Integrating Safety Management through the Bowtie Concept

A move away from the Safety Case focus

Mr. Anthony P. Acfield and Dr. Robert A. Weaver
Airservices Australia
GPO Box 367, Canberra 2601, ACT
anthony.acfield@airservicesaustralia.com, rob.weaver@airservicesaustralia.com

Abstract
To ensure that safety processes such as risk management, change management and incident investigation deliver maximum value, it is essential that they are effectively integrated. As well as providing a means to represent risk, the Bowtie concept also provides a strong basis for integrating these safety processes, both internally within an organisation and cross-organisationally.

This paper provides an overview of how these processes can be integrated, why this integration is essential and why a change in focus from traditional Safety Cases to Bowtie Risk Management is needed within the safety engineering industry. As well as this, the paper describes in detail how a Bowtie Risk model can be used at the heart of safety requirements elicitation and a safety change management argument.

The aim of the paper is to effectively demonstrate that a risk-based approach to safety management, using the Bowtie concept, provides an effective means of achieving both this integration and shift in safety argument methodology.

Keywords: Integration, Bowtie, Risk, Safety Case.

1 Introduction
A Safety Management System (SMS) provides a systematic way to control all processes relating to the management of safety for a system or organisation. The International Civil Aviation Organisation (ICAO) Safety Management Manual (ICAO, 2009) identifies the following functions of an SMS:

- a) Identify safety hazards;
- b) Ensure the implementation of remedial action necessary to maintain agreed safety performance;
- c) Provide for continuous monitoring and regular assessment of the safety performance; and
- d) Aim at continuous improvement of the overall performance of the safety management system.

To achieve these functions, ICAO identifies the elements shown in Figure 1 as necessary for a successful SMS. While the SMS concept brings together all elements of a safety process into one system, manual or document, it is only when these elements are successfully integrated that the value of the processes can be maximised.

Within an SMS, six key processes need to be integrated to provide the heart of effective safety management:

- Management of Safety Accountabilities;
- Hazard identification;
- Risk assessment and mitigation;
- Safety performance monitoring and measurement;
- The management of change; and
- Incident investigation.

Many approaches to safety management integrate some of these processes. However, it is rare that all of these processes are successfully integrated within the application of a Safety Management System. This lack of integration can lead to safety management being under valued and approached in a “tick box” manner due to the true benefits of the processes not being realised.

Without process integration, we may not concentrate design effort on the correct safety hot spots, which will occur in operation. Similarly, we may not understand which events and occurrences during operation truly represent precursors to or indicators of more severe incidents. Without ownership of risks and controls by operational authorities, safety management can be outsourced to safety departments rather than being actively engaged in by those that have the ability to affect safety performance.

Copyright © 2012, Australian Computer Society, Inc. This paper appeared at the Australian System Safety Conference (ASSC 2012), held in Brisbane 23-25 May, 2012. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 145, Ed. Tony Cant. Reproduction for academic, not-for-profit purposes permitted provided this text is included.
1.1 Current Industry Focus on Safety Cases

Currently the primary technique used for integrating safety processes is the Safety Case, which provides an argument as to why the system is believed to be safe to deploy in its intended operational context (Kelly 1998). Safety Cases were originally developed in the Nuclear Industry with the UK Windscale accident in 1957 providing an impetus. In a similar way, the UK Piper Alpha Disaster and Lord Cullen’s subsequent public inquiry (Cullen 1990) led to recommendations for the use of Safety Cases for Offshore Installations. Cullen’s 1990 report is commonly seen as an important milestone in the promulgation of Safety Cases.

Since that time, the Safety Case as a concept has grown in stature to the extent that it is now recommended practice in many safety related industries. Standards and guidelines for systems, hardware and software usually require the development of a Safety Case for the certification process before operational use. The “Safety Case” has become terminology used by CEOs (The Australian, 2011) and it is often seen as the panacea for safety process integration. While internationally and cross industry there is alignment on the definition of a Safety Case, there is less clarity on when its use is appropriate. This has led to the over proliferation and application of the concept in ways which do not add value.

While the Safety Case concept is effective during change management for integrating the results of safety processes through the construction of a safety argument and supporting safety evidence, the authors believe that the concept is not as effective during operational service. We contend another concept - Bowtie - is more effective during operations for integrating safety processes and that the current industry focus on Safety Cases should be changed to a focus on Operational Risk Management using concepts such as Bowtie.

