




UK NUCLEAR SAFETY CASE FORUM GUIDE

Right First Time Safety Cases: How to Write a Usable Safety Case Issue 1, March 2014

	Name	Signature
Prepared by:	Carolyn Page on behalf of Workstream 2	
Endorsed by	Paul Sutton Workstream 2 Lead	
Approved by:	Keith Murphy/ Paul Sutton Chair, Safety Case Forum	

1 PURPOSE OF A UK NUCLEAR INDUSTRY SAFETY CASE FORUM GUIDE

- 1.1 Safety Case Forum Guides are produced by representatives of nuclear operators (nuclear site licensees and other companies with nuclear operations in the UK). Their purpose is *to provide guidance that is useful to a wide range of UK nuclear operators*. Such Guides do not set mandatory requirements on any nuclear operator, nor do they identify minimum standards. Guides provide a tool kit of methods and processes that nuclear operators can use if appropriate to their sites and facilities. The responsibility for justifying arguments in Safety Cases remains with nuclear operators.
- 1.2 The Safety Case Forum reports to the UK nuclear industry Safety Directors Forum (SDF). The companies represented at the Safety Case Forum include companies that cover:
- civil and defence activities;
 - design, operation and decommissioning of nuclear facilities;
 - low hazard and high hazard nuclear facilities.¹

2 INTRODUCTION

- 2.1. *'The Safety Case regime has lost its way. It has led to a culture of 'paper safety' at the expense of real safety.'* This is a direct quote from 'The Nimrod Review', undertaken by Charles Haddon-Cave QC, which highlighted many failings with the Nimrod Safety Case (Reference 1). Haddon-Cave goes on to describe the production of the Nimrod Safety Case as *'a story of incompetence, complacency, and cynicism'* and with reference to the Safety Case states that *'the best opportunity to prevent the accident to XV230 was, tragically, lost.'* In reality, findings presented in 'The Nimrod Review' with respect to the Nimrod Safety Case may be just as applicable to other Safety Cases in other industries.
- 2.2. Safety Cases should be 'Right First Time'; the right case, produced at the right time and to the right quality. If a Safety Case is well written, proportionate, technically accurate and flexible, it will be easy to implement, easy to comply with and therefore more likely to be worked to. Improvements in the way in which Safety Cases are produced and presented should result in Safety Cases being simpler, clearer and more readily understood by all stakeholders. This should in turn enable improved configuration control and result in Safety Cases that are easier to keep up to date and ultimately, an overall improvement in safety.
- 2.3. The SDF Safety Case Forum recognises that Safety Cases are notoriously long, complicated, overly technical and difficult to follow. Some licensees feel that they are producing Safety Cases for the regulator, not for themselves and yet they frequently fail to satisfy the regulator being accused

¹ Companies and organisations represented at the Safety Case Forum include: AWE plc, Babcock International Group plc, BAE Systems plc, Dounreay Site Restoration Limited, EDF Energy plc, GE Healthcare, Horizon Nuclear Power, Imperial College London, LLW Repository Ltd, Magnox Limited, Ministry of Defence, NDA Radioactive Waste Management Directorate, Research Sites Restoration Ltd, Rolls-Royce plc, Sellafield Ltd, Springfields Fuels Limited, Studsvik UK Ltd, United Kingdom Atomic Energy Authority, URENCO UK Limited

of producing Safety Cases that do not “tell the story” and Safety Cases where the “claims, argument evidence trail goes cold”.

- 2.4. Therefore, the SDF Safety Case Forum have produced this guide following a recommendation made in ‘The Nimrod Review’; that Safety Cases should be based on six principles (see SHAPED below). Further to this, it is the considered view of the SDF Safety Case Forum that usable, ‘Right First Time’ Safety Cases fundamentally also depend on good Preparation (PSHAPED).



- 2.5. This guide has a dedicated section to **Preparation**, **Home grown** and **Proportionate**. As there is a natural overlap between the intent of **Succinct**, **Accessible**, **Easy to understand** and **Document-lite**, a combined section follows to cover these remaining aspects of **PSHAPED**, collectively termed ‘Usability’.
- 2.6. This guide also includes a high level checklist that could be used by authors, checkers or peer reviewers to confirm that Safety Cases are indeed fit for purpose (appendix 1). Furthermore, to provide inspiration, a ‘Tool Kit’ and examples that have been used by Licensees or Authorisees to set expectations around the Safety Case process, to simplify Safety Cases or to communicate their content more effectively are provided (appendices 2 and 3). Where appropriate, these are referred to at the end of each PSHAPED section.
- 2.7. Finally, it is noted that this guide intentionally focuses on the following aspects of producing ‘Right First Time’, usable Safety Cases: strategy, ownership, proportionality and presentation. Safety Case Forum guides concerned with technical methods are addressed by a separate workstream SDF Safety Case Forum.

3 PREPARATION

- 3.1 The first step in ensuring that Safety Cases are **SHAPED** is **Preparation**. Preparation is needed as Safety Cases frequently fail because scope changes, the right people are not involved or interactions are not understood. Preparation entails derivation of arrangements for Safety Case development work and specification of Safety Case deliverables. Therefore before beginning the Safety Case it is essential to address the following:



- 3.2 **Obtain resources:** the Safety Case must be adequately funded, however, equally important is ensuring that the right people have been identified to support the generation of the Safety Case. It is therefore important to involve the relevant senior managers who control both budgets and resources. Leadership should be provided by the Safety Case Owner who should be the senior person in charge of the plant for which the Safety Case is required and has the overall responsibility for safety on the plant i.e. the duty holder. A Suitable Qualified and Experienced Person (SQEP) Safety Case Manager who is responsible for the delivery and implementation of the Safety Case should also be identified.
- 3.3 SQEP resources are needed for all steps in the Safety Case process (including Intelligent Customer resources where applicable).
- 3.4 It is important that the plant owner appreciates the value that plant knowledge and experience brings to the Safety Case. The inclusion of plant personnel as part of the Safety Case team will give confidence that the Safety Case will be both accurate and capable of being implemented (including clarity of operating and maintenance requirements). Failure to involve plant personnel from the beginning is likely to result in documentation containing errors or omissions and Safety Cases that are not optimal in terms of using existing plant equipment and operational controls. Such Safety Cases are frequently thrown out in the latter stages of the process, alternatively they may be implemented but cause the plant operational problems. In either case the result is often programme delays and increased cost. Even where the plant is brand new operational experience can be gained from people who operate similar and interfacing plants.
- 3.5 Key responsibilities should be identified including how confirmation of the validity of the Safety Case assumptions will be established and who will confirm that the Safety Case is in line with the current status of the plant or design.
- 3.6 All key users of the Safety Case should be identified and represented within the team to ensure that the Safety Case will meet user requirements. The Safety Case authors must not work in isolation but collaboratively with the design team, plant representatives and other users.

