Office for Nuclear Regulation

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 Revision 4		
Date Issued:	July 2016	Review Date:	July 2019
Approved by:	Graham Heys	Professional Lead	
Record Reference:	Trim Folder 1.18.1211. (2016/230683)		
Revision commentary:	This is a "minor refresh" and has been updated to be fully compatible with ONR Safety Assessment Principles 2014. It incorporates minor additional explanations. A more extensive update is in preparation, but will need some stakeholder engagement prior to issue. In the meantime the current version is fit for purpose.		

TABLE OF CONTENTS

Published 07/16

1. INTRODUCTION

1.1 This technical assessment guide is guidance to ONR inspectors on the purpose, scope and content of safety cases.

1.2 The previous update brought in developments in ONR thinking, particularly following the Haddon-Cave report into the Nimrod crash [1]. This revision is another evolutionary update with changes made to ensure full compatibility with the 2014 major revision of the Safety Assessment Principles [2].

2. PURPOSE AND SCOPE

2.1 The purpose of this document is to provide ONR inspectors with broad guidance on safety cases. The guide sets out the purpose of nuclear safety cases and expectations on how they are used, their overall qualities, how they may be structured and what information they should contain.

2.2 Guidance is also provided on common problems with safety cases based on ONR's experience (Appendix 1). Safety case shortcomings identified in the Nimrod Review are set out in Appendix 2.

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

2.4 The guide does not address the following in any depth:

- arrangements for the production of safety cases and the implementation of these arrangements;
- periodic reviews of safety cases;
- specific activities that safety cases cover;
- environmental and non-nuclear safety issues that licensees may include in safety cases.

2.5 More detailed guidance is given elsewhere e.g. assessment guide NS-TAST-GD-050 [3] and inspection guides NS-INSP-GD-014 [4] and NS-INSP-GD-015 [5].

2.6 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 licensee 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 the suite of Technical Assessment Guides.

2.7 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 licensees and other stakeholders the standards that ONR expects to be met in safety cases.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

LICENCE

3.1 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, respectively.

3.2 For the whole of a facility's life cycle, the safety of any activity must be substantiated and documented. Exceptions are only permitted for unforeseen events and emergencies when rapid responses are needed for safety purposes. With well-planned safety management arrangements such events should be extremely rare, but when they arise they need to be handled within the context of emergency arrangements that require as far as practicable risk assessments to be undertaken, responses planned and records made at the time.

OTHER RELEVANT LEGISLATION

3.3 In addition to the nuclear licence condition requirements, safety documentation may be required under other legislation (e.g. IRR 1999, REPPIR 2001, MHSAW 1999) or to meet the requirements of other regulators (e.g. EA, SEPA).

3.4 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. In judging whether licensees have complied with their legal duties ONR makes use of the risk management procedures explained (for example) in Reducing Risks, Protecting People document. The fundamental requirement is that the safety case should demonstrate how risks are reduced to levels that are As Low As Reasonably Practicable (ALARP).

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

SAPS

4.1 The Safety Assessment Principles for Nuclear Facilities (SAPs) [2] 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 of [2]) 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). As identified in the Application of the SAPs Section and The Regulatory Assessment of Safety Cases Section of the SAPs, during safety case assessment inspectors should use the principles proportionately commensurate with the radiological hazards presented.

4.2 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 [2]). 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.

WENRA REACTOR SAFETY REFERENCE LEVELS

4.3 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 Reference Safety Levels (RSLs), 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 RSLs [6] are identified as Relevant Good Practice for existing Civil Nuclear Reactors (see section 4 of [7]).

4.4 Safety cases are directly addressed in Issue N of WENRA's report on reactor Reference Safety Levels [6]. "Contents and updating of safety analysis report (SAR)". 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 appendix (Issue N) within the WENRA RSLs provides some useful guidance and has been taken into account in this guidance.

IAEA SAFETY STANDARDS

4.5 IAEA General Safety Requirements, GSR Part 4, 2009, "*Safety Assessment for Facilities and Activities*" [8] states that Safety Assessments (safety cases) are to be undertaken as a means of evaluating compliance with safety requirements (and thereby the application of the 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, 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 is provided in IAEA reports (e.g. [9] and [10]).

