safety case will contain no false claims and each demonstrated claim will contribute to the overall objective of the safety case. An example of a safety claim might be: “the fuel maintains its integrity as a barrier to fission product release in normal operation and anticipated faults”. In some cases, claims may be hierarchically structured, with claims supported by lower-level claims.
* Arguments (or reasoning) explain how the claims are (or will be) shown to be true. Arguments provide the link between claims and the evidence necessary to support them. For example, an argument might show that a method has produced applicable evidence that is sufficient to demonstrate the validity of the claim. An argument may be subject to stated assumptions, limitations and/or context appropriate to the specific case, which should be made clear.
* Evidence is the set of facts that, via the arguments, aims to provide adequate confidence in the claim. In order for the claims, arguments and evidence to be complete within a safety case, all claims must be underpinned by adequate evidence. The evidence used should be of sufficient quality, commensurate with the magnitude of potential risks and complexity of the system of interest. An adequate demonstration of key safety claims usually needs the support of multiple legs with different types of evidence. Examples of evidence are: safety analysis calculations and results, code verification and validation reports, operational experience data, experimental/test results, engineering analysis and human performance data.

The presentation of safety claims through to arguments and evidence within the safety case should be carefully considered and implemented so that the resulting safety case flows and makes sense to those with responsibility for safety. Some dutyholders have chosen to explicitly identify safety claims and set out a structure for their supporting arguments and evidence (this is often referred to as a claims arguments evidence (CAE) approach). To provide context to guide inspectors, further details are given in Appendix 4. ONR does not prescribe the approach to presentation of safety claims through to arguments and evidence within the safety case. The optimised approach may differ for different dutyholders and facility types, and different safety disciplines; however, it is expected that any approach taken should provide auditability of evidence to support key safety claims.

*Safety case documentation structure*

A safety case should be structured in a logical manner and be demonstrably complete. It should be accessible, understandable and useable to those who are responsible for safety to enable safe management of the activity in question (para. 96 of SAPs [1]). The safety case is important to a wide range of roles, for example:

* those who interact directly with the facility, such as the operators who control the conditions within the facility and those who maintain the facility;
* senior management who are responsible and accountable for safety, who rely upon the safety case for accurate and objective information on risks and control measures to make informed decisions that may affect safety;
* technical or engineering staff who, when carrying out work to review operational or safety performance of the facility, will need to understand dependencies and interactions within the safety case.

Key users of the safety case should be involved at relevant stages in its development, production/review and implementation.

Safety cases are typically made up of multiple documents, so that appropriate information is accessible to the relevant end user. The precise structure and scope of the documentation will be a matter for the dutyholder to determine taking into account the complexity of the safety case and the needs of its users. IAEA guidance for the safety analysis report for new nuclear power plants in [9] represents one potential starting point for documentation structure, but it would be expected to be developed further to reflect UK regulatory expectations for a safety case. In most circumstances, a safety case will comprise a hierarchy of documents. This approach can significantly improve the usability and accessibility of the safety case, and in particular can bring out key aspects of the safety case to users and decision makers.

The top tier document should describe the facility and its operation, summarise the main hazards and the safety functions required to control them, explain the means of delivering these functions, and summarise the main conclusions, including whether risks are reduced ALARP. It should be meaningful if read in isolation, as well as providing the main entry point and clear links (‘sign-posting’) to the safety case documentation as a whole. For large or complex safety cases, the top tier summary document is sometimes known as the Safety Report.

Figure 2 provides an example tier approach to safety case documentation. In this example the overall safety report is supported by facility safety reports which in turn are supported by multiple operational, design and assessment and build justifications. These justifications are further supported by multiple documents; this level of documentation typically contains the evidence that the safety claims made in the high level documentation are met. The safety case is the totality of the documentation required to demonstrate safety. The dutyholder’s position on what documents they describe as being within the safety case can vary. Inspectors should make their opinion on the adequacy of the safety case based on the available information, not what dutyholders consider within, or outside, their safety case. Typically the top tier documents in the safety case will contain the core of the safety claims (or ‘assertions’) and high level arguments (or ‘reasoning’) and increasingly detailed technical documents and supporting analysis will be presented in lower tiers. The safety claims and arguments should be coherent, consistent and readily understood. At the lowest level there are likely to be the substantiation and design details, experimental results, data on reliability, relevant operational experience, etc. The language and terminology used at each level should be understandable to its target audience; the top tier documents are likely to have a much wider audience than some of the lower tier documentation (such as complex modelling or analysis). Inspectors should expect the readability of each level of safety documentation to be in line with its expected target audience. Further guidance on the approach to safety case structures for GDA is given in [15].

Safety cases should be structured in a top-down fashion. The high level claims within a facility’s safety case should be clearly articulated and these broken down into claims on plant, equipment and personnel (ie safety functions). These claims can then be linked and supported by arguments and evidence to demonstrate that the claims will be met. Inspectors should be cautious where the safety documentation only provides arguments and evidence level information and the overall safety claims have not been established or clearly articulated. It might not be appropriate to assess such cases until the top level claims are clearly established.



***Figure 2*** *– Example of hierarchy of safety case documentation (definitions of acronyms given in glossary and abbreviation listing). Note, some aspects may span multiple sections, eg. principle of ALARP should apply across the safety case.*

*Conservatism and optimism*

In the Ladbroke Grove Rail Inquiry, Lord Cullen noted that safety cases should “*encourage people to think as actively as they can to reduce risks*.” The safety case should be clear in its treatment of optimism, uncertainty and conservatism in demonstrating a balanced and honest argument (SAP SC.5). This is captured in paragraphs 103-104 of the SAPs:

*“The safety case should present a balanced view of the level of knowledge and understanding, and of the resultant risks. It should provide a proportionate justification that includes appropriate conservatism but without undue pessimism. Otherwise, it can mislead those who need to use the safety case to take decisions on risks and on managing safety. An unbalanced case will also fail to identify areas where more work might be needed, either to support the current conclusions or to provide a valid basis for any subsequent work if the safety case needs to be revised (eg due to a proposed plant modification or a change to the operating regime or procedures). This principle encompasses optimism and uncertainties in the design of a facility (eg material properties, defects and dynamic behaviour) and in the basis of the safety case (eg analytical methods and codes, underlying assumptions, data, margins and factors of safety). Areas of uncertainty should be offset by appropriate levels of conservatism.*

*To ensure that risks are understood and can be managed appropriately, potential weaknesses in the design or the safety case should be identified clearly (eg in the summary or main conclusions of the safety case). Mitigating measures that have been or can be applied to address the weaknesses should also be identified. It should also be made clear how any outstanding safety significant issues are being, or will be, addressed.”*

Balancing optimism, uncertainty and conservatism in a safety case may require detailed understanding of factors across a number of different areas. This again highlights the importance of the safety case having a logical structure and being accessible and understandable by all users. Inspectors should consult with specialist counterparts where complex cross-specialism risk balance arguments are presented if it is unclear how the final conclusion has been reached. For example, section 4 of ONR’s GDA guidance to requesting parties provides guidance on where different specialist topic areas will interact [15].

The nine numerical targets in the SAPs provide a framework to consider and balance risk associated with normal operations, faults conditions and severe accident considerations. Consideration of relevant targets, and the optimism or uncertainty assumed in the analysis, can inform a holistic view of whether risks are reduced ALARP. Further guidance on consideration of numerical targets and ALARP is given in the SAPs [1] and ONR’s TAG on ALARP [7].

*Safety case strategy*

Experience has shown that it is beneficial for dutyholders delivering more significant or complex projects to produce a safety case strategy document early, to promote effective planning and early stakeholder engagement. The documentation framework should be defined before work begins on the safety case. This will ensure there is a clear and logical structure, aiding both its production and subsequent implementation. The completed framework should include a detailed plan of the individual documents required. This can prove useful in identifying potential ‘holes’ at an early stage and it helps in monitoring progress towards completion. It can also support the strategy for maintenance of the safety case (SAP SC.7). The detailed plan can of course change, as work progresses, with documents being added or deleted. The safety case strategy should also link to the facility lifecycle and strategy for subsequent stages of the safety case, including decommissioning. Further ONR guidance on decommissioning strategy is given in [20].

A safety case strategy might also be developed to manage the generic design assessment of a new reactor type, taking on board lessons learnt from previous GDA work. Lessons learned from previous GDA work across a wide range of topic areas are captured in [15].

