The UK Nuclear Industry Good Practice Guide To:

**Keeping Safety Cases**

**‘Live’**



This Nuclear Industry Good Practice Guide was produced by the Safety Case Forum and published on behalf of the Nuclear Industry Safety Directors’ Forum (SDF)

**Issue 1 – March 2020**

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Issue Number** | **Revision Date** | **Changes** |
| Issue 1 | March 2020 | Initial Publication |
|  |  |  |

It is recognised that – through the experience of using this Guide – there may be comments, questions and suggestions regarding its contents.

In the first instance, any such comments should be sent to the following email address

safetycaseforum@awe.co.uk

Author: Alan Hall (AWE)

Contributions have been provided through the Safety Case Forum by  
all participating members, particularly:

Bryan Dods (Dounreay)

Calum Powrie (Horizon Nuclear Power)

Stuart Bowers (Rolls-Royce)

Dave Graham (Magnox)

Gary Lewis (Urenco UK)

Kevin Masson (Sellafield)

Graeme Duffy (AWE)

Andy Lethern (Westinghouse)

Alex Jones (Dounreay)

Steve Brinsden (NNL)

This document was reviewed and approved by the Safety Case Forum  
of the Safety Directors’ Forum.

# Foreword

This guide is produced as part of a suite of Safety Case Forum Guides that describe a different approach to the Periodic Review of Safety (PRS). The other guides are identified in the references.

This alternative approach to the PRS seeks to reduce the work, resource and financial peeks associated with the 10-yearly review and replace them with a progressive, rolling, day-to-day normal business approach to the PRS.

In order to support the successful introduction and sustainability of this alternative approach to the PRS, it is considered essential that the safety case must be kept up-to-date, or “live”. This guide looks at ways in which a “live” safety case can be implemented and maintained.

The proposals in this guide are described in a way that should allow different sized organisations, irrespective of their business position within the nuclear fuel cycle, to gain the confidence necessary to adopt the proposals, and realise the associated benefits.

These proposals do not have to be expensive to implement, although it is recognised that preliminary work is likely to be necessary to get the organisation into a position to properly adopt these proposals. However, the benefits that will accrue from having an up-to-date safety case are considered to outweigh the costs of adoption and are described within the guide.

This guide provides a framework within which to work and allows the exact arrangements to be tailored for the individual needs of each organisation.

Although it is possible to implement this guide on its own, it is recommended that it is read, carefully considered, and where practical, implemented as part of the suite of guides that describe the new approach to the PRS.

It is hoped that the Safety Directors of the member organisations, as well as members of the Office for Nuclear Regulation, will support these proposals to the extent that they encourage their implementation across the industry.

## Safety Directors’ Forum

In a sector where safety, security and the protection of the environment is, and must always be the number one priority, the SDF plays a crucial role in bringing together senior level nuclear executives to:

* Promote learning;
* Agree strategy on key issues facing the industry;
* Provide a network within the industry (including with Government and regulators) and external to the industry;
* Provide an industry input to new developments in the industry; and,
* To ensure that the industry stays on its path of continuous improvement.

It also looks to identify key strategic challenges facing the industry in the fields of environment, health, safety, quality safeguards and security (EHSQS&S) and resolve them, often through working with the UK regulators and Government, both of whom the SDF meets twice yearly. The SDF members represent every part of the fuel cycle from fuel manufacture, through generation to reprocessing and waste treatment, including research, design, new build, decommissioning, care and maintenance and waste disposal. The Forum also has members who represent the Ministry of Defence (MoD) nuclear operations, as well as “smaller licensees” such as universities and pharmaceutical companies. With over 25 members from every site licence company in the UK, every MoD authorised site, and organisations which are planning to become site licensees, the SDF represents a vast pool of knowledge and experience which has made it a key consultee for Government and regulators on new legislation and regulation.

The Forum has a strong focus on improvement across the industry. It has in place a number of subject-specific sub-groups looking in detail at issues such as radiological protection, human performance, learning from experience and the implementation of the new regulatory framework for security. Such sub-groups have developed a number of Good Practice Guides which have been adopted by the industry.

## Safety Case Forum

This Guide has been produced by the Periodic Review Forum, a workstream of the Safety Case Forum, which is in turn a sub-group of the SDF.

The Safety Case Forum was established in June 2012 and brings together a wide range of representatives of nuclear operators, from all the Licensees and Authorisees across the UK, including:

* Civil, commercial and defence activities;
* Design, operation and decommissioning of nuclear facilities;
* Research facilities.

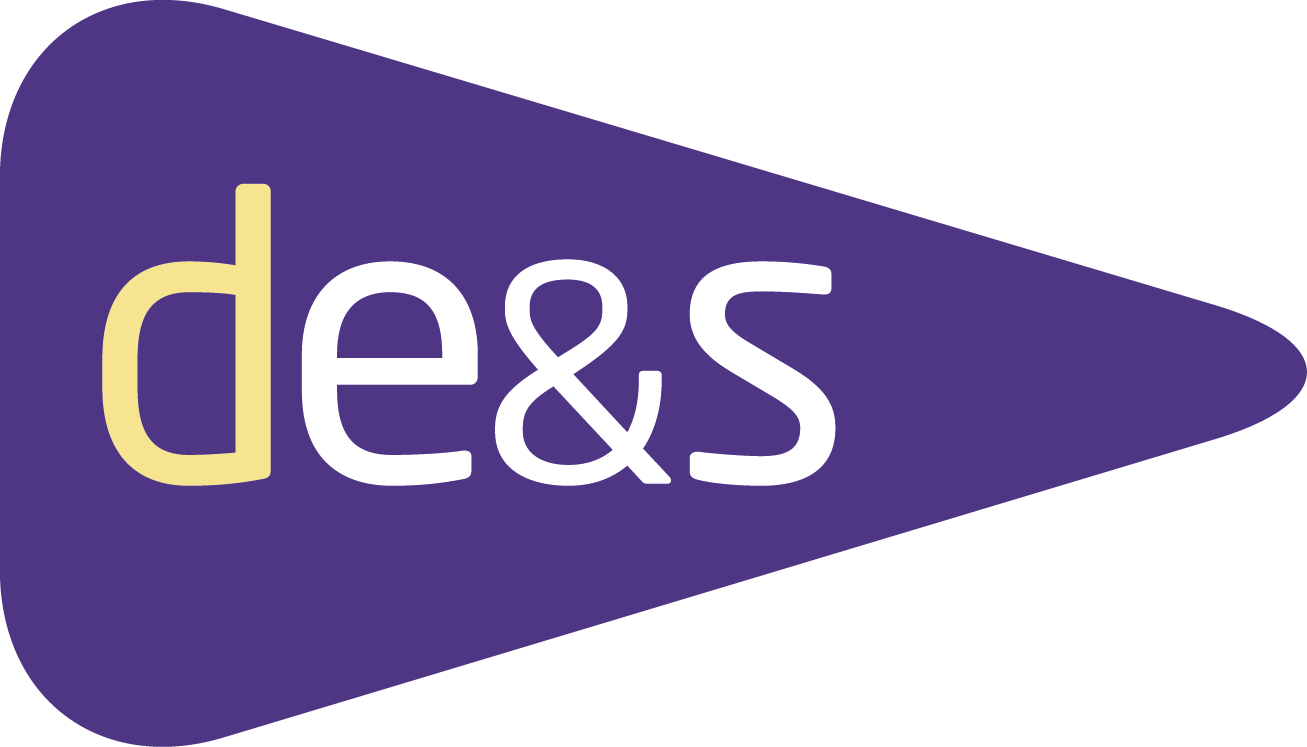
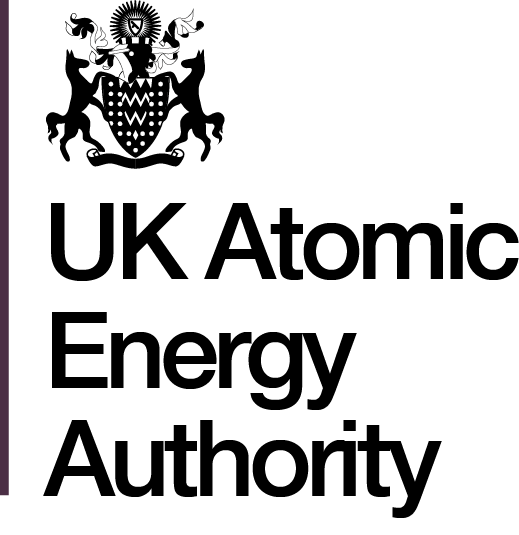
The purpose of the Safety Case Forum is to provide guidance that is useful to, and will benefit the widest possible range of UK nuclear operators.

Such guidance is not mandatory, nor does it seek to identify minimum standards. It aims to provide a tool kit of methods and processes that nuclear operators can use if appropriate to their sites and facilities.

These guides are intended to improve the standardisation of approach to the delivery of fit-for-purpose safety cases, while improving quality and reducing the cost of production. They are designed to cater for all stages of a facility’s life cycle and for all processes within that life cycle. This includes any interim, continuous and periodic safety reviews, allowing for the safe and efficient operation of nuclear facilities.

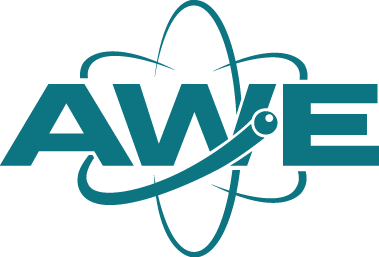
When using the information contained within these guides, the role of the Intelligent Customer shall always remain with the individual nuclear operator, which shall retain responsibility for justifying the arguments in their respective Safety Cases. The ONR and the Defence Nuclear Safety Regulator are consultative members of the Safety Case Forum.

The following companies and organisations are participating members of the Safety Case Forum:

Safety Case Forum Guides are available on the Nuclear Institute Website;

<http://www.nuclearinst.com/SDF-safety-cases>

**Disclaimer**

This UK Nuclear Industry Guide has been prepared on behalf of the Safety Directors’ Forum by a Technical Working Group. Statements and technical information contained in this Guide are believed to be accurate at the time of writing. However, it may not be accurate, complete, up to date or applicable to the circumstances of any particular case. This Guide is not a standard, specification or regulation, nor a Code of Practice and should not be read as such. We shall not be liable for any direct, indirect, special, punitive or consequential damages or loss whether in statute, contract, negligence or otherwise, arising out of or in connection with the use of information within this UK Nuclear Industry Guide.

This guide is produced by the Nuclear Industry. It is not prescriptive but offers guidance and in some cases a toolbox of methods and techniques that can be used to demonstrate compliance with regulatory requirements and approaches.

**Contents**

[Foreword 3](#_Toc30156642)

[Safety Directors’ Forum 4](#_Toc30156643)

[Safety Case Forum 4](#_Toc30156644)

[1 Introduction 9](#_Toc30156645)

[1.1 Background 9](#_Toc30156646)

[1.2 Aims 9](#_Toc30156647)

[1.3 Scope 10](#_Toc30156648)

[1.4 Target Audience 10](#_Toc30156649)

[2 The Life Cycle 11](#_Toc30156650)

[2.1 The Safety Case Life Cycle 11](#_Toc30156651)

[2.2 Cultural and Behavioural Changes 11](#_Toc30156652)

[2.3 The Changing Landscape 11](#_Toc30156653)

[3 Regulation 13](#_Toc30156654)

[3.1 Regulatory Expectations 13](#_Toc30156655)

[4 The Subject Matter 15](#_Toc30156656)

[4.1 Discussion 15](#_Toc30156657)

[4.2 Strategy 15](#_Toc30156658)

[4.3 Benefits 16](#_Toc30156659)

[5 Management System Requirements 17](#_Toc30156660)

[5.1 The Generic Safety Case Model 17](#_Toc30156661)

[5.2 The Management System 18](#_Toc30156662)

[6 Factors Necessary to Keep the Safety Case Live 19](#_Toc30156663)

[6.1 Discussion 19](#_Toc30156664)

[6.2 Ownership 19](#_Toc30156665)

[6.3 File Structure and Safety Case Index 20](#_Toc30156666)

[6.4 Data Storage 21](#_Toc30156667)

[6.5 During the Concept and Design Development Phases 21](#_Toc30156668)

[6.6 During the Operational Phase 22](#_Toc30156669)

[6.7 During Decommissioning and Disposal 22](#_Toc30156670)

[7 Options for Updating the Safety Case 23](#_Toc30156671)

[7.1 Drivers to Update the Safety Case 23](#_Toc30156672)

[7.2 Rolling Programme of Update and Implementation 23](#_Toc30156673)

[7.3 Governance 24](#_Toc30156674)

[7.4 Options for Change 24](#_Toc30156675)

[7.5 Proposals for the Implementation of Option 3 25](#_Toc30156676)

[8 To Update the Safety Case, or, Not? 27](#_Toc30156677)

[8.1 That is the question! 27](#_Toc30156678)

[9 Audit Trails - The Golden Thread 30](#_Toc30156679)

[9.1 Discussion 30](#_Toc30156680)

[9.2 The Engineering Schedule 30](#_Toc30156681)

[9.3 The Procedures Schedule 30](#_Toc30156682)

[9.4 The Golden Thread 30](#_Toc30156683)

[9.5 Real-Time, Live Updates to the Safety Case 31](#_Toc30156684)

[10 Interfaces with other Business Processes 32](#_Toc30156685)

[11 Performance Measuring the “Live” Safety Case 33](#_Toc30156686)

[11.1 Discussion 33](#_Toc30156687)

[11.2 Performance Management 34](#_Toc30156688)

[11.3 Monitoring of Safety Assessments 35](#_Toc30156689)

[11.4 Controls and Metrics 35](#_Toc30156690)

[11.5 Self-Assessment 38](#_Toc30156691)

[11.6 Health Checks 38](#_Toc30156692)

[11.7 Key Point Reviews 38](#_Toc30156693)

[11.8 Audit and Inspection 39](#_Toc30156694)

[12 Recommendations 40](#_Toc30156695)

[13 Glossary 41](#_Toc30156696)

[14 References 42](#_Toc30156697)

[Appendix A: The Generic Safety Case Model - Constituent Parts 43](#_Toc30156698)

[Appendix B: The Safety Case Report 44](#_Toc30156699)

[Appendix C Safety Case Index and Modular File Approach - Example 45](#_Toc30156700)

[Appendix D: The Drivers for Change 47](#_Toc30156701)

[Appendix E: An Example of an Engineering Schedule Template 48](#_Toc30156702)

[Appendix F: An Example of a Procedures Schedule Template 49](#_Toc30156703)

**Figures**

[Figure 1: Example of a Simple Interaction Diagram between Disciplines 20](#_Toc30156704)

[Figure 2: Resolution of the Complexity Concept 29](#_Toc30156705)

[Figure 3: Performance Management 35](#_Toc30156706)

# 1 Introduction

## 1.1 Background

The Safety Case Forum works under the direction of the Safety Directors’ Forum and has a remit to provide guidance to standardise where possible, and improve as much as is practical, the way in which the safety case is produced and presented.

Part of that remit is to review and recommend changes to the way in which the Periodic Review of Safety (PRS) is undertaken.

This guide should be read in conjunction with the Safety Case Forum Guide for: “Monitoring, Interim Review and Continuous Improvement” [Ref. 1]. The two guides are complimentary, and together describe a vision for a radically different approach to the Periodic Review of Safety and the on-going maintenance of the Safety Case.

The new approach is for a devolved and rolling PRS, which encourages nuclear operators to take an increased ownership of the process. There is an explicit expectation (where it is appropriate to do so) of a shift towards a rolling, “Monitoring, Interim Review and Continual Improvement” [Ref. 1] process, maximising the benefit by utilising the outputs from the rolling PRS process to update, and keep up-to-date, the facility safety case (and therefore the Site Safety Case) and to feed current assessment and analysis information into other business decision making processes.

The overall aim of the improvement is to bring the PRS activities within the scope of normal day-to-day business. This does not remove the need for the 10-yearly Periodic Review of Safety, but will reduce that activity to just a review, rather than a wholesale re-write of the safety case.

This guide must also take into consideration that other drivers exist for modifications and changes that could also require updates to the safety case.

The strategy for the PRS can only be fully effective if, in parallel, there is positive and effective management action undertaken to keep the safety case up-to-date. Indeed, the current interpretation of custom and practice seems to encourage modification justifications to accumulate without mandating any update of the safety case. Increasingly however, this behaviour is being recognised as counter-productive, costly and requiring increased resources overall, when considered in the long-term.

This guide is an aspirational, forward looking vision, and supports the aim of driving the integration of PRS activities into mainstream day-to-day business to enhance and better manage risk. This has a parallel expectation and opportunity associated with it; to drive regular safety case updates. So, the way in which the safety case is managed must also be modernised for the organisation to be able to reap the full benefit from the change.

Keeping safety cases live, making sure there is a clear and visible safety argument, should not just be about regulatory compliance. Organisations involved in the nuclear industry spend huge amounts of money on safety and should be actively seeking to gain the maximum benefit from the money that is being spent. Having a clear and visible safety argument within a live safety case would allow the use of up-to-date information to feed other business processes to ensure the organisation is not only compliant but can utilise the information to assist in making important strategic and tactical business decisions.

## 1.2 Aims

This document aims to explore how the suite of documents, comprising the safety case, could be kept up-to-date and what it might take to achieve that.

## 1.3 Scope

The work presented in this document covers all elements that comprise a nuclear safety case, throughout the full life-cycle of a facility and encompasses the interfaces with all monitoring and performance measuring activities, interim reviews and the Periodic Review of Safety.

## 1.4 Target Audience

There is an aspiration, a hope, that this document will be widely read by those persons actively engaged in the preparation and implementation of safety processes; the production of a safety case, Safety Case Owners, Safety Case Managers and those requiring safety cases to be prepared, but also, those Company Directors with a responsibility for safety within their own organisations.

# 2 The Life Cycle

## 2.1 The Safety Case Life Cycle

The engineering design process for a new nuclear facility has evolved significantly over recent years, taking advantage of new computer capabilities as they have become available.

In parallel, the fundamental safety case process has remained fairly similar, although, as with engineering, the advantage of new computer capabilities has also assisted in carrying out very complex processes better and quicker, producing ever more accurate information and reducing the overall time taken to complete the task.

The design, manufacture and commissioning phases are intense and complex, requiring robust configuration and management control over all aspects of the build, which extends and includes the safety case and its supporting documentation.

During operations, although modifications and changes take place, this phase of the life cycle presents its own challenges and both engineering and safety considerations are different from those experienced during build.

Likewise, on completion of operations, during clean-out, decommissioning and disposal, engineering and safety considerations are different again.

Throughout the life cycle of a facility, the safety case has to run in parallel with engineering, feeding from, and providing input into, the engineering design process but at the same time the compilation of the safety case, through assessment and analysis, has to adapt and change to meet the challenges of each phase, and the proposals set-out in this guide describe how this could be achieved while still maintaining a clear and visible safety argument.

It is clear therefore, that engineering, safety and configuration control, are inextricably linked throughout the whole process. These enduring and inseparable relationship are key to keeping the safety case live.

## 2.2 Cultural and Behavioural Changes

The essence of this proposal is about the most effective way to manage change. Not for the sake of change, but to make change generate something that is altogether better and more useful. However, not everybody or every organisation can easily adopt, or adapt and implement change successfully.

The approach being outlined in this guide requires an in-grained safety ethic in order to transform into the day-to-day normal business ‘periodic review’ of safety activities. In order to optimise the benefits, the culture and behaviour will have to be re-focused on the vision of how best to keep the safety case up-to-date in amongst everything else that is being done; to allow a clear story to be told and a clear argument (with supporting evidence) to be presented, not only to demonstrate compliance and ALARP but to aid better understanding and drive intelligent decision making.

In parallel with any attempt to implement these proposals it is advisable, and recommended, that a “hearts and minds” campaign is initiated to change (or at least modify) the culture and behaviours of personnel to support the implementation of these proposals.

## 2.3 The Changing Landscape

These proposals indicate how the new processes and systems are expected to work. However, not every organisation is at the same stage of their evolution, or organisational maturity. Each organisation will employ slightly (or vastly) different ways to achieve their business objectives and because the nuclear industry represents organisations working on all aspects of the nuclear fuel cycle, they will not all have the same goals.

