

NUCLEAR SAFETY DIRECTORATE - BUSINESS MANAGEMENT SYSTEM

TECHNICAL ASSESSMENT GUIDE GUIDANCE ON THE PURPOSE, SCOPE AND CONTENT OF NUCLEAR SAFETY CASES

T/AST/051

ISSUE 001

Approved By: *Colin Waker*

Colin Waker

Issue Date: 14/05/02

Open Government Status: Fully Open

Review Date: 13/05/05

Contents

Purpose and Scope

Relationship to the Nuclear Site Licence and other relevant legislation

Definition of a Nuclear Safety Case

The Purpose of a Nuclear Safety Case

Overall Qualities of a Safety Case

The Structure and Content of a Nuclear Safety Case

The Nuclear Safety Case in Context

Safety Cases for Different Stages of a Plant's Life Cycle

Site Wide Safety Cases

Specific Requirements for Post-Operation and Decommissioning

Ownership, Management and Maintenance of Safety Cases

References

[Table 1.] **Principal Stages of a Nuclear Plant Life Cycle and Associated Safety Cases**

[Figure 1]. **The Nuclear Safety Case in Context**

[Appendix 1]. **Deterministic and Probabilistic Analysis**

[Appendix 2]. **The Nuclear Safety Case in Context; Typical Contents of Each Element**

[Appendix 3]. **Site Wide Safety Case**

1. Purpose and Scope

1.1 It is intended that the guide will be used by inspectors in the Health and Safety Executive's (HSE) Nuclear Installations Inspectorate (NII) when

considering the adequacy of licensees' safety cases and arrangements for their production and management. It does not set out how NII regulates these arrangements nor the activities that safety cases cover. Comments on this guide, and suggestions for future revisions should be recorded on a Process Improvement Feedback Form (PIFF) in accordance with **DBP003**.

1.2 The purpose of this guide is to provide generic guidance to NII inspectors on what is required by NII from licensees in their safety cases for licensed nuclear installations. The guide sets out the purpose of nuclear safety cases, their overall qualities, how they may be structured and what information they may contain, noting that the actual content of safety cases is a matter for licensees to decide. There is also coverage of how safety cases may be managed and maintained. The guidance is all set into the context of the requirements of the nuclear site licence.

1.3 The guide embodies NII's expectations of safety cases for nuclear plants, notably reactors and process plants handling radioactive materials. It is recognised however that under occasional circumstances, or in specialist plant, additional factors will need to be considered and addressed in the safety case. Licensees may choose to address environmental and non nuclear safety issues in their safety cases but these are not within the scope of this guide.

1.4 The scope of the guide covers whole plant safety cases over the full life cycle. It also encompasses safety cases, and revisions to safety cases, for part of a plant, a plant modification or a specific topic.

1.5 Although the guide has been developed for NII's own use, it indicates to licensees and other stakeholders the standards that the NII expects. It is expected that this guide will influence the issues which should be addressed in safety cases during the various stages¹ of the life of a nuclear plant or facility. The guide does not prescribe the detail nor the depth that needs to be addressed; these remain the responsibility of the licensee and will be dependent upon the specifics of each safety case.

2. Relationship to the Nuclear Site Licence and other relevant legislation

2.1 The Nuclear Installations Act, 1965 (as amended) requires any operator of a defined nuclear installation to be licensed and gives the HSE the powers to "attach to the licence such conditions as may appear to be necessary or desirable in the interest of safety". The sections of the Nuclear Installations Act relating to the licence and inspection of sites (sections 1, 3-6, 22 and 24A) are "relevant statutory provisions" under the HSW Act 1974^[1]. Thus these sections of

pre-existing law are subject to regulation and enforcement by HSE.

2.2 There are 36 standard Licence Conditions (LC) attached to all Nuclear Site Licences^[2, 3]. The Licence Conditions relating to safety cases are:

1) Licence Condition 14 sets the primary requirement for a licensee to “make and implement adequate arrangements for the production and assessment of safety cases consisting of documentation to justify safety during design, construction, manufacture, commissioning, operation and decommissioning phases of the installation”.

2) Licence Condition 23 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 and to identify the conditions and limits necessary in the interests of safety”, and refers to these limits and conditions as Operating Rules.

3) Licence Conditions 19 (construction or installation of new plant), 20 (modification to design of plant under construction), 21 (commissioning), and 22 (modification or experiment on existing plant), specifically require the licensee to provide adequate documentation to substantiate the safety of the proposals.

4) Licence Condition 15 requires the licensee to “make and implement adequate arrangements for the periodic and systematic review and assessment of safety cases”.

5) Licence Condition 35 requires that “the licensee shall make and implement adequate arrangements for the decommissioning of any plant or process which may affect safety”, it also states “the arrangements shall include a requirement for provision of adequate documentation to justify the safety of proposed decommissioning and shall where appropriate provide for the submission of this documentation to the Executive”.

2.3 Thus for the whole of a plant’s life cycle, the safety of any activity must be substantiated and, whenever possible, 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 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.

2.4 Section 2 of the HSW Act requires “every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees”. Section 3 of the Act requires “every employer to conduct his undertaking in such a way as to ensure, so far as is reasonably practicable, that the persons not in his employment who may be effected thereby are not thereby exposed to risks to their health or safety”. In judging whether licensees have complied with their legal duties NII makes use of the risk management procedures explained in Reducing Risks, Protecting People⁴ document. The fundamental requirement is that the licensee shall take measures to reduce risks As Low As Reasonably Practicable (ALARP). Guidance on the meaning and use of the concept of ALARP in HSE’s decision making is available from HSE’s website⁵. Principles for assessing nuclear safety cases are detailed in NII Safety Assessment Principles⁶ and NII Technical Assessment Guide on ALARP⁷.