In Section 2 of this paper, we provide an overview of some of the issues surrounding the application of the Safety Case concept during operations. In Section 3 we go on to introduce the Bowtie concept as an approach to Risk Management and in Sections 4 and 5 we demonstrate how this technique can be used to effectively integrate safety processes during operations, while still maintaining a strong link with the development of change focussed Safety Cases. Section 6 provides a conclusion regarding the importance of having effectively integrated safety processes and why it is important to centralise our SMS processes around a concept such as Bowtie, as opposed to a concentration on Safety Case development. It also draws a link between the concepts suggested in this paper and some of the conclusions of Charles Haddon-Cave QC in his review of the loss of the RAF Nimrod XV230 in Afghanistan in 2006 (Haddon-Cave 2009).

2 Change in Focus from Safety Cases to Bowtie

Over the past 20 years, there has been an increasing focus in many safety industries on the Safety Case as the central pillar of the safety processes as defined in an SMS. With the growth of the Safety Case concept, the authors believe that insufficient attention has been given to the different roles for which Safety Cases are being used. In this section, we explore some of the issues to do with current application of the Safety Case concept and we suggest that it may not be appropriate to focus on the Safety Case during operation. Instead, it is believed that a focus on Operational Risk Assessments (or more traditionally Risk Registers) during operation is more appropriate. We believe that in some areas the Safety Case concept has grown larger than is of value and a refocussing of the industry back to risk management is needed.

Historically, the one term “Safety Case” has been used for two different purposes – safety change management and operational safety management. It is the authors’ experience that these two areas require fundamentally different approaches due to the fact that different information is available at these times and the information is used in different ways to make different types of decisions. We believe that the Safety Case concept (as it is traditionally known – safety argument & evidence) is most applicable in the area of change management, while its value is diminished in operations.

As discussed in the following sections, there is a significant difference between a Safety Case for continued operation and a Safety Case for change management. In this paper, the terms “Operational Safety Case” and “Change Management Safety Case” are used to signify these two different types. Different industries use other terminology, for example the Eurocontrol Safety Case Development Manual (Eurocontrol, 2006) uses the terms “Project Safety Case” and “Unit Safety Case”. However, the principle is the same and, as explained below, Safety Cases do not all perform the same role.

2.1 Change Management Safety Case and Placing Arguments within Safety Plans

Change management includes commissioning and decommissioning as well as change in application or operation of a system or service. For change management, safety arguments in Safety Cases (and Safety Plans) have two primary purposes:

- As part of planning, to determine what activities need to be conducted to ensure acceptable levels of safety for the system or service during and after the change; and
- As part of acceptance/certification/endorsement to assist in convincing risk owners and other stakeholders (including regulators) that the change is acceptably safe.

Both are important. However, more importance should be placed on the first item – planning – as it occurs earlier in the development process and thus in general has a greater impact on ensuring or “designing in” safety. When reviewing Safety Case literature, most guidance concentrates on placing arguments in the Safety Case (rather than the Safety Plan). This does not achieve the greatest cost/benefit from the safety argument development process.

In recent times, we have seen a great focus on the development of Safety Cases and, with the growth of the concept, a whole Safety Case development industry has
grown up. Detailed techniques for argument creation and presentation have been established. For example, the Goal Structuring Notation (GSN) (Kelly 1998) since its establishment in the 1990s has been extended to include many advanced argumentation concepts Patterns, Modularity, Assurance Levels to name a few (Origin Consulting 2011). The extent to which these additional concepts add value above and beyond a Safety Case template and a well written clear argument (particularly during certification) is yet to be fully demonstrated. Concepts such as GSN (and the extensions to the notation) provide freedoms which may present Safety Case developers (particularly inexperienced ones) with more problems than added benefits. The number of people applying these concepts and the lack of argument prescription means that we may be seeing as many issues with notation based safety arguments as we see with those written in natural language.

Given the limited budgets available for undertaking safety work during change management, the time invested in the development of a complex safety argument reduces the time spent on other safety activities. It is questionable whether this time is best spent in argument construction or whether greater effort in Risk Management and Safety Requirements definition is more appropriate. Across all industries, the majority of changes would need to make the same risk based argument and the same Safety Requirements Validation argument. Thus it would be more advisable to prescribe these processes and invest the time in conducting them and describing results (product & process) rather than creating bespoke arguments. Depending upon the level of risk, the level of process prescription can be varied. This is in-line with approaches defined in standards for software assurance such as DO-178B (RTCA EUROCAE 1992). Freedoms of Safety Case structure and argument construction may well be wasting valuable resources, which could be spent adding greater safety value.

In summary, it is possible that we have invested too much time focussing on the Safety Case rather than designing safety into a system and preparing for safety management during operations.

In change management, the traditional Safety Case concept (with the use of safety argument and evidence) whether in natural language or the Goal Structuring Notation (Kelly 1998) is at its most useful. However, its use should be controlled carefully. As we describe in the next section, once the transition into operations occurs, the Safety Case concept loses its value.

2.2 Operational Safety Cases

When it comes to “Operational Safety Cases”, the focus of purpose shifts from achieving operational acceptance and certification to:

- knowing what the risk baseline is;
- understanding whether it is acceptable; and
- determining what direction the risk-level is going.

Practically, the case for safety at this stage should be heavily focussed on risk management without the need for an explicit safety argument. Here we need to know whether the in-service experiences that are occurring validate the risk assessment or whether they imply that the risk assessment needs updating. The risk assessment is managing changes that occur in the environment and the system, which are not subject to a change management process. At this stage, the accessibility of the risk assessment, including an understanding of controls and their effectiveness is more important than the truth of a historical argument at the point of commissioning. The argument is implicit within the risk assessment.

Change Management Safety Cases tend to be written from the perspective of the point of certification, with events before this written in the past tense, system attributes in the present tense and in-service planned activities in the future tense. This grammatical approach to the argument, while totally appropriate for making the decision to deploy, or change the system or service, exacerbates the static nature of Safety Cases during operation. Safety Cases can become frozen in time as they enter operation.

During operations, the authors believe that maintenance of a large complex Safety Case with a safety argument is not appropriate. The terminology of risk (ISO 31000 (ISO 2009)) inherently contains a standardised safety argument and these principles should be applied at this stage. This is because Operational Authorities who hold safety accountabilities are more likely to find risk concepts more understandable and relevant than argumentation concepts. Terms such as Threats, Controls, Likelihood and Consequence are more applicable to operational services and operational safety processes (e.g. investigations and event reporting) than safety argument terms such as Claims, Goals, Strategies, Justifications and Evidence.

Within operations, the safety argument is usually the same – it is a risk based argument focussing most commonly on the As Low As Reasonably Practicable (ALARP) principle. Other safety arguments, such as legal compliance, are also usually implicit through the application of procedures (e.g. application of a Manual of Air Traffic Services in Air Traffic Control). Thus we do not need to manage or maintain an explicit safety argument. In fact, focussing on maintaining a Safety Case during operations can remove effort from more practical integration of safety processes.

During a development project we need to prepare for a risk focussed operation. Given that the majority of accidents occur during operations, the change management process, while developing a Safety Case for commencement of operations, should also prepare for operational safety management. Often the change process concentrates on the former of these rather than the latter.

Having said this, during operations it is still necessary to maintain a record of what high level goals should be achieved when a change is made to that specific system or service. This would be the upper section of a safety argument, but is something that would most likely be generic to all changes, concise and provide a starting point for any future change management Safety Plans and subsequent Safety Cases.

We believe that the focus for operational safety management should be operational risk management rather than safety arguments (within a Safety Case). This focus means that the term “Operational Risk Assessment”
is more appropriate than “Operational Safety Case”, “Unit Safety Case” or “Risk Case” (as identified by Haddon-Cave). At the operational stage of the lifecycle they are not a “Case” in the traditional sense of the word and their focus is on risk management, not the argument. Like the Safety Case, the Operational Risk Assessment should be a logical concept, which might be recorded as a document, within a software tool or a combination depending on what is fit for purpose.

The authors propose that the Bowtie concept is not only a useful technique for recording Operational Risk Assessments, but that it is also appropriate for integrating the key safety processes described in Section 1. The Bowtie concept is introduced in the next section.

3 Bowtie Concept

The Bowtie concept (ABS Consulting, 2012) was originally developed by The Royal Dutch / Shell Group and provides a means by which risk information, that would commonly appear in a risk register, can be represented graphically. The resultant diagram (Figure 2) approximates the shape of a Bowtie. Bowtie has been applied in Oil and Gas Exploration and Production, Chemical Processing, Defence and Security, Shipping (including ports and harbours), Packaging and Logistics, Medical, Aviation, Mining, and Emergency Response (ABS Consulting, 2012). The concept is used by Airservices Australia to manage its Operational Risk Baseline.

The Bowtie concept can be used to represent risk associated with Systems, Services, Processes and Organisations. In order to define an organisation’s entire Operational Risk Baseline, Bowtie diagrams must be developed representing all Hazards and Top Events associated with the service provision (Figure 3), addressing both system failure and organisational failure.

![Figure 2: Bowtie Diagram (Sharif 2011)](image)

Each Bowtie presents a single Hazard & Top Event combination and pictorially represents the Threats that can lead to the Top Event (release of the Hazard), and the Consequences that may be produced as a result. Also represented are the Controls in place to prevent each Threat from releasing the Hazard and the Controls in place to mitigate the severity and/or likelihood of each Consequence. It should be noted that the term “Top Event” is used here in a way that the term “Hazard” is used in some industries. In Bowtie terminology the term Hazard is used to describe the activity - e.g. “driving” is a Hazard and “inability to decelerate” is a Top Event. With this approach, there can be multiple Top Event Bowties associated with a hazardous activity. Threats can be both internal and external to the system. Consequences are as per traditional risk terminology “outcome of an event affecting objectives” (ISO, 2009) and occur at the system boundary. As with other notations, it is essential to ensure discipline with respect to terminology and the application of concepts.

![Figure 3: Bowtie Operational Risk Baseline](image)

The Bowtie concept can be used to represent risk associated with each Top Event can be assessed. The likelihood of the worst credible Consequence can be determined qualitatively or quantitatively, through a combination of the likelihoods of occurrence of each Threat and success of each Control. Once determined, this likelihood can be combined with the Consequence’s severity in order to obtain a risk level for the Top Event.

3.1 Benefits of the Bowtie Concept

The main advantage of the Bowtie concept is that it provides a visual representation of risk, including not only each applicable element, but more importantly, the relationships between them. It is this relationship illustration that enables many of the benefits of the concept when compared with textual or tabular risk information (in a similar way to the use of GSN for safety arguments). It allows areas of concern, such as inadequately controlled Threats or Consequences, to be readily identified and subsequently targeted for further treatment. It is the authors’ experience that this visualisation of the interactions between risk elements allows the representation to be more easily comprehended and understood by those with accountability for the risk in question, who are generally not experts in safety and risk (and the associated semantics), but rather experts in the applicable subject matter (e.g. Air Traffic Control). This is crucial if risk management is to be an activity undertaken by those who are accountable for safety rather than being outsourced to a safety department.

The linear nature of the Bowtie concept (Threat leads to Top Event leads to Consequence) facilitates the linking of sequential Hazards. For instance, one Hazard’s outcomes may be a subsequent Hazard’s causes depending upon your area of concern (or your system boundary). This can be performed both internally within an organisation and also involving an organisation’s vendors, stakeholders and customers and is described in Section 4.

A further benefit of the Bowtie concept is the ability to include elements from domains traditionally treated separately, on a single representation. Threats due to human error, procedure error, equipment failure and also external, management and organisational factors that can each contribute to a common Top Event can all be represented on a single Bowtie. Additionally, Controls from each of these aspects can be included regardless of the nature of the parent Threat, such as equipment based
control of a human error Threat or procedural control of equipment failure. Beneath this top level representation of risk, safety engineering techniques (such as Fault Tree Analyses, Event Tree Analyses, FMEAs, HAZOP Studies, Common Cause Analyses, Software Assurance Techniques and Human Factor Analyses) can be linked to provide greater analysis and, where practical, quantification to a level which is of benefit. This is essential as (with all techniques) Bowtie does not provide all necessary information for safety analysis. For example, the Bowtie Concept is not a suitable basis for conducting common cause analysis.