It will be incumbent on individual organisations to review where their organisation is placed, relative to the proposals in this guide. They should carry out an appropriate gap analysis between their current management system status and that management system status required support the proposals set-out in this document and be able to demonstrate regulatory and legal compliance; then implement the requisite change programme.

Proposals for performance measurement of the live safety case are provided in Section 0 and these should also be carefully considered for incorporation into the organisational change programme.

# 3 Regulation

## 3.1 Regulatory Expectations

The regulatory framework of Safety Assessment Principles, the Technical Assessment Guides and the Technical Inspection Guides, exist for the guidance of Inspectors in their regulatory roles, but, as they are publicly available documents it would be unwise, if not fool-hardy, to ignore the expectations of the Regulator and the in-sight the guides provide.

In the ONR’s Technical Assessment Guide 51, [Ref. 2] there are specific expectations describing what the safety case is for, how it should be used, and why.

|  |  |  |
| --- | --- | --- |
| Sect. 6 | Para 6.4 | The safety case is important to those who interact directly with the facility, for example the operators who control the conditions within the facility and those who maintain the facility. |
| Sect. 6 | Para 6.4 | The safety case is also important to senior management who are responsible and accountable for safety. They rely upon the safety case for accurate and objective information on risks and control measures to make informed decisions that may affect safety. |
| Sect. 6 | Para 6.4 | The key users of the safety case should be involved in its development, production/review and implementation. |
| Sect. 6 | Para 6.5 | The safety case should be a living document which is subject to review and change as time proceeds. For example, the safety case may change due to important changes to the facility, its mode of operation, or the understanding of safety related issues. It may also change in the light of operating experience or periodic review. |

Within the same Technical Assessment Guide there are expectations regarding how the information in the safety case should be used to manage safety.

|  |  |  |
| --- | --- | --- |
| Sect. 9 | Para 9.1 | It should always be remembered that the documented safety case is not an end in itself. It forms an important part of how the licensee manages safety. |
| Sect. 9 | Para 9.1 | The requirements of the safety case need to be implemented and managed effectively to deliver safety. |

The guide goes on to explain exactly how the safety case should be used. It should be noted that the guide explicitly identifies the safety case as the key and pertinent document.

|  |  |  |
| --- | --- | --- |
| Sect. 9 | Para 9.1 | The licensee must ensure continually that the safety case is consistent with the as-built facility and that the facility is operated and maintained in accordance with safety case requirements and assumptions. The licensee must have effective processes to ensure these objectives are achieved. |

The guide progresses to describe how the regulator expects the safety case to be managed.

|  |  |  |
| --- | --- | --- |
| Sect. 12 | Para 12.1 | The licensee is legally responsible for the safety case and its adequacy. |
| Sect. 12 | Para 12.1 | Those who have direct responsibility within the licensee for delivering safety should have ‘ownership’ of the safety case. |
| Sect. 12 | Para 12.1 | Ownership is not a ‘figure head’ role. It requires an understanding of the safety case and the limits and conditions derived from it and the responsibility to ensure it is adequately managed and maintained. |
| Sect. 12 | Para 12.2 | It is important that the safety case is kept up-to-date during each stage of a facility life cycle. This will include the impact of facility/plant modifications, new information (from research, additional analyses, etc.) and the outcome from periodic reviews. |
| Sect. 12 | Para 12.2 | The safety case should also be reviewed and if necessary updated to take account of the lessons from operational experience and incidents. This should include experience from a range of sources, including: within the facility in question; elsewhere on the site or the licensee; the nuclear industry in the UK or internationally; and other (relevant industrial) sectors. |
| Sect. 12 | Para 12.3 | Any updates should encompass changes to safety case documentation (revision or replacement) plus amendments to rules, instructions, drawings, operational procedures and training requirements. Documentation which no longer forms part of a current safety case, or which has been superseded, should be identified and archived. This information still forms part of the formal historical record, and remains subject to the arrangements made under Licence Condition 6. |

It can be deduced from these extracts that there is a regulatory expectation associated with the way the safety case is used, maintained and managed, equally, there is a clear expectation that the safety case should be kept up-to-date (“live”). Note, that in all cases the guide refers to the safety case and not to any particular sub-part, and certainly not to the composition, collection and accumulation of modification safety justifications, separate from the safety case.

There is therefore, a clear expectation that the safety case should be kept up-to-date; but what does this mean in practice?

# 4 The Subject Matter

## 4.1 Discussion

The concept of a safety case being kept up-to-date and “live” is relatively easy to understand, but is much more difficult to translate into a set of technical requirements, that can be implemented in practice.

“LIVE” in this context, for all practical purposes, means making sure that the approved or authorised safety case presents a clear and visible safety argument, that it properly reflects the current facility’s operational status and the configuration of the plant, processes or equipment, along with its future intent. This will include any engineering and associated administrative or operational requirements.

To remain ‘live’ the safety case must be actively managed and kept under robust configuration control. It should be updated as a result of any modification or change action, so that at any point in time the safety case best reflects all the known hazards and the status of their associated control measures; and therefore, that the overall level of risk posed by the facility is ALARP, is fully understood and is being appropriately managed.

From benchmarking activities undertaken by the Safety Case Forum, across the industry, in late 2016, the knowledge gained, suggests that as modifications and changes take place, the information contained within them tends to remain in separate modification safety reports and is not incorporated into the body of the safety case, meaning the “case for safety” becomes ever more fragmented, encompassed by, and held across, many additional modification or change related documents.

The threat to the “Safety Case” itself, is that it becomes more and more out-of-date as each modification or change is carried out. In these circumstances the full safety case picture becomes increasingly less obvious to the point where it no longer tells a coherent, consistent, factual or clear and transparently visible story.

While attempting to keep the safety case “live” consideration must be given to the information requirements necessary to do this; and how this could not only provide benefit to the safety case but how the contents and output from an up-to-date safety case could interface and provide benefit into other aspects of company business.

## 4.2 Strategy

The strategy adopted for the presentation in this guide is as follows:

1. There is an initial assumption that a safety case exists and that it is up-to-date and provides a clear and visible safety argument (this is a fundamental requirement, and a baseline requirement from which to start).
2. This guide identifies the significant elements of the safety case and which of these should be updated as a result of a modification, or change, to keep the safety case live.
3. This guide will identify how the outputs from assessment processes, including the PRS (in the form of the monitoring, interim review and continual improvement activities) interface with, and drive updates to, the safety case.
4. This guide also identifies that all changes must be processed through the (modification and change) LC/AC 22 process and how the change process and the safety case interface with each other, understanding what type of information is necessary in order to keep the safety case live.
5. This guide shows how a modular layout of the safety case may expedite efficient and effective safety case updates.
6. Guidance is provided on when updates would be required, or the maximum period between updates, or the conditions necessary to drive an update to the safety case.
7. This guide investigates the potential conditions necessary to allow for live updates to the safety case.

## 4.3 Benefits

The following, in no particular order of priority or suggested level of benefit, are considered to be the main benefits or advantages to the industry, of adopting and implementing a process by which the safety case is continually kept up-to-date, they include:

**Immediate Benefits:**

* At any point in time the safety case will reflect all the known hazards with the status of their associated engineered and administrative control measures, and therefore, reflect the overall level of risk posed by a facility;
* For multi-facility sites, if the outputs from a number of facility assessments are fed into a Nuclear Site Safety Case then their up-to-date contributions will accurately demonstrate the overall level of risk carried by the business, for that site;
* Specific outputs can provide benchmarking opportunities, and opportunities to learn from other industry organisations;
* Specific outputs from the safety case can be fed into the management of risk within the business. This would include;
* Comparisons of similar risks between facilities.
* Identification of individual and cumulative risks, to aid planning, determine renewal programmes and the siting of new facilities.
* Enabling strategic investment, or non-investment, decisions.

**Ongoing Benefits:**

* The safety case will be the single comprehensive “master” source of information (rather than working through multiple modification safety justifications) to obtain the current hazard, risk and safety related information;
* The safety case will properly reflect the operational status and future intent of the facility, plant, processes or equipment, including any associated administrative/operational requirements;
* Advantageous interfaces between the safety case outputs and any other associated business processes or procedures can be identified and implemented, providing valuable technical and safety support into important business decision-making processes;
* Overall long-term ability to more accurately forecast a predictable resource loading and budgetary cost (removal of peak resource loading);
* Significant reduction in resource, and time, required to undertake the next Periodic Review of Safety;
* Continual control and proportionate management of risk reduction activities, from greater visibility of the outputs from the live Safety Case.

# 5 Management System Requirements

## 5.1 The Generic Safety Case Model

The safety case, for anything other than the simplest process, or item of equipment, will usually comprise a number of reports, documenting the claims being made, the assessments that have been carried out, along with the evidence that has been accumulated and the conclusions that have been reached, to allow safe operations to take place.

In the nuclear industry there are many such reports, as illustrated in Appendix A: The Generic Safety Case Model - Constituent Parts. These are just some examples of what may be required, since different parts of the nuclear industry will require different combinations of reports and each individual organisation will determine and generate what it needs to support its own business.

Previous benchmarking activities indicate that the strategic approach to the safety case presents information on a number of different aspects, which are summarised below:

1. The Safety Case Report (a top-level document usually describing the Claims and principal Arguments being put forward).
2. The Assessments (the detailed technical Arguments).
3. The detailed Evidence.
4. The Forward Action Plan – Continual Improvement Activities.

**The Safety Case Report:**

This should be a top-level document which describes the Claims made for the facility, plant, process or equipment and presents the arguments made to support and justify the claims. An example of the generic contents for a Safety Case Report are presented in Appendix B: The Safety Case Report. It must be recognised that this represents a generic list and that each organisation will necessarily tailor the contents of the Safety Case Report to meet their own requirements.

The Safety Case Report is written as simply as possible, describing the claims and the supporting arguments, referring to the more detailed technical reports where necessary, avoiding technical complexity where possible, so that it can be easily understood by its target audience. In so doing, The Safety Case Report should stand the test of time, typically requiring little change, unless there is a material change in the scope of operations.

As well as presenting safety claims, arguments and supporting evidence, the safety case must demonstrate that the facility, plant, process or equipment complies with any relevant law in the siting, use and effect it may have on its workers, or the public. Additionally, there is always the requirement to demonstrate that risks are ALARP and that all operations comply with the Licence Conditions for the site.

**The Assessments:**

These are usually separate documents, referenced from the Safety Case Report, compiled to describe, define and present the detail of specific discipline arguments which are used to support the claims that are being made. For any particular facility, plant, process or equipment these are likely to be varied, and multiple, aiding different strands of the argument to present a comprehensive, logical and complete picture of the technical justification being presented. In many cases the outcome from the assessments will also provide the evidence to support the arguments.

**The detailed Evidence:**

Where the assessments require further supporting work such as modelling, reliability data, experimental data, and other related types of information then this evidence will usually be referenced from the individual assessment reports.

**The Forward Action Plan:**

There are a wide variety of changing circumstances that would drive the need to consider changes to a facility, plant, process or individual item of equipment. These commonly call for modifications to be made to the hardware, software, administration or resources required to operate.

These changes, when considered in tandem with the legal requirement to maintain risks As Low As Reasonably Practicable (ALARP) require an on-going, formal and robustly managed and configured, change control process. Any change control process must satisfy the requirements of License/Authorisation Condition 22. This continual improvement activity is managed through the identification and implementation of items on a Forward Action Plan.

## 5.2 The Management System

In order to keep a safety case live, the organisation’s Management System needs to reflect the structure of the documentation within the safety case and provide the necessary procedures to undertake the assessment work, to provide the evidence necessary to compile the safety case. This structure is likely to be different, for different organisations, throughout the nuclear fuel cycle.

The management system needs to be comprehensive, covering all aspects of the compilation of the safety case, and specifically reflect the aspects of the process that ensure the safety case is updated regularly in-line with the proposals in this document.

There are also supporting business processes, such as governance and regular management review, that will need to support the production and maintenance of the safety case.

# 6 Factors Necessary to Keep the Safety Case Live

## 6.1 Discussion

There will inevitably be some work involved in aligning processes, probably updating and changing the management system in particular, to ensure that the processes are adequately described and recorded; to put an organisation into the position to be able to implement these proposals. Thereafter, because the management system is properly defined, keeping the safety case live should be just another part of normal business.

## 6.2 Ownership

The Ownership aspects, particularly Leadership and Management for Safety [Ref. 3] are considered to be fundamental to the successful implementation of the proposals in this guide.

The Owner of the safety case, and the Safety Case Manager working on their behalf, are key individuals in the process for keeping the safety case ‘live’. However, there are other key participants including, but not limited to, engineering, configuration control and quality management.

The organisations’ management system should unequivocally state that the safety case is to be maintained but without the active participation and drive of the Owner, and the leadership and instruction from the Safety Case Manager, along with the active participation of all the other supporting disciplines, it is unlikely that a safety case can, or will, be kept up-to-date.

Figure 1, is an example of a simple organisational diagram which illustrates the interactions between disciplines necessary to enable the safety case to be kept up-to-date.

Therefore, it is hoped that, not only the organisation (Safety Director) but also the Safety Case Owner and the Safety Case Manager, can appreciate and understand the benefits of maintaining a ‘live’ safety case, such that they will include all the supporting disciplines to help implement, and drive, the necessary actions to achieve this goal within their own organisation.

Notwithstanding, the Safety Director also has a vested interest in ensuring the safety case properly and accurately reflects the facility, plant, process or equipment in-use and consequently the level of risk being carried by the organisation.



Figure 1: Example of a Simple Interaction Diagram between Disciplines

## 6.3 File Structure and Safety Case Index

To gain maximum benefit from the information contained, and to reduce as far as possible the effort required to maintain a “live” safety case, the information must be structured and stored in such a way as to:

* Be easily accessible;
* Have the capability to define (or re-define) the extant safety case at any point in time;
* Be easy to update;
* Be kept under robust configuration control at all times.

A modular approach to the file structure is advocated, such that individual topics or subject areas are contained within specific modules, which are themselves kept under robust configuration control.

Within the arguments and evidence produced and recorded within each module there should be no “spill” across modules, but instead, referencing should be used so that any updates or amendments to text within a module will avoid as much as possible, other modules needing to change.

Each module contains specific subject information, but additionally, different versions of different modules are capable of being identified (the advantage of robust configuration control). Thus, as the life cycle progresses, so does the version of the safety case which is extant at that time, “keeping the safety case live”.

The Safety Case Index, is a file that contains information relating to all the component parts (and all the different issues of the component parts) of the safety case, and provides an index to all those parts, but, crucially, it indicates the extant component parts of the current version of the safety case.

The Safety Case Index is the singular file that defines the ‘live’ safety case, it provides the reference to the modules comprising the ‘live’ safety case. It identifies the particular issue that is currently extant and the go-to documents that comprise the approved and authorised safety case.

The Safety Case Index and the module concept are illustrated in Appendix C Safety Case Index and Modular File Approach - Example.

The Safety Case Index is illustrated as a spreadsheet, but could equally be a database or word type document, which identifies each component part of the safety case and further identifies the different issues of that component part. It will describe the issue status of each part, that being either:

* Current ‘Live” Safety Case Module;
* Archived Module; or,
* Proposed Future Issue Module.

It is therefore vitally important that the Safety Case Index is kept under strict configuration control, to ensure that the extant safety case is always properly identified and defined.

The Safety Case Index could also be extended to include document reference numbers, or more usefully, active hyper-links to the individual files or documents.

Robust configuration control and the ability to identify the appropriate ‘live’ file within each module are considered to be fundamental to the successful implementation of the proposals in this guide.

## 6.4 Data Storage

The layout illustrated in Appendix C Safety Case Index and Modular File Approach - Example, lends itself very well to being set-up, either in a manual file structure format, or in a proprietary software package (e.g. Documentum, Sharepoint or Meridian).

The advantage of a proprietary software package is that it will robustly implement configuration management and control which would otherwise rely on the administrator, or operator, within a manual file structure set-up. Never-the-less, when set-up properly, either approach could achieve the same end result of good organisation, ease of access and robust configuration control, where the documents would be capable of being independently updated under formal version control.

## 6.5 During the Concept and Design Development Phases

The description of a modular file structure set-up would be capable of being applied in a new-build scenario where everything is essentially starting anew.

n the new-build scenario, the opportunity exists to design the optimum structure and the best presentation of the safety case from the start; and to build the case in a way which would easily satisfy the requirements of the proposal being described in this document.

The modular approach to the safety case would be constructed as the on-going work was recorded and presented, keeping topics contained within each module and referencing out to other associated and supporting modules.

The claims and arguments within the Safety Case document itself would also develop as the project progressed, with the case being developed and presented at each key project/safety stage, i.e. PSR, PCSR, PCmSR, POSR and OSC.

As is the case with design development, modules would experience multiple amendments, changes and updates, but robust configuration control of the modular filing system and accurate update of the Safety Case Index would ensure that the live file within the module is always identified and available.

## 6.6 During the Operational Phase

During the operational phase of the facility life cycle, modifications and changes would continue to take place; these would usually be identified from the drivers described in Section 7.1.

Any modifications being developed for future introduction could be matured under appropriate configuration control within the relevant module, but would not be part of the live safety case at this stage, until governance approval had been given and the Safety Case Index had been updated.

## 6.7 During Decommissioning and Disposal

It is generally accepted that the operational phase continues after facility shutdown through POCO and carries on until bulk hazard removal (e.g. defueling) is completed.

At this point the change from operations to decommissioning and disposal will have an impact on the modules of the safety case, some will no longer be relevant, or be required, while there may be the need for new modules not previously necessary during the operational phase.

The organisation’s strategy for its activities during decommissioning and disposal can be supported through the continued use of the modular structure and the configured files within each of these modules, adding or removing modules as necessity dictates.

During POCO and defueling, and carrying-on into the decommissioning activities, the need for modifications and changes is likely to increase. This may prompt a change in the periodicity of the governance meetings to meet the programme demands, nevertheless, the approach remains valid.

This can, in some circumstances, be off-set by producing a bounding safety case that adequately covers the foreseeable future decommissioning activities, therefore requiring less frequent modification or change.

# 7 Options for Updating the Safety Case

## 7.1 Drivers to Update the Safety Case

The safety case comprises many and varied elements, changes to anyone of which, could, over time, drive a proposal for a modification or change to the facility.

Examples of the types of drivers for change fall into a number of different groupings, these include but may not be limited to:

* Knowledge Based;
* Risk Based;
* Event Based;
* Time Based.

More detailed examples are provided in Appendix D: The Drivers for Change.

## 7.2 Rolling Programme of Update and Implementation

The number of modifications or changes is usually, and most significantly, linked to one or more of the following criteria, which are not in any particular order of priority:

* Age of facility, plant, processes or equipment;
* Degree of manual operation required;
* Dependence on technological processes (particularly software issues);
* Changes in international, national or specific technical standards;
* Changes in regulatory requirements;
* Emergent problems from a programme of self-audit, plant walk-downs, management reviews or outcomes from assessments.

Individual organisations should be able to review their own modification history and be able to predict, with reasonable accuracy, the numbers, and categories of changes that it could expect. So, dependent on the presence of the facilities, plant, processes or equipment satisfying these criteria, the organisation could be expected to fairly accurately predict the throughput of modification proposals in each category.

The problem then becomes one of co-ordination and timing, or relative priority, for the implementation of these modifications, coupled with the most effective and efficient means of applying any updates to the safety case; always keeping in-mind that all aspects of the safety justification have to be approved and ‘in-place’ prior to implementing the modification.

It should also be noted that there is considered to be an over-riding importance in maintaining the audit trail, line-of-sight or “Golden Thread” during all actions to update the safety case.

An idealised viewpoint might suggest that the safety case should be updated on every occurrence of a modification or change, to ensure the safety case is “live”, but on a more practical level this would be very difficult to achieve for a variety of reasons, particularly for existing facilities that have historically approached the safety case structure from a different direction, which (in itself) is a significant reason for adopting the modular style approach.

When considering all these arguments, and keeping in-mind the time frame necessary to generate any updates to the safety case ahead of implementation, it is suggested that modifications be “collected together” into batches and developed for input into the governance process to meet a scheduled rolling programme within an annual cycle, whatever periodicity is considered the most operationally practical for the individual organisation.

## 7.3 Governance

**Fundamental baseline assumption:** The safety case is only considered to be “live” if it is reviewed and updated as necessary, and approved, on a periodicity of no more than 12 months, or on a frequency that is demonstrably in proportion to the identified risk.

Reference should also be made to the complimentary Safety Case Forum guide on “Governance of the Periodic Review of Safety” [Ref. 4] which it is recommended should also be read in conjunction with this guide.

It is suggested that the most effective and efficient way of applying changes to meet this requirement is by using a time-based rolling programme of governance for updates to the safety case.

This is suggested, in order to stand-back from adhoc implementation, potentially reduce the frequency of governance meetings, and produce a more drum-beat approach to change control that will provide an appropriate amount of time to implement the safety case and engineering updates.

The time previously dedicated to producing modification safety justifications can instead be utilised to keep the safety case up-to-date, where the relevant safety case module(s) could be presented to governance instead of the modification safety report.

If a scheduled programme of governance was introduced, based on a periodicity best suited to the individual organisation then engineering design changes and their associated modification safety justifications would be “collected together” and worked-up and processed through the appropriate governance meeting before being approved for implementation.

This would ensure the baseline safety case was fully in-line with the engineering configuration of the facility and would remain so, until the next update.

It is recognised that there would still be a need for “emergency” changes but these would follow the same process, with additional governance meetings when required, and would be the exception rather than the rule.

## 7.4 Options for Change

For any nuclear facility, the control of change is crucial to the overall safe operation of that facility.

An organisation’s Change Control Process (which must satisfy the requirements of LC/AC 22) should deal with all changes to the configuration baseline within the organisation. There should be no changes undertaken that would alter the configuration baseline of the facility, and potentially therefore the safety case, without the necessary level of scrutiny being applied.

Any proposed change is usually categorised in terms of its impact on safety, generally by way of an assessment of the consequences from it being ill-conceived or inadequately implemented. The chosen categorisation then indicates a particular governance route, to ensure adequate scrutiny without excessive time, programme or cost implications.

To this extent it may be an acceptable practice to have a “log of minor changes”, to accumulate changes that have no impact on the configuration of the facility/plant/equipment/procedures, because they don’t affect the safety claims and have no impact on the delivery of the safety function. However, these minor changes must still be incorporated during the regular update and approval of the baseline safety case.

**Option 1 – Eventually:**

Update and re-baseline the full safety case as and when required; when it is considered that the number of changes (and thus the growing pile of modification safety justifications) makes the safety case out-of-date, delivers a fragmented story, is incoherent or where the picture has become unclear.

This may be considered a viable and cost-effective approach for smaller organisations where the safety case is less than complicated. However, this option would only be considered adequate if the safety case was fully updated, reviewed and approved, on an annual basis.

**Option 2 – Minimum Selected Update:**

Update only the minimum safety case documentation considered necessary to reflect the changed configuration baseline and the assessed position of the plant on an on-going basis.

This would include as a minimum the Hazard Register, the Fault Schedule, the relevant supporting assessment report(s), the Engineering Schedule, the Schedule of Procedural Safety Measures and the Safe Operating Envelope. This may allow a longer period of time to pass before the safety case could be considered fragmented, incoherent or unclear, before it will need to be re-baselined, and up-issued again.

An organisation may consider this option viable because key safety case documents are being updated and while this may provide headline information the full risk profile may not be readily apparent, with the information needed to make important business decisions not easily available without additional work.

This option would only be considered adequate if the safety case was fully updated, reviewed and approved, on an appropriately regular basis.

**Option 3 – Regular, Comprehensive:**

Update the full safety case, on a rolling program (described in Section 7.3 - Governance) as a result of working-up any modification and change proposals that are locked-in to meeting the scheduled governance programme.

Operational history has demonstrated the drawbacks to using Options 1 and 2, and the huge cost associated with the Periodic Review of Safety when the safety case does not fully reflect the configuration of the facility it represents, and is only updated (re-baselined) on an in-frequent basis.

## 7.5 Proposals for the Implementation of Option 3

It may be necessary for some organisations to fundamentally restructure their safety case(s) before contemplating the implementation of the proposals in this guide.

The idealised structure of the safety case has already been described, noting that each organisation will determine the number and type of modules they will require to support their safety case(s).

In order to implement a time-based rolling programme, and in order to bring modification proposals together to meet a particular governance meeting dead-line, the integration and alignment of several different company processes will be necessary around fixed governance date(s). These processes would probably include but are not limited to (and is likely to be different for each organisation):

* The engineering design process;
* Production of the safety justification;
* The LC 22 or Company Change processes;
* The Nuclear Safety Committee process;
* The safety case writing, update and publication processes;
* Procurement processes;
* Risk reviews;
* Engineering implementation;
* Safety requirements implementation.

All these processes would need to be aligned, if not integrated, and planned to fit around a regular fixed governance process, with appropriately timetabled dates; and it may be that the governance meetings would have to be longer in order to include all modification and change requests coming forward at that time.

It is recognised that the aspects (described above) that make up the programme will take different time periods to mature, this is only trying to explain a concept, as there are many other things that may come into play, such as the necessity for a plant shut-down in order to implement the engineering fixes.

The most appropriate frequency would probably depend on the number and category of the modifications being reviewed and this could be determined on a historical basis, as described in Section 7.2.

Within this system, the safety case would always reflect the plant status between governance meetings. The safety case would be kept up-to-date and would always reflect the facility, plant, process or equipment, as the safety case has to be approved and authorised prior to the implementation of the engineering and procedural controls.

# 8 To Update the Safety Case, or, Not?

## 8.1 That is the question!

The thrust of this Guide is to drive the continual update and maintenance of the safety case. This should be done in such a way that the potentially large number of amendments to the safety case resulting from modifications/changes to plant/process are continually monitored, to ascertain if the baseline safety case is being kept up-to-date; whilst maintaining the clarity and the visibility of the safety argument and the baseline safety case documents as the primary reference for the safety justification.

The drivers for updating the safety case primarily originate with the persons having the authority, and the intrinsic business necessity, for the information within it [Ref. 3]. These persons may include:

* The Licensee/Authorisee (legal accountability);
* The Director with safety responsibility (strategic/policy implementation);
* The Safety Case Owner (tactical implementation/duty holder);
* The Safety Case Manager (production and maintenance of the safety argument).

There is a continual emphasis within commercially-minded organisations, not to spend money unnecessarily and this seems to have been a key factor in organisations allowing the accumulation of modification safety justifications while not up-dating the safety case. The inclusion of widened, or redefined, boundaries of the safety case to include modification safety justifications, has been an action which appears to preclude the need to update the safety case, without ensuring, or maintaining, the clarity of the safety argument.

The difficulties that this builds-up over time are well known and come to a head when undertaking a Periodic Review of Safety, which inevitably then includes a re-write of the safety case.

In order to be able to prioritise, and programme, updates to the baseline safety case and meet the requirement within this document to keep the safety case live there needs to be a process which can balance the level of risk and the required financial resources, against the ever-decreasing clarity and lack of visibility of a clear safety argument.

The decision to up-date (or not) the safety case, to maintain a clear and visible safety argument, **must not** be led purely by financial considerations, rather it should be based on the complexity of the suite of documents which present the safety argument. The concept of complexity considers how visible and clear the argument is, and how difficult is it to follow the argument through the documentation suite. This should also be tempered by the level of complexity and the lack of clarity the organisation is prepared to accept, and this is likely to vary from one organisation to another.

The level of complexity of the documentation containing the safety arguments is actually a difficult and very subjective decision to make, it is likely to be different for each Licensee/Authorisee and includes a consideration by the organisation of some, or all of the following:

* The relevant good practice adopted by the organisation;
* The prioritisation of risk and the appetite for carrying, or alleviating, risk across the business;
* The management of risk to achieve an ALARP solution;
* Modern standards when considered against the type of plant, or equipment under consideration, its age and remaining operational life;
* The likely level of change or flux incurred over the review period;
* The categories, or significance of the changes being processed and implemented;
* The accessibility, the visibility and clarity of the safety argument.

If very few modifications are being undertaken then a case can be made that the argument within the safety case is still considered to be clear and visible.

At the opposite end of the spectrum, dependent on the category and complexity of the changes on a high hazard installation, it may not require many modifications for the safety argument to be diluted to the extent that it is not visible and not clear. In this situation, any change of key personnel (such as the safety case owner or manager) would compound the problem because fewer people (if any) would have an overarching and clear view of the composition of the safety arguments.

For these reasons, the following process is proposed as a solution for the decision on whether, or not, to up-date the safety case; keeping in mind that this guide still requires a review, update where necessary, and approval, to take place annually.

Figure 2 illustrates for example, the accumulation of a number of modification safety justifications against various documents within the boundaries of a specific safety case. The “levels” described, show how modifications can be introduced that have implications on previously implemented modifications, thus increasing the level of complexity and obscuring visibility when trying to understand the safety argument.

The colour code adopted for this example is a simple RAG (Red, Amber, Green) approach, increasing from green through to red, the necessity to up-date the baseline safety case by incorporating the modification safety justifications into the relevant safety case documents; always keeping in-mind the necessity to complete this action on an annual basis anyway in order to meet the requirements for keeping the safety case “live”.

Each licensee organisation, or perhaps each facility, would have to set its own “rules”, but this example describes one type of approach, where on reaching a Red colour, it would indicate that an update to the baseline safety case documentation is required to incorporate all the modifications in that line. Any Amber colour might cause the safety case manager to consider updating the baseline safety case if another change were to be introduced.

If this type of diagram is produced and maintained in support of a safety case, then it becomes increasingly clear as modifications are implemented, when, and how much work may be required to update the baseline safety case.

In organisations that budget work on an annual basis this would also provide a “look ahead” facility, or the ability to project in advance the work that could be required in the next financial period, to meet the requirement to keep the safety case live.

When planning future workload and considering modifications that will generate ‘up-and-coming’ safety work, a process as well as a behavioural change, needs to take place, such that potential changes are assessed against the complexity diagram to determine whether a modification safety justification is appropriate, or in fact (due to the complexity of the safety argument that will be built-in from implementation of the modification) the baseline safety case documentation should be updated.