ADVICE TO INSPECTORS

5. DEFINITION OF A NUCLEAR SAFETY CASE

5.1 The guidance in the SAPs identified 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.'[2].

5.2 The term 'nuclear safety case' may relate 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. The licensee may wish to produce holistic safety cases in which both nuclear and non-nuclear risks are considered. However, since this guidance applies specifically to nuclear safety aspects, the term 'nuclear safety case' is shortened to safety case.

6. THE PURPOSE OF A SAFETY CASE

6.1 The primary purpose of a safety case is to provide the licensee with the information required to enable safe management of the facility or activity in question. Therefore it should be understandable to and useable by those with direct responsibility for safety. The SAPs say:
"*The process for producing safety cases should take into account the needs of those who will use the safety case to ensure safe operations. It is essential that the safety case documentation is clear and logically structured so that the information is easily accessible to those who need to use it (see paragraph 87). This includes designers, operations and maintenance staff, technical personnel and managers who are accountable for safety*…"[2]

6.2 A safety case should communicate a clear and comprehensive argument that a facility can be operated or that an activity can be undertaken safely. The safety case for a facility or activity should demonstrate that the associated risk and hazards have been assessed, appropriate limits and conditions have been defined and adequate safety measures have been identified and put in place.

6.3 In particular, the purpose of a safety case is described in para 101 of the SAPs[2]:

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'[1] 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.

[1] For additional guidance on defence in depth, see [2], in particular SAP EKP.3 and associated guidance paragraphs 149-152.

6.4 The safety case is a key element to enable safe management of the facility or activity in question. It is important to those who interact directly with the facility, for example the operators who control the conditions within the facility and those who maintain the facility. It is also important to senior management who are responsible and accountable for safety. They rely upon the safety case for accurate and objective information on risks and control measures to make informed decisions that may affect safety. Therefore, the key users of the safety case should be involved in its development, production/review and implementation.

6.5 The safety case should be a living document which is subject to review and change as time proceeds. For example, the safety case may change due to important changes to the facility, its mode of operation, or the understanding of safety related issues. It may also change in the light of operating experience or periodic review.

7. 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;

7.1 Intelligible

The safety case should be intelligible and structured logically to meet the needs of those who will use it (e.g. operators, maintenance staff, technical staff, managers accountable for safety). To achieve this:

- There should be a sufficient description of the facility, its purpose and its operation, to serve the purpose of the safety case.
- All descriptions and terms should be easy to understand by the key users.
- All arguments should be cogent and be developed coherently.
- All references and supporting information should be identified and be easily accessible.
- There should be a clear trail from claims through the arguments to the evidence that fully supports the conclusions, together with commitments to any future actions.
- Operational requirements, including maintenance, etc. should be clearly defined.

7.2 Valid

- A safety case should accurately represent the current status of the facility in all physical, operational and managerial aspects.
- It should reflect changes that have arisen from previous modifications, revised operating methods, operating experience, examination and test results, different analytical methods and periodic reviews.
- For new facilities or modifications, the safety case should accurately represent the design intent.

7.3 Complete

- A safety case should comprehensively analyse the activities associated with normal operation, identify and analyse the faults of potential safety concern and demonstrate that risks are ALARP. The ALARP argument should include

explanation of the options for alternative designs or approaches that were considered at the initial stages.

- A safety case should contain the information necessary to show that the facility is adequately safe and what will be needed for it to remain so over the period for which the safety case is valid.
- There should be reference out from the safety case to important supporting work, such as engineering substantiation. The safety case should be able to act as an entry point for accessing all relevant supporting information on which it is built.