- 3.7 **Establish a clear scope and purpose for this Safety Case:** what do we want this Safety Case to do? It is essential to gain a common understanding of why we need the Safety Case and in particular why we need this one. Relevant and appropriate standards and criteria must be established and any known problem areas together with the degree of difficulty posed should be identified. The Safety Case that is being written must be consistent with any over-arching strategy and any interactions and dependencies must be understood and agreed by relevant stakeholders.
- 3.8 **Make the process work for you:** ensure that Safety Case production process requirements and constraints are understood. Involve the Safety Case process owner at this stage in order to:
1. establish the health of the Safety Case process and any specific measures required to ensure it remains robust for the Safety Case in question;
 2. identify any mandatory elements; and
 3. identify the inherent flexibility within the process so as to avoid application of unnecessary constraints.

Remember that the requirement for the use of templates etc may be necessary where consistency is important but it is essential that the Safety Case is bespoke. This is a useful time to engage the independent assessors and those responsible for checking the output particularly if the approach to be taken is novel.

- 3.9 **Use Learning From Experience (LFE):** identify any relevant learning from experience and ensure that it is appropriately incorporated into the Safety Case generation process. LFE should be drawn from the approaches of other licensees and include any known problems that have been experienced with previous Safety Cases. These are traditionally not covered in Operating Experience (OPEX) systems.
- 3.10 **Understand what success will look like:** establish a set of Fit-for-Purpose requirements against which you will measure the output. Consider who will test the output and fitness for purpose (links to 'obtain resources' above). Ensure that fitness for purpose requirements encompass accessibility and usability.
- 3.11 Establish an architecture for the totality of the Safety Case and agree it with stakeholders so that expectations are aligned, gaps can be identified, progress can be monitored and changes during development can be managed.
- 3.12 One indicator relating to the fitness for purpose of a Safety Case is to use recognition statements (Tool 3).
- 3.13 **Establish and maintain a strategy for the delivery of the Safety Case:** how will the Safety Case be generated and approved? It is assumed here that the approach has already been subject to optioneering and the defined approach is deemed to be As Low as Reasonable Practicable (ALARP). The strategy and rationale with respect to outsourcing Safety Case work should be addressed at this stage as this can have a significant effect on delivery.
- 3.14 Once a strategy has been established, a plan and programme can be generated, baselined on the requirements and architecture for the final

product. The plan and programme must be realistic (as opposed to simply making the Safety Case fit the time decreed by others).

- 3.15 Ensure that the strategy together with the plan and programme is adhered to or reviewed and revised appropriately. Consider external validation at key points in the development to independently confirm that the strategy and scope is being delivered and that if there is any deviation, it is adequately explained and justified. The Safety Case Owners should ensure they have a good understanding of how the Safety Case is progressing with respect to the plan and identify early any issues that may impact on the success of the Safety Case. The use of the Safety Case health check or a similar approach may be useful here (Tool 2).

Preparation Tools		
1	Nuclear Safety Requirements Specifications & Statement of Safety Case Strategy	Can be used to formally identify a 'problem statement' and propose an associated strategy for the Safety Case.
2	Issues register & Technical Forum	Can be used to track, highlight and address issues identified during production of the Safety Case.
3	The Peer Assist process	Can be tailored for specific problems large or small and could be useful in aiding the Safety Case Owner to formulate and express their expectations.
4	The Safety Case Health Check	A tool for using leading indicators to establish the health of a Safety Case and the likelihood of failure.
5	Recognition Statements	Can be used to gain confidence in the Safety Case process.
6	Principles and Guidance	An effective way of establishing the required team and engendering their values, requirements and expectations.

4 HOME-GROWN

- 4.1 It is essential to establish clear ownership of the Safety Case. It is expected that the owner is the person who has or will have ultimate responsibility for the safety of the plant and personnel operating it. The role of the owner is one of leadership, giving direction and support and to ensure that the right people are available to support the project. A good Safety Case Owner will:
- Ensure commitment from the team.
 - Establish resourcing in terms of funding and personnel is adequate.
 - Ensure the availability of a Project Manager to ensure delivery to appropriate timescales.
 - Ensure that all specified roles are appropriately filled and responsibilities are clear.
 - Identify the intelligent customer for a) individual pieces of work (safety assessments, substantiation reports etc.) and b) the totality of the case i.e.: how it fits together and is fit for purpose (who will do the fit for purpose test?).
- 4.2 Whilst the Safety Case Owner should be a formal role identifying the person with ultimate responsibility, it is equally important that the Safety Case is considered as belonging to the plant and the people who operate and maintain it. The Safety Case must not be considered as belonging to the authors of the documentation.
- 4.3 It is vital that the team producing the Safety Case are the best people for the job – the Appropriate Team, herein referred to as the “A team”. The key experienced personnel must not be considered to be “too important” to spare the time in the generation or review of a Safety Case. It is these people that **must** be involved. The A team must be knowledgeable, competent and have the correct behavioural skills.
- 4.4 Typically the A team would contain:
- Operators to feed in operational experience from this or similar plants and to make sure that the operational controls can be implemented as described.
 - Maintainers to feed in experience of working on this or similar equipment to make sure that the equipment claimed is as described, can be relied on and can be maintained.
 - Plant Managers who will have to live with the Safety Case that is produced.
 - Authors (Safety Assessors and Design Engineers) to generate safety assessments and substantiation reports that will form the basis of the Safety Case. These people are unlikely to be based on this or other plants but prior to writing the documentation they must establish a good understanding of the plant through plant visits and meetings with plant personnel.
 - A representative of the Safety Case Owner acting as the ‘controlling mind’.
- 4.5 Other personnel such as technical support, Radiation Protection Adviser (RPA), OPEX teams and assurance personnel may also be appropriate. Other key stakeholders may need to be engaged at various points of the process and these should be identified as soon as possible.

- 4.6 The A team must be involved from the development of the purpose and scope throughout all stages of the project. Rules of engagement should be established including a commitment to honesty and telling it how it is rather than attempting to identify only the good news (Tool 4). Use of the A team will enable the unknown, uncertainties and assumptions to be minimised and clarified thus giving the most robust basis for the case that is to be produced.
- 4.7 Focus must be on the end users and their involvement throughout to ensure that the outputs **demonstrate that the risks are ALARP** (or will be ALARP once improvements are made) and are in a form that is understandable and usable.