3. Definition of a Nuclear Safety Case

3.1 The term ‘nuclear safety case’ may relate to a site, a plant, part of a plant, a plant modification, or a set of significant issues. In subsequent discussion ‘nuclear safety case’ is shortened to ‘safety case’.

3.2 A safety case is the totality of documented information and arguments which substantiates the safety of the plant, activity, operation or modification in question. It provides a written demonstration that relevant standards have been met and that risks have been reduced as low as reasonably practicable (ALARP).

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

4. The Purpose of a Nuclear Safety Case

4.1 The purpose of a safety case is to establish and demonstrate in written form that the plant, process, activity, modification, etc. being proposed:

- 1) are soundly assessed and meet required safety principles;

- 2) conform to good nuclear engineering practice and to appropriate criteria, standards and codes of practice;
- 3) are adequately safe during both normal operation and fault conditions;
- 4) are, and will remain, fit for purpose;
- 5) give rise to a level of nuclear risk to both public and workers which is ALARP; and
- 6) have a defined and acceptable operating envelope, with defined limits and conditions, and the means to keep within it.

4.2 The safety case also forms the basis for delivering safe operation. The analysis it provides of normal operation and possible accidents should identify the measures that need to be implemented to realise the required safety standards. These measures include: operating rules and instructions; examination, maintenance and testing requirements; minimum staffing levels in key areas (eg. control rooms); staff training needs; and emergency procedures.

4.3 The normal approach for establishing safety in nuclear installations begins with robust engineering design with defence-in-depth. The safety case should show how these have been achieved, and how safety functions have been identified and delivered. Deterministic analysis should be included covering both normal operations and fault behaviour and may be supported by appropriate probabilistic analysis to judge the significance of uncertainties, show that risks are balanced, and demonstrate compliance with numerical risk criteria. Further details are given in **Appendix 1**. In addition, there should be a demonstration that risks are ALARP. This demonstration should include the options that have been considered and justify those chosen.

4.4 The safety analyses require an input of engineering and operational knowledge and judgement. It is therefore important to have active co-operation between designers, analysts and operators, and adequate referencing to establish clear links with supporting documentation.

4.5 The safety case also provides a means, for example, of:

- 1) Aiding training and awareness of personnel in the safety aspects of the plant;

- 2) Providing the context within which changes must be reviewed;
- 3) Providing information on designers' understanding and intentions with respect to the plant/facility; and
- 4) Providing a means by which operators of the plant understand the significance and achievement of plant safety.

5. Overall Qualities of a Safety Case

5.1 There are several features which are fundamental to a good safety case. These are summarised here in terms of nine overall qualities. The subsequent sections of this guide translate these qualities into more specific points. The safety case should be;

1) *Complete* - All reasonably foreseeable threats to safety should be identified. It should be shown that the plant incorporates adequate protection against these threats, or that their contribution to the overall risk is negligible. All foreseeable plant states should be covered, including transients and non-steady state conditions such as start up and shutdown sequences.

2) *Clear* - The safety case should highlight the key points in terms of both strengths and weaknesses. There should be a clear statement as to the nature and magnitude of the significant hazards, and the protection in place to prevent or mitigate their effects. The safety case needs to be readily accessible as well as understandable. It should be possible to navigate easily around the safety case documents to find relevant information. The basis of all assumptions, conclusions and recommendations should be given and any unresolved issues explained and justified. Clarity needs to extend to correct referencing of supporting information. It is important that the basis for the level of safety portrayed in the documentation is clearly evident to all users, including the regulator.

3) *Rational* - The safety case should be reasonable and sensible. It should provide cogent, cohesive and logical arguments to support the conclusions. This includes the arguments in support of claims that risks have been reduced so far as is reasonably practicable.

4) *Accurate* - The safety case should accurately reflect the 'as is' state of the plant, equipment, processes and procedures.

5) *Objective* - The arguments developed in the safety case should be supported with factual evidence (ie. documented, measurable, etc.). The necessary understanding of the behaviour of novel systems or processes should be established from appropriate research and development. Claims relating to the integrity or performance of engineering features should be supported in the engineering substantiation documents. The link between engineering and safety provisions should be demonstrated in line with the requirements of defence-in-depth. In the absence of directly relevant data, the use of inferred or extrapolated information needs to be carefully substantiated. There is a need to provide visibility of the sensitivity to assumptions to validate the robustness of associated claims. The adequacy of operational procedures, managerial controls and resources should be demonstrated by task analysis to an appropriate level.

6) *Appropriate* - The analytical methods used to substantiate safety together with computer code assessments should be shown to be fit for purpose with adequate verification and validation. If a limit on the validity of an approach exists, evidence is required to show that the approach is used within the valid region. Any assumptions that have been made should be identified and shown to be appropriate. Where safety is demonstrated using claims on previous experience, sufficient evidence should be presented to show that equivalent principles, criteria and standards to those previously used have been applied, and that existing data are relevant to the new facility.

7) *Integrated* - The safety case should be holistic so that there are clear links between the safety analysis and the engineering substantiation. It should also define where it depends on other external facilities and services, for example grid supply, and specify and substantiate clearly any associated assumptions that are being made. There should also be clear links from the safety case to operational requirements and constraints to be implemented in other documents (see **figure 1**).