7.4 Evidential

The arguments developed in the safety case should be supported with verifiable and relevant evidence (i.e. documented, measurable, etc.). This should encompass:

- Identification of key assumptions and the basis for these.
- The degree of sensitivity to key assumptions (sensitivity studies may be needed for key data assumptions).
- The link between engineering and safety provisions should be demonstrated in line with the requirements of defence-in-depth.
- Claims relating to the integrity or performance of engineering features should be supported in the engineering substantiation documents.
- The necessary understanding of the behaviour of novel systems or processes should be established from appropriate research and development.
- The analytical methods used to substantiate safety, including any computer code analyses, should be shown to be fit for purpose with adequate verification and validation. If a limit on the validity of an approach exists, evidence should be provided to show that the approach is used within the valid region or the use of inferred or extrapolated information needs to be carefully substantiated.
- Where safety is demonstrated using claims based on previous experience, sufficient evidence should be presented to show that it is relevant to the new safety case.

7.5 Robust

- A safety case should demonstrate that the nuclear facility will or does conform to good nuclear engineering practice and sound safety principles, including defence-in-depth and adequate safety margins.
- The arguments and evidence presented in the safety case should be proportionate to the exposed hazards and risks.

7.6 Integrated

- Hazards from and dependencies on other facilities or external services (e.g. grid supplies) should be identified and related claims or assumptions should be substantiated. The safety case should be integrated with and reference the safety cases and documents for such dependencies.

7.7 Balanced

In the words of Lord Cullen at the Ladbroke Grove Rail Inquiry, safety cases should “encourage people to think as actively as they can to reduce risks.” Therefore:

- 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).

7.8 Forward looking
The safety case should demonstrate that the facility will remain safe throughout a defined life-time. To achieve this, a safety case:

- Should demonstrate 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.
- Should take account of the effects of ageing and degradation on the facility.
- Should 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.

8. THE STRUCTURE AND CONTENT OF A SAFETY CASE

8.1 A safety case should be structured in a logical manner and be demonstrably complete. It should be accessible and understandable to those responsible for safety. There is explicit guidance in paras 100-102 of the SAPs[2] but this can be restated as that the safety case should readily provide answers to the following questions:

1. What does the safety case cover (a new site/facility, facility extension, modification)?
2. What does the site/facility, etc. look like (site layout, design, key features)?
3. What must be right and why (e.g. structural integrity, performance)?
4. How is this achieved (e.g. regulations, codes, standards and specifications)?
5. What can go wrong (faults, hazards – internal and external)?
6. What prevents/mitigates against it going wrong (e.g. protection systems, redundancy, diversity, procedures)?
7. What if it still goes wrong (risk/consequences, emergency arrangements)?
8. Are the risks ALARP?
9. What could be done to make it safer; what areas need further work (e.g. substantiation, research) and what are the limitations and uncertainties)?
10. What must be done to implement the safety case (e.g. operating limits and conditions, procedures, maintenance, resource and training requirements)?

11. How long will the safety case be valid (e.g. full life time or shorter due to life limiting features)?
12. What happens at the end-of-life (decommissioning principles / strategy)?

8.2 Some licensees have found it beneficial to produce a safety case strategy document early on in a significant project 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 use. The framework should be developed into 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. The detailed plan can of course change, as work progresses, with documents being added or deleted.

8.3 The precise structure and scope of the documentation will be a matter for the licensee to determine taking into account the significance of the hazard, the complexity of the safety case and the needs of key users. A safety case may comprise a hierarchy of documents. The top tier will contain the core of the safety arguments and increasingly detailed technical documents and supporting analysis will be presented in lower tiers. At the lowest level there are likely to be the engineering substantiation and design details, possibly including experimental results, data on reliability, relevant operational experience.

8.4 The claims in a safety case should be supported by robust arguments and evidence. The evidence may be based on: scientific laws; application of relevant codes and standards; calculational analysis (e.g. fault analysis, DBA, PSA); direct evidence from testing and operational experience; or prior research. The evidence supporting the safety claims should be relevant, of an appropriate quality, sufficient and commensurate with the potential risks and complexity of the system of interest. Different types of evidence are usually needed to support 'multi-legged' arguments for safety claims.

8.5 For large or complex safety cases it is useful to have a top tier summary document, sometimes known as the Safety Report. This approach can significantly improve the usability and accessibility of large complex safety cases, 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. The safety arguments should be coherent, consistent and readily understood. It should be meaningful if read in isolation, as well as providing the main entry point and clear links to the safety case documentation as a whole.