To this extent, the complexity diagram provides very good visibility of the need to programme future baseline safety case updates. This in-turn will assist in identifying (well in advance) resource requirements and their availability within the programme, leading to a more efficient and effective allocation of a scarce resource.

Figure 2: Resolution of the Complexity Concept



# 9 Audit Trails - The Golden Thread

## 9.1 Discussion

The key to having a “live” safety case, one which has clear and visible safety arguments, is being able to access the arguments quickly and easily, and to be able to update it effectively and efficiently; hence the recommended modular approach.

The importance of a ‘line-of-sight’ within any suite of safety documentation, to demonstrate the adequate consideration and assessment of hazards related to a facility, and its operations, is absolutely imperative.

This guidance proposes a format for the Engineering and Procedures Schedules to ensure that they are structured, methodical, and comprehensive, which also enables the “Golden Thread” to be established in order to allow a clear line-of-sight to demonstrate that hazards associated with a facility are adequately controlled and managed.

## 9.2 The Engineering Schedule

The Engineering Schedule allows examination of various faults associated with identified hazards to determine engineered safeguard requirements and assessment against those engineered safeguards already in-place. The Engineering Schedule also provides a structure to provide tracking, and the evidence of resolution of all engineering shortfalls from any assessment process (such as the Periodic Review of Safety for the Facility, but it works equally well for any other assessment process).

As was described for the Safety Case Index, the Engineering Schedule could benefit from having active-links to the appropriate version of the document being identified.

An Engineering Schedule Template is given in Appendix E: An Example of an Engineering Schedule Template.

## 9.3 The Procedures Schedule

Similarly, a Procedures Schedule identifies the links between the faults and the requirements for procedural controls in the form of Operating Rules and Key Safety Actions. This is applicable where there are shortfalls in engineering and no other engineering claims or improvements can be justified.

As was described for the Safety Case Index and the Engineering Schedule, the Procedures Schedule could benefit from having active-links to the appropriate version of the document being identified.

A Procedures Schedule Template is given in Appendix F: An Example of a Procedures Schedule Template.

## 9.4 The Golden Thread

These schedules present the links within the documentation suite comprising the safety case which are required to provide the auditable trail for any particular hazard; the “Golden Thread”.

The layout of, and the hyper-links within, the Engineering and Procedure Schedules provide a straight forward means to enable a review of the “Golden Thread” for its adequacy; this should also help identify and facilitate the update, or rewrite, of the appropriate parts of the Safety Documentation, should this be required.

During any management review of the safety case, any interim review of safety, or as part of the periodic review of safety, it should be established that the “Golden Thread” is clearly adequate and visible throughout the documentation suite.

## 9.5 Real-Time, Live Updates to the Safety Case

Over time, and with the experience of having implemented the proposals described in this guide, it may be possible to take the view that the safety case could be updated in real-time; that being for each modification that drives a configuration change, necessitating an update to the safety case.

It is believed that, ultimately, the proposals in this guide could support such a move.

This may seem, at this point in time, to be a step too far, but is the progressive, next-step, that may be possible if a fundament change to the way in which Governance is implemented, could be affected.

It is recognised that Governance, and the Nuclear Safety Committee, play a very important role in challenging proposals to ensure they have been properly considered, so the balance to these suggestions would be a periodic refresh to the “Authority to Operate” or the “Case for Continued Operation” where all modifications and changes would be carefully considered by the submission of the up-to-date Safety Case as part of the renewal of the “Authority to Operate” or “Case for Continued Operation”. Alongside the annual approval of the safety case.

Conversely, the safety case should be up-to-date and approved before the “Authority to Operate” or “Case for Continued Operation” is approved.

The Safety Case Forum have considered governance of the Periodic Review of Safety against the wider aspects of Governance within an organisation. Refer to the Safety Case Forum guide on Governance of the Periodic Review of Safety [Ref. 4].

# 10 Interfaces with other Business Processes

One other important aspect of keeping the safety case up-to-date, not generally considered as significant, is the potential to feed information from the safety case into other business processes. There seems to be very little use made of the information currently available from the assessments brought together in the baseline safety case.

This guide actively promotes the use of the information as a feed-in to other business processes.

What information can be used? and where could it be used? This would have to be the subject of informed investigation within each organisation; however, the following are presented for consideration:

* Information input into a nuclear site safety case;
* Information to assess the adequacy of corporate leadership and management for safety;
* Corporate service provision necessary to meet the safety case requirements. The identification of common corporate support for safety across multiple nuclear facilities where the response to the corporate demand delivered to a number of facilities could change the individual facilities ALARP argument. This may include an assessment of the vulnerabilities associated with the delivery of the service provision in response to demand, and confirmation the demand can be met;
* Assess the adequacy of the safety management system to compile, maintain and sustain the safety case;
* Assess the adequacy of the organisational structure to support nuclear safety;
* To assist in defining the required safety culture and behavioural aspects of the work force to successfully manage nuclear safety;
* Information input into business risk management, and risk profiling;
* Information to assist in business development strategies;
* Validation that dose risk figures from nuclear facilities, as a whole, are within the relevant targets for BSL and BSO and that overall risk is reduced ALARP;
* Information that assists in assessing compliance with the site licence;
* Information feed into facility and site wide accident management, planning and preparedness, and the assessment of the adequacy of corporate accident management planning and preparedness;
* Determination of the facility, or site risk profile, identification of the dominant hazards and their respective controls;
* Understand site external hazards and controls.

# 11 Performance Measuring the “Live” Safety Case

## 11.1 Discussion

Performance measuring does not confine itself to generating statistics, or producing charts, for pre-defined aspects of the safety case. Performance measuring must confirm, so far as is reasonably practical, that all aspects that influence the completeness, the condition, or the quality of the safety case argument are being checked, amended or updated as necessary to keep the safety case current.

Taken together, these aspects are the primary reasoning for requiring an annual review and approval in order for the safety case to be declared “live”.

Each individual organisation must be responsible for implementing their own means of measuring their performance. However, the remainder of this section provides some suggestions for the type of information it may be prudent to track.

The following indicate the aspects of the safety case that should be in-place, and working effectively in order to achieve a live safety case. They are:

1. The safety case should have a formally recognised Owner. The owner of the safety case should ideally be the person that is accountable and holds the Authority to Operate for the plant or process covered by the safety case.

The owner is ultimately responsible for the production and content of the safety documentation; hence the owner is responsible for the provenance, integrity and appropriate use of supporting information and data; and for integrating the various contributions into a cohesive and comprehensive suite of safety documentation. This would include the following aspects of the safety case:

* It must clearly define the boundaries of the asset, product and activities covered by the assessment;
* Ensure a robust and comprehensive hazard identification process has been affected and regularly reviewed;
* Ensure a suitable and sufficient safety assessment is carried out on the asset, product or activity and the significant findings are formally recorded in the safety documentation;
* Engage the relevant technical disciplines and secure any other resources that are required, ensuring effective integration of all aspects of the safety assessment;
* Allow sufficient time in the programme and secure appropriate and adequate funding to carry out the safety assessment;
* Ensure all controls derived in the safety assessment are in-place and being maintained;
* Ensure significant hazards, risks and controls are communicated to all people who may work, be present or otherwise be affected by the facility, product and/or activities;
* Ensure any significant changes to hazards, risks or controls are reviewed, formally documented, updated where necessary and communicated to all people who may be affected;
* Ensure the production of an appropriate Formal Safety Justification or other safety document, as necessary;
* Ensure that all personnel engaged in the safety assessment are competent;
* Monitor and manage safety assessment performance;
* Implement all findings derived or arising from the safety assessment through design or operation and maintain the safety case up-to-date such that it remains configured with the actual status of the project or facility;
* Derive a Forward Action Plan (FAP), ALARP Issues List or other form of action register that specifies and then tracks the owner’s commitments over a specified period of time to reduce risk such that it is as low as reasonably practicable (ALARP).

Additionally:

1. The safety case should have a formally recognised Safety Case Manager. The safety case manager is responsible, on behalf of the Owner, for managing the assessments, compiling the information and keeping the safety case up-to-date, and live.

## 11.2 Performance Management

The effectiveness and efficiency of safety assessment is reliant on a range of organisational and cultural factors that are much broader than just the technical aspects of the assessment. An organisation’s attitude to, and arrangements for, safety assessment are recognised by the ONR as an indicator of its broader abilities in Leadership and Management for Safety.

The principal aim of performance management is to assist the Safety Case Owner to assess whether the conditions necessary for delivery of a ‘Right First Time Safety Case’ exist in their area of responsibility.

The arrangements comprise a range of tools and reporting mechanisms, utilising intelligence from various sources within the work environment.

The arrangements described in this guide are focused on the processes around safety assessment and would complement other corporate arrangements that may exist for checking the quality of the outputs from the assessment processes, e.g. Independent Peer Review.

A performance management framework for all forms of safety assessment is illustrated in Figure 3.

For any given safety case, or suite of assessments, the performance will be affected by a number of diverse factors, including dependencies on other projects, or facilities and factors outside the core safety assessment activity, e.g. compatibility of programmes, maturity of design, material state, quality of facility records, etc. These are depicted below the dotted line in Figure 3.

These factors should be recorded in a narrative associated with the safety assessment performance data, to enable the Safety Case Owner to understand any issues or potential remedies, and identify any relevant good practice.

Typically, the organisation will be looking for consistency, and effectiveness, from the corporate safety management system arrangements, when applied across the business. The performance data should support reviews and improvements to these arrangements, or allow for intervention, or support, if issues are more isolated. The information flows are depicted above the dotted line in Figure 3.



Figure 3: Performance Management

## 11.3 Monitoring of Safety Assessments

The Safety Case Owner should make appropriate arrangements for monitoring and managing the performance of the safety assessments and the compilation and update of the safety case. As the safety assessment develops, progress against the programme and against the identified performance indicators should be measured.

Relevant performance data should be reported by the Safety Case Owner, to the appropriate governance body, as part of the Company’s overall performance management arrangements.

Safety Case Managers, on behalf of the Safety Case Owner, should collect, analyse and interpret data on safety assessment work and provide accurate and timely reports on the status of the safety assessment.