Home-grown Tools

3	The Peer Assist process	Can be tailored for specific problems large or small and could be useful in aiding the Safety Case Owner to formulate and express their expectations.
5	Recognition Statements	Can be used to gain confidence in the Safety Case process.
6	Principles and Guidance	An effective way of establishing the required team and engendering their values, requirements and expectations.

5 PROPORTIONATE

- 5.1 The depth of the Safety Case is **proportionate** to the hazards/risks/complexity of the assessed operation (noting that risks in particular are not always well understood at the start of a Safety Case project).
- 5.2 When preparing the Safety Case:
- For lower hazard operations, use simpler methods of fault identification, e.g. SQEP review, or desk-top study, rather than a Hazard and Operability (HAZOP) study.
 - Use methodologies that are appropriate for the potential consequences, for example Low Consequence Methodology.
 - Use methodologies that are **proportionate** in themselves. For example the depth of engineering substantiation, and the extent of reporting of the substantiation, are related to the safety function class. Similarly, the depth of Human Factors analysis is **proportionate** to the extent of safety-dependence on human actions.
 - Use semi-quantitative and qualitative techniques as appropriate. Use fully quantitative techniques where appropriate, for example when Basic Safety Objectives may be approached or exceeded or if they present a simpler and clearer argument.
 - Avoid over-pessimism that artificially inflates the significance of a hazard.
 - Avoid optimism. The organisation responsible for safety of the operation is involved in the **preparation** of the Safety Case, encouraging realism.
 - Key assumptions should be underpinned. Where appropriate, sensitivity studies should be used to determine how sensitive the basis of assumptions are.
 - Apply ALARP **proportionately**, for example:
 - ❖ if there are major/significant shortfalls, demonstrate full consideration of options;
 - ❖ if there are minor shortfalls, use a qualitative checklist; or
 - ❖ if there are no shortfalls, demonstrate ALARP proportionality.
- 5.3 A **proportionate** Safety Case looks like this:
- Due emphasis is placed on hazards and findings, **proportionate** to their significance to the overall safety argument.
 - The extent of pessimistic assumptions is made clear, including their broad effect on the assessed numerical risk.
 - The Safety Case presents a balanced account, taking into consideration the level of knowledge and understanding.
 - Designated equipment and procedures, that the Safety Case requires to be implemented in the facility, are **proportionate** to the hazard.
 - Where most of the inventory has been removed from a facility as part of decommissioning, the depth of the baseline Safety Case reduces **proportionately**.
 - The summary safety report focuses on key hazards/risks, with brief acknowledgement of other hazards/risks.
- 5.4 The degree of scrutiny applied to the Safety Case is **proportionate** to the credible conservative consequences of potential accidents (noting that the declared consequences in the Safety Case are themselves subject to independent review).

Proportionate Tools

2	Issues register & Technical Forum	Can be used to track, highlight and address issues identified during production of the Safety Case.
3	The Peer Assist process	Can be used, for example, to collaboratively work through real examples of applications of proportionality or used to confirm approach is proportionate, e.g. approach to engineering substantiation.
7	Proportionality Matrix	Can be used to help determine the relevant proportionate Safety Case activity at defined steps, according to the level of hazard.

Proportionate Examples

4	Integrated Risk Assessment Process	Can be used as a proportional means of assessment for low radiological consequence activities and environmental hazards.
---	------------------------------------	--

6 USABILITY

- 6.1 A usable, and therefore useful, Safety Case should be **accessible, easy to understand, succinct** and **'document-lite'**.
- 6.2 It is important that users can access the Safety Case to easily understand the hazards and risks on their facility, and what keeps the facility safe. Key users can be easily deterred from reading a safety case simply because it is too long. At first sight, 'Document-lite' looks to be impossible for a safety case, which in practice is either a document or (more likely) a whole suite of documents, but 'Document-lite' doesn't mean the safety case in totality comprises only a few documents. The term 'Document-lite' reflects the need for a focussed, well structured safety case that clearly presents the safety arguments and the information necessary to operate safely. Technical detail and supporting information should be presented in lower level documentation.
- 6.3 Length can also be the enemy of clarity, so succinctness can improve the understanding of those who read the safety case.
- 6.4 Usable Safety Cases should:
- **Focus on managing risk.** The documentation is an important output from this process, but should not be treated as an end in itself.
 - **Clearly define the scope, and keep within it.** Do not attempt to include what is (or will be) in another document.
 - **Focus on what the key users and stakeholders need to know.** The Safety Case must tell the story. It should be easy to identify the key hazards and risks on the plant and the link between safety and engineering substantiation must be apparent (Examples 1, 4, 6, 7).
 - **Be easy to navigate.**
 - ❖ Think about how the layers of information fit together and how the users of the safety case will be able to navigate their way through the safety case.
 - ❖ Don't let a prescribed safety case structure (or individual document structure) prevent you from being succinct – challenge the structure if appropriate.
 - **Present information clearly and concisely.** Keep it short, sharp and focussed. Do not ramble. Text alone is unlikely to efficiently convey all of the information presented within a Safety Case; other techniques may be more effective in particular instances. Consider alternatives (or supplements) to text for presenting each piece of information recognising the needs and capabilities of the various user groups, such as:
 - ❖ Photographs – they can illustrate a piece of equipment more effectively than text alone (although be aware that they may not photocopy well).
 - ❖ Tables and graphs (tables are better than graphs for giving structured numeric information; graphs are better for indicating trends and making broad comparisons).
 - ❖ Timelines and fault progression diagrams (to easily see the progression of a fault with associated timescales if appropriate to feed into crucial decision making in response to a fault (Example 6)).
 - ❖ Flowcharts (ideal for presenting a Safety Case decision making process for use on a facility (Example 3)).
 - **Be easy to understand.** Where text is preferred, use plain English where practicable and avoid obscure and difficult to understand language;

keep the punctuation simple. Use the most appropriate grammatical tense for the type of document (e.g. passive is useful for descriptive texts, active is appropriate for instructions). When addressing comments, consider removing (or slimming down) text rather than forever expanding the text to address many different comments.