**The Relationship between the Safety Case and Engineering Key Principles**

The SAPs state that the underpinning safety aim for a nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility (EKP.1). The sensitivity of the facility to potential faults should be minimised (EKP.2) and the design should provide defence in depth against potentially significant faults and failures (EKP.3). Safety functions and associated safety measures should be identified by structured analysis (EKP.4, EKP.5). Defence in depth in the safety case is considered further below.

*Defence in Depth*

The SAPs expect that the safety case demonstrates defence in depth (SAP EKP.3); paragraph 152 states that defence in depth is generally applied in five levels which should be, as far as practicable, independent from one another. The methodology should ensure that if one level fails, it will be compensated for, or corrected by, the subsequent level. The objectives of these levels are listed in Table 1 in the SAPs [1], and summarised here:

* Level 1: Prevention of abnormal operation and failures by design.
* Level 2: Prevention and control of abnormal operation and detection of failures.
* 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 protecting against further fault escalation and mitigation of the consequences of severe accidents.
* Level 5: Mitigation of radiological consequences of significant releases of radioactive material.

The safety case should consider all levels of defence in depth. The number and type of safety measures and physical barriers will depend on the magnitude of the radiological hazard, the consequences of their failure and the safety margins demonstrated. Where potential consequences are high, the safety analysis does not end with the provision of level 3 protective measures, it should extend to the fourth and fifth levels of defence in depth. The design of the facility should include provisions for emergency preparedness and response, which may include, for example, the necessary emergency power supply, provisions for fire protection, and evacuation of personnel.

To determine whether defence in depth has been adequately demonstrated, inspectors should consider whether priority has been given to: reducing the number of demands on safety systems and challenges to the integrity of barriers; preventing the failure or bypass of a level of defence in depth when challenged; preventing the failure of one safety system or barrier leading to the failure of another; and preventing significant releases of radioactive material if failure of one or more physical barriers does occur. Appropriate measures to ensure reliability and effectiveness of the required levels of defence in depth should be identified and implemented, and events which could result in simultaneous failures of multiple barriers or layers of defence in depth should be considered. Guidance on the categorisation of safety functions and classification of structures, systems or components systems important to safety is considered in [16]; an analogous approach should be used for safety functions delivered by human action (paragraph 164 in the SAPs [1]).

The safety case should demonstrate that potential severe accident states that result in an early or large release of radioactivity have been practically eliminated, as expected by UK and international guidance, notably:

* SAPs paragraphs 611, 666 [1];
* IAEA Specific Safety Requirements SSR 2/1 [12];
* WENRA Safety Reference Levels for existing reactors [6]; and,
* Nuclear Safety Directive of the European Union (as amended 2014), Article 8A(1) (as discussed in [7]).

Inspectors should consider both specific claims of practical elimination made for individual plant states or accident conditions and the holistic claim made for the entire facility, taking into account relevant uncertainties, particularly those due to limited knowledge of extreme physical phenomena (eg the behaviour of molten reactor cores). A plant state with the potential for a large or early release should not be considered to have been practically eliminated simply on the basis of meeting probabilistic criteria. Instead, any claims made on SSCs or human action in relation to practical elimination need to be substantiated appropriately. Note, the safety case may present an adequate case without specific use of the phrase ‘practical elimination’. For existing facilities it may not always be possible to demonstrate ‘practical elimination’; in such cases the safety case should still demonstrate adequate management of the severe accident state to reduce risks ALARP. Further guidance in the context of new reactor design, including lessons learnt from past GDA work, is given in ONR’s guidance on generic design assessment [15].

**Site Wide Safety Case**

For sites where there are multiple facilities, the licensee may choose to produce separate safety cases for specific facilities, activities, functions or parts of a site, together with a site wide safety case. The purpose of a site wide safety case is to demonstrate that the site as a whole is safe and to substantiate dependencies and claims made on it by individual facility safety cases (e.g. facility interfaces, common services and emergency arrangements). It should show that the safety cases for a set of facilities are comprehensive, consistent and adequately integrated. Individual facility safety cases should refer to the site wide safety case and other relevant safety cases, as necessary. Further guidance is given in ONR SAPs paragraph 133-139 (SAP ST.6).

The site wide safety case should cover ‘whole licensee’ aspects such as safety management, safety culture and organisational capability (see [14] and ONR Leadership and Management for Safety SAPs [1]). These topics should be addressed, as appropriate, in facility safety cases but the site wide case is more able to demonstrate that the licensee has an adequate organisational structure and resources, safety policy and safety management arrangements to manage interactions between facilities and operate the whole site safely.

The site wide safety case should capture the safety significance of key services, major hazards and significant safety issues for the site as a whole, and provide the information required to safely manage these. For large or complex sites, it is useful to summarise the site wide safety case in a top tier report.

The site wide safety case should consider the overall hazards and risks of the site as a whole and make comparisons of these risks against relevant risk criteria (e.g. SAP NT.6, NT.7 & NT.9). Further, the site wide case should consider the overall site wide emergency response and management aspects to ensure these have been considered on a site wide basis.

Where the licensed site is adjacent to, or forms an enclave within another licensed site, then both licensees must give consideration in site wide safety cases to any shared services or shared emergency arrangements and to the impact that one may have, as an external hazard, on the other. Adequate arrangements need to be made to ensure that information is shared to enable the above considerations to be taken into account.

In addition to nuclear facility interactions, SAP ST.5 states that “the safety case should take account of any hazardous installations on or off the site that might be affected by an incident at the nuclear facility”. Damage to other installations may exacerbate the consequences of accidents or impact upon the emergency response, and so could challenge reasonable practicability arguments in the safety case. This principle should be applied to transport infrastructure in the vicinity of the facility as well as to fixed installations. The extent to which this is covered in the safety case should be proportionate to the hazard and risks associated with a particular facility or operation. Where relevant, common cause effects should be considered within the analysis.

Site-wide safety cases should be subject to periodic review and reassessment. The total suite of safety cases on the site and their periodic review schedules should be set out by the licensee. The timing of periodic reviews of safety cases is discussed in [3].

**The Safety Case in context – Ownership, Management and Review (SC.7, SC.8)**

*Safety Case Implementation*

It should always be remembered that the documented safety case is not an end in itself. It forms an important part of how the dutyholder manages safety. The requirements of the safety case need to be implemented and managed effectively so that the facility can be operated and maintained in a safe manner (SAP SC.6). Paragraph 106 in the SAPs states:

*The safety case should justify how the requirements identified within it will be implemented effectively. The means of implementation considered should include:*

1. *the operating limits and conditions (operating rules) required to ensure that the facility is operated safely at all times;*
2. *the procedures and instructions that need to be followed;*
3. *the required examination, inspection, maintenance and testing regimes justified in or assumed by the safety case;*
4. *control, supervision, qualification and training and other safety management requirements; and*
5. *inputs to emergency planning.*

The safety case should explicitly identify the implementable requirements of the case. These should be effectively transposed to implementation documentation as part of the dutyholders safety case implementation processes. Further, once the safety case is implemented these requirements should be enforced on the facility. There should be an auditable and visible route from the safety case, to the implementation documentation and on to the facility.

Fundamental to the safety case are the principles, standards and criteria which the licensee intends to maintain. They will include design standards, safety criteria and general standards of safety management. They should be mutually consistent and their selective use should be avoided. It is important that the licensee’s standards and criteria do not conflict with any statutory duties and requirements.

*Safety Case Ownership*

The dutyholder is legally responsible for the safety case and its adequacy. Those who have direct responsibility within the dutyholder’s organisation for delivering safety should have ‘ownership’ of the safety case (SAP SC.8). For example, ownership of a safety case for a specific facility should reside within the operational line management. Ownership is not a ‘figure head’ role. It requires an understanding of the safety case, operations of the facility it justifies, and the limits and conditions derived from it. The safety case owner should have responsibility to ensure it is adequately managed and maintained.

Ownership of the safety case is likely to change in line with the different stages of the facility lifecycle (e.g. at the design stage, ownership could be within a project team). Transfer of ownership should be a formal process with clear handover, and acceptance, of responsibilities.

In addition to the role of safety case owner, it is good practice for a dutyholder to have a separate role of safety case process owner. The latter is responsible for the whole process for producing safety cases. This includes process review and improvement to ensure good quality, fit for purpose safety cases are produced consistently. Further guidance on the safety case process is provided in NS-INSP-GD-014 [4]).