8) *Current* - The plant safety case must be reviewed, revised and updated to ensure it remains current. As the plant passes through its life cycle, the development of the safety case should be managed to ensure it remains valid at any point in time. The content of a safety case may also change if the plant undergoes a significant modification, or a series of minor modifications which have a

significant cumulative effect on safety. A safety case is therefore a living suite of documents which should reflect the current state of the facility in all the physical, operational and managerial aspects.

9) *Forward looking* - the safety case should demonstrate that the plant will remain safe throughout a defined life time.

6. The Structure and Content of a Nuclear Safety Case

6.1 A safety case should be structured in a logical manner and be demonstrably complete. It should contain all the information necessary to demonstrate safety. This information should be easily accessible and understandable. As a guide, the answers to the following questions should be readily obtained:

1) What is the safety case for (a new site/facility, plant extension, modification)?

2) What does the site/plant, 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. codes, standards, specifications)?

5) What can go wrong (faults, hazards)?

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) What could be done to make it safer ("Optioneering" and ALARP considerations)?

9) What must be done to implement the safety case (e.g. operating procedures, limits and conditions, maintenance)?

10) How long will the safety case be valid (e.g. full life time or shorter due to life limiting features)?

11) What happens at the end-of-life (decommissioning principles / strategy)?

6.2 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.

6.3 There are a number of different types of documented information which underpin the safety arguments. These may include:

- 1) Identification of faults and hazards and compilation of a comprehensive fault schedule⁸1.
- 2) Criteria for choosing the Design Basis faults and hazards (i.e. those faults and hazards for which design measures are explicitly claimed in the safety case).
- 3) Deterministic analysis of the design against these faults to show a robust tolerance of them.
- 4) Determination of the safety functional requirements of the structures, systems and components important to safety.
- 5) Determination of limits, conditions and associated trip and alarm settings and a comprehensive protection schedule.
- 6) Task analysis of important operations.
- 7) Substantiation that the plant will deliver the safety requirements.
- 8) Probabilistic safety analysis
- 9) Identification of suitable emergency arrangements.

6.4 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 and complexity of the safety case.

6.5 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 calculations, experimental results and data on reliability and relevant operational experience, etc. At the other end of the scale, for example long-term storage of low level radioactive material, a relatively simple safety case is normally appropriate that sets out requirements for periodic inspection to ensure that containment remains sound and that storage conditions remain conducive to long-term stability.

6.6 For large or complex safety cases it is strongly recommended that licensees produce a top tier document referred here to as the Safety Report. The Safety Report should describe the plant 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 presented in a Safety Report should be coherent, consistent and readily understood. It should be meaningful if read in isolation, as well as providing the main entry point with clear links to the safety case as a whole.

6.7 There needs to be an auditable trail within the document structure providing clear referencing to all the information (e.g. analyses, test results) which contributes to the demonstration of safety and which underpins the conclusions of the safety case.

6.8 **Section 2 of Appendix 2** shows the typical contents of a well constructed safety case for a fully operational facility. The contents, whilst extensive, can not be considered exhaustive since each safety case will have different requirements.

7. The Nuclear Safety Case in Context

7.1 It should always be remembered that the safety case is essentially a set of documents. It is only if the findings from these are properly implemented in appropriate forms of output and those outputs properly managed that safety will be assured. Examples are included in **Appendix 2, Section 3**. The licensee must ensure the safety case is consistent with the as-built plant and that the plant is operated and maintained in accordance with safety case requirements and assumptions. The licensee must have an effective process for ensuring these objectives are achieved through its arrangements under Licence Conditions.

7.2 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. They will include design standards, safety criteria and general standards of safety management. They should also 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 which emanate from the HSW Act and the regulations developed under it.

7.3 The contextual elements are shown in **Figure 1**, described in **Appendix 2** and can be summarised as the definition of safety, the demonstration of safety, the implementation of safety and the monitoring and maintenance of the safety case.

8. Safety Cases for Different Stages of a Plant's Life Cycle

8.1 In the life cycle of a plant 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 plants under design or construction the safety case at each stage should contain enough detail to give confidence that the safety intent will be achieved in subsequent stages.

8.2 The principal stages in the life cycle for a plant, 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.

8.3 The various stages listed in **Table 1** result from significant steps in plant definition, though a particular plant 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.

8.4 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 plant 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 plants.

8.5 Supplementary documents can 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 plant will be maintained and quality assured during construction and installation work, or

2) to demonstrate the safety of a temporary plant modification by defining and substantiating, for a limited period of time, operations which are outside the normal envelope prescribed by existing rules and instructions.

8.6 The development of a safety case is an interactive process which should ensure lessons are learned and fed back before going forward. The documents should be completed in step with the design. However, to ensure that the engineering proceeds in such a manner that the safety requirements will be confidently 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). It is important also that the life cycle of the facility is reflected in all stages, for example decommissioning feasibility should be taken into account during design.

9. Site Wide Safety Cases

9.1 A licensee may choose not to include all operations which may affect safety on a site in a single safety case, but instead produce separate safety cases for specific plants, operations or parts of a site. In such cases a site wide safety case should also be produced to demonstrate that the set of safety cases is comprehensive, consistent and adequately integrated. It should also cover any site wide matters which are not included in the specific safety cases (e.g. common services, pipebridges and emergency arrangements). Site wide safety cases should be treated in the same manner as plant specific safety cases and be subjected to the same requirements in terms of review and reassessment. The purpose and typical content of a site wide safety case is shown in **Appendix 3**.

