PUTTING THE SAFETY CASE TO WORK

BY

PETER BROOKES

ABSTRACT

The purpose of this paper is to describe the development of a retrospective safety case for complex vessels in a challenging environment. The fact that the vessels in question are nuclear powered submarines is incidental to this purpose. We shall be dealing with the safety case for the submarine 'platform'; that is, all aspects of the vessel except its nuclear propulsion and weapons, which have their own highly developed safety cases.

Introduction

When the decision was taken to create retrospective safety cases for vessels up to 30 years old, one of the major requirements was that the safety case must be of as much practical use as possible. It was not acceptable to use resources merely to get a 'tick in the box' and fill a cupboard full of safety case reports.

While the safety case is still very much a work in progress, the results so far suggest that we have been able to make the safety case into a valuable resource for many different users.

Background to the submarine safety Case

Submarine Support Organisation

The Royal Navy has 14 nuclear powered submarines in service and a further 3 Astute Class submarines are being built. Engineering support for the in-service submarines is provided by the Ministry of Defence's Submarine Support Integrated Project Team (SUBIPT). The SUBIPT has placed a single major contract for assistance with many aspects of its support task. Since its inception in 1998 this contract has been held by the Submarine Support Management Group (SSMG), which is a team of three companies: Devonport Management Limited (DML), BMT Defence Services Limited, and SEA Limited. The team is led by DML.

The introduction of the Astute Class is the responsibility of the MOD Attack Submarine IPT. This class will have a safety case to meet all modern standards and its development has been an integral part of the design and build process. However, there is no direct linkage between this and the retrospective safety case for in-service submarines being developed by SUBIPT and SSMG.

In-Service Submarines

Current Royal Navy submarines are of three classes; Swiftsure, Trafalgar, and Vanguard. The ten Swiftsure and Trafalgar Class are 'hunter-killer' submarines designed primarily to engage other submarines, the four vessels of the Vanguard Class carry the nation's Trident nuclear deterrent. The oldest submarine in service, HMS Sovereign was commissioned some 32 years ago and the youngