Effective Safety Case Development in the RAN

Paul Barnes
BMT Design & Technology
pbarnes@bmtdt.com.au

Abstract
A Safety Case is required for all strategic materiel acquisitions made by the Defence Materiel Organisation (DMO) however the concept of reducing risk is problematic in the acquisition of any materiel system that is off-the-shelf. Without proper scoping and understanding of the purpose of a Safety Case in this context, an inordinate amount of effort can be expended in constructing arguments around a system that has already been committed to, that is not going to change and hence is already designed with appropriate consideration for risk. Throughout this paper, an approach to defining, bounding and executing an equipment Safety Case in the RAN acquisition environment is explored. The paper demonstrates that without a clear Safety Case framework in place, the Safety Case remains open ended, fails to add value to an acquisition program and, most importantly, it fails to achieve its primary purpose.

INTRODUCTION
A Safety Case is required for all strategic materiel acquisitions made by the Defence Materiel Organisation (DMO). The Safety Case argues that requirements of the regulatory authorities have been satisfied and risks associated with the system have been reduced to an acceptable level. The concept of reducing risk is however problematic in the acquisition of any materiel system that is acquired as an ‘off-the-shelf’ system, or if not off the shelf, something that is not new and has been done before albeit with a limited degree of tailoring. Without proper scoping and understanding of the purpose of a Safety Case in this context, an inordinate amount of effort can be expended in constructing arguments around a system that has already been committed to, that is not going to change and hence is already designed with appropriate consideration for risk. Throughout this paper, a measured and pragmatic approach to defining, bounding and executing a Safety Case as a materiel supplier and acquirer in the RAN acquisition environment will be explored. The approach will focus on ensuring those involved in the development and approval of a Safety Case have a clear understanding of why the Safety Case is being constructed and that unambiguous criteria upon which to make risk acceptance decisions have been agreed. As will be discussed further in this paper, the key factors in defining effective acceptability criteria are how well the risks are understood, whether or not the equipment has an already established practice and novelty of the technology.

This paper will briefly review the shortcomings of a well-known safety case and provide an overview of the regulatory framework driving the need for Safety Cases. It will discuss the importance of setting of risk acceptance criteria by considering industry best practice techniques for the development of efficient and effective Safety Cases.
SAFETY CASE REVIEW

A recent notable report is the inquiry into the Nimrod accident, where an XV230 Nimrod aircraft (Figure 1) suffered a catastrophic mid-air fire as a result of a fuel coupling leak and subsequent fuel pooling adjacent to high temperature duct, leading to the total loss of the aircraft and the death of all 14 personnel on board.

Prior to the loss, a retrospective Safety Case was conducted as required by MOD policy, which did not result in the specific cause being addressed.

The inquiry was sensational due to the scathing criticism of the team behind the Nimrod Safety Case and explicit naming of persons and organisations for criticism. Even though the Safety Case itself did not itself cause the fire, it was identified as the best (and subsequently wasted) opportunity to prevent the disaster.

![Figure 1 – Nimrod XV230 Aircraft](p7, D)

This review had the impact of raising the profile of ‘safety’ in the acquisition and operation of military equipment around the world; however its key message was not simply ‘do more safety’.

Although the disaster is related to legacy equipment, the report represents a great opportunity to reflect on and improve how we do business in acquisition.

The Nimrod investigation found the conduct of military Safety Cases to be ineffective and wasteful with claims such as:

- There is a bias towards Equipment risks, even though the greatest risk to life is operational;
- Documentation is of Byzantine complexity (no-one can really understand it);
- Military equipment Safety Cases have been modelled on major industrial installation Safety Cases however the scope and scale of the problem in military equipment is much more limited;
- A shift away from proper risk analysis has occurred with an ever-increasing reliance on a complex matrix and culture of process, paper, meetings, and ‘box-ticking’ as a substitute for sound thinking;
- False comfort is found in compliance and complexity;
- Regulations are too complex, prolix (wordy), and obscure; and
- The meaning of ALARP is not sufficiently understood.
Acknowledging the findings of Nimrod is important from not just a cost and schedule point of view, but from a view of ensuring effort is expended as a result of a well-defined need, with the aim of achieving the regulatory requirements which are required of us.

Simply put, an effective Safety Case can only be achieved with:

- An understanding of where Safety Case fits in to the overall capability lifecycle and regulations;
- An understanding of responsibility and accountability;
- A set of clear objectives (why it’s being done and what it’s trying to achieve);
- A well-defined scope; and
- Clearly defined risk acceptability criteria.

THE CAPABILITY LIFECYCLE AND NAVY REGULATION

The Safety Case is a Navy tool used as part of the Naval Regulatory System and is intended to apply across the capability lifecycle from concept through to disposal. Throughout this lifecycle, different regulators are responsible for defining the regulatory standards and codes which must be applied.

The acquisition of the equipment is one very small part of the lifecycle [Figure 2]. It should be noted that there is no mandated requirement for the equipment Safety Case to be a complex and infinitely detailed piece of work which aims to capture every aspect of through life safety, such as those applied to major industrial installations or activities [22.29, D]. It should be balanced with novelty and risk.

Whilst equipment designers manage the risks associated with the equipment they design (through their engineering processes), actual Safety Cases are generated by suppliers because they are mandated through the ASDEFCON template, with which significant defence acquisitions must adhere. Unlike the equipment Safety Case, the Navy Safety Case is required to address every stage of the capability lifecycle.

![Figure 2: Navy Safety Case](image)

THE REQUIREMENT FOR A SAFETY CASE

The need to conduct a Safety Case is usually driven by regulators who are implementing legislative requirements (to conduct a Safety Case), in order to satisfy their responsibilities and accountabilities. Review of legislation in other industries provides some useful context as to why Safety Cases are completed, as well as how the self-regulation applied within Navy fits into this picture.

Legislation in Wider Industry

Commonwealth occupational safety law only extends the requirement to conduct a Safety Case to Major Hazard Facilities (MHF), where an MHF is a facility which stores threshold quantities of prescribed chemicals (in other words oil refineries, chemical plants and large fuel and chemical storage sites where large quantities of hazardous materials are stored, handled or processed) [B]. The Safety Case in this instance is only required to address the management of major incidents which
relate to endangering people as a result of spills or ignition of the prescribed chemicals. In the Offshore Oil industry, a Safety Case is also required [K] however the Safety Case only addresses accidents with the potential to cause multiple fatalities of persons at or near the facility, and covers both the facility design and its operation through life.

For example, in instances where the Safety Case is mandated as the primary method of managing risks, a safety performance goal is set in legislation, allowing the operator to determine the most appropriate methods for the control of risk. This allows the operator to tell the regulator why the facility is safe, and what codes and standards will be used to achieve this purpose [A].

The regulator accepts the Safety Case and it becomes the basis for safety compliance in the absence of an industry-wide prescriptive regime.

On the balance of evidence across the industry, goal setting and management system-based safety regimes, supported by the Safety Case, are seen as the most appropriate means of preventing accidents at Major Hazard Facilities [E].

**Legislation in the civil maritime community**

From the Australian commercial shipping point of view, the Work Health and Safety Act does not apply and instead the industry is regulated through either the Occupational Health and Safety (Maritime Industry) Act 1993 [12A, H] and the Navigation Act 2013. These acts are regulated by AMSA, where prescriptive, maritime-specific rules for maritime safety must be complied with. Compliance with recognised rules, such as SOLAS, implies acceptable risk [M] with respect to the context in which they are intended to be applied and are not goal based standards.

For clarity, the International Maritime Organisation (IMO) have implemented goal based standards for oil tankers and bulk carriers which will come into effect in 2016 however these are not intended for use by the general maritime community. The intent is that the goals must be derived into rules by the Classification Societies, to be subsequently applied as prescriptive rules by the designer [C].

**Legislation in Defence**

Without delving too far into the legislative side of safety in Defence, the RAN are only subject to the generic (i.e. non-maritime) Work Health and Safety legislation.

From a materiel acquisition point of view, the Navy Technical Regulatory Authority (TRA), who is responsible for regulating Design, Construction and Maintenance, recognises the fact that there is no direct legal obligation to comply with proscriptive maritime safety rules such as SOLAS and as such operates a regulation regime called the Naval Technical Regulatory System (NTRS) [I].

The TRA identifies regulatory and materiel requirements using a risk based approach, which reflect international, civil and military practice and the requirements of the Royal Australian Navy (RAN). These requirements must then be satisfied by the organisation designing or supplying the equipment.

In this instance, prescriptive requirements are mandated by a Technical Regulator, however an equipment Safety Case is also required by ASDEFCON. As such, the objective of the equipment Safety Case appears to be a general assurance activity which overlays the prescriptive regulatory activity, validating the pre-determined technical regulatory requirements, identifying any gaps in these requirements, and a reinforcement of the general engineering practice of considering risk in any design decision.
SAFETY CASE SCOPE
The scope of the equipment Safety Case is limited to the equipment being supplied and the issue is simply: “Is this piece of equipment safe to operate?” [22.29, D].

There is only so much that can be done with respect to risk at the equipment level in the context of the capability lifecycle, which includes in-service operation.

As Haddon Cave found, far too much focus is placed on the equipment whilst, as is the case with aircraft [19.10, D], the highest Risk to Life is likely to be Operational and hence, not necessarily the suppliers problem.

In addition, the effectiveness of a Safety Case for equipment (or technologies) whose requirements are already largely set and agreed by the Technical Regulatory Authority is extremely limited. This is generally reinforced in Mortimer’s Defence Procurement and Sustainment Review [Q] where it is claimed that off-the-shelf procurement involves less risk as a result of relying on mature solutions based on well-developed and understood technologies.

Figure 3, whilst focussing on the potential cost, schedule and risk implications of moving away from Off-The-Shelf technologies, illustrates how little scope there is for any influence on the set requirements basis of an existing technology (“OTS requirements”).

![Figure 3 - impact on cost, schedule and risk of volume of requirements](image)

**RISK ACCEPTABILITY CRITERIA**
The argument regarding risk is often driven by widely differing risk perceptions amongst stakeholders. In research regarding public perception of risks (such as nuclear power), risk perceptions were found to be often subjective and emotional where the fears often do not match the facts [R].

5 of 10
The introduction of legislative terms such as As Low As is Reasonably Practicable (ALARP) into day-to-day activities does not help either, as these terms introduce ambiguity.

Regardless of the acronyms SFARP, ALARP, SFAIRP or any permutation of those, we need to understand the criteria on which we are going to accept risk.

If we require lawyers to interpret terms such as ALARP, then the underlying safety activity is flawed and not intuitive. We should be able to fulfil our obligations by relying on the regulatory expertise and experience by complying with Naval regulatory requirements, and recognising wider industry practices.

Although a common misconception, conducting a Safety Case and arguing ALARP does not mean we have to continually raise standards and implement the highest standards of risk control just because someone else has, nor should we be insisting on all perceivable risk controls (one on top of the other) [F].

Acceptance of risk needs to be based on sound judgement and knowledge against clear criteria; and as explained in the Nimrod report [19.27, D] practices based on process, paper and form filling are counterproductive.

Setting Criteria

In order to argue that the risk associated with a piece of equipment has been reduced ALARP, we do not need to dissect every element of the system and conduct endless hazard identification workshops to ensure we have implemented every materiel control possible, nor do we need to justify why we have not implemented another layer of controls, through a cost-benefit exercise.

The Safety Case should be completed within a clear framework comprising a thorough understanding of why it is being done, as well as clear criteria on which risk is accepted. If the acceptance criteria can be set, in a simple qualitative form, this type of activity can be avoided to an extent that risk is considered acceptable because we understand it and know how to deal with it; not because we have made it acceptable by generating a ream of paper in its regard.