- **Be easy to access.** If databases, spreadsheets or proprietary software is used, consider what information may be needed by the various users and whether they have access to it. As appropriate, provide software, training and/or extract relevant information in the form that users require. (Tool 6, Examples 1, 2, 3, 4, 5, 6, 7)
- **Flow well.** Keep the text logical. Do not write anything that adds nothing (or very little) to the safety argument.
- **Minimise repetition:**
 - ❖ When using information/data from another document, summarise the information/data, and reference out (using hyperlinks if possible) to the other document, so that any interested reader can delve into how the information/data is derived.
 - ❖ Sometimes repetition is useful and important, for example to summarise (perhaps in tabular format) the key equipment and procedures that are important to safety. Some repetition may improve accessibility to a plant operator, for example if it means all information relating to a specific hazard is in place (i.e. makes it easier to navigate).
- **Use up to date, relevant references/supporting information.** In the absence of directly relevant data, the use of inferred or extrapolated information needs to be carefully substantiated.
- **Be clear on what needs implemented.** Operating and maintenance requirements, including key operating limits and conditions, should be identified clearly to avoid ambiguity and/or interpretation, This is an essential link between the written safety case and safety on the plant.
- **Allow key users and stakeholders to test success in whether a safety case is accessible, easy to understand, succinct and 'document-lite'.**

Usability Tools		
8	Safety Case IT Tools	Supports a 'live' Safety Case with improved access to, and presentation of, relevant data and information sources.
--	Usable Safety Case Checklist (Appendix 1)	Suggests some key considerations for a usable Safety Case.
Usability Examples		
1	Safety Case on a Page	Can be used to summarise the main information from the Safety Case in a style that is easily accessible. It allows the main hazards and controls for a facility to be visible on plant and understood.
2	Safety Case Assumptions	Can be used to capture assumptions on which the Safety Case is based (and which operators have no control over) and allow them to be compiled into a complete, comprehensive list ensuring consistency across the Safety Case which may be kept live without repeating them in the relevant assessments.
3	Flowcharts	A good way of presenting information, for example a key decision making process, in a clear and logical manner which may be difficult to explain or may be open to interpretation if written as text only.
4	Integrated Risk Assessment Process	Can be used as a proportional means of assessment for low radiological consequence activities and environmental hazards.
5	Visual management of safety designations	Provides a succinct summary of information in a style that is easily accessible. It allows the main hazards and controls for a facility to be visible on plant and understood. It can be used as part of training, as pre job briefs and displayed local to the hazard.
6	Timeline with 'swim lanes'	Maps different faults onto a single timeline. Provides a succinct summary of information in a style that is easily accessible and easy to understand. It can be used in assessments, as part of training, as pre job briefs and displayed local to the hazard.
7	Alarm Sequence Colour Charts	Can be used to help explain the order in which alarms occur (those identified in the Safety Case and normal plant alarms) for a complex fault. The principle could be applied to other indicators or layers of defence for a fault.

7 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
<http://www.official-documents.gov.uk/document/hc0809/hc10/1025/1025.pdf>

8 FURTHER READING/FURTHER INFORMATION

- 8.1 Safety Assessment Principles for Nuclear Facilities, Health and Safety Executive, 2006 Edition, Revision 1
<http://www.hse.gov.uk/nuclear/saps/saps2006.pdf>
- 8.2 ONR Nuclear Safety Technical Assessment Guide: The purpose, scope, and content of Safety Cases. NS-TAST-GD-051, Revision 3. HSE. July 2013.
http://www.hse.gov.uk/nuclear/operational/tech_asst_guides/ns-tast-gd-051.pdf
- 8.3 Technical Inspection Guide: LC14 Safety Documentation. NS-INSP-GD-014. Revision 2. HSE. May 2013.
http://www.hse.gov.uk/nuclear/operational/tech_insp_guides/ns-insp-gd-024.pdf
- 8.4 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
<http://www.official-documents.gov.uk/document/hc0809/hc10/1025/1025.pdf>
- 8.5 Safety Directors' Forum Safety Case Forum website
<http://www.nuclearinst.com/SDF>

APPENDIX 1: USABLE SAFETY CASE CHECKLIST

The purpose of this appendix is to facilitate the production (and update) of usable Safety Cases. Consider the following:

PREPARATION	Complete?
Identify the Safety Case Manager and Safety Case Owner.	
Identify key users of the Safety Case to be included in the generation of the Safety Case.	
Identify SQEP resources (and associated key responsibilities of those resources) for the generation, substantiation and implementation of the Safety Case and secure funding for those resources. This must include plant personnel.	
Establish a clear scope and purpose for the Safety Case.	
Understand Safety Case process requirements; involve Safety Case Process Owner to identify mandatory elements and opportunities for flexibility within the process.	
Identify LFE and incorporate it into the Safety Case generation process.	
Establish a set of fit for purpose requirements of the Safety Case to measure the output against. This must include usability.	
Determine and agree the strategy for delivery of the Safety Case incorporating a realistic plan and programme.	
HOME-GROWN	Complete?
Ensure the Safety Case owner leads, directs and supports generation and implementation of the Safety Case.	
Establish the "A team" early. The "A team" must be knowledgeable, competent and have the desirable behavioural skills.	
Identify other stakeholders and engage them at the appropriate stages in the process.	
PROPORTIONATE	Complete?
Ensure that the depth and level of scrutiny applied to the safety case is proportionate to the hazards being considered. For example; fault identification, methodologies, the depth of engineering substantiation (and reporting of); the depth of Human Factors analysis etc is appropriate for the level of risk.	
Ensure any equipment and/or safety measures are proportionate to the level of risk.	
Ensure the Safety Case presents a balanced account.	
Ensure ALARP is applied proportionately to any shortfalls associated with the Safety Case.	

USABILITY	Complete?
Use plain English where practicable throughout the Safety Case.	
Use visual aids where relevant to better present information in the Safety Case, e.g. tables, graphs, flowcharts, timelines etc. Consider using each of the tools and examples provided.	
Present information clearly and concisely.	
Minimise repetition.	
Keep the Safety Case succinct (with technical detail and supporting information in lower lever documents).	
Test the usability of the Safety Case with key users.	
OVERALL	Complete?
Confirm that the Safety Case tells the story.	
Ensure it is clear what the main hazards are and what keeps the plant and people safe.	
Confirm the Safety Case demonstrates that the risks are ALARP.	

APPENDIX 2: TOOL KIT FOR USABLE SAFETY CASES

TOOL 1 **Nuclear Safety Requirements Specifications and Statement of Safety Case Strategy** used by Magnox Ltd

Nuclear Safety Requirements Specifications (NSRS) are used to demonstrate that the Company's nuclear safety criteria are being met. They are effectively "problem statements" used to detail up-front:

- the nuclear safety case issues that need to be addressed; and
- the reliability and integrity requirements for any modification.

The NSRS is a brief pro-forma document that aims to provide an early input into the planning process by presenting guidance on nuclear safety issues and technical skills requirements. The process of preparing and agreeing an NSRS is designed to encourage team working and to avoid costly rework. Consequently, the NSRS will normally be prepared and agreed prior to the commitment of significant resources.