*Maintaining Safety Cases*

It is important that the safety case is kept up to date during each stage of a facility lifecycle, so that it is consistent with the as-built facility (or as-designed facility, for new build projects) and operated and maintained in accordance with safety case requirements and assumptions (SAP SC.7). This will include the impact of facility/plant modifications, new information (from research, additional analyses, etc.) and the outcome from periodic reviews. The safety case should also be reviewed and if necessary updated to take account of the lessons from operational experience and incidents. This should include experience from a range of sources, including: within the facility in question; elsewhere on the site or within the dutyholder’s organisation; the nuclear industry in the UK or internationally; and other relevant sectors. Thus, the safety case should be a suite of living documents which is subject to review and change as time proceeds. The dutyholder should have effective processes to ensure these objectives are achieved.

Any updates should encompass changes to safety case documentation (revision or replacement) plus amendments to rules, instructions, drawings, operational procedures and training requirements. This should be done in accordance with the dutyholder’s change control process (e.g. LC22 arrangements). Further guidance on inspection of management of modifications (including the safety case) for facilities under construction and operational plants is given in NS-INSP-GD-020 [21] and NS-INSP-GD-022 [22]. Documentation which no longer forms part of a current safety case, or which has been superseded, should be identified and archived. This information still forms part of the formal historical record, and remains subject to the arrangements made under Licence Condition 6.

Licence Condition 15 requires that “*the licensee shall make and implement adequate arrangements for the periodic and systematic review and reassessment of safety cases*”. Further guidance on periodic reviews is provided in NS-TAST-GD-050 [3].

**Overall Qualities of a Safety Case**

There are several features which are fundamental to a good safety case. These are summarised here in terms of eight overall qualities. The safety case should be ***complete***, ***intelligible***, ***valid***, ***evidential***, ***robust***, ***integrated***, ***balanced*** and ***forward*** ***thinking***. These terms are expanded on below.

|  |
| --- |
| **INTELLIGIBLE** *– understandable and accessible to meet the needs of its users* |
| * The safety case should be structured logically to meet the needs of those who will use it (e.g. operators, maintenance staff, technical staff, managers accountable for safety), using descriptions/terms that are readily understood.
* It should present a clear and coherent trail from safety claims (assertions), through the arguments (reasoning) to the evidence that supports the conclusions. Claims and arguments across the safety case should be consistent.
* All references and supporting information should be identified and be easily accessible.
* Operational requirements, including maintenance, operating rules etc. and commitment to any future actions should be clearly defined in the safety case.
 |
| **VALID** *– accurately represents the plant status and operations* |
| * The safety case should accurately represent the current status and design intent of the facility in all physical, operational and managerial aspects.
* It should reflect changes that have arisen from past modifications, revised operating methods, operating experience, examination and test results, different analytical methods and periodic reviews.
 |
| **COMPLETE** *– analyses all activities and modes of operation* |
| * The safety case should describe the facility, its purpose and operation
* It should identify and analyses activities associated with normal and faults of safety concern, including all identified states such as start-up/shutdown
* It should demonstrate that risks are ALARP, and identify any actions required to manage risks ALARP in the future.
 |

|  |
| --- |
| **EVIDENTIAL** *– claims & arguments should be supported by verifiable evidence* |
| Arguments in the safety case should be supported by verifiable and relevant evidence. Evidence should be shown to be relevant to the current (and future) safety case. For example:* Identification of key assumptions and their basis, and sensitivity to these assumptions.
* Substantiation of integrity of claims on performance on engineering or human performance.
* Analytical methods used to substantiate safety should be shown to be fit for purpose and valid for the application.
 |
| **ROBUST** *– conforms to relevant good practice with robust defence in depth* |
| * The safety case should demonstrate that the facility will/does conform to good nuclear engineering practice and safety principles, including defence in depth and adequate safety margins.
* The arguments and evidence presented should be proportionate to the hazards and risks.
* The link between engineering and safety provisions should be demonstrated in line with the principles of defence-in-depth.
 |
| **INTEGRATED** *– interactions with other facilities/services analysed* |
| * Hazards from and dependencies on other facilities, internal or external services (eg grid supplies, heating, ventilation and air conditioning) should be identified and related claims or assumptions substantiated.
* The safety case should be integrated with and reference the safety cases for such dependencies.
 |
| **BALANCED** *– recognise areas of optimism, uncertainty, weakness and improvements to present a balanced view of risk.* |
| * The safety case should encourage people to think as actively as they can to reduce risks.
* A safety case should present a balanced account, taking into consideration the level of knowledge and understanding. Areas of uncertainty should be identified, not just strengths and claimed conservatism.
* Potential weaknesses or areas for improvement in the facility design or the safety argument should be explained clearly and openly (e.g. in the summary or main conclusions of the safety case).
* The necessary understanding of the behaviour of novel systems or processes should be established from appropriate research and development.
 |
| **FORWARD LOOKING** *– considers safe operation for the facility’s defined lifetime* |
| The safety case should:* Demonstrates adequate control of radiological hazards before any associated risks actually exist.
* Identify the important aspects of operation and management that need to be implemented to maintain safety, including maintenance, inspection and testing regimes and operating limits and conditions.
* Detail any constraints that will apply in the facility’s life-time.
* Account for the effects of ageing and degradation on the facility.
* Identify the radioactive waste management arrangements e.g. disposal routes for waste.
* Consider the safety case for decommissioning to an adequate extent.
* Identify any unresolved issues along with the timescale for their resolution. Any further work, analytical or physical (e.g. inspections) needed to support the through-life safety case should be identified with the timescale for completion.
 |

**Common Problems, Shortcomings and Traps within Safety Cases**

ONR has considerable experience of reviewing and assessing dutyholders’ safety cases in support of its regulatory activities. It is important that inspectors learn from this experience and are made aware of the common problems that have arisen in the past and which they may encounter in the future. Appendix 1 has further information on the common types of problem, presented for comparison against the qualities introduced in paragraph 5.62 above.

It is also important that ONR learns from other sectors where there is a requirement to produce safety cases. The Nimrod Review [2] provides a comprehensive and valuable source of learning into how safety cases can go wrong, along with advice on how to address the shortcomings. This has direct relevance to nuclear safety cases and aligns with some of ONR’s experience (see Appendix 1). Some of the key points from the Nimrod Review are highlighted in Appendix 2. Inspectors are encouraged to read [2]; the safety case aspects are covered in Chapters 9 to 11 and 22.

Dutyholders should also be applying learning from their own experience (including significant issues identified by ONR) and from elsewhere (including outside the nuclear sector, including the Nimrod Review). Inspectors should look for evidence that this is happening and ask dutyholders how lessons have been applied to deliver improvements to safety cases.

Significant or persistent issues with safety cases are indicative of underlying problems with the way they are produced. Inspectors should ensure that the causes of such problems are addressed, not just the symptoms. See NS-INSP-GD-014 [4] for further guidance.