Where relevant good practice is a fit to the particular circumstances then decisions (such as a design decisions or specific risk control) on risk reduction action are straightforward [L] and good practice is very likely to be good enough. Risk does not have to be imagined or created nor analysed to death; it has to be understood and dealt with pragmatically. The risk should be accepted as being managed (either formally or informally) and put to rest, or if deemed unacceptable, recorded as a potential issue for design change.

The majority of work in the RAN environment is likely to sit within good practice criteria, as equipment from platform systems to weapon systems are not novel and are often developed and deployed by other countries and used in service prior to being integrated onto RAN platforms. The scope to influence the design and risk is often extremely limited and any reason to do so is often subjective.

Regardless of this, the good practice argument may however require further work where [J];

- Established good practice does not exist;
- Is out of date;
- The situation is complex; or
The relevance of individual good practice is agreed as being questionable.

Using a decision framework
A method for assisting in making decisions regarding risk was proposed by the UK Offshore Operators Association and used by the Australian National Offshore Petroleum Safety and Environmental Management Authority [Figure 4]. It represents a pragmatic interpretation regarding handling of risks where decisions are categorised into three discrete levels (A, B and C).

![Figure 4: Risk Related Decision Support Framework](G)

In a nutshell, this framework asks the question ‘are the risks we are dealing with something very novel or are they nothing new’. For risks which are nothing new, Codes and Standards are directly relevant to the decision making process however very novel situations are driven by the values of society (for example, what fatality rate is considered acceptable given the benefit of a particular industrial activity to society).

Important aspects to note in the application of the framework are its focus on:

- How well risk is understood and not how ‘risky’ it is or is not perceived to be;
- Whether or not the activity is already an established practice; and
- How new or unusual (or novel) the technology is.

Novelty is not necessarily dictated by the particular knowledge of those people involved in a project, and should encompass what has actually been done in the world that we live in. Something may be operationally novel to a particular user group however that does not mean the equipment itself is novel. Novelty to a particular user group or organisation will drive additional effort however not necessarily in the equipment domain.
The concept of the risk-decision framework would assist any RAN acquisition and should be applied from first pass through to delivery, the focus of which should be across the capability and all of its regulatory domains. Understanding where the real risk areas are and what techniques and rules will be used to manage these risks is fundamental to managing schedule, budget and focus of everyone involved and will still provide the necessary safety assurance aligned to the real risk.

**ALTERNATE MEANS OF DEFINING ACCEPTABILITY CRITERIA**

Quantitative Acceptability Criteria provides an alternative means upon which to make risk-decisions. Although this type of criteria (and the associated analysis) is unlikely to be set and used at the acquisition level within the RAN, its application within the wider maritime community has been investigated in order to determine its applicability to the RAN regulatory environment.

**Arguing outside of, or against good practice**

If a particular risk is perceived as falling outside of the intolerable and broadly acceptable regions, and good practice cannot be identified, a more complex determination may have to be made to determine whether or not the risk is acceptable. A Cost Benefit Analysis (CBA) may assist in this determination and could be used to compare risk reduction options that are on the table where the CBA could range from a simple calculation through to a detailed analysis [L].

In conducting a CBA, the acceptable risk (and hence acceptability criteria) will need to be defined and could be based on [M]:

- comparison hazards in other industries where good data and documentation is maintained;
- comparison with natural hazards;
- comparison with risks we normally take in day-to-day life; and
- comparison with previous decisions such as those made in codes and standards.

Given the potential complexity of such an approach, this type of risk reduction activity would be most effective as a long term investment by the RAN, with the aim of continual improvement of safety, cost and schedule where regulatory rules are continually improved and made relevant to the naval application. Scope for this type of continual improvement is very limited or not practical if it is asked of individual acquisition programs or individual suppliers. The Naval Ship Code (ANEP-77) may provide a similar forum that the civil maritime domain employs where the required critical mass of naval data and experience to perform and implement these assessments can be achieved – this code has already derived into safety related Rules and Regulations for Naval Ships by Classification Societies such as Lloyds Register [S].