Statement of Safety Case Strategy presents anticipated safety arguments at a level sufficient to:

- Allow project stakeholders to confirm that the safety submission approach is consistent with the agreed project objective and overall project strategy.
- Allow confirmation by stakeholders that the approach is acceptable taking account of; the project requirements, relevant issues external to the project, the significance of the project and its potential impact upon the Company.
- Show how the key safety issues will be addressed to show compliance with the relevant safety criteria.
- Identify the key technical inputs required to secure the safety case.
- Identify the risks associated with the key technical inputs.
- Allow all members of the project team to see the link between their work and the safety case requirements and thus allow early recognition of events detrimental to the proposed strategy.

The Statement provides a formal record of the agreed strategy and of any revisions that follow. It is recommended that a draft statement is prepared early in the project as an input to setting the overall project strategy and a formal statement produced once the overall project strategy has been agreed.

TOOL 2 **Issues Register and Technical Forum** used by Magnox Ltd

Issues Register supplements the NSRS (Tool 1) by recording (and facilitating sentencing of) key nuclear safety issues that arise during the safety case production process. An issue is, therefore, a matter arising during the production process that has (or could have) a significant bearing on the safety case arguments.

The **Technical Forum** provides technical support and advice to the Safety Case Manager to address emergent issues during the safety case production process on major/complex projects. INSA should be part of the core membership to ensure that they are exposed to the safety case production process and, in particular, provides an opportunity for them to offer an early view on the acceptability (or otherwise) of the proposed approach.

TOOL 3 Peer Assist
used by Sellafield Ltd

Peer assist is a flexible, collaborative team problem solving tool. It can be used to produce a robust scope and strategy that will lead to a Safety Case that is home grown, proportionate to the risk, implementable, flexible and thus likely to be worked to.

The peer assist is owned by the facility and execution is facilitated and supported by Safety Case teams, Engineering and Plant as appropriate. When the Safety Case strategy is well defined the peer assist can be used to identify potential barriers and their solutions, validate the approach, consolidate the team and secure high level buy-in. It promotes ownership of the outcome through collaborative team working and therefore the Safety Case is likely to succeed.

Peer assist can be applied at any time or any stage in the lifecycle of a Safety Case and it can be applied to any size of problem from an entire project to a single task. It can be used to help resolve issues, to further seek innovation, to seek proportionality, validate or support novel approaches. Peer assist need not be a 'one stop shop': the process can be revisited in the same, smaller or different teams as the strategy and the Safety Case develops.

TOOL 4 Safety Case Health Check
used by Dounreay Site Restoration Ltd

A tool which involves a review of leading indicators that act as an early warning that a Safety Case is about to be de-railed.

The indicators to be considered include, but are not restricted to:

- **Multiple changes in scope** – does the Safety Case accurately reflect the required scope or has it been “cobbled together” and forced to look like it fits?
- **Changes in funding** – has the Safety Case been able to fully explore all aspects or have some areas been trimmed back? Has this affected the scope?
- **Changes in customer** – has the direction and scope of the Safety Case changed? Has the revised scope also included a revised production timescale? Does the customer own the documentation or have they merely inherited it?
- **Changes in personnel** – including Safety Case Owner, Safety Case Manager, Project Manager, Author and Independent Nuclear Safety Assessment (INSA) Assessor – has the Safety Case production process had a core thread running through it which can maintain an overview of purpose and quality?
- **External feedback** – is there any third party feedback e.g.: tier 2 or tier 3 assurance, INSA comments or Regulator response to submitted Safety Case documentation? Are there areas of concern? Are there any trends that might suggest deterioration in quality?

This tool could be built into the assurance process, or project management processes. As a guide it is suggested that three months is an appropriate review period and if more than 2 applicable flags are identified a review to ensure the Safety Case is not de-railed should be prompted.

TOOL 5 Recognition Statements
used by the Atomic Weapons Establishment (AWE) Aldermaston

A tool to gain confidence that the Safety Case process and associated Safety Case Improvements are being actively implemented.

It is recommended that the Safety Case Owner asks himself the following questions:

- Do I see and hear engineers, operators, Safety Case personnel and other contributors working together to identify and address safety issues as part of their normal routine?
- Do I hear designers, Safety Case personnel and other contributors challenging perceptions, assumptions, custom and practice?
- Do I see that the safety argument presented in safety documentation is logical, transparent and founded firmly on evidence that relates to the true state of the design, facility, system or activity that the Safety Case relates to?
- Do I hear that process operators, maintainers and other facility personnel have been engaged in the preparation of the Safety Case and find the outputs useful in helping them understand what they have to do to control hazards?
- Do I hear discussions about how to reduce risks further, even if the Safety Case concludes that risks are acceptable?

- Do I see that decisions have been made by taking full consideration of the safety issues, that they incorporate measures to manage any residual risks and that the outcomes are reflected in safety documentation?
- Do I see that safety documentation has undergone an appropriate process of review and approval, culminating in commitment from the person responsible to actively manage the risks that have been identified?
- Do I see only quality assured, fit for purpose safety documentation being submitted for review and/or approval in line with the 'right first time Safety Case' principle?
- Do I hear that regulators have confidence in the Safety Case process and the Safety Cases it produces?

TOOL 6 Principles and Guidance
used by Sellafield Ltd

Principles and guidance is a strategy paper written collaboratively by the whole "A team" to promote buy in from all stakeholders on their allocated roles and responsibilities.

The purpose of the collaboratively produced paper is to:

- identify the strategy for delivery of the Safety Case;
- identify the scope of the Safety Case;
- identify the team and their roles and responsibilities;
- highlight the behaviours and commitment needed from the team and Senior Management to support this view;
- outline the timescales for the revised process explaining what the proposed document submissions will be and when; and
- provide the regulator and Management with confidence that the process employed fulfils regulatory requirements.

TOOL 7 Proportionality Matrix
developed by Magnox Ltd, used by LLWR

The Proportionality Matrix can be used to help determine the relevant proportionate Safety Case activity at defined steps, according to the level of hazard.

The level of hazard used in the matrix is not defined numerically, but approximates to high, intermediate and low and should reflect the potential radiological consequences from faults/hazards. Whilst not specifically identified as criteria in the matrix, factors such as the novelty/complexity of safety arguments, the magnitude of safety margins and the level of reliability required should influence the effort expended in developing a Safety Case.