9. THE SAFETY CASE IN CONTEXT

9.1 It should always be remembered that the documented safety case is not an end in itself. It forms an important part of how the licensee manages safety. The requirements of the safety case need to be implemented and managed effectively to deliver safety. The licensee must ensure continually that the safety case is consistent with the as-built facility and that the facility is operated and maintained in accordance with safety case requirements and assumptions. The licensee must have effective processes to ensure these objectives are achieved.

9.2 Fundamental to the safety case are the principles, standards and criteria which the licensee intends to maintain. These must, as a minimum, meet statutory requirements

and in particular, show that risks to individuals will be acceptably low and ALARP. 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.

10. SAFETY CASES FOR DIFFERENT STAGES OF A FACILITY'S LIFE CYCLE

10.1 In the life cycle of a facility from conception through to decommissioning, there are various key stages which require special consideration. The safety case for each stage should demonstrate the safety of that stage before it commences and should be forward looking to subsequent stages. Any constraints imposed on subsequent stages should be identified in the safety case. For facilities under design or construction the safety case at each stage should contain sufficient detail to give confidence that the safety intent will be achieved in subsequent stages.

10.2 The principal stages in the life cycle for a facility, the associated safety cases and their particular purpose are shown in Table 1. Sub-division of a project into principal stages is carried out under the arrangements for Licence Conditions 19 to 22. It is preferable that a separate safety case is produced for each of the major stages.

10.3 The various stages listed in Table 1 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.

10.4 In some cases, where the installation is complex, the nine stages identified may not be sufficient and subdivisions would be useful or beneficial. For example a safety case for construction may need to be divided into civil construction and facility installation stages. Similarly a safety case for commissioning may need to be divided into one or more non-active and active stages. In fact, commissioning initially with non-active materials is normal practice for all major new nuclear process facilities.

10.5 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. 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.

10.6 Development of a safety case should be an interactive process and ensure that lessons are learned and applied before going forward to the next stage. For new projects, documents should be completed in step with the design. However, to ensure that the engineering proceeds in a manner that provides confidence that the safety requirements will be met, it is important that a satisfactory safety case is achieved before certain stages in the project commence (i.e. design, construction, commissioning, operation, and decommissioning). Some areas will need to progress at an early stage (e.g. human factors) to influence the design. It is important that the whole life cycle of the facility is taken into consideration in all stages, for example decommissioning feasibility should be taken into account during the design stage.

11. SITE-WIDE SAFETY CASES

11.1 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 (etc.) are comprehensive, consistent and adequately integrated. Individual facility safety cases should refer to the site-wide safety case, as necessary.

11.2 In addition, the site-wide safety case should cover 'whole licensee' aspects such as safety management, safety culture and organisational capability (see [11] and [12]). 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 operate the whole site safely.

11.3 The site-wide safety case should enable the reader to understand the significance of key services, major hazards and significant safety issues for the site as a whole. The reader should be able to understand the main arguments substantiating safety, how hazards are properly controlled, why the site's risks are acceptably low, and the improvements necessary, in the interest of safety. For large or complex sites, it is useful to summarise the site-wide safety case in a top tier report (see para 7.5).

11.4 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.

11.5 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].

12. OWNERSHIP, MANAGEMENT AND REVIEW OF SAFETY CASES

12.1 The licensee is legally responsible for the safety case and its adequacy. Those who have direct responsibility within the licensee for delivering safety should have 'ownership' of the safety case. 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 and the limits and conditions derived from it and the responsibility to ensure it is adequately managed and maintained.

12.2 It is important that the safety case is kept up to date during each stage of a facility life cycle. 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 the licensee; the nuclear industry in the UK or internationally; and other sectors.

12.3 Any updates should encompass changes to safety case documentation (revision or replacement) plus amendments to rules, instructions, drawings, operational

procedures and training requirements. 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.

12.4 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].

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

12.6 In addition to the role of safety case owner, it is good practice for a licensee 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]).