In civil maritime, CBA is conducted through programs such as the European Union funded SAFEDOR [N], where Formal Safety Assessments based on complex models and industry data are used to challenge IMO rules to effect change on the basis of monetary benefit, and relate both to the addition and removal of safety features from the rules. These assessments are not completed against individual vessels, and are applied broadly across the maritime domain to drive both cost and risk reduction.

**Formal Safety Assessment**

The conduct of formal hazard assessment is not feasible at the level that the majority of acquisitions occur within the RAN environment, and leverage must be made of the work that has already occurred within the maritime space.
Whilst Formal Safety Assessment (FSA) is not the primary method used by IMO to make rule changes and is historically uncommon [M], IMO FSA’s are completed by large teams of experts from various flag state members, often including multiple organisations and universities [N]. These FSA’s are then submitted to IMO for committee review and potential implementation, and are a technique which can be used to drive improvement and complement reactionary measures such as learning from disasters.

Classification Societies inherently leverage these changes as part of their Naval Ship Rules, which make appropriate references to conventions such as SOLAS to achieve ANEP-77 objectives.

IMO FSA considers the Gross and Net Cost of Averting a Fatality (GCAF and NCAF respectively), and compares that with a pre-determined cost which society is willing to pay to avert that fatality. NCAF differs in that it considers the economic benefit as well as the cost of implementing the control whilst GCAF only considers the cost of the control itself.

A complex model with specific route and vessel scenarios is developed using statistical data in order to calculate the likelihood of a fatality both with and without the proposed control in place.

**FSA Examples**
Notable FSAs are those which drove change regarding helicopter spots on passenger ships and the use of an Electronic Chart Display and Information System (ECDIS).

- **Helicopter Landing Spots [P]**
  - Following an IMO ruling to require a helicopter landing area on all passenger ships to assist in passenger evacuation, an FSA was conducted and submitted to IMO for consideration which found the cost of averting a fatality using this methodology ranged between $12 million and $73 billion dollars for the specific case studies assessed; far in excess of what society is willing to pay, resulting in the rule being repealed by IMO.

- **ECDIS [O]**
  - An FSA was conducted which found that mandatory installation of ECDIS will reduce grounding collisions and grounding related fatalities by a third; and whilst not considered feasible from a life-saving perspective alone (GCAF), the economic benefits (NCAF) associated with avoiding grounding (environmental and property damage costs), exceeded the cost of implementation and was hence enacted by IMO.

**CONCLUSION**
The Safety Case without a defined purpose, scope or risk acceptance criteria is an open ended activity which does not assist in managing risk and as such does not add value to the acquisition process. The ability for a designer or supplier to the RAN to conduct detailed analysis is limited, often unfounded and is not required by law.

Placing the Safety Case in context and reflecting on the practices of industry in a pragmatic and common sense approach can assist in achieving targeted effort and successful Safety Case delivery, through the application of the systematic techniques such as the risk decision framework.

Continuous improvement of safety with respect to specific Naval applications and detailed analysis of available data should be vigorously pursued by the RAN however the most effective forum for this is not considered to be within an acquisition program.
REFERENCES
A. National Offshore Petroleum Safety Authority "Prescription and Standards", CP-08/2010
C. Gary Horn “IMO Goal-Based Ship Construction Standards”, INTERTANKO Latin American Panel, Lima Peru, September 2010
D. Charles Haddon-Cave QC, The Nimrod Review
I. Royal Australian Navy “Naval Technical Regulatory System”, ABR6492
J. Health & Safety Executive, “Reducing Risks, Protecting People”, 2001
N. European Union, “SAFEDOR' completes four years of research on safe and innovative ship design, operation and regulation” http://ec.europa.eu/research/transport/projects/items/_safedor__completes_four_years_of_research_on_safe_and_innovative_ship_design__operation_and_regulation_en.htm
P. DNV, Formal Safety Assessment Helicopter Landing Area On Cruise Ships, 97-2053
Q. David Mortimer AO, Going to the Next Level, the report of the Defence Procurement and Sustainment Review”, 2008
R. David Ropeik “How Risky Is It, Really? Why Our Fears Don’t Always Match the Facts”