Extract from proportionality matrix				
Process Steps	Hazard			Comments
	High	Medium	Low	
Identify risk activities and associated hazards	Full HAZOP process, HAZOP 0, 1, 2 etc	Simple HAZOP, Safety walk-down	Desktop HAZID by SQEP. Review of fault sequences for similar facilities.	Normal HAZID methods, HAZOPS etc can be high effort activities with numerous contributors. Where the hazard is low (and the process is not complex) simpler methods should be considered.
Consequence	Potentially more effort required to obtain realistic results i.e. modelling.	Same as high hazard	Simplified assessment – make simplifying assumptions Sufficient to demonstrate that even with overly pessimistic (but still realistic) assumptions, consequences remain low.	High effort activity. Dose assessments for deterministic cases should be conservative. Cut-offs (at very low dose levels) are a measure of proportionality. Sensitivity analysis can support the justification of realistic assumptions.
Deterministic Assessment	Develop fault schedule for significant faults with on- & off-site consequences - determine requirements for safety measures or safeguards, dependent upon the exact combination of Initiating Event Frequency (IEF) and potential consequence. Demonstrate Design Basis Accident Analysis (DBAA) requirements are met or justify ALARP if not.		Select faults for application of Low Consequence Methodology (LCM).	Proportionality by default in that consequences drive designations appropriate to the hazard.
Substantiation - Engineering	DB1/DB2 regions – full substantiation of claimed measures (functional capability, adequate reliability & integrity). Independent Technical Assessment/Design Verification.	LC region – demonstrate good engineering practice.	ALARP region – not formally claimed, no substantiation required, good engineering practice is sufficient.	Substantiation of structures, systems and components (SSCs) can be a high effort activity. Proportionality is applied by classification of SSCs based on significance of consequences they protect against.

TOOL 8 Safety Case IT Tools
used by Sellafield Ltd

A method of working that supports having a 'live' Safety Case, with IT system/tools providing the enabling elements to managing key production, implementation and maintenance data/information. The key benefits include;

- Significant reduction in Safety Case administration in Safety Case teams, assessors and engineering across the delivery business units.
- Improved access to and presentation of relevant data and information sources.
- Consistency in approach to data and documentation management – improving the potential for a more mobile skilled work force.

The solution to this identified need comes in three forms noting that each individual component may or may not be used in totality;

Safety Case Index

The Safety Case Index provides an intranet based 'window' into Safety Case information and documentation that already exists and is maintained elsewhere in multiple other managed systems. The desire is to provide direct access to existing information, not to duplicate information, thereby not taking additional storage space or becoming out of date

Safety Assessment Tool

An optional tool: assessments use a more 'spreadsheet-like' approach to the presentation of key safety assessment information, rather than the traditional Word document approach. This enables early production and clear, concise presentation of safety assessment data to key functions, facilitating earlier and structured collaboration and providing a sound basis for decision making and final assessment production. Critically, it also provides the source configuration data used by the Safety Case Configuration System

Safety Case Configuration Database

The Safety Case Configuration Database is a repository for all necessary data, information and references required to support the Safety Case and to produce the clearance certificate for a Safety Case. It reduces the administrative burden of managing this data and reusing this data where required, i.e. the 'write once, use many' principle. Furthermore it will encourage centralisation and be a step towards reducing the proliferation of Microsoft Access databases currently used to record this type of information locally.

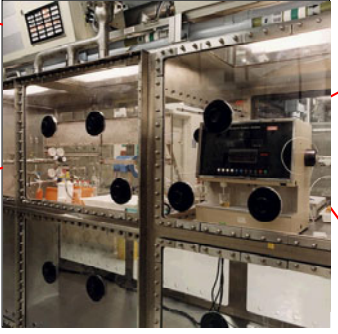


APPENDIX 3: EXAMPLES FROM USABLE SAFETY CASES

EXAMPLE 1 Safety Case On a Page
used by the Atomic Weapons Establishment (AWE) Aldermaston

Safety Case on a Page can be used to summarise the main information from the Safety Case in a style that is easily accessible. It allows the main hazards and controls for a facility to be visible on plant and understood. It can be used as part of training, as pre job briefs and can be displayed local to the hazard.

Safety Case On A Page – The significant process hazards and controls on YOUR plant



(5) Safeguard
State the safety function of the control measure here

(1) Safeguard
State the safety function of the control measure here

(4) Mitigation
State the safety function of the control measure here

(3) Safeguard
State the safety function of the control measure here

(2) Safeguard
State the safety function of the control measure here

PROCESS AREA NAME

- Main Hazards**
Hazard ⚠ Hazard ⚠ Hazard ⚠
- Operating Instructions**
Operating Instruction - Reference of relevant Operating Instruction
- Operating Rules**
Operating Rule 1 – Text of Operating Rule 1 to be written here
Operating Rule 2 – Text of Operating Rule 2 to be written here
- DAP Requirements**
DAP Requirement 1 – Text of DAP Requirement 1 to be written here
DAP Requirement 2 – Text of DAP Requirement 2 to be written here
- Safe Operating Envelope**
Safe Operating Envelope - Reference of Safe Operating Envelope

What can go wrong?	What safety controls PREVENT the hazardous event from occurring?	Hazardous Event	What safety controls MITIGATE the hazardous event?	Consequence
--------------------	--	-----------------	--	-------------

Initiating Event A	(1) Safeguard		Mitigation	
Initiating Event B	Safeguard	Description of event	Mitigation	Consequence ⚠
Initiating Event C	(2) Safeguard	Description of event	Mitigation	Consequence ⚠
Initiating Event D	Safeguard		Mitigation	Consequence ⚠
Initiating Event E	(5) Safeguard	Description of event	Mitigation	Consequence ⚠
Initiating Event F	(5) Safeguard			
Initiating Event G	Safeguard			
Initiating Event H	Safeguard			
Initiating Event I	Safeguard			

Remember 'STAR' – Stop, Think, Act, Review. If in doubt... ASK!

ENGINEERED CONTROLS

PROCEDURAL CONTROLS

SCoSP Ref:	SCoAP/xxxx/xxx	Issue 1	July 2011
Safety Case Ref:	xxx/xxx/xxx/xxx	Issue x	xxxx 20xx
Owned By:	X.Xxxxx (Process Supervisor)		

EXAMPLE 2 Safety Case Assumptions
used by Sellafield Ltd

The purpose of the Safety Case Assumptions document is to present appropriate realistic, bounding, generic assumptions used in support of the Safety Case, as well as definitions of a number of generic terms used throughout the Safety Case.

Generally, the assumptions would previously have been identified in Safety Assessments, but relate to parameters over which the plant operators have no control, and therefore are included in a single document without repeating them as Operating Assumptions in the relevant assessments. This enables the assumptions on which the Safety Case is based to be compiled into a complete, comprehensive list ensuring consistency across the Safety Case which may be kept live.

Individual assumptions can be colour coded according to discipline (e.g. Radiological, criticality etc) to easily identify where the requirement originates. They could fall into three categories, as follows (not intended to reflect their relative importance).

- Primary: Fundamental properties of feedstocks and process materials.
- Secondary: Plant and process parameters, or fundamental assumptions about plant operations.
- Tertiary: Procedural and personnel related assumptions, but over which the operators do not have direct day-to-day control.