1. REFERENCES

|  |  |
| --- | --- |
| 1 | Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0. November 2014. <http://www.onr.org.uk/saps/index.htm> |
| 2 | The Nimrod Review; An Independent Review into the Loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006, Charles Haddon-Cave QC, October 2009 |
| 3 | ONR Nuclear Safety Technical Assessment Guide - Periodic Safety Reviews (PSR), NS-TAST‑GD-050 Revision 7, July 2017  |
| 4 | ONR Nuclear Safety Inspection Guide - LC14 Safety Documentation, NS‑INSP-GD-014, Revision 3, May 2016  |
| 5 | ONR Nuclear Safety Inspection Guide – LC15 Periodic Review, NS‑INSP‑GD-015 Revision 3, April 2016  |
| 6 | Western European Nuclear Regulators’ Association - WENRA. * Safety Reference Levels for existing reactors. September 2014.
* Radioactive Waste Treatment and Conditioning Safety Reference Levels, October 2016
* Waste and Spent Fuel Storage Safety Reference Levels, April 2014
 |
| 7 | ONR HOW2 – Nuclear Safety Technical Assessment Guide – Guidance on the Demonstration of ALARP (as low as reasonably practicable), NS-TAST-GD-005, Revision 9, March 2018.  |
| 8 | Safety Assessment for Facilities and Activities, IAEA General Safety Requirements, GSR Part 4 Rev. 1, 2016.[www.iaea.org](http://www.iaea.org)  |
| 9 | Format and Content of the safety analysis report for Nuclear Power Plants, IAEA Safety Guide No. GS-G-4.1, 2004. [www.iaea.org](http://www.iaea.org) |
| 10 | Safety Assessment for the Decommissioning of Facilities using Radioactive Materials, IAEA Safety Guide No. WS-G-5.2, 2009. [www.iaea.org](http://www.iaea.org) |
| 11 | Safety of Nuclear Fuel Cycle Facilities, IAEA Specific Safety Requirements SSR-4, 2017. |
| 12 | Safety of Nuclear Power Plants: Design, IAEA Specific Safety Requirements SSR 2/1 (Rev 1), 2016 |
| 13 | Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Specific Safety Requirements SSR 2/2 (Rev 1), 2016 |
| 14 | Leadership and Management for Safety General Safety Requirements, GSR Part 2, 2016. [www.iaea.org](http://www.iaea.org) |
| 15 | New Nuclear Power Plants: Generic Design Assessment Technical Guidance, ONR-GDA-GD-007 (Rev 0), May 2019 |
| 16 | Categorisation of Safety Functions and Classification of Structures, Systems and Components, NS-TAST-GD-094 (Rev 0). |
| 17 | Limits And Conditions For Nuclear Safety (Operating Rules), NS-TAST-GD-035 (Rev 5). |
| 18 | Reference no longer used. |
| 19 | ONR “Risk informed regulatory decision making”, June 2017 <http://www.onr.org.uk/documents/2017/risk-informed-regulatory-decision-making.pdf>  |
| 20 | Decommissioning, NS-TAST-GD-026 (Rev 4) |
| 21 | ONR Nuclear Safety Technical Inspection Guide – LC20 Modification to design of plant under construction, NS‑INSP‑GD-020 Revision 4, May 2016 |
| 22 | ONR Nuclear Safety Technical Inspection Guide – LC22 Modification or experiment on existing plant, NS‑INSP‑GD-022 Revision 4, January 2018 |
| 23 | ONR “Licensing Nuclear Installations”, 5th Edition, September 2019. |
| 24 | ONR Guide “Purpose and Scope of Permissioning”, NS-PER-GD-014 Revision 6 |
| 25 | Security Assessment Principles for the Civil Nuclear Industry, Revision 0, 2017 http://www.onr.org.uk/syaps/ |

1. GLOSSARY AND ABBREVIATIONS

ALARP As low as reasonably practicable

CAE Claims, arguments and evidence

DAP Duly Authorised Persons

DBA Design Basis Analysis

EIMT Examination, inspection, maintenance and testing

EKP.x (SAP) Engineering Key Principle number ‘x’

FA.x (SAP) Fault Analysis number ‘x’

GDA Generic Design Assessment

GSR General Safety Requirements (IAEA documentation)

HSWA74 The Health and Safety at Work etc Act 1974

IAEA International Atomic Energy Agency

IRR(s) Ionising Radiation Regulation(s)

LC.x Licence Condition number ‘x’

MHSAW Management of Health and Safety at Work

NT.x (SAP) Numberical Target number ‘x’

OSR Operational Safety Report

PCSR Pre-Construction Safety Report

POSR Pre-Operational Safety Report

PSA Probabilistic Safety Analysis

PSR Periodic Safety Review

QA Quality Assurance

REPPIR Radiation Emergency Preparedness and Public Information Regulations

RP Radiological Protection

SAA Severe Accident Analysis

SAP(s) Safety Assessment Principle(s)

SAR Safety Analysis Report

SC.x (SAP) Safety Case number ‘x’

ST.x (SAP) Siting number ‘x’

SFAIRP So far as is reasonably practicable

SQEP Suitably qualified and experienced person

SRL Safety Reference Level

SSR Specific Safety Requirements (IAEA documents)

SSC Structure, System and Component

SyAP(s) Security Assessment Principle(s)

TAG Technical Assessment Guide(s)

UK United Kingdom

WENRA Western European Nuclear Regulators’ Association

APPENDIX 1: COMMON PROBLEMS WITH SAFETY CASES

This appendix summarises some of the common problems with safety cases that have been encountered by ONR. They are grouped in accordance with the eight qualities of a safety case identified in the advice to inspectors section of this TAG.

The list below is not intended to be exhaustive. This appendix should be read in conjunction with Appendix 2 which has extracts from the Nimrod Review with respect to shortcomings in safety cases. Further specific learning relating to the Generic Design Assessment process is captured in [A1.1]. The Safety Case Forum also produce industry guidance on behalf of the Safety Directors’ Forum[[5]](#footnote-5), much of which seeks to address issues with safety case production. Inspectors should be aware of this guidance, which is published on the Safety Directors’ Forum webpages.

Significant or persistent issues with safety cases are indicative of underlying problems with the way they are produced. Inspectors should ensure that the causes of such problems are addressed, not just the symptoms. See NS-INSP-GD-014 [4] for further guidance.

**1 INTELLIGIBLE**

Much of the safety case is written in the form of a technical dissertation with insufficient attention paid to the needs of the users, hence the document does not provide a sufficiently clear view of the safety case to facilitate safe operation. This is frequently due to a lack of involvement of the likely users in the production and review of the safety case and/or the lack of a ‘usability’ test before the safety case is signed-off. There is a difference between a safety case being technically sound and being fit-for-purpose.

Excessive detail is presented in the head safety case document making it unnecessarily long. As a result, the significant safety claims and threads of the safety arguments cannot be readily found. This can be due to repetition or to a ‘cut and paste’ approach, where considerable information and detail are incorporated in the head safety case document rather than being referenced.

The auditable trail from the head document to key information in support of important safety claims can be difficult to follow. This includes inconsistencies between different parts of the case to an extent that safety arguments are ambiguous or undermined.

The problems above can be caused or exacerbated when large, complex safety cases are assembled by producing many documents that are reviewed and approved individually. The whole safety case is assumed to be fit-for-purpose when all the individual documents have been signed-off.

**2 VALID**

The claims and assumptions made in the safety case do not reflect the actual state of the facility. This may be due to as-built differences between the design and the actual facility, the effects of subsequent modifications and concessions, ageing and degradation effects, a lack of operator input or a lack of knowledge and familiarity of the facility by the safety case authors.

The safety case has insufficient consideration of the cumulative impact on safety due to modifications.

The safety case doesn’t take proper account of incidents that have occurred in the facility or elsewhere. Incidents are usually considered as part of longer term periodic review processes but there should be more direct links between OPEX systems and impact on the extant safety case.

**3 COMPLETE**

The safety case strategy and scope is inadequate. This can be due to time pressure and/or lack of consideration of viable options before deciding on the course of action. The resultant safety case may be technically correct but it is not the appropriate case for the circumstances.

ALARP arguments are presented retrospectively after decisions have been made and the ALARP justification is ‘tagged on’ at the end of a safety case. If there is inadequate consideration of options at the safety case strategy stage, or an inappropriate option is selected, the outcome is unlikely to satisfy ALARP requirements.

The fault analysis is incomplete or flawed due to: a lack of understanding of operational processes; inadequate consideration of fault scenarios; a failure to identify fault scenarios that may have important implications for nuclear safety (e.g. fire hazards); a superficial treatment of human factors; frequency claims for unlikely events that are unrealistically low; treatment of external hazards separately when they may be linked (e.g. earthquake and tsunami).

There is a failure to identify protection measures which are suitable and sufficient for the identified hazards.

The safety case confuses safety categorisation (the process of determining the safety significance of safety functions) and safety classification (the process of determining the level of technical rigour to be applied to structures, systems and components (engineering) and human based safety claims (human factors)). A failure to adequately deliver an overall safety function results.

The need to include in a safety case all structures, systems and components (SSC) important to meeting a safety function may not be recognised (e.g. the adequacy of service supplies for a facility may not be treated in a safety case).

If design targets or the numerical targets in the SAPs are shown to have been met, the design is claimed to be ALARP. It is not appreciated that an ALARP justification should show that the risks to workers and public have been reduced so far as is reasonably practicable, irrespective of whether the design targets or BSL and BSO levels have been met.

**4 EVIDENTIAL**

There is inadequate engineering substantiation because of a lack of evidence to support the safety functional requirement claims made in the safety case for engineering structures, systems and components.

Expert judgement is invoked where there is a lack of evidential support to safety case claims without sufficient rigour and challenge. Care is needed to ensure the use of judgement is appropriate, in the context of the safety case, and is duly conservative when dealing with uncertainty.