13. COMMON PROBLEMS, SHORTCOMINGS AND TRAPS WITH SAFETY CASES

13.1 ONR has considerable experience of reviewing and assessing licensees' 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.

13.2 It is also important that ONR learns from other sectors where there is a requirement to produce safety cases. The Nimrod Review [1] 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 [1]; the safety case aspects are covered in Chapters 9 to 11 and 22.

13.3 Licensees 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 in particular). Inspectors should look for evidence that this is happening and ask licensees how lessons have been applied to deliver improvements to safety cases.

13.4 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.

14. REFERENCES

1 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

2 Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0. November 2014.
http://www.onr.org.uk/saps/index.htm

3 ONR HOW2 – Nuclear Safety Technical Assessment Guide - Periodic Safety Reviews (PSR), NS-TAST-GD-050 Revision 3, April 2013

4 ONR HOW2 – Nuclear Safety Inspection Guide - LC14 Safety Documentation, NS-INSP-GD-014, Revision 2, May 2016

5 ONR HOW2 – Nuclear Safety Inspection Guide – LC15 Periodic Review, NS-INSP-GD-015 Revision 2, April 2016

6 Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels. WENRA. September 2014. www.wenra.org.

7 ONR HOW2 – Nuclear Safety Technical Assessment Guide - The Demonstration of ALARP (as low as reasonably practicable), NS-TAST-GD-005, Revision 7, December 2015.

8 Safety Assessment for Facilities and Activities, IAEA General Safety Requirements, GSR Part 4, 2016. 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

10 Safety Assessment for the Decommissioning of Facilities using Radioactive Materials, IAEA Safety Guide No. WS-G-5.2, 2009. www.iaea.org

11 The Management System for Facilities and Activities, IAEA Safety Requirements, GS-R-3, 2006. www.iaea.org

12 ONR HOW2 – Nuclear Safety Technical Assessment Guide - Function and Content of a Safety Management Prospectus, NS-TAST-GD-072, Revision 2, 2013.

15. GLOSSARY AND ABBREVIATIONS (EXAMPLE LIST)

ALARP	As low as reasonably practicable
BPEO	Best Practicable Environmental Option
BSL	Basic Safety Level
BSL(LL)	Basic Safety Level (legal limit)
BSO	Basic Safety Objective
CBA	Cost Benefit Analysis
CCF	Common Cause Failure
CNS	Civil Nuclear Security (Office for Nuclear Regulation)
DBA	Design Basis Analysis
DBE	Design Basis Earthquake
DEPZ	Detailed Emergency Planning Zone
HSE	Health and Safety Executive
HSWA74	The Health and Safety at Work etc Act 1974
IAEA	International Atomic Energy Agency

NDA	Nuclear Decommissioning Authority
NEPLG	Nuclear Emergency Planning Liaison Group
OBE	Operating Basis Earthquake
PSA	Probabilistic Safety Analysis
PSR	Periodic Safety Review
SAP	Safety Assessment Principle(s)
SFAIRP	So far as is reasonably practicable
SEPA	Scottish Environment Protection Agency
SSC	Structure, System and Component
TAG	Technical Assessment Guide(s)
WENRA	Western European Nuclear Regulators' Association