9.2 It is strongly recommended that the site wide safety case is summarised in a top tier Safety Report, with an auditable trail to the documentation that comprises the case. The total suite of safety cases on the site and their periodic reviews should be referenced and form part of an audit trail. Individual plant safety cases should also refer to the site wide safety case, and their dependencies on site wide services.

9.3 The Safety Report 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 risk is ALARP, and the improvements necessary, in the interest of safety, arising from any given periodic review.

9.4 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.

10. Specific Requirements for Post-Operation and Decommissioning

10.1 A number of nuclear power plants and process plants handling radioactive materials are reaching the end of their life, and may start decommissioning in the near future. Due to the importance of this issue, this section provides further guidance on post-operation and decommissioning safety cases.

10.2 Where there is a time delay between the end of operation and the start of decommissioning the operational safety case will need to be revised or replaced to reflect the new plant status. The resulting post-operation safety case will be the key document setting out how arrangements for care and maintenance will enable the plant to be managed safely in the post-operational period. This safety case may need to be reviewed and updated periodically depending on the length of time before start of decommissioning.

10.3 At the start of the plant lifecycle, limited information will be available on decommissioning although at least the feasibility should be demonstrated. However, during later lifecycle stages decommissioning should be increasingly taken into account.

10.4 The process of decommissioning may continue for some time. A safety case or a systematic series of developing safety cases, will be required for this period. It is also important to note that some activities that are essential to enable decommissioning to take place may increase risks temporarily, for example, remedial work, plant installation or waste retrievals. Such activities need to be fully considered, substantiated, and monitored.

10.5 For many decommissioning projects there is incomplete information about the state of plant internals (degree of contamination, waste hold-up, etc.) and

therefore limited ability to plan precisely how to manage dismantling and cleanout. This makes production of a detailed and reliable safety justification, in advance of any activities, very difficult. What is needed in these cases is a managed process that allows the necessary information to emerge in a controlled manner, subject, so far as is reasonably practicable, to two important conditions:-

1) Each individual activity should be capable of being undone or at least halted without additional hazard, in case unexpected dangers come to light. Where difficulties are experienced in meeting this condition consideration should be given to splitting the activity into small enough elements that allow it to be met, or to more detailed optioneering in order to avoid the activity. If in spite of these actions an irrevocable activity cannot be avoided, the most careful planning and substantiation of the activity itself and of contingency arrangements is needed to deal safely with all that can be foreseen and with margins to allow for the unexpected.

2) The succession of activities should be planned so that the earlier ones provide information that assists in managing the later ones.

10.6 What is needed is to devise a strategic document referred to herein as a Decommissioning Strategy to set out in broad terms the approach that is to be followed, and then to divide up the decommissioning into several smaller jobs. Each of these jobs can often be equivalent to intrusive maintenance or post-spillage decontamination, and requires a risk assessment, method statement and peer review. Usually normal works procedures such as the plant modification procedure can be applied. Information gained from early tasks is fed back into subsequent tasks so that uncertainties decrease and confidence increases over time.

10.7 During operation of the plant the Decommissioning Strategy will need to be developed and reviewed. Towards the end of plant life, and before the plant ceases to operate as originally intended, this strategy will need to be finalised.

10.8 For the more complex decommissioning projects which are to be carried out in stages, there may be a requirement for a documented Safety Strategy Overview to describe the safety strategy for the project as a whole and covering one or more plants (i.e. over and above the individual Decommissioning Strategy documents mentioned above). This is to describe how safety will be managed throughout the proposed decommissioning programme for the project.

10.9 At the end of decommissioning a Post-Decommissioning Clearance Safety

Case will need to be produced to demonstrate that there has ceased to be any danger from ionising radiation from anything on the site.

11. Ownership, Management and Maintenance of Safety Cases

11.1 The licensee is legally responsible for the safety case. However, it is those employees of the licensee who have direct responsibility for delivering safety who should have 'ownership' of it. By this we mean an understanding of the safety case and limits and conditions derived from it.

11.2 Production

1) The responsibilities for production, revision, review and document control should be clearly defined as part of licence compliance arrangements and be discharged by suitably qualified and experienced people. Where the licensee itself does not produce all of the safety case and uses contractors for this purpose, at all times the licensee must possess (in-house) the technical capability to understand its safety case and act as an 'intelligent customer'⁹.

2) The responsibility for producing and maintaining a safety case may change as the plant moves through its life cycle. For example, in the design stage, the safety case may be developed and owned by a design team who eventually hand over responsibility and ownership to the 'operator'. The safety management system should explain how relevant information is transferred (e.g. there should be a system in place to take forward design assumptions into operations) and demonstrate that there are mechanisms in place to ensure that the safety case is fully adopted and implemented. This also applies to a plant at the end of its operational life when responsibility and ownership for the safety case may pass from the operator to a decommissioning group.

11.3 Peer Review and Independent Assessment

As part of the production process a safety case should undergo appropriate verification controls and a formal approval process to check, amongst other things, that: the safety case is complete; key safety assumptions are valid and have been subject to a sensitivity check; appropriate robust methods and data have been used; that calculations are correct; and that the plant and operational details documented are consistent with the actual plant and its operations. In addition, and where necessary, there should be independent safety assessment

by suitably qualified and experienced assessors, who are independent of the authors and verifiers and those directly responsible for the plant's operations. Following independent assessment, safety cases should be considered by the licensee's Nuclear Safety Committee (NSC). When the licensee's arrangements contain a safety classification system based on safety significance, these arrangements may restrict the independent safety assessment and reference to the Nuclear Safety Committee to the more significant safety cases.