Justification is provided against each assumption and can be based on a combination of, for example, technical reports, analytical results, customer specifications etc

The document can also include such things as; Gloveboxes, Gas Feeds and Flowrates and Associated Instrumentation, Generic Release Fractions and Decontamination Factors, Generic Base Event Data, Radiological Consequences etc.

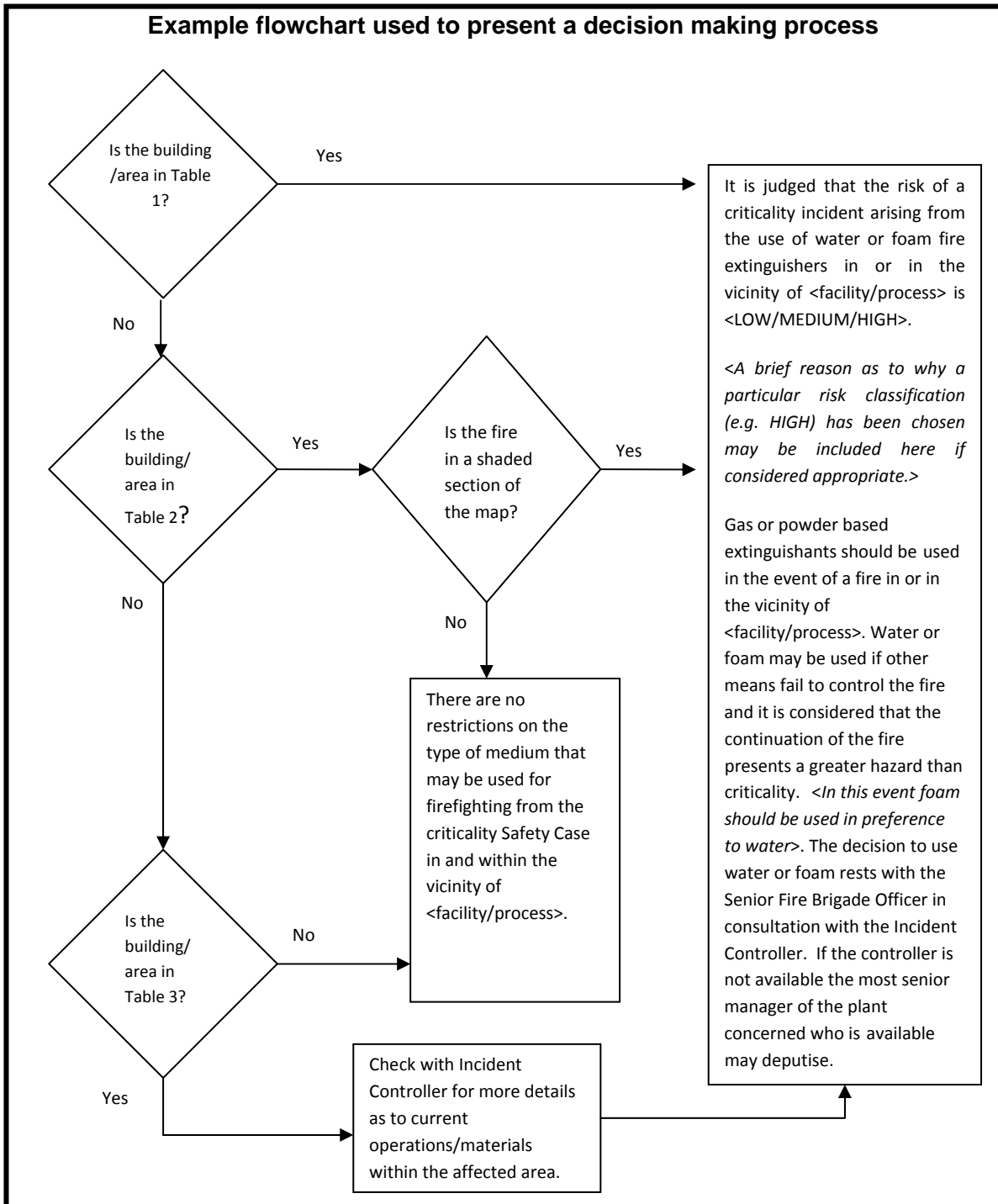
Example table to present Safety Case wide assumptions

	ASSUMPTION	JUSTIFICATION
<i>PRIMARY ASSUMPTIONS (FEEDSTOCKS AND PROCESS MATERIALS)</i>		
1	e.g. The maximum density of material 1 is X.	Proportionate justification
2	e.g. The enrichment of material 1 is Y.	Proportionate justification
<i>SECONDARY ASSUMPTIONS (PLANT/PROCESS)</i>		
3	e.g. [insert plant] operates at a throughput of no greater than Z.	Proportionate justification
4	e.g. The maximum inventory of a container used for transfer or storage is B.	Proportionate justification
<i>TERTIARY ASSUMPTIONS (PLANT/PROCESS)</i>		
5		Proportionate justification
6		Proportionate justification

EXAMPLE 3 Simple Flowcharts
used by Sellafield Ltd

Flowcharts are a good way of presenting information, for example a key decision making process, in a clear and logical manner which may be difficult to explain or may be open to interpretation if written as text only.

In this example, firefighting advice was previously a very long listing of all the buildings on site with a Y/N against each entry to indicate whether or not restrictions on the use of water were in place. This has been replaced by a single flow sheet, three short tables and a few marked-up images.



EXAMPLE 4 Integrated Risk Assessment Process (IRAP)
being developed by Devonport Royal Dockyard Ltd

The Integrated Risk Assessment Process (IRAP) is a Safety Analysis tool which allows for the proportionate means of assessment for low radiological consequence activities and environmental hazards.

Basis of IRAP – Objectives of the process:

- Proportional safety analysis.
- One process which is used to assess risks to workers, public and the environment.
- Introduces concept of risk reduction to inform design.
- Utilises nuclear processes where appropriate i.e. implementation and management.
- Screening at a proportionate level.
- Threshold Limits: On Site - 20mSv Off Site - 1mSv (for facilities/activities on the Licensed Site).

The Safety Report for an IRAP assessment seeks to compile the most important information to the Plant Manager (and/or Safety Case Owner) in a simple, easy to use format. The assessment which underpins the headlines is held in a number of supporting documents.

The Safety Report aims to:

- context the assessment at a high level;
- detail the scope of activities;
- identify the highest risk activities covered by the assessment;
- define the engineering and administrative arrangements required; and
- conclude on the current level of risk.