3.2 Safety by Design

When managing an Operational Risk Baseline defined in the Bowtie format, a clear priority order can be applied to reducing risk through Safety by Design (or Safety Engineering):

- **Remove Hazards** – Changes at the service level that remove Hazards completely, eliminating the risk from the baseline;
- **Remove Threats** – Changes at the system level that remove potential causes of a Top Event;
- **Reduce Threats** – Changes at the system level that render the potential causes of a Top Event less likely to occur;
- **Prevent Top Events** – Changes at the system or unit level that make the potential causes less likely to lead to a Top Event (i.e. additional or improved preventative control); and
- **Reduce Consequences** – Changes at the system or unit level that reduce the likelihood or severity of the potential outcomes of the Top Event (i.e. additional or improved recovery control).

This hierarchy is more effective than the traditional hierarchy of control, which tends to focus more towards Work Health and Safety concepts rather than risk management concepts. In reality, using the hierarchy described above, the closer the risk treatment approach is to the top of the list, the harder it is to achieve. In all of the above cases, care must be taken that the change being applied, while intending to remove or reduce one element, does not have the contrary effect, or result in the addition or exacerbation of other elements. One method of achieving this is using any proposed changes to Bowtie elements to generate safety objectives and requirements; this process is described in Section 5.

4 Integration of Safety Processes

The recording of an Operational Risk Baseline using the Bowtie format affords the opportunity for the integration of safety processes that this paper contends is so essential for effective safety management. This section will demonstrate how this integration can be achieved, both through an organisation’s internal safety management processes and across the linkages between organisations.

4.1 Internal Integration

The internal integration of an organisation’s safety processes such as operational risk management, safety change management and event reporting & incident investigation is a straightforward process when centred on an Operational Risk Baseline defined using the Bowtie concept (figure 4).

**Figure 4: Internal Safety Process Integration**

Key to this integration is the use of the concept as the “centre” of the related safety processes and primarily, use of the Bowtie concept to define, record, assess, maintain and accept accountability for the Operational Risk Assessments that make up the risk baseline associated with the organisation’s service provision. An effective Operational Risk Baseline must record the contribution to the overall “risk picture” from all aspects of the organisation that play a role in the provision of the end service, not simply that of the operational arms. The Bowtie concept provides a mechanism for not only the inclusion of these upstream considerations but also for demonstration of how they interact. This is made possible by the linear nature of the concept, allowing the outcomes of Hazards from supporting areas of the business, such as system maintenance, to be linked to the causes of Hazards from the operational areas to which they contribute, as shown in Figure 5.

**Figure 5: Operational Risk Baseline Linkages**

Once defined, the Bowtie based Operational Risk Baseline must then be integrated with other related safety processes, the most important (from this integration point of view) being event reporting, incident investigation and change management.

The linking of an organisation’s event reporting and incident investigation processes with its Operational Risk Baseline provides benefits for not only those processes, but also for the baseline itself. This requires the establishment of suitable monitoring and reporting of the occurrence of Threats, Top Events and Consequences as well as the success and failure of Controls, and the investigation of these incidents where appropriate. Often safety monitoring focuses too much on the events which occur on the right hand side of a Bowtie...
Risk Baseline should be linked to those of its industry bodies, peer organisations and customers. With those of its vendors, service providers, regulatory industry, through the linking of an organisation’s Bowties ability for integration of baseline information across an traditional operational risk registers is the improved performance of the service in the context of the risk that they have accepted. The benefit to the Operational Risk Baseline comes through the ability for the continual review and validation, or otherwise, of the Operational Risk Assessments through the incorporation of ongoing in-service data. However, we must also integrate this operational safety management with the safety change process.

Integration of an organisation’s safety change management procedures with its Operational Risk Baseline, involves a closed-loop process whereby changes’ potential effects on the baseline are identified and managed (one method of achieving this is described in Section 5) with the impacts realised through implementation fed back into a subsequent baseline iteration upon change commissioning. This allows those accountable for the safety of the service to understand each change’s impact on their accepted and known baseline, and provide re-acceptance of the revised Operational Risk Baseline upon transition to the change.

4.2 Integration with Other Organisations

An additional advantage of the Bowtie concept over traditional operational risk registers is the improved ability for integration of baseline information across an industry, through the linking of an organisation’s Bowties with those of its vendors, service providers, regulatory bodies, peer organisations and customers. Similar to the internal linking of sequential Hazards described in Section 4.1, an organisation’s Operational Risk Baseline should be linked to those of its industry counterparts (Figure 6) in order to provide clarity as to how its:

- Threats may be influenced by the Consequences of vendors, suppliers, service providers and regulatory bodies if applicable;
- Consequences may impact the Threats of those customers relying on the service provided for the safe provision of their own service; and
- Hazards and Top Events interrelate with those of its peer organisations.

Figure 6: Industry Linking of Operational Risk

Linking Operational Risk Baseline Bowties in this way provides an organisation with greater visibility and understanding of how breakdowns in its service provision may affect the industry as a whole, and in turn how it may be affected by breakdowns of service from other related organisations. This approach provides a structured means for dialogue between organisations. This is essential when one organisation sees an issue as critical while others may not agree. The highly integrated and complex nature of services and systems means that systematic approaches are needed for these dialogues.

5 Deriving Safety Objectives & Requirements from Bowtie Changes

At the heart of integrating a Bowtie based Operational Risk Baseline with an organisation’s operational safety change management process is the use of this baseline in the derivation and decomposition of Safety Objectives and Safety Requirements. It is through the satisfaction and substantiation of these derived objectives and requirements that a baseline that is considered acceptably safe is demonstrated to remain so under the change in question.

In order for the process described in the remainder of this section to be applied successfully, the service subject to change must have a defined Operational Risk Baseline that is considered correct and complete and is accepted by the relevant authorities. During the Preliminary Hazard Identification (PHI) phase of the change, this Operational Risk Baseline must be examined and all potential negative impacts due to the change identified. The impacts are described at this stage as “potential”, as they may or may not be realised through change implementation. Potential negative impacts on the baseline include:

- Exacerbating an existing Threat;
- Adding a new Threat to an existing Top Event;
- Removing or weakening an existing Control;
- Adding a new Consequence to an existing Top Event;
- Exacerbating an existing Consequence; and
- Adding a new Top Event.

In order to ensure safety objectives and requirements are imposed for both intended and unintended potential negative baseline impacts, all baseline elements that fall within the scope of change, regardless of positive or negative intent, are identified as having potential negative impacts in this analysis. For example, the intent of a...
change may be to strengthen a particular Control, however the possibility of adverse effects must be managed therefore the potential negative baseline impact is identified.

For new systems or services, establishment of a baseline would occur in a similar way to that described above after initial Preliminary Hazard Identification.

### 5.1 Service Safety Objectives

During the Functional Hazard Assessment (FHA) phase of the change, the change’s potential impacts on the Operational Risk Baseline are used to derive the Service Safety Objectives for the change.

Once all potential negative impacts on the Operational Risk Baseline have been identified, these impacts can be used to impose Service Safety Objectives. A Service Safety Objective is imposed upon a Top Event’s Consequence whenever a potential negative impact has been identified for a Bowtie element upstream of that Consequence. The Service Safety Objectives are of the form:

Consequence X due to Top Event Y shall occur no more frequently than \( \phi \)

Where \( \phi \) for existing unimpacted Consequences is that Consequence’s existing frequency of occurrence. \( \phi \) for new or exacerbated Consequences is the frequency of occurrence of that Consequence that would result in an acceptable level of risk, as defined in the organisation’s hazard risk matrix.

Satisfaction of the imposed Service Safety Objectives is necessary and sufficient to ensure the service under change remains acceptably safe.

For example, two potential negative impacts on elements of Top Event A have been identified (Figure 7) due to the change in question.

![Figure 7: Potential Negative Impacts](image)

Impact 1 – It has been identified that the change has the potential to exacerbate Threat T₂. Threat T₂ is upstream of all Consequences of the Top Event, therefore Service Safety Objectives are imposed upon all Consequences:

- Consequence C₁ due to Top Event A shall occur less frequently than \( \phi₁ \);
- Consequence C₂ due to Top Event A shall occur less frequently than \( \phi₂ \).