16. APPENDICES

Appendix 1: Common problems with safety cases

Appendix 2: Nimrod Review - Safety case shortcomings & traps

TABLE 1
PRINCIPAL STAGES OF A NUCLEAR FACILITY LIFE-CYCLE AND ASSOCIATED SAFETY CASES

Major stage of Facility life cycle	Associated safety case (SC)	Particular purpose of safety cases
Early design	Preliminary Safety Case	o To make a statement of design philosophy, the consideration of design options and a description of the resultant conceptual design sufficient to allow identification of main nuclear safety hazards, control measures and protection systems. o To provide a description of the process being adopted to demonstrate compliance with the legal duty to reduce risks to workers and the public SFAIRP. o To provide details of the safety principles and criteria that have been applied by the licensee (or Requesting Party) in its own assessment processes, including risks to workers and the public. o To broadly demonstrate that the principles and criteria are likely to be achieved. o To provide an overview statement of the approach, scope, criteria and output of the deterministic safety analyses. o To provide an overview statement of the approach, scope, criteria and output of the probabilistic safety analyses. o To specify the site characteristics to be used as the basis for the safety analysis (the 'generic siting envelope') o To provide explicit references to standards and design codes used justification of their applicability and a broad demonstration that they have been met (or exceptions justified). o To provide information on the quality management arrangements for the design, including design controls; control of standards; verification and validation; and the interface between design and safety. o To give a statement giving details of the safety case development process, including peer review arrangements, and how this gives assurance that nuclear risks are identified and managed. o To provide Information on the quality management system for the safety case production. o To identify and explain any novel features,* including their importance to safety. o To identify and explain any deviations from modern international good practices. o To provide sufficient detail for ONR to satisfy itself that SAPs and WENRA reference levels are likely to be satisfied. o To provide, where appropriate, information about all the assessments completed by other (including overseas) nuclear safety regulators. o To identify outstanding information that remains to be developed and its significance. o To provide information about any long-lead items that may need to be manufactured. o To provide information on radioactive waste management and decommissioning. * *The definition of a novel feature is any major system, structure or component not previously licensed in a nuclear facility anywhere in the world.*
Pre-Construction and Installation (including modifications)	Pre-Commencement (Construction) Safety Case	o To define the documentary scope and extent of the safety case. o To explain how the decisions regarding the achievement of safety functions ensure that the overall risk to workers and public will be reduced SFAIRP. o To provide responses to outstanding regulatory issues from the Preliminary Safety Case. o To provide sufficient information to substantiate the claims made in the Preliminary Safety Case. o To provide sufficient information to enable ONR to assess the design against all relevant SAPs.

Major stage of Facility life cycle	Associated safety case (SC)	Particular purpose of safety cases
		o To demonstrate that the detailed design proposal will meet the safety objectives before construction or installation commences, and that sufficient analysis and engineering substantiation has been performed to prove that the plant will be safe. o To provide detailed descriptions of system architectures, their safety functions and reliability and availability requirements. o To confirmation and justify the design codes and standards that have been used and where they have been applied, non-compliances and their justification. o To provide information on fault analyses including Design Basis Analysis, Severe Accident Analysis and PSA. o To justify the safety of the design throughout the plant's life cycle, from construction through operation to decommissioning, and including on-site spent fuel and radioactive waste management issues. o Where appropriate, to identify potentially significant safety issues raised during previous assessments of the design by other (including overseas) nuclear safety regulators, and explanations of how their resolution has been or is to be achieved. o To identify the safe operating envelope and the operating regime that maintains the integrity of the envelope. o To confirm: a) which aspects of the design and its supporting documentation are complete; b) which aspects are still under development and identification of outstanding confirmatory work that will be addressed. Where necessary, the safety case should be updated to reflect the above additional details.
	Pre-Inactive Commissioning Safety case	o To demonstrate that the facility as-built meets relevant safety criteria and is capable of safe operation. o To enable the production of a programme of safety commissioning activities that will:- • demonstrate as far as practicable the safe functioning of all systems and equipment, • prove as far as practicable all safety claims, • confirm as far as practicable all safety assumptions, • confirm as far as practicable the effectiveness of all safety related procedures. • To list aspects of safety that cannot be demonstrated inactively.
	Pre-Active Commissioning Safety case	o To sentence any shortfalls revealed during inactive commissioning. o To demonstrate that the inactive commissioned facility continues to meet relevant safety criteria and is capable of safe operation. o To demonstrate 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. • To enable the production of a programme of safety commissioning activities that will:- • demonstrate the safe functioning of all systems and equipment where not already demonstrated • prove all safety claims where not already proved • confirm all safety assumptions where not already confirmed • confirm the effectiveness of all safety related procedures where not already confirmed as effective. o To demonstrate that there are no aspects of safety that remain to be demonstrated after active commissioning. o To identify limits and conditions necessary in the interest of safety. o To demonstrate compliance with the legal duty to reduce risks to workers and the public SFAIRP.