The Safety Case Owner should act on any intelligence suggesting that the programme, or the integrity of the safety assessment, may be at risk. The Safety Case Owner should take appropriate steps to deal with identified shortcomings and/or accept the associated risks to programme or integrity of the safety assessment, communicating appropriately with all other relevant stakeholders.

From time to time an independent Health Check, audit or inspection of local arrangements for managing the production of safety assessments and for keeping the safety case up-to-date, may be carried out. The Safety Case Owner and Manager, and their project teams, should accommodate such reviews and respond appropriately to the findings.

## 11.4 Controls and Metrics

The following table illustrates the relationship between threats to achieving safety assessments of sufficiently high quality and integrity, and the controls that ought to be in place to prevent this happening.

The Threats and Controls are defined at a relatively high-level, because it is not really necessary to provide a greater level of detail to identify adverse trends. The identification of any adverse trends should be sufficient to “home-in” on the areas of interest in order to investigate more fully or in much greater detail, to pin-point the root cause of the issue.

It can be difficult, but nevertheless very important to correctly define and measure the variable that best identifies any changing trends. The right-hand column of the following table, has been left blank so that each organisation may undertake and record its own analysis, and identify the feature or characteristic that would best define or measure the performance associated with the safety case, at that point in the production process.

| **Threats** | **Controls** | **Aspects to be Measured** |
| --- | --- | --- |
| Inadequate Planning | 1. Company programme should ensure an adequate level of resource, support, facilities and timescale for safety case production and should ensure de-confliction with other safety cases, PRS and major operational tasks. |  |
| Inadequate Strategy to update Safety Case. | 1. Appointment of SQEP personnel. 2. Suitable independence between production, maintenance and review teams, and challenge activities. 3. Roles and accountabilities clearly defined. 4. Stakeholder engagement prepared and Regulatory interface understood. 5. Project teams undertaking modifications have appropriate understanding of safety case requirements. 6. Where appropriate, safety case specification/strategy that aligns with the programme. 7. Any changes to the modification programme have appropriate configuration control and have undergone analysis of impact assessment. 8. The verification, Peer Review and Stakeholder plans are aligned to the safety case update programme. 9. There are sufficient SQEP resources available to meet the programme. |  |
| Inadequate Safety Management System | 1. The organisation has established robust, proportionate processes and procedures to assist in the assessment and production of safety cases. 2. The appropriate procedures are followed in the production of the assessments and the safety case. 3. Safety documentation is proportionate and commensurate with the change categorisation. 4. Peer Review undertake ongoing reviews and health checks. 5. Stakeholder awareness. 6. Project teams are following the programme. 7. Safety case specification is maintained in-line with project configuration. 8. Configuration management strictly applied to safety documentation. |  |
| Inadequate Stakeholder Review | 1. Documents submitted for stakeholder review in accordance with the project plan. 2. Project team understands the importance of stakeholder review activities. 3. Configuration management is strictly applied to documents during the stakeholder review process. |  |
| Inadequate Verification | 1. Documents submitted for verification in accordance with the project plan. Verification resources available. 2. Project team understands the importance of verification activities on safety documents. 3. Configuration management is strictly applied to documents during the verification process. |  |
| Inadequate Governance | 1. Safety documentation submitted to Peer Review on programme. 2. Peer Review produce formal report on safety assessment and/or safety case report. 3. Safety documents submitted to NSC for advice. 4. Safety documentation submitted to Governance for approval. |  |
| Inadequate Regulatory Liaison | 1. Where requested or agreed, safety documentation made available to the ONR, and DNSR if applicable. |  |

## 11.5 Self-Assessment

The Safety Case Manager should continuously assess the efficiency and effectiveness of the safety assessment activities being undertaken within their area. This may involve a review of the cultural status of the modification or update project taking into account the leadership and the personalities involved in managing that project.

The Safety Case Manager should take steps to address any issues and, if appropriate, escalate any issues considered to warrant the intervention of the Project Manager or Safety Case Owner. The Safety Case Owner should continuously monitor safety assessment performance across the project utilising all the sources of intelligence at their disposal.

The Safety Case Owner, or Manager, should provide constructive intervention where issues have been identified.

Individual organisations will need to define and implement the type of self-assessment they require, dependent on the outcomes they are currently experiencing and the outcomes they wish to experience in the future.

## 11.6 Health Checks

In addition to the provisions for ‘self-assessment’ described above, from time to time it may be desirable for an independent person to carry out a health check on a given safety assessment.

The health check may be best performed ‘in-confidence’ to encourage open and honest discussion and should engage with all affected parties. A safety assessment health check may also form part of an investigation or other form of ‘review, learn and improve’ activity.

A health check should take the form of a ‘peer-to-peer’ review and is usually carried out by a trained and authorised Safety Assessment Specialist, acting within specified terms of reference.

A health check may be requested by the Safety Case Manager, or at the discretion of the Safety Case Owner, as a result of intelligence received, and may be carried out in conjunction with other review activities such as a Management Walkthrough.

Each health check should be structured around a question set, constructed specifically for the intended safety assessment process, which should form part of the specified terms of reference.

To maintain confidentiality, the findings and any actions arising from a health check should be disseminated only to the Safety Case Owner, Safety Case Manager, and any stakeholders explicitly identified in the terms of reference.

By their very nature these health checks are focused on particular aspects of the safety assessment, and each organisation will therefore need to generate their own question sets to meet the requirements, and circumstances, of their own investigation.

## 11.7 Key Point Reviews

For large, complex or otherwise significant safety projects, reviews may be carried out at key points in the lifecycle, to ensure the safety assessment is fit for purpose, and to enable the project to proceed.

These Key Point Reviews usually form a part of broader, project, or business governance arrangements. For example, in order to proceed from one development phase to the next, or to release a Hold-Point for a Category A modification.

A question set, developed and adapted, as appropriate, for the appropriate point in the life-cycle should be used in the Key Point Review.

In many ways, the proposed safety case annual review is a Key Point Review, being a stage gate that ensures the safety case is as up-to-date as possible before commencing the next period of operations.

## 11.8 Audit and Inspection

Depending on other business requirements, it may be necessary for other stakeholders to audit, inspect or monitor projects and/or facilities with respect to safety assessment.

While it is not possible to control these undertakings, any results or outputs from these audits and inspections should be made known to the Safety Case Owner and Manager, who will then be required to implement any recommendations.

# 12 Recommendations

During the production of safety assessments individual organisations should identify the parameters that best reflect the aspects of performance which they wish to measure, however, there are two situations which are considered so fundamentally important that they should be identified separately. These are:

**Pre-Production:** In order to set-off the project in the right direction, it is necessary to properly define the:

* Scope of the safety case;
* The strategy for the compilation of the safety argument; and the,
* Safety case production programme.

It is recommended that these aspects of the safety case should be subject to review and approval prior to commencing the safety assessments and thereafter have mandated performance reports at regular points throughout the programme.

**Post-Production during Operations:** Even although the safety case has been produced, there will undoubtedly be modifications and changes taking place that will require associated safety assessments to be undertaken, that change the configuration of the facility and therefore the safety case.

This document proposes an annual review and approval of the safety case to ensure all modifications and changes are captured and the safety case is updated accordingly.

It is recommended that the annual review and approval of the safety case, should coincide with, or be part of, any review and renewal of an Authority To Operate, such that the review considers the following, with the express purpose of ensuring the safety case is as up-to-date as possible:

* The total number of modifications or changes undertaken on the facility, plant or process covered by the safety case;
* The number of these modifications that required an associated safety assessment, and which of these were approved for implementation;
* The number of safety assessments for completed modifications **that have been** incorporated into the safety case;
* The number of safety assessments for completed modifications **that have not been** incorporated into the safety case, and the detailed reasons why;
* The number of modifications in the governance pipeline that will be implemented in the next reporting period.

It is also recommended that each organisation check their LC/AC 22 process (and amend it as necessary) to ensure that the process requires the safety analysis associated with a modification to be incorporated into the safety case before the modification can be closed; as having been successfully completed.

# 13 Glossary

| **Term** | **Definition** |
| --- | --- |
| PRS | Periodic Review of Safety |
| ALARP | As Low As Reasonably Practicable |
| ONR | The Office for Nuclear Regulation |
| PSR | Preliminary Safety Report |
| PCSR | Pre-Construction Safety Report |
| PCmSR | Pre-Commissioning Safety Report |
| POSR | Pre-Operational Safety Report |
| OSC | Operational Safety Report |
| POCO | Post Operational Clean Out |
| LC | License Condition |
| AC | Authorisation Condition |
| ATO | Authority To Operate |

# 14 References

|  |  |
| --- | --- |
|  | **Title** |
|  | The UK Nuclear Industry Guide to: Monitoring, Interim Review and Continuous Improvement in Periodic Review of Safety. |
|  | ONR’s Technical Assessment Guide 51: The Purpose, Scope and Content of Nuclear Safety Cases. Revision 4, July 2016. |
|  | The UK Nuclear Industry Guide to: The Periodic Review of Leadership and Management for Safety. |
|  | The UK Nuclear Industry Guide to: Governance of the Periodic Review of Safety. |

# Appendix A: The Generic Safety Case Model - Constituent Parts

A1. The “live” Safety Case breaks down into the following generic constituent parts:

1. The Safety Case Report; the top tier summary report – comprising the Claims and the high-level Arguments.
2. The Assessments; comprising the detailed arguments and the evidence to support the arguments.

* Scope and Boundaries document;
* Safety Case Specification;
* HAZID Reports;
* Hazard Register;
* Fault Schedule;
* Normal Operations Schedule;
* Hazard Assessments (HAZANs);
* Risk Summary/ALARP/BAT Assessment;
* Human Factors Assessment Report;
* Engineering Schedule;
* Schedule of Administrative Controls;
* Engineering Design Substantiation Reports;
* Safe Operating Envelope;
* ALARP/BAT Issues List;
* Waste Management Report;
* Register of Environmental Aspects;
* Decommissioning Report.

1. The Implementation; detailed validation evidence that the safety controls and safety measures, identified in the safety case, are being implemented.

* Implementation Plan;
* Manning/Resourcing;
* EIMT/Maintenance Schedule;
* Operating Rules;
* Operating Procedures/Instructions;
* Training;
* Safety Case Owner/SQEP/DAP Appointments;
* Plant Labelling of Safety Measures;
* Plant Configuration Control;
* Commissioning of safety case requirements;
* Self-Verification/Audit;
* Facility Emergency Response Plan.