Impact 2 – It has been identified that the change has the potential to weaken one of the Controls of Consequence C₂. The Control is upstream of only Consequence C₂; therefore a Service Safety Objective is only imposed upon Consequence C₂:
and used to decompose the Service Safety Requirements into Functional and Performance Safety Requirements. During PSSA a complete set of human errors and functional failures at the equipment, procedure, training and (enabled by the use of the Bowtie approach) organisational level for the service changes must be identified. Also during PSSA, if applicable, a complete set of functional failures at an appropriate level of design decomposition for the equipment changes must be identified. Once identified, in order to allow these failures and errors to be used in the decomposition of the Service Safety Requirements, they must then be linked to their corresponding potential negative Operational Risk Baseline impacts identified during PHI. i.e. Each functional failure or error is linked to the impacted Threat it may cause, or impacted Control it may degrade. This allows the lower level safety techniques to be linked to the Bowtie risk assessment. The method of decomposition is dependant on the type of Service Safety Requirement and the type of potential impact through which it was derived:

- **Service Safety Requirements imposed on the rate of occurrence of a Threat.** Decomposition is achieved through the imposition of Functional and Performance Safety Requirements addressing each failure or error identified as a potential cause of that Threat;
- **Service Safety Requirements imposed on the sufficiency of a set of Controls due to a potential impact on the set’s parent Threat or Consequence.** Decomposition is achieved through the imposition of Functional and Performance Safety Requirements (a) across the Controls within the applicable Control set in order to ensure their effectiveness, and/or (b) specifying the establishment of new additional Controls as required;
- **Service Safety Requirements imposed on the sufficiency of a set of Controls due to a potential impact on a Control within the set.** Decomposition is achieved through the imposition of Functional and Performance Safety Requirements as per (a) and (b) above, as well as (c) addressing each failure or error identified as a potential cause of erosion of the impacted Control.

In each of these three cases, the decomposition of each Service Safety Requirement must continue until satisfaction of the resultant set of Functional and Performance Safety Requirements is considered necessary and sufficient to satisfy the parent Service Safety Requirements.

Continuing with the example above; functional failures F₁, F₂ & F₃ and Human Error E₁ have been identified through analysis of the change in question. The failures and errors have been linked to the potential baseline impacts to which they may contribute, as shown in Figure 8:

The Service Safety Requirement, The rate of occurrence of Threat T₂ shall be acceptable, is a requirement imposed on the rate of occurrence of a Threat. Therefore, Functional and Performance Safety Requirements are imposed to address each of the linked failures and errors:

- Failure F₁ shall occur no more frequently than Rate R₁;
- Failure F₂ shall occur no more frequently than Rate R₂;
- Failure F₃ shall not be a single point of failure leading to Threat T₂;
- Human Error E₁ shall trigger a system warning message.

The Service Safety Requirement, The Controls for Threat T₂ shall be sufficient in reducing the likelihood that the Threat causes Top Event A, is a requirement imposed on the sufficiency of a set of Controls due to a potential impact on the set’s parent Threat. Therefore, Functional and Performance Safety Requirements are imposed to ensure the effectiveness of the Controls:

- Control P₁ of Threat T₂ shall be maintained;
- Control P₂ shall be more effective in preventing Aspect X of Threat T₂ through…;
- Control P₃ of Threat T₂ shall remain independent of Controls P₁ & P₂.

Additionally, the Functional and Performance Safety Requirement specifying a new Control is imposed:

- Control P₄ shall be added to manage the occurrence of Threat T₂.

The Service Safety Requirement, The Controls for Consequence C₄ shall be sufficient in reducing the likelihood that Top Event A causes the Consequence, is a requirement imposed on the sufficiency of a set of Controls due to a potential impact on a Control within the set. Therefore, Functional and Performance Safety Requirements are imposed to ensure the effectiveness of the Controls and add additional Controls:

- Control R₁ of Consequence C₄ shall be actively monitored;
- Control R₂ shall be maintained;
- Control R₃ shall be maintained;
- Control R₄ shall be added to Consequence C₅;
- Control R₅ shall be added to Consequence C₅;

Additionally, Functional and Performance Safety Requirements are imposed to address each of the linked failures and errors:

- Failure F₁ shall occur no more frequently than Rate R₅;
- Failure F₁ shall be annunciated on the HMI.

In each of these cases, the decomposition would continue until the resultant set of Functional and
Performance Safety Requirements are considered sufficient to address each linked functional failure and human error and to ensure substantiation of the parent Service Safety Requirements.

5.4 Transition Safety Requirements

The process described so far has concentrated on the derivation and decomposition of Safety Requirements aimed at ensuring the system or service is acceptably safe under the applicable change, i.e. that the Service Safety Objectives are achieved. However, Transition Safety Requirements, at the service and then functional and performance levels, must also be derived and decomposed in order to ensure an acceptably safe transition, i.e. that the Service Safety Objectives are maintained during transition to the change.