Example table from Safety Report used to summarise risk

Exposure Group	Residual Risk Level	Consequence
Environmental	Medium	Medium residual risk of a potentially significant environmental affect leading to high risk of regulator enforcement.
Operators	Medium	Medium residual risk of an accidental exposure to an operator of up to 20mSv effective dose.
Public	Low	Low residual risk of an accidental exposure to the public of up to 1mSv effective dose.

EXAMPLE 5 Visual management of safety designations
used by Research Sites Restoration Ltd

Similar to Safety Case on a Page, displaying key safety designations is a powerful example of a succinct summary of information in a style that is easily accessible. It allows the main hazards and controls for a facility to be visible on plant and understood. It can be used as part of training, as pre job briefs and displayed local to the hazard.

B■■■■-KSRE & SRE

Key Safety Related Equipment & Safety Related Equipment



**There are NO KSRE or SRE
Items or Plant in B■■■■**



B■■■■-KSMR & SMR

Key Safety Management Requirements & Safety Management Requirements

- KSMRs and SMRs are instructions to tell you what to do or what not to do
- KSMRs and SMRs are largely used when it is not possible or appropriate to install engineered protection
- An example is Wear an EPD in Radiation Controlled Areas
- KSMRs and SMRs are identified in your Operating & Maintenance Instructions

There are NO KSMR in B■■■■



SMR

SMR No	Description
21	





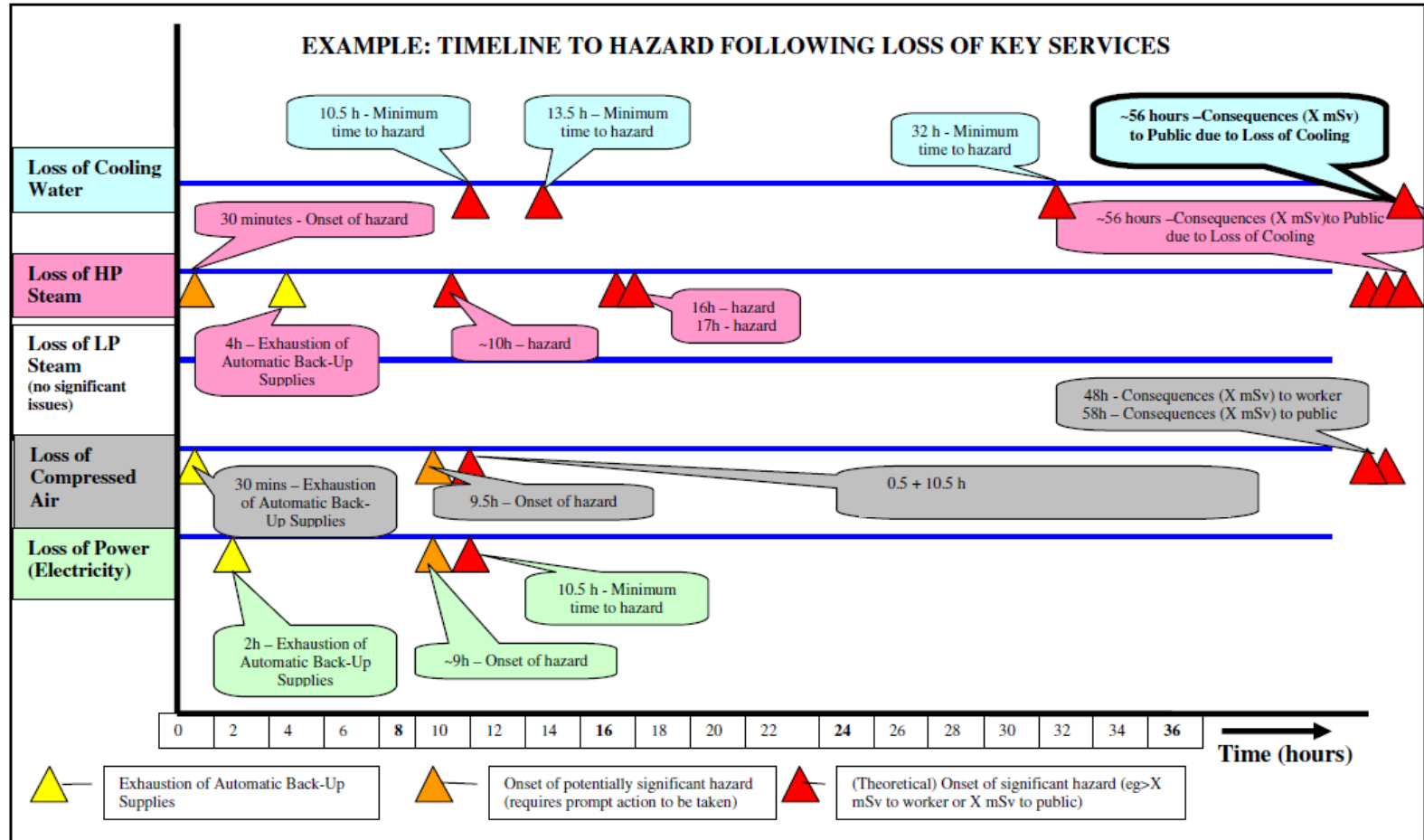
Research Sites
Restoration Ltd

Care & Maintenance
Department

Safety Advisor
■■■■■
Ext. ■■■■

EXAMPLE 6 Timeline with 'swim lanes' used by Sellafield Ltd

The example provided maps loss of key services onto a timeline where each key service appears as a 'swim lane' and so can be used to assist in prioritising the response to the developing situation. This is another powerful example of a succinct summary of information in a style that is easily accessible and easy to understand. It can be used in assessments, as part of training, as pre job briefs and displayed local to the hazard.



EXAMPLE 7 Alarm Sequence Colour Charts
used by Sellafield Ltd

Alarm sequence colour charts can be used to help explain the order in which alarms occur (those identified in the Safety Case and normal plant alarms) for a complex fault without the need for a fault sequence progression diagram or fault tree. With these charts you can quickly see:

- Which faults have most or least defence in depth.
- Common protections against multiple fault sequences.
- The impact of equipment failure or running under substitution arrangements for a Safety Mechanism.
- New or changed levels of designation if a new safety assessment is being implemented.
- Normal plant / control system alarms which may not otherwise be claimed in the underlying assessment.

Example table used to summarise sequence of alarm initiation during faults

Initiating event	Plant item affected	Alarm/Trip progression										
		1	2	3	4	5	6	7	8	9	10	
Title of Initiating Event 1	X	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier
Title of Initiating Event 2	Y	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier			
Title of Initiating Event 3	Z	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	Alarm description and identifier	

Key	Currently SM (and remain so)	New SM from PSR	Currently SRE (and remain so)	SRE from PSR	Normal plant control system Priority 1 alarm
-----	------------------------------	-----------------	-------------------------------	--------------	--