Major stage of Facility life cycle	Associated safety case (SC)	Particular purpose of safety cases
Pre-Operation	Pre-Operational Safety case	o To demonstrate that the facility (as built and commissioned) meets the safety standards and criteria set down in the pre-commencement safety case. o To demonstrate that detailed analysis has been undertaken to prove that the facility will be safe. o To demonstrate that all necessary pre-operational actions have been completed, validated and implemented. o To identify limits and conditions necessary in the interest of safety. o To demonstrate compliance with the legal duty to reduce risks to workers and the public SFAIRP.
Operation	Facility or Station Safety Case or Site-Wide Safety Case if relevant Updated as necessary Periodically reviewed	o To demonstrate safety of operation for a defined period. o To demonstrate compliance with the legal duty to reduce risks to workers and the public SFAIRP. o To take account of experience to review and changes that have been necessary, and ensure the safety case is still valid. o To review the safety adequacy of the facility in the light of its current and projected condition and against modern safety standards and expectations. o To take a strategic look forward to consider facility lifetime and contingency requirements.
Post Operation	Post-Operational Safety Case	o To demonstrate that the facility is adequately safe for post operations care and maintenance activities prior to start of decommissioning (if such a period is appropriate). o To demonstrate compliance with the legal duty to reduce risks to workers and the public SFAIRP.
Pre-Decommissioning	Safety Strategy Overview (applies in complex decommissioning projects only)	o To describe how safety will be managed through the proposed decommissioning programme for the project. o To demonstrate that there will be a progressive, timely and systematic reduction of hazard. o To define safety goals and criteria for the project as a whole. o To demonstrate compliance with the legal duty to reduce risks to workers and the public SFAIRP.
Decommissioning	Decommissioning Strategy	o To set out in broad terms the approach that is to be followed during decommissioning. o To substantiate in principle the safety of the decommissioning task and demonstrate that there will be a progressive and systematic reduction in hazard. o To define safety goals and criteria for the decommissioning task. o To demonstrate compliance with the legal duty to reduce risks to workers and the public SFAIRP.
	Safety Case for Decommissioning Operations	o The individual safety justification for each of the potentially many very small, short jobs. These include risk assessments, method statements and peer reviews, and can often be normal works procedures such as those for facility modifications.
Post-Decommissioning	Post-Decommissioning Clearance Safety Case	o To demonstrate that there has ceased to be any danger from ionising radiation from anything on site.

Note: More information on ONR's expectations for PSRs and PCSRs is given in the document 'New Nuclear Power Stations - Generic Design Assessment – Guidance to Requesting Parties'. Although the guidance is specific for new nuclear power stations, it is nevertheless indicative of ONR's expectations for other types of new facilities.

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 section 7 of the main text. The list 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.

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 engineering rigour to be applied to structures, systems and components).

The need to include in a safety case all structures, systems and components (SSC) important to safety 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 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.

The safety case doesn’t distinguish between the design basis (what the facility has been designed to do and the major assumptions made in its design) and the design base analysis (analysis of accidents for which designer makes explicit safety provisions)

There is confusion between PSA and PRA – taken as respectively complex models and simple models of risk analysis/acceptance. The mixing of the two approaches can in some cases be problematic, and should be guarded against.

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.

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 licensees.

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's 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:

http://www.official-documents.gov.uk/document/hc0809/hc10/1025/1025.pdf. .

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[2]' 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

[2] The term used by one of BAE Systems' employees drawing up the Nimrod Safety Case in 2004

interest in having levels of safety with which all involved are comfortable."[3] 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.[4]

(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?*'[5] 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...*").

---

[3] BOI (Board of Inquiry) Report, Part 5, Commander-in-Chief Air Command's Comments dated 2 November 2007.

[4] 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".*

[5] Safety Critical Systems Club Newsletter, Volume 17, No. 2, January 2008, pages 31-3

(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*'[6] 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.

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.[7] The quality of the argument cannot be judged by the node-count on such documents or number of colours used.

[6] *i.e.* the argument has become bald assertion or 'meta-discussion.

[7] 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.