11.4 Staff Awareness

The safety case should be used as a vehicle to enable staff to be made aware (via provision of appropriate training) of the safety significance of the plant. The licensee should use, as far as possible, its own staff in the production and maintenance of safety documentation and it should make the whole safety case available to appropriate staff.

11.5 Maintenance

1) It is important that the safety case is kept up to date. Significant changes may occur during operations such as modification, incidents, revised life expectancy, etc. Such changes should be recorded and taken forward as necessary in an updated safety case, which accurately and readily reflects the current situation.

2) Where referenced data and information underpin analyses and assumptions arrangements are needed to ensure that when relevant new information comes to light a review is conducted to check whether and how safety cases they support are affected.

3) 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.

11.6 Modification

During each stage of a plant life cycle modifications may have to be made to the buildings, plants, operations, processes or existing safety cases. All modifications should be documented and categorised according to their potential safety significance based upon hazards, taking into account any transitional plant state. The appropriate level of discussion of a modification, and the type of safety case

documentation to be produced, will depend on its scope and safety significance. Any modification should not be considered full and complete until any necessary changes to safety case documentation (amendment or replacement), amendments of rules, instructions, drawings, operational procedures and training requirements, etc. have been completed. Identification of such amendments is an important element when proposing the modification.

11.7 Periodic Review

1) Licence Condition 15 requires that “the licensee shall make and implement adequate arrangements for the periodic and systematic review and reassessment of safety cases”. The purpose of this Licence Condition is to ensure that throughout its life, each plant remains adequately safe and that its safety case is kept up to date.

2) Two type of reviews are required, interim reviews, and major safety reviews. The latter are commonly referred to as Periodic Safety Reviews (PSRs)¹⁰.

3) Interim reviews are carried out to provide regular confirmation that the safety case remains valid and that the safety of mid-term future operations will continue to be demonstrated by the case. They should cater for components whose behaviour or nature may change significantly and if necessary bring forward the date of the next PSR. Such reviews would normally be expected every one to three years (e.g. at the time of periodic outage for reactors). The licensee’s arrangements should also initiate reviews if new information indicates any significant change in safety case assumptions.

4) The purpose of a Periodic Safety Review is to determine, by means of a comprehensive assessment, whether the plants, processes, management, operations and facilities covered by a safety case remain as safe as reasonably practicable when judged against modern standards. It should also determine that ageing and other time-related phenomena will not compromise safety, particularly before the next PSR. The maximum period between PSRs is normally ten years.

12. References

1. Health and Safety at Work Act 1974, Ch 37. HMSO. ISBN 0 10 543774 3

2. Nuclear Site Licences under the Nuclear Installations Act 1965 (as amended) Notes FOR APPLICANTS, ISBN 0 7176 0795 X

3. Licence Condition 36 - <http://www.hse.gov.uk/nsd/cond36.htm>

4. Reducing risks, protecting people, HSE's decision-making process, 2001, ISBN 0 7176 2151 0

5. Principles and guidelines to assist HSE in its judgements that duty-holders have reduced risk as low as reasonably practicable, <http://www.hse.gov.uk/dst/alarp1.htm>

Assessing compliance with the law in individual cases and the use of good practice, <http://www.hse.gov.uk/dst/alarp2.htm>

Policy and guidance on reducing risks as low as reasonably practicable in design, <http://www.hse.gov.uk/dst/alarp3.htm>

6. Safety Assessment Principles for Nuclear Plants, 1992, ISBN 0 11 882043 5

7. Technical Assessment Guide, Demonstration of ALARP, **T/AST/005**

8. Technical Assessment Guide, Fault Analysis, **T/AST/044**

9. Technical Assessment Guide, Principles for the assessment of a Licensee's "Intelligent Customer Capability" (Licensee's Technical and Engineering Capability), **T/AST/049**

10. Technical Assessment Guide, Licence Condition 15, Periodic Safety Reviews (PSRs), **T/AST/050**

11. Managing for Safety at Nuclear installations, 1996, ISBN 0 7176 1185 X

12. The Ionising Radiations Regulations 1999, ISBN 0 11 085614 7

13. The Tolerability of Risk from Nuclear Power Stations, 1988, ISBN 0 11 886368 1

RELATED DOCUMENTS:

Technical Assessment guide, Deterministic Safety Analysis & Use of Engineering

Principles in Safety Assessment, **T/AST/006**

Technical Assessment Guide, Probabilistic Safety Analysis, T/AST/030

Technical Assessment Guide, Severe Accident Analysis, T/AST/007

Technical Assessment Guide, Transient Analysis for DBAs in Nuclear Reactors, **T/AST/034**

Technical Assessment Guide, Validation of Computer Codes and Computational Methods, **T/AST/042**

Technical Assessment Guide, Management of Radioactive Materials and Radioactive Waste at Nuclear Licensed Sites, **T/AST/024**

Technical Assessment Guide, Management for Safety, **T/AST/039**

Table 1. Principal Stages of a Nuclear Plant Life Cycle and Associated Safety Cases