Conservatism is included in the safety case to address specific uncertainties. However, this conservatism is then eroded inappropriately to compensate for other uncertainties or weaknesses in the safety case. The greater the degree of uncertainty the less scope there is to try to ‘claw back’ the assumed margins.

At an early stage of a safety case, an unsupported assumption is made (e.g. two safety systems are sufficiently far apart in the context of fire safety) but later sections of the safety case treat the judgment as fact, despite there being no substantiation.

The safety case makes claims on the robustness of the plant and the ability of the operator to take appropriate and timely action, but with little or no substantiation for human factors aspects (including the effects of abnormal conditions).

**5 ROBUST**

The safety case does not specify clearly the safety case claims or engineering codes and standards that need to be met.

To compensate for difficulties in providing a sound engineering substantiation, the safety case makes inappropriate claims and/or ’trade-offs’. For example, over reliance is placed on probabilistic arguments or elaborate, complex or restrictive operating procedures are invoked. It should be recognised that there may be technical reasons why these may be necessary, and that they may not always be unacceptable, but such approaches should always attract additional scrutiny.

**6 INTEGRATED**

All the expected elements are present in a safety case but there is no clear ‘route map’ or indication to show how the different parts fit together.

Claims made on external services are not fully identified and there are no references to where evidence for such claims can be found.

**7 BALANCED**

The safety case reflects a ‘good news culture’, which can be indicative of an underlying assumption of safety. The safety case does not give sufficient emphasis to difficulties or areas of uncertainty that may be important for safety. These can be underplayed or argued away. Problems that should have been resolved to support the safety case can instead be deferred to a forward action plan with uncertain timescales for addressing the issues.

When expert judgment is invoked it usually provides a ‘positive’ answer in support of claims in the safety case, without the need for further work or investment to improve safety. On balance, there must be situations where appropriate use of judgement should conclude that the claims cannot be supported without improvements. The adage should be ‘assume it’s unsafe until proven safe’ rather than ‘it’s safe unless someone can prove it’s unsafe’.

The results of a PSA are sometimes used to justify ‘doing nothing’, instead of undertaking further work and investment in plant improvements. The analysis can look impressive but in reality is founded on insufficient or unreliable data. This is not made clear in the safety case (particularly the summary or head document) and decision makers therefore do not have a balanced view of the risks.

**8 FORWARD LOOKING**

The safety case for an ageing facility is based on the as-built design and does not take adequate account of ageing and degradation processes or modifications.

Measures required to maintain the safety case through life (e.g. EMIT, further work on unresolved issues) are not identified clearly.

**References:**

A1.1 New Nuclear Power Plants: Generic Design Assessment Technical Guidance, ONR-GDA-GD-007 (Rev 0), May 2019

APPENDIX 2: NIMROD REVIEW - SAFETY CASE SHORTCOMINGS & TRAPS

**1 INTRODUCTION**

An independent review into loss of RAF Nimrod XV230 over Afghanistan in 2006, which resulted in the deaths of 14 servicemen, was chaired by Charles Haddon-Cave QC. The report was published in 2009. It is wide-ranging and includes a comprehensive dissection of the problems and shortcomings of the safety case for the Nimrod aircraft. The report has major relevance to anyone involved with safety cases, not least ONR and nuclear dutyholders.

The more generic types of shortcomings and traps with safety cases identified in the Nimrod Review are reproduced below. This encompasses work by Dr Tim Kelly of the University of York and endorsed by Charles Haddon-Cave in his report.

It is not sensible to set out here the full account of safety case issues detailed in the Nimrod Review. Instead, inspectors should read the relevant sections of the report for themselves to understand the extent of the issues and the wider relevance. The safety case aspects are covered in Chapters 9 to 11 and 22. It is a well-structured and readable report, with good summaries at the start of each chapter.

See the link below to access the report:

 <https://www.gov.uk/government/publications/the-nimrod-review>

**2 SAFETY CASE SHORTCOMINGS**

Charles Haddon-Cave identified the following shortcomings common to safety Cases:

*(1) Bureaucratic length*

Safety Cases and Reports are too long, bureaucratic, repetitive and comprise impenetrable detail and documentation. This is often for 'invoice justification' and to give Safety Case Reports a 'thud factor'.

*(2) Obscure language:*

Safety Case language is obscure, inaccessible and difficult to understand.

*(3) Wood-for-the-trees:*

Safety Cases do not see the wood for the trees, giving equal attention and treatment to minor irrelevant hazards as to major catastrophic hazards, and failing to highlight, and concentrate on the principal hazards.

*(4) Archaeology:*

Safety Cases for 'legacy' platform often comprise no more than elaborate archaeological exercises of design and compliance documentation from decades past.

*(5) Routine outsourcing:*

Safety Cases are routinely outsourced by Integrated Project Teams (IPTs) to outside consultants who have little practical knowledge of operating or maintaining the platform, who may never even have visited or examined the platform type in question, and who churn out voluminous quantities of Safety Case paperwork (`bumpf[[6]](#footnote-6) ’ and outsized GSN (Goal Structured Notation) charts) in back offices for which IPTs are charged large sums of money.

*(6) Lack of vital operator input:*

Safety Cases lack any, or any sufficient, input from operators and maintainers who have the most knowledge and experience about the platform. ….any review of the Nimrod Safety Case (NSC) "must involve appropriate air and ground crews in order to ensure that current practices are fully understood; those personnel, after all, both know most about how our aircraft are operated and flown, and also have the greatest personal interest in having levels of safety with which all involved are comfortable."[[7]](#footnote-7) Operators at RAF Kinloss were not even aware of the existence of the original Nimrod Safety Case.

*(7) Disproportionate:*

Safety Cases are drawn up at a cost which is simply-out of proportion to the issues, risks or modifications with which they are dealing.

*(8) Ignoring age issues:*

Safety Cases for 'legacy' aircraft are drawn up on an 'as designed' basis, ignoring the real safety, deterioration, maintenance and other issues inherent in their age.

*(9) Compliance only:*

Safety Cases are drawn up for compliance reasons only, and tend to follow the same, repetitive, mechanical format which amounts to no more than a secretarial exercise (and, in some cases, have actually been prepared by secretaries in outside consultant firms). Such Safety Cases tend also to give the answer which the customer or designer wants, i.e. that the platform is safe.

*(10) Audits:*

Safety Case audits tend to look at the process rather than the substance of Safety Cases.[[8]](#footnote-8)

*(11) Self-fulfilling prophesies:*

Safety Cases argue that a platform is 'safe' rather than examining why hazards might render a platform unsafe, and tend to be no more than self-fulfilling prophesies.

*(12) Not living documents*:

Safety Cases languish on shelves once drawn up and are in no real sense 'living' documents or a tool for keeping abreast of hazards. This is particularly true of Safety Cases that are stored in places or databases which are not readily accessible to those on Front Line who might usefully benefit from access to them. (The NSC was only fully accessible from one computer terminal at BAE Systems at Chadderton).

**3 SAFETY CASE TRAPS**

Charles Haddon-Cave commented that the above criticisms are not new, nor confined to Safety Cases for military platforms. He also highlighted an article entitled ‘Are Safety Cases Working?’[[9]](#footnote-9) by Dr Tim Kelly of the University of York. This listed seven examples or ‘traps’ to avoid. Charles Haddon-Cave suggested that the article should be compulsory reading for many of the current purveyors of Safety Cases and these are the ‘traps’ reproduced from the report:

*(1) The “Apologetic Safety Case”:*

Safety Cases which avoid uncomfortable truths about the safety and certifiability of systems in production so that developers do not have to face the (often economically and politically unacceptable) option of re-design (“X doesn’t quite work as intended, but it’s OK because...”).

*(2) The Document-Centric View:*

Safety Cases which have as their aim to produce a document. Dr Kelly describes this as ‘the biggest bear-trap’. The goal of Safety Cases should not simply be the production of a document; it should be to produce a compelling safety argument. We should not be reassured by “paper, word-processor files, or HTML documents”. There was a danger of “spending a lot of money to produce a document” of no safety benefit.

*(3) The Approximation to the Truth:*

Safety Cases which ignore some of the rough edges that exist. For example, Safety Cases which claim in a Goal Structured Notation diagram that ‘All identified hazards have been acceptably mitigated’[[10]](#footnote-10) and direct the reader to the Hazard Log when, in reality, the mitigation argument is not so straightforward.