1. Legal and Statutory Duties;

* Legal and Statutory Compliance.

1. Continuous Improvement (ALARP);

* Forward Action Plan.

# Appendix B: The Safety Case Report

B1. The generic Safety Case Report can be broken down into the following constituent parts:

1. Executive Summary.
2. Contents.
3. Introduction.
4. Plant Description and Operating Philosophy.
5. Operational History.
6. Hazard Identification Summary.
7. Summarise and Reference the Fault Schedule.
8. Facility Hazard Category.
9. Description of Assessment Methodologies.
10. Safety Assessment Summary: e.g.

* Normal Operations / Fault Conditions;
* Conventional Hazard / Risk Assessment;
* Chemotoxic Hazard / Risk Assessment;
* Environmental Hazard / Risk Assessment;
* Explosives Hazard / Risk Assessment;
* Nuclear Hazard / Risk Assessment;
* Radiological Hazard / Risk Assessment.

1. Additional Assessment Reports (summarised and referenced):

* Waste Management Arrangements;
* Decommissioning.

1. Summarise and Reference the Engineered and Administrative operational safety measures.
2. Review of the adequacy of Plant and Process engineering:

* Engineering Substantiation;
* Human Factors Substantiation.

1. Identify and Reference the Safe Operating Envelope / Limits & Conditions.
2. Safety Management Arrangements.
3. Overall ALARP/ Risk Summary.
4. Conclusions.
5. References.

# Appendix C Safety Case Index and Modular File Approach - Example

C1. This is an example (only a part) of how the Safety Case index might look, it is the singular file that defines the ‘live safety case’ and is therefore, by default, a live document itself. It clearly indicates the safety case component (document) and the particular issue that is currently extant. The documents identified as “current”, together, form the approved safety case. The Safety Case Index must be kept up-to-date to ensure that the extant safety case is properly identified and defined.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **SC Component** | **Issue 1 Status** | **Issue 2 Status** | **Issue 3 Status** | **Issue 4 Status** | **Issue 5 Status** | **Issue 6 Status** |
|  | | | | | | |
| Safety Case Report | Current | Future |  |  |  |  |
| Scope and Boundaries document. | Archive | Current | Future |  |  |  |
| Safety Case Specification. | Archive | Current | Future |  |  |  |
| HAZID Reports. | Archive | Archive | Current |  |  |  |
| Hazard Register. | Archive | Archive | Current |  |  |  |
| Fault Schedule. | Archive | Archive | Current |  |  |  |
| Normal Operations Schedule. | Archive | Archive | Current |  |  |  |
| Hazard Assessments (HAZANs). | Archive | Archive | Current |  |  |  |
| Risk Summary/ALARP/BAT Assessment. | Archive | Archive | Current | Future |  |  |
| Human Factors Assessment Report. | Archive | Archive | Current | Future |  |  |
| Engineering Schedule. | Archive | Archive | Current | Future |  |  |
| Schedule of Administrative Controls. | Archive | Archive | Current | Future |  |  |
| Engineering Design Substantiation Reports. | Archive | Archive | Current |  |  |  |
| Safe Operating Envelope. | Archive | Archive | Archive | Current | Future |  |
| ALARP/BAT Issues List. | Archive | Archive | Current | Future |  |  |
| Waste Management Report. | Archive | Current | Future |  |  |  |
| Register of Environmental Aspects. | Archive | Archive | Current |  |  |  |
| Decommissioning Report. | Archive | Current |  |  |  |  |
| Archive: Past issues of this component part of the safety case. | | | | | | |
| Current: The component parts that comprise the current approved and authorised safety case. | | | | | | |
| Future: The parts of the safety case that are being actively worked-on for future approval and authorisation | | | | | | |
| **The currently approved and authorised safety case components could be high-lighted for visibility and ease of recognition.** | | | | | | |

The above example illustrates a mature safety case which would look similar to the file structure presented below, where there are a number of archive copies of each component part of the safety case (shown in blue) with the current approved and authorised files (shown in green) and with some on-going work to update or otherwise up-issue certain component parts of the safety case in the future (shown in red).



# Appendix D: The Drivers for Change

D1. Examples of the drivers for change fall into a number of different groupings, these include, but are not limited to:

D2. **Knowledge Based:**

* Post implementation checks and shortfalls;
* As a result of deficiencies found at Audit;
* Checks of records identifying shortfalls or deficiencies;
* Permissioning requirement checks necessitating additional changes;
* Implementation plans highlighting deficiencies;
* Design Safety implementation plans requiring modification;
* Readiness reviews identifying shortfalls.

D3. **Risk Based:**

* As a result of any material changes increasing the risk;
* An emergent issue not previously considered, such as a New Fault Sequence;
* Following a Gap Analysis that identifies deficiencies;
* Changes in throughput.

D4. **Event Based:**

* Changes to operational scope of a facility;
* Modifications for a myriad of reasons including the output from the Monitoring, Interim Review and Continual Improvement activities associated with the PRS;
* Changes to management system Standards and Procedures;
* Facility, plant, process or equipment changes from operating, to care and maintenance;
* Based on LFE – internal/external/key events;
* Based on analysis of reliability data;
* Organisational changes, necessitating different ways of working;
* Hold Point Control Plan requirements;
* Changing Regulatory or legal requirements;
* Change in international standards.

D5. **Time Based:**

* Pre-defined, rolling time-based program;
* Following timetabled changes;
* Based on the output from the Monitoring, Interim Review and Continual Improvement activities of the Periodic Review of Safety;
* Annual Health Checks and Reviews;
* ATO Initiation, or removal;
* Reaching next facility Life Cycle Point.

# Appendix E: An Example of an Engineering Schedule Template

(The text alignment is only to facilitate the inclusion of all the explanatory text)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ref. No. SSC** | **Fault Ref** | **Fault Description** | **Fault IEF (per year)** | **Fault Unmitigated Consequence (mSv)** | **Safety Function** | **(Demand) Safety Functional Requirement** | **Specific Safety Functional Requirements** | **SF Category** | **Authorisee SF Ref.** | **Number of safeguards required against the Fault** | **SSC Class** | **Substitution Arrangement or Planned Plant Outage Required** | **Engineering Substantiation** | **SSC System** | **SSC Sub-System** | **Shortfall Identified** | **Category of Shortfall** | **Shortfall Management / Final Solution** | **Shortfall Close-Out** | **EMIT** | **Maintenance Ref.** | **Maintenance instruction/WI etc.** | **Periodicity** |
| Unique identifier for the SSC and item name. | Reference identifier of the Fault for which the SSC is claimed against as allocated in the HAZAN. | A brief description of the Fault Initiation and Fault Sequence. | Fault IEF per year estimate. | Fault unmitigated consequence estimate. | The Safety Function being addressed by the SSC. | The Demand Safety Functional Requirement being addressed by the SSC. | The performance parameter against which the SSC can be tested to demonstrate the safety intent is met. The SSFR to be uniquely identified. | The Safety Function Category associated with the Fault as a result of the Fault IEF and Unmitigated Consequence. | Reference of any of the applicable Authorisee SF Requirements for which the SSC is being claimed. | The number of required safeguards as a result of the SF Category | The Class assignation of the SSC. | Identification of the SSC as:  No - SSC is a Passive Permanently Available (PPA) System, or  No - SSC is Further Safety Measure (FSM) or  Yes - SSC is Required Safety Measure (RSM), | Evidence Summary and Reference for the Engineering Substantiation documentation. | Identification of the type of SSC for Engineering Substantiation  (e.g. Tooling, Building Structure, Process equipment) | Identification of the type of SSC for Engineering Substantiation Discipline purposes (e.g. mechanical, electrical, civil) | Unique Reference and description of the Design Substantiation Shortfall (in sufficiency and/or suitability against the Fault as a result of Design Basis safeguard requirements and the Engineering Substantiation) or Shortfall in Safety Justification. | Category of the shortfall in terms of Safety Significance. | Shortfall resolution, options, actions or acceptability. Shortfall resolution to be uniquely identified to demonstrate link to shortfall. | Evidence Summary and Reference to the Shortfall Close-out documentation. | The EMIT Schedule Reference for the SSC and type of maintenance  e.g. Visual Inspection, Proof Load Test). | The Maintenance Reference for the SSC. | Reference to the document detailing the required maintenance/work inspection to be undertaken on the SSC. | Maximum Period between maintenance / tests. |

Note 1 - Template Columns should not be deleted or substituted and additional columns should not be added. Any Column information which is not relevant should have a recorded entry of N/A.

Where a document or hard reference is included, a hyper-link could/should be inserted to the appropriate article, to facilitate and enable ease of tracking and document “call-up”.

# Appendix F: An Example of a Procedures Schedule Template

(The text alignment is only to facilitate the inclusion of all the explanatory text)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Safety Function** | **Fault Ref** | **Fault Description** | **(Demand) Safety Functional Requirement** | **Procedural Controls** | **Candidate Operating Rule (OR) / Candidate Key Safety Action (KSA)** | **Confirmed as OR/KSA Y/N** | **Maintenance Ref.** | **Justification / Comment** |
| The Safety Function to which the operational/procedural control applies. | Reference identifier of the Fault for which the operational / procedural control is claimed against as allocated in the HAZAN. | A brief description of the Fault Initiation and Fault Sequence. | The Demand Safety Functional Requirement being addressed by the operational / procedural control. | The Procedural Control  (e.g. Operating Instruction for the activity) | Uniquely identified Operating Rule or Key Safety Actions associated with the operational / procedural control. The unique identification to indicate the status of the control (Operating Rule or Key Safety Action). | Identification of confirmation of ORs, KSAs or not | Reference for any of the applicable Maintenance Requirements for which the operational / procedural control is being claimed. | Reference to the documentation through which the control is promulgated / implemented. |

Note 1 - Template Columns should not be deleted or substituted and additional columns should not be added. Any Column information which is not relevant should have a recorded entry of N/A.

Where a document or hard reference is included, a hyper-link could/should be inserted to the appropriate article, to facilitate and enable ease of tracking and document “call-up”.