Major Stages of a Plant Life Cycle	Associated Safety Cases	Particular Purpose of Safety Cases
Early Design	Preliminary Safety Case	<p>•To make a statement of intent to construct and operate a nuclear facility</p> <p>•To demonstrate that the plant in principle is capable of being constructed and managed safely throughout all life cycle changes</p> <p>•To discuss the significant options and define and justify the ones chosen</p>

		<p>ÿTo indicate the safety criteria and objectives</p> <p>ÿTo provide a broad demonstration that in principle the criteria are likely to be achieved</p>
<p>Pre- Construction and Installation (including modifications)</p>	<p>Pre- Commencement (Construction) Safety Case</p>	<p>ÿTo demonstrate the detailed design proposal will meet the safety objectives prior to commencement of construction or installation</p> <p>ÿTo demonstrate that the plant is capable of being operated within safe limits</p> <p>ÿTo demonstrate that construction and installation activities will result in a plant of appropriate quality.</p> <p>ÿTo demonstrate that sufficient analysis has been performed to prove that the plant will be safe</p> <p>ÿTo identify outstanding confirmatory work</p> <p>ÿTo demonstrate that risk will be ALARP</p> <p>ÿ To demonstrate the feasibility of decommissioning</p>

Pre- Commissioning

Pre- Inactive Commissioning
Safety Case

ÿTo demonstrate that the plant as-built meets relevant safety criteria and is capable of safe operation

ÿTo 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

ÿTo list aspects of safety that cannot be demonstrated inactively

Pre- Active Commissioning
Safety Case

ÿTo sentence any shortfalls revealed during inactive commissioning

ÿTo demonstrate that the inactive commissioned plant continues to meet relevant safety criteria and is capable of safe operation

ÿTo demonstrate that the active commissioning activities can and will be carried out safely

ÿTo 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

		<p>related procedures where not already</p> <p>confirmed as effective</p> <p>ÿTo demonstrate that there are no aspects of safety that remain to be demonstrated after active commissioning</p> <p>ÿTo identify limits and conditions necessary in the interest of safety</p>
Pre- Operation	Pre-Operational Safety Case	<p>ÿTo demonstrate that the plant (as built and commissioned) meets the safety standards and criteria set down in the pre commencement safety case</p> <p>ÿTo demonstrate that detailed analysis has been undertaken to prove that the plant will be safe</p> <p>ÿTo demonstrate that all necessary pre-operational actions have been completed, validated and implemented</p> <p>ÿTo identify limits and condition necessary in the interest of safety</p>
Operation	Plant or Station Safety Case or Site Wide Safety Case if relevant	<p>ÿTo demonstrate safety of operation for a defined period</p> <p>ÿTo take account of experience</p>

	Updated as necessary	<p>ÿTo review any changes that have been necessary, and ensure the safety case is still valid</p>
	Periodically reviewed	<p>ÿTo review the safety adequacy of the plant in the light of its current and projected condition and against modern safety standards and expectations</p> <p>ÿTo take a strategic look forward to consider plant lifetime and contingency requirements</p>
Post Operation	Post- Operational Safety Case	ÿTo demonstrate that the plant is adequately safe for post operations care and maintenance activities prior to start of decommissioning (if such a period is appropriate)
Pre- Decommissioning	Safety Strategy Overview (applies to complex decommissioning projects only)	<p>ÿTo describe how safety will be managed through the proposed decommissioning programme for the project</p> <p>ÿTo demonstrate that there will be a progressive, timely and systematic reduction of hazard</p> <p>ÿTo define safety goals and criteria for the project as a whole</p>

Decommissioning	Decommissioning Strategy	<p>ÿTo set out in broad terms the approach that is to be followed during decommissioning</p> <p>ÿTo substantiate in principle the safety of the decommissioning task and demonstrate that there will be a progressive and systematic reduction of hazard</p> <p>ÿTo define safety goals and criteria for the decommissioning task</p>
	Safety Case(s) for Decommissioning Operations	ÿThe 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 plant modifications
Post- Decommissioning	Post-Decommissioning Clearance Safety Case	ÿTo demonstrate there has ceased to be any danger from ionising radiation from anything on the site.

FIGURE 1 - THE NUCLEAR SAFETY CASE IN CONTEXT

Inputs to the safety case:-

DEFINITION OF SAFETY	Safety policy	inc. principles and objectives
	Safety criteria	inc. statutory limits
	Safety standards	inc. international, national and licensee specific codes and standards

	Research and development	to determine appropriate criteria, standards, etc.
The achievement of which are demonstrated by a safety case which includes:-		
DEMONSTRATION OF SAFETY (The safety case)	Deterministic analysis	inc. the identification of limits and conditions in the interest of safety
	Engineering Substantiation	to show safety function delivery with appropriate integrity
	Probabilistic safety analysis	inc. sensitivity analysis
	ALARP arguments	inc. options considered
Which provides operational requirements and constraints to be implemented by:-		
IMPLEMENTATION OF SAFETY	Health and safety management system, monitoring, review and audit	[Managing for Safety at Nuclear Installations ^[11]]
	Operating rules and instructions	see LC 23 and 24
	Examination, inspection, maintenance and test schedules	see LC 28
	Emergency plans and instructions	see LC 11
and which is monitored and maintained by		
MONITORING AND MAINTENANCE OF THE SAFETY CASE	Safety case management processes	inc. modifications to plant & safety case
	Periodic review	inc. interim reviews
	Maintenance (etc) records	see LC 28
	Dose records	see IRR ^[12]
	Operating data	inc. incidents

APPENDIX 1 - DETERMINISTIC AND PROBABILISTIC ANALYSIS

The safety case for a nuclear plant (or modification etc) should be based upon a robust design, defence-in-depth and deterministic analysis of normal operations and fault behaviour. The latter should consider faults that are reasonably foreseeable during the lifetime of the plant and for which provisions have been designed into the plant to prevent or mitigate them. This is known as Design Basis Accident (DBA) analysis. In addition, a deterministic analysis should be undertaken of more severe faults and failures which have not been specifically protected against in the design and which, in the extreme, could lead to large releases of radioactivity. This constitutes the severe accident analysis.