*(4) Prescriptive Safety Cases:*

Safety Cases which have become run-of-the-mill or routine or simply comprise a parade of detail that may seem superficially compelling but fails to amount to a compelling safety argument.

*(5) Safety Case Shelf-Ware:*

Safety Cases which are consigned to a shelf, never again to be touched. The Safety Case has failed in its purpose if it is “so inaccessible or unapproachable that we are happy never to refer to it again.”

*(6) Imbalance of skills:*

The skills are required of both someone to develop the Safety Case and someone to challenge and critique the assumptions made. Too often, the latter skills are missing.

*(7) The illusion of pictures:*

People are ‘dazzled’ by complex, coloured, hyper-linked graphic illustrations such as Goal Structured Notation or ‘Claims-Arguments-Evidence’ which gives both the makers and viewers a warm sense of over-confidence.[[11]](#footnote-11) The quality of the argument cannot be judged by the node-count on such documents or number of colours used.

APPENDIX 3: GUIDANCE ON THE RELATIONSHIP BETWEEN STAGES OF A NUCLEAR FACILITY LIFE-CYCLE AND THE ASSOCIATED SAFETY CASES

This appendix provides guidance to ONR assessors on the relationship between the potential principal stages in the lifecycle for a facility and the associated safety cases.

## 1 Preamble

ONR does not impose any particular model of facility lifecycle, nor does it mandate a specific model of which safety cases it requires and what their precise content should be. Instead, it recognises that different facilities may require different approaches.

In general, the organisation undertaking the development (licensee, requesting party, etc.) purposes a facility lifecycle which recognises the need for a staged approach to safety case submissions, and ONR ensures that this meets their regulatory needs. This will include appropriate regulatory hold points and sufficient time for ONR assessment and permissioning activities to be agreed with ONR.

The approach to design development and safety case evolution may be dependent on a number of factors including nature of the facility in question, precedent, regulatory expectations and dutyholder requirements. These strategic aspects fall under ONR permissioning guidance for submissions [A3.1, A3.2] rather than assessment guidance. ONR assessors must ensure that they are clear how assessment work that they carry out fits into the project strategy.

The strategy for safety case evolution should align with the project objectives at each stage of the project. The safety case scope should be defined for each stage in advance.

Within this annex, this is illustrated using some generic terms for the various stages of the facility lifecycle and for the safety case submissions. This is to illustrate how early engagements give some reduced regulatory risk for the licensee, but also gives the regulatory opportunities to influence the project before options are closed out. It is assumed that each stage builds upon the information in the preceding stage. Further guidance on regulatory expectations in the context of Generic Design Assessment is given in [A3.3].

## 2 SIMPLE MODEL OF Lifecycle STAGES AND SAFETY CASE SUBMISSIONS

The figure below (Figure A3.1) shows an example, based on a complex project, such as a nuclear power station design/build to illustrate this annex. The terms used are further developed throughout this section.

In the figure, it is assumed that there are a number of specific lifecycle stages from “Early design” to “Post decommissioning”. The operating organisation (or licensee, requesting party, etc.) has defined a through-life safety case strategy, which has the benefit for them of allowing them to get regulatory feedback on important aspects of their project, so that they can reduce their regulatory uncertainty. There has been interaction with the regulator (specifically ONR, but may include other regulators) so that the regulator can ensure sufficient regulatory influence to discharge their responsibilities to stakeholders, including the public.

The figures shows that safety case submissions in advance of key changes in risks. In reality, there may also be the need for ONR to request that submission dates allow ONR adequate timescales for assessment activities and decision making processes. Each stage is expanded upon in the following sections.



**Figure A3.1**: Simple model of lifecycle stages and safety case submissions. Titles of different stages are illustrative of what might be used.

## 3 Generic lifecycle stages

For the simple model in this annex, the lifecycle stages and their purposes are described below. Further generic considerations that apply across all lifecycle stages are given later in this section.

### Early design

In this lifecycle stage, the operating organisation sets the design philosophy, outlines the design options and justifies the ones chosen. They may give a description of the resultant conceptual design to regulators and engage on the safety case strategy. The case should broadly outline how relevant safety principles and criteria are likely to be achieved to demonstrate that the facility can be managed safely throughout its lifecycle.

Safety cases associated with this lifecycle stage may have titles such as Design Safety Concept, Preliminary Safety Report (PSR), Paper of Principle (PoP), etc. Many of the drivers at this stage will be internal to the company (licensee, requesting party, operating organisation), but sharing early design safety cases with the regulator may have advantages both for project planning purposes and to understand potential project and regulatory risks.

It is normal to specify the site characteristics at an early stage of design. These are important to a range of design considerations, such as civil foundations and drainage requirements, and also to the challenges from external hazards. In some major projects such as the nuclear new build programmes, “generic siting envelopes” have been proposed to give bounding conditions for design, but there is still a need for site-specific information to feed into later safety case submissions.

Also at this stage, or the subsequent pre-construction stage, the operating organisation should identify and explain any novel features, or deviations from modern international good practices, and their importance to safety.

### Pre-Construction and Installation

This is an important lifecycle stage since at this point a paper design starts to become physical reality. It is therefore important that the safety case demonstrates that the detailed design proposal will meet the safety objectives before construction or installation commences. At this stage sufficient analysis and substantiation of safety function claims should have been performed to prove that the plant can be safely operated, otherwise there are significant project and regulatory risks. The facility design would normally be expected to be ‘frozen’ at this point (or equivalent[[12]](#footnote-12)), and design changes subject to a formal change control process to allow adequate consideration of their impact on facility safety/operation.

This lifecycle stage may cover a series of separate sub-stages. Even when the operating organisation commits to a project, there may be details to work out on the precise design, and some aspects of design may lead others. Any outstanding confirmatory work should be clearly identified.

Safety cases associated with this lifecycle stage may have titles such as Pre-Construction Safety Report (PCSR), or Pre-commencement Safety Report, etc. The safety case should provide detailed descriptions of system architectures, their safety functions and reliability and availability requirements, and it should also confirm and justify the design codes and standards that have been used and where they have been applied, along with any non-compliances and their justification.

At either this stage or the previous one, ONR may require the operating organisation to provide confidence on a variety of project-wide aspects that will flow through the remainder of the project. This will include:

* information on the quality management arrangements for the design, including (but not limited to):
* Standards and design codes to be applied and demonstration of how they are met;
* Design controls, control of standards, validation and verification, and interface between design and safety;
* Safety case development processes, including peer review arrangements and nuclear safety assurance;
* Quality management system for development of the safety case and design.
* information on radioactive waste management and decommissioning strategies.

### Pre-Operation

This lifecycle stage is likely to be the end of installation and start of plant commissioning. Again this stage may include several sub-stages. In particular, the strategy may choose to designate “inactive” commissioning work, in which risks are related to conventional safety only, from “active commissioning” work in which nuclear material or radioactive isotopes are present. This is an important lifecycle stage since this is the point at which the plant presents nuclear or radiological risks.

Safety cases associated with lifecycle stage may have titles such as pre-Inactive Commissioning Safety report (PICSR), Pre-Active Commissioning Report (PACSR), Pre-Operational Safety Report (POSR), etc. The purpose of these safety cases will be to demonstrate:

* that the facility as-built meets relevant safety criteria and is capable of safe operation;
* that the active commissioning activities can and will be carried out safely and that the operating procedures for commissioning are supported by the safety case;
* that a programme of safety commissioning activities have been produced that will, as far as practicable:
* demonstrate the safe functioning of all systems and equipment,
* prove all safety claims on equipment will be delivered,
* confirm the effectiveness of safety related procedures.
* ensure that there are no aspects of nuclear or radiological safety that remain to be demonstrated after active commissioning.

Particularly in the active commissioning mode, many of the aspects of the operational safety case (see later) will need to be in place. In particular, operating procedures will need to have been developed, and these need to also be compatible with the limits and conditions necessary in the interest of safety. In fact, commissioning operating procedures may be more onerous than those that will be in the operating safety case, because of the need for additional assurance in commissioning. These aspects of the future operational safety case may be embedded in a commissioning safety report or described in a pre‑operational safety case. If there are any aspects of safety demonstration that cannot be demonstrated at a particular sub-stage, a safety justification and clear plan for future commissioning work should be present.

### Operation

This lifecycle stage is the main operational phase of the plant or facility.