This is achieved through the application of the same process, refocussed on the change transition. Operational Risk Baseline impacts must be re-examined to identify how these impacts may be potentially heightened during the transition, such as:

- Temporary exacerbation of a new Threat or further exacerbation of an existing Threat;
- Temporary further weakening, possibly to the point of full suppression, of an existing Control; or
- Temporary exacerbation of a new Consequence or further exacerbation of an existing Consequence.

These transition impacts are then used to derive the Service Transition Safety Requirements. Through identification and linking of the functional failures and human errors that can result in these additional impacts during transition, the Service Transition Safety Requirements can then be decomposed into a set of necessary and sufficient Functional and Performance Transition Safety Requirements through the process described above.

5.5 Satisfaction and Substantiation

The top-down process of derivation and decomposition of the objectives and requirements produces a logical flow of objectives and requirements (Figure 9) that can be satisfied and substantiated from the bottom-up.

Through the maintenance of necessity and sufficiency, the Functional and Performance Safety Requirements are the risk mitigation means by which the Service Safety Requirements are met and therefore the Service Safety Objectives are both achieved by the change and maintained during its transition. At this base level, satisfaction and substantiation of the specific and measurable requirements derived flows upward to demonstrate satisfaction of each Service Safety Requirement, which in turn flows up to demonstrate achievement and maintenance of each Service Safety Objective.

It is this demonstration of achievement and maintenance of the Service Safety Objectives that provides the basis for the argument that the service in question will remain acceptably safe during and under the applicable change.

![Figure 9: Logical Flow of Objectives & Requirements](image-url)

By using the Bowtie concept as the centre of the change management requirements definition process, qualitative and quantitative requirements can be established which relate specifically to the operational risk being managed. Depending upon the type of change and the in-service experience of the system, the focus for equipment, procedural, training or managerial requirements can be varied.

Focussing effort during the change on establishing the correct set of requirements and gaining agreement from all stakeholders on how to manage the operational risk is a value adding process, which is closer to managing operational safety than the development of a bespoke safety argument. Instead using this approach, the safety argument is embedded within the risk assessment.

6 Conclusions

6.1.1 Haddon-Cave’s Nimrod Review

The approach documented in this paper is aligned with Haddon-Cave’s Nimrod Review conclusions, in that during operations the focus should be on operational risk, rather than safety arguments. The concepts in this paper align to Haddon-Cave’s recommendation that “A paradigm shift is required away from the current verbose, voluminous and unwieldy collections of text, documents and GSN diagrams to Risk Cases which comprise succinct, focussed and meaningful hazard analysis which stimulate thought and action”.

Haddon-Cave’s indentified attributes for “Risk Cases” remain appropriate:

- Succinct;
- Home-grown;
- Accessible;
- Proportionate;
- Easy to understand; and
- Document-lite.

Operational Risk Assessments in the Bowtie notation provide a means of achieving this. As well as these attributes, we would also include “in-service experience based” and “timely” within the list.
Instead of Risk Case, the term Risk Assessment is more appropriate as it implies that some action needs to be taken. An Operational Risk Assessment is not a static item. Instead it changes, based upon the continual evaluation of the risk baseline, in line with the process documented in the Safety Management System.

6.1.2 Bowtie

In this paper, we have shown how maximum value of safety processes such as risk management, change management and incident investigation is achieved if they are effectively integrated. Further to this, we have provided an overview of how the Bowtie concept provides a strong basis for integration both internally within an organisation and cross-organisationally.

Safety Cases have their place and certainly argumentation is essential. However, when demonstrating a top level claim for a safety document (Safety Case / Operational Risk Assessment), it is important to remember the context in which decisions will be made based on the document. There is a difference between the one-off decision to commission and the ongoing judgement to continue operating.

We contend the Bowtie concept provides a good framework for establishing Operational Risk Assessments and, as previously discussed, can connect all elements of a Safety Management System together. We encourage using concepts such as Bowtie as a strong approach for integrating all safety processes. Changing the focus within safety processes from Safety Cases to Bowtie Risk Management will improve end-to-end safety management.

7 References