To supplement and support the deterministic analysis, a probabilistic safety analysis (PSA) may be required. The requirement, depth and level of the PSA should be commensurate with the significance of the hazard. The PSA will provide the means to: identify failure scenarios; confirm the effectiveness of defence-in-depth provisions; search for weaknesses in the design; show there is a reasonable balance of risk for all hazards and operations; and derive numerical estimates of risk. The PSA provides a quantitative input to the ALARP case and it can provide estimates of the relative benefits (in terms of risk reduction) of improvements.

A brief description of these analyses is given below. Further details can be found in the NII Safety Assessment Principles⁶, notably on pages 6 to 10 with respect to fault analysis.

Deterministic Analysis

Normal Operation

The performance of the plant (structures, systems and components) under normal operating conditions should be analysed to demonstrate that all parameters (e.g. pressures, temperatures, stresses) are within allowable design values and that there are adequate margins of safety. This will include a comparison of the results of the analysis with relevant design code requirements and expected factors of safety.

The analysis of normal operating conditions should also consider doses of ionising radiation, to both members of the work force and the public. This should show that dose levels are (or will be) within the dose limits of the Ionising Radiations Regulations 1999¹² and have been made ALARP.

Design Basis Accident (DBA) Analysis

DBA analysis is a robust technical assessment of how the plant or operation in question responds to and is tolerant of fault conditions. It requires a thorough listing of all faults (i.e. a good fault schedule) that could occur during each foreseeable operating state. The investigation of potential consequences and the identification of effective protective measures

requires such techniques as analysis of plant transients, hydraulic studies and stress analysis (including the tolerance of plant and structures to defects in materials).

The safety case should include validation of the methods and models used for the DBA analysis. Uncertainty is allowed for by biasing the data and assumptions to ensure conservatism. Sensitivity studies should also be carried out to examine the effects of variations in key parameters (e.g. decay heat, heat transfer) to ensure there are no 'cliff edge' effects. That is, to demonstrate tolerance to a small increase in the severity of a design basis fault without there being a disproportionate increase in consequence. If there are 'cliff edge' effects, then measures need to be taken to prevent or mitigate against them (e.g. by design changes to the plant).

The DBA contributes to the identification of the plant's operating limits and conditions, as required by LC23, and to the demonstration that there are suitable and sufficient safety mechanisms (LC27).

Severe Accident Analysis

Severe accident analysis looks at severe faults and failures which are beyond the design basis and which could lead to large releases of radioactivity. The severe accident analysis should identify the potential failures of barriers to the release of radioactive material or of the shielding against direct radiation and determine the consequences of such failures. Efforts must be made to demonstrate that the likelihood of such failures occurring is very low.

The severe accident analysis differs from the design basis analysis in that it should be performed on a best-estimate (rather than a conservative) basis. This is because it contributes to severe accident management strategies and provides realistic guidance on emergency response actions. The severe accident analysis also provides an input to the Probabilistic Safety Analysis (PSA).

The safety case should include validation of the methods and models used for the severe accident analysis.

Probabilistic Safety Analysis (PSA)

The role of the PSA is to provide a systematic analysis of the plant and the role of its safety provisions. It is used to model complex interactions and is able to reveal design weaknesses that the application of engineering principles alone cannot guarantee to prevent. The PSA also helps identify where there is undue reliance on particular design features or on human performance, etc. Design changes can be considered if necessary, their effect can be analysed and optimised using the PSA. Ultimately, the PSA should give confidence that the plant's safety and protection features are suitable and sufficient.

The PSA provides an estimate of overall plant failure probabilities and the risks from the plant. This enables a comparison to be made with risk targets and provides an indication of whether or not the overall risk from the plant is tolerable¹³. The PSA thus contributes to the demonstration that risks are ALARP. Options for improvements can be investigated, using the PSA to compare their relative benefits and to estimate the reductions in risk.

It is important that the PSA is based upon the actual (or intended) design of the plant and uses data relevant to that plant. PSA requires an input of engineering and operational knowledge and judgement. If the PSA is done on the intended design it will need to be revisited if the intentions change after the PSA is complete, or when operational experience indicates that assumptions in the PSA are not borne out in reality.

It must be recognised that the PSA numerical results are not precise; they are estimates of the levels of risk and of the relative contributions to the overall risk from the plant. To enable meaningful comparisons the PSA should be based on best-estimate data where possible.

The safety case should include validation of the methods, models and assumptions used for the PSA. The analysis should include sensitivity studies to gauge the significance of the uncertainties regarding the methodology, modelling assumptions and data inputs. There should also be independent checking of the analysis and the PSA results - including a 'believability' check.

APPENDIX 2 - THE NUCLEAR SAFETY CASE IN CONTEXT; TYPICAL CONTENTS OF EACH ELEMENT

This Appendix provides more detailed examples of the type of information that should be contained in each of the elements shown in **figure 1** - namely: definition of safety; demonstration of safety; implementation of safety; and monitoring and maintenance of a safety case.