Safety cases associated with this lifecycle stage may have titles such as Facility Safety Case (FSC), Station Safety Case (SSC), Station Safety Report (SSR), etc. In most cases, especially for complex plants or facilities, the operational safety case will be hierarchical, and in some cases separate cases within this hierarchy may apply at different times (for example the hierarchy may include safety cases for operational modes and for shutdown modes).

In some cases, the safety case will only cover a defined period – for example where there are known time-dependent mechanisms that mean re-validation of the basis of operation will be necessary (possibly following inspection or other evidence gathering).

The purpose of the operational safety case will be to demonstrate:

* that the facility as-built meets relevant safety criteria and is capable of safe operation;
* that the operating procedures provide sufficient control that operations will remain within the limits and conditions of safe operation;
* compliance with the legal duty to reduce risks to workers and the public SFAIRP.

Since the operational phase may be quite lengthy, it is unlikely that the safety case will remain unchanged throughout. There may be modifications to plant, equipment failures, or an improved understanding of underpinning safety case information. The operational safety case may need to be updated as necessary to take account of any changes, and ensure that there is still a valid safety case for operations.

### Post Operation

This lifecycle stage is assumed to be immediately after the end of the operational phase, at a time when post operational clean out (POCO) activities and care and maintenance activities will be carried out prior to the start of decommissioning.

There may be significant overlap between the post-operations lifecycle state and the Operations and Pre-Decommissioning lifecycle stages, and licensees may not distinguish between them. For example, it is common for POCO to be conducted under the Operational Safety Case, with modifications as required. Should the licensee make significant changes to the safety case during POCO, the inspector should check to see if this constitutes decommissioning, and whether a decommissioning safety case is expected.

Safety cases associated with this lifecycle stage may have titles such as Post-Operational Safety Case (POSC), Post-Shutdown Safety Case, or similar. Their purpose would be:

* To demonstrate that the facility is adequately safe for the activities planned prior to start of decommissioning, and that plant and equipment necessary for safety remains in adequate condition and is maintained as such until it is no longer needed;
* that the operating procedures relevant after the end of operations continue to provide sufficient control that operations will remain within appropriate limits and conditions of safety;
* To provides evidence of optioneering to underpin the scope of future work, and how this has formed the hazard and waste management strategies for this and subsequent stages.

### Pre-Decommissioning

This lifecycle stage represents a more strategic phase which is particularly relevant for complex decommissioning projects. It is intended to represent a stage in which decisions are made on how safety will be managed through the proposed decommissioning programme for the project. As previously stated, the licensee may choose not to distinguish between this stage and the Post-Operation lifecycle stage.

The timing of the decommissioning should be rigorously justified, but should occur promptly where this is reasonably practicable. Should decommissioning need to be deferred (eg if there is a net safety benefit in doing so), then this should be explicitly justified in the safety case as appropriate. The safety case should justify the continuing safety of the facility for the period prior to its decommissioning (SAP DC.3).

Where adequate levels of safety cannot be demonstrated, prompt decommissioning should be carried out and, where necessary, prompt remedial and operational measures should be implemented to reduce the risk.

Safety cases associated with this lifecycle stage may have a titles such as Safety Strategy Overview, or similar. At a high level, it should describe how safety will be managed through the proposed decommissioning programme for the project. The purpose would be:

* To demonstrate that there will be a progressive, timely and systematic reduction of hazard.
* To define safety goals and criteria for the project as a whole.

### Decommissioning

This lifecycle stage represents the main phase (or phases) of decommissioning. The licensee may recognise reductions in potential consequences especially to the public. There may however be more “hands-on” activities with potential for worker exposure. The changes in risk profile at this lifecycle stage may lead the licensee to make wide-ranging changes to their safety case arrangements. These changes would fall under ONR permissioning guidance rather than assessment guidance, and when agreed will influence which safety cases ONR assess and to what depth.

The safety cases and associated documents relating to this lifecycle stage may have a titles such as Decommissioning Strategy, Safety Case for Decommissioning Operations, or similar. Additionally individual safety cases for certain decommissioning tasks may be necessary.

Decommissioning Strategy cases would document a more detailed strategic approach to be followed during decommissioning.

* To demonstrate that there will be a progressive and systematic reduction in hazard;
* That appropriate infrastructure and resources are maintained to allow the proposed decommissioning activities to be carried out.

Safety Cases for Decommissioning Operations may be developed for phases of decommissioning in which a variety of tasks are to be carried out to achieve a decommissioning objective. These cases would define safety goals and criteria for the decommissioning tasks covered by, and show what controls and procedures will be provided to allow the tasks to be carried out safely.

Safety cases for individual decommissioning tasks will provide the safety justification for each of the potentially many very small, short jobs. These include risk assessments, method statements and peer reviews, and can be developed under procedures similar to those for small modifications to the facility.

### Post-Decommissioning

This lifecycle stage is related to site closure. There may be additional legal requirements associated with this lifecycle stage, such as environmental submissions, but these are not related to this assessment guidance.

The nuclear/radiological safety case (which may be called a Post-Decommissioning Clearance Safety Case) will be written to demonstrate that there has ceased to be any danger from ionising radiation from anything on site.

## 4 Considerations that apply through the various lifecYCLe phases:

### Flow through from one life-cycle stage to the next

The lifecycle model assumes that issues unresolved at early design is addressed in pre‑construction, and those in pre-construction addressed prior to operating. There is a need to show (as examples):

* Claims made in the preliminary safety report, or any outstanding issues are resolved in the preconstruction safety report, or carried forward (at increasing regulatory risk) to be resolved before operation;
* That the design intent of the preliminary safety report has been met by the more detailed design in the preconstruction safety report;
* That safety objectives set in the preliminary safety report are substantiated by the evidence, including engineering substantiation of later safety submissions

### ALARP and Optioneering

There is also a flow through of issues related to ALARP. At early design stages, the design concept selected should be capable of reducing risks SFAIRP. As the design progresses there is a need to document the evidence that this is being achieved through design and by the development of appropriate operating procedures and practices. Documenting both the options adopted and those rejected is important in design stages, but some detail may be relegated to supporting material of the safety case document hierarchy in later lifecycle stages

### Periodic review

In general periodic review processes will commence at the start of operations. These will look at the condition of the plant, changes in standards, operational experience (OPEX) etc., and project the safety case forward into the next period of operating and to future lifecycle phases. The review should provide confidence in the safety adequacy of the plant going forward, and provide a strategic look forward for contingency requirements. More detailed guidance is given in the ONR TAG on periodic safety reviews [A3.4].

In some cases, operating organisations have chosen to adopt a periodic review process during the construction phase. This has been to provide confidence in the condition of plant and its suitability for operation prior to operation.

## References:

|  |  |
| --- | --- |
| A3.1 | ONR Guide - Purpose and Scope of Permissioning, NS-PER-GD-014 Revision 6 |
| A3.2 | ONR “Licensing Nuclear Installations”, 5th Edition, September 2019. |
| A3.3 | New Nuclear Power Plants: Generic Design Assessment Technical Guidance, ONR-GDA-GD-007 (Rev 0), May 2019 |
| A3.4 | ONR Nuclear Safety Technical Assessment Guide - Periodic Safety Reviews (PSR), NS-TAST‑GD-050 Revision 7, July 2017 |

APPENDIX 4. CLAIMS ARGUMENTS EVIDENCE STRUCTURES WITHIN THE SAFETY CASE

The structure within the safety case should be carefully considered, and should be implemented in such a way that the resulting safety case flows and is easily understood by its target audience. This appendix gives further information on a claims arguments evidence (CAE) mindset and its application, including example structures and approaches.

It is worth reiterating that ONR does not prescribe the approach to structuring a safety case. The example schemes presented here may be useful for certain facility types or disciplines. Variations may be appropriate to optimise application. For example, the use of a defined CAE structure as the primary presentation technique may be more readily applicable for requirements-based aspects of the safety case (eg engineering and systems) than for complex safety analysis that is better supported by other well recognised techniques.

Appropriate use of a CAE creates a mindset that can provide advantages in effectively building and presenting an adequate safety case to demonstrate that risks have been reduced ALARP. The key aspects of this mindset are: explicitly defining what the case is trying to argue, understanding what claims this depends on, and showing that the planned or available evidence is sufficient to support the claims. In other words, every claim must be supported by evidence, and evidence has no value unless it is appropriately linked to a claim. CAE can potentially highlight any weaknesses, uncertainties or gaps in the overall safety demonstration (marked by missing or insufficient claims, arguments and/or evidence).