The typical contents set out below relate to a fully operational plant or facility. These should not be considered exhaustive because each safety case will be different and there could be other factors to consider. Also, these contents encompass different types of nuclear installations (e. g. reactors, reprocessing facilities) - the detail needs to be tailored to the nature of the plant or facility.

1. Definition of Safety

To demonstrate safety, it is first necessary to define 'safety' - namely the principles, criteria,

requirements and standards that need to be achieved. This will include the following:

- Safety principles (including ALARP concept).
- Safety objectives and limits (including levels of risk).
- Radiological protection targets and statutory limits.
- Design criteria and code requirements.
- Design basis requirements (e.g. fault tolerance and hazard withstand capability).
- Engineering standards.
- Material specifications.
- Quality requirements.
- Research and development to determine appropriate criteria, standards, etc.

2. Demonstration of Safety

This constitutes the safety case. In addition to analyses (etc) which demonstrate safety, it encompasses information which is required to enable the safety case to be understood (e.g. design details). It also includes the identification of requirements to implement safety (e.g. operating limits and conditions, maintenance, inspection and testing requirements). The safety case contents should cover (where appropriate):

- Site location - including topography, geology and proximity to population areas.
- Site layout - including location of plant(s) in question and site boundary.
- Plant description - including key function(s) and processes involved.
- Form and inventory of hazardous materials.
- Operating history of similar plants (if any).
- Operating pattern (e.g. shift or day operation).
- Novel design features.

- Proposed lifetime of the plant.
- Requirements for external services (e.g. electrical supplies, cooling water).
- Interfaces with other plants or facilities.
- Key design parameters (e.g. temperature and pressure).
- Key design data (e.g. design loadings, design transients).
- Design details - including main structures, systems and components.
- Safety categorisation of structures and systems.
- Engineered safety features and systems - including defence-in depth & diversity.
- Protection systems.
- Safety-related systems (e.g. control and instrumentation).
- Essential electrical supplies - including back-up generators and batteries.
- Containment and ventilation systems.
- Internal and external hazard identification and protection measures - including fire, flood, seismic and extreme environmental conditions.
- Equipment qualification proposals and results.
- Fault identification and fault schedule.
- Fault analysis - methodology and deterministic design basis and beyond design basis analyses.
- Human factors analysis - including man-machine interfaces and manning levels.
- Probabilistic safety analysis - including risk estimates.
- Demonstration of ALARP - qualitative and quantitative arguments (including “optioneering”).

- Radiological protection measures and dose assessments (operators and public).
- Radioactive waste handling and storage facilities.
- Plant condition monitoring and process sampling systems.
- Commissioning plans and test results.
- Through-life monitoring, maintenance, testing and inspection requirements.
- As-built information - including key plant drawings and construction records.
- Decommissioning strategy.
- Identified operational limits and conditions.
- Outstanding issues which need to be resolved, their importance and the work required to resolve them (with timescales).

3. Implementation of Safety

The definition and demonstration of safety are essentially documentary evidence of the standards of safety the plant can achieve. Implementation measures are needed to realise these standards and deliver safety case requirements. These measures include:

- Health and safety management system, monitoring, review and audit.
- Safety culture.
- Safe working practices.
- Quality assurance plans and procedures.
- Staff qualification and training programme.
- Adequate resources and staffing levels.
- Operating rules and instructions.
- Examination, maintenance, testing and inspection programme.

- Plant severe accident management plans.
- Site emergency plan.
- Radioactive waste management policy and strategy.
- Transport details for radioactive and other hazardous substances.

4. Monitoring and Maintenance of the Safety Case

It is necessary throughout the lifetime of the plant to periodically confirm the safety case is still valid and its requirements are being met. This will include the following:

- Safety case management processes.
 - Periodic safety reviews - including impact of all plant modifications.
 - Monitoring, inspection and test results.
 - Material properties degradation measurements (ageing mechanisms).
 - Transient measurements.
 - Plant performance and reliability data.
 - Quality assurance audit findings and corrective actions.
 - Operating experience feedback results and actions.
 - Radiation dose and chemotoxic exposure levels.
 - Radioactive discharge levels.
 - Research and development programmes to resolve any outstanding issues or areas of uncertainty.
-

APPENDIX 3 - SITE WIDE SAFETY CASE

1. Particular Purpose

- To demonstrate that the site as a whole is safe and to substantiate dependencies and claims made on it for individual plant safety cases.

2. Content

2.1 Site and Plants Description

- Description of the site and principal operations.
- Interfaces between plants (existing and proposed).
- Interfaces with other facilities, sites (existing and proposed).
- Plant dependencies on common services and other plants and demonstration of adequate provision of same, especially for events that can affect several plants at the same time, e.g. Seismic.

2.2 Safety Philosophy Throughout Site Life Cycle

- Principal operations, key safety hazards and risks, including overall site risk.
- Demonstration that all operations which may affect safety are addressed.
- Site wide topics such as:
 - staffing.
 - organisational structure.
 - radiological protection.
 - emergency planning.
 - management of radioactive waste.
 - environment impact.

- Emergency arrangements, especially the integration of site wide and plant arrangements.

2.3 Hazard Identification and Risk Management

- Overall hazards and risks from the whole site, including:
 - internal hazards.
 - external hazards.
- Safety substantiation, how hazards are controlled and why risks are ALARP.

1 The term stage as used in this guide encompasses both phases and stages as used in Licence Conditions.