A CAE mindset might contrast with, for example, compliance that relies on strictly following a set standard or process, without considering whether this adequately reduces risks or the value and relevance of constituent requirements.

CAE can be particularly useful for planning a safety case because it can describe the purpose and requirements of evidence that has yet to be produced.

Detailed notations and rules, supported by automated tools, can facilitate more rigorous and consistent application of a CAE structure, but are only helpful when following and serving the application of a CAE mindset rather than attempting to drive it. Dutyholders have found that programmes for adoption of CAE structures led by tool use have been unproductive because of a failure to understand and apply the above fundamental concepts. In addition, a detailed CAE structure can give an illusion of proficiency and rigour that is unfounded without effective challenge and grounding in reality, as highlighted in Appendix 2.

Demonstrating that a claim is valid will generally involve different roles and teams. A CAE structure may provide an effective mechanism for effective communication and clarification between all the people and teams that need to work together to build the complete case. The CAE structure may make use of other approaches at particular points; for example, the fault schedule can be a powerful tool for linking engineering claims to the fault analysis.

*Example CAE structure and rules*

Claims are generally structured in a hierarchy. Often it is helpful to formulate a top-level claim that is a statement of the overall contention for the scope of the safety case under development. Example top level claims are:

* Dosing the fuel storage pond with sodium hydroxide is beneficial to safety, and all associated nuclear safety risks have been reduced to as low as is reasonably practicable;
* It is safe to restart the reactor with the graphite in its current condition, and operate for a period of X years at normal operational thermal powers.

Note that these claims may contain terms (such as “it is safe” and “current condition”) that can be made more precise in supporting lower level claims.

Alternatively, a case may have a small set (eg between 3 and 8) of top level claims that follow a general template.

Claims can be broken down into lower level claims (subclaims) that should together be equivalent to the original claim above them, in the context of the specific circumstances of the case.

Evidence is the information that demonstrates that a claim is true. In other words, evidence successfully closes out a claim. In a safety case, this is usually presented in terms of a reference to a document(s) or part of a document(s) where the information can be found. For the evidence to be relevant and sufficient, it has to be closely related to the claim it supports. Hence each bottom-level claim should be drafted with the available evidence in mind, or evidence should be created specifically for its target claim(s).

Arguments relate claims with evidence. One way to view the argument is as the set of (sub)claims that together link a higher-level claim to the available evidence. These can be expressed as an explicit claim structure, as textual discourse or some combination of the two. A detailed explicit claim structure can provide greater rigour and clarity, but can also lead to increased complexity and loss of comprehension. Hence a balance must be struck or it may be appropriate to provide both perspectives.

Alternatively, the term argument may be used to denote the extra elements (or reasoning rules) needed to justify the links between claims and their subclaims, and, if necessary, between bottom-level claims and their evidence. Recent IAEA guidance for control and instrumentation systems [Ref A4.1] takes this approach. The arguments should include documented assumptions, limitations and context appropriate to the specific case, and supporting information that makes the link applicable.

Links between claims and their subclaims (or evidence) can be characterised by standard reusable arguments, depending on how the claim is broken down. One example approach [Ref A4.2] for breaking down claims can be summarised as:

* refine (into more specific and precise terminology),
* substitute (with different but equivalent claims),
* divide (into lower-level constituents),
* calculate (based on contributing values) or
* terminate (with evidence).

Effective construction of a CAE structured case is usually achieved by devising appropriate claims top-down from the overall objective, creating subclaims that can be backed by available or realistically producible evidence. A secondary bottom-up perspective, to see what claims the available evidence may support and how relevant it is, helps ensure the available evidence is fully utilised. Multiple legs with diverse evidence are often necessary, recognising that some legs will provide greater confidence than others. Additional technical perspectives may be needed, to ensure for example that the case demonstrates adequacy against the requirements for every relevant technical discipline. Claims and arguments should

be verified and corrected as the evidence becomes available. Generally, substantial iteration is required to reach an optimal structure.

Different groups within the dutyholder may take responsibility for particular claims (which for them become their top claim). For example, a control and instrumentation specialist team may take responsibility for substantiating that a computer based safety system behaves and performs according to the claims made for it in the safety case.

CAE can be presented using predefined notations and rules (for examples, see Ref A4.2, A4.3) and automated tool support is also available. The presentation can be graphical, tabular and/or text-based, and in practice an optimal solution will often combine these. However, it is important that the case is understandable and useable in its given context and does not provide false confidence through complexity alone (a key finding of the Haddon-Cave report summarised in Appendix 2).

Useful questions for an ONR inspector to consider are:

* Is the case understandable and useable?
* Is the top level claim well matched to the overall safety objective?
* Is the scope of the top level claim (and/or its next tier supporting claims) explicit and appropriate (for example in terms of the boundaries between what is within the case’ control and assumptions outside its control)?
* Is the set of claims complete (do they cover every area relevant to the case)?
* For each claim of interest, are its subclaims an appropriate decomposition (eg in terms of sufficiency and completeness)?
* Is every bottom-level claim of interest adequately supported by appropriate evidence?
* Is every piece of offered evidence sufficiently compelling support for the claim (rather than just information) and does it actually match the real world situation?
* Does the case include and address relevant counter claims, evidence and arguments – has sufficient critical thinking been applied?
* Are all relevant assumptions documented and justified?
* Does the overall structure provide adequate confidence?

**References**

|  |  |
| --- | --- |
| A4.1 | Dependability assessment of software for safety instrumentation and control systems at nuclear power plants, IAEA Nuclear Energy Series NP-T-3.27 |
| A4.2 | Claims, arguments and evidence (CAE). [https://claimsargumentsevidence.org](https://claimsargumentsevidence.org/) |
| A4.3 | Goal structuring notation (GSN). <https://www.goalstructuringnotation.info/> |

1. For the purposes of this guide, no significant differentiation is made between nuclear and radiological safety and the two may be used interchangeably in some instances. [↑](#footnote-ref-1)
2. IRR - Ionising Radiation Regulations 2017, REPPIR - Radiation (Emergency Preparedness and Public Information) Regulations 2019, COMAH – Control of Major Accident Hazards 2015 (enforced by a competent authority comprising ONR and the appropriate environmental agency), MHSAW - Management of Health and Safety at Work Regulations 1999, HSWA – Health and Safety at Work etc Act 1974. [↑](#footnote-ref-2)
3. The IAEA use of the term “safety assessment” is interpreted in this TAG as being a significant component of the safety case. [↑](#footnote-ref-3)
4. SyAPs – ONR’s Security Assessment Principles [25] [↑](#footnote-ref-4)
5. The Safety Directors’ Forum is a voluntary organisation with a vision to promote and maintain a safe, secure, sustainable UK Nuclear Industry. To help achieve this vision, it produces and issues guidance to the nuclear industry. <https://www.nuclearinst.com/Safety-Directors-Forum> [↑](#footnote-ref-5)
6. The term used by one of BAE Systems’ employees drawing up the Nimrod Safety Case in 2004 [↑](#footnote-ref-6)
7. BOI (Board of Inquiry) Report, Part 5, Commander-in-Chief Air Command’s Comments dated 2 November 2007. [↑](#footnote-ref-7)
8. Charles Haddon Cave referred to Lord Cullen when quoting the evidence of a number of witnesses, including Major Holden, Transport Safety Consultant, formerly Inspector of Railways, who drew attention to weakness in auditing: *“My concern has been that there has been a lack of penetration in the audits, which have tended to chase paper trails rather than check that what should be going on on the ground is, in fact, going on. This lack of penetration may, in part, be due to the lack of skill of the auditors but it may also lie in the belief that all that is required is a pure compliance audit of the accepted safety case. The vital question as to whether or not the safety case itself is adequate and appropriate to the circumstances is seldom asked”.* [↑](#footnote-ref-8)
9. Safety Critical Systems Club Newsletter, Volume 17, No. 2, January 2008, pages 31-3 [↑](#footnote-ref-9)
10. *i.e.* the argument has become bald assertion or ‘meta-discussion. [↑](#footnote-ref-10)
11. Some Goal Structured Notation diagrams are yards long and cover an entire wall. Rather than being merely one aid to structured thinking, Goal Structured Notation appears to have become an end in itself. [↑](#footnote-ref-11)
12. The nature of the particular project may influence the point at which the design (or stages of the design) is frozen. Further guidance in the context of generic design assessment is given in [A3.3]. [↑](#footnote-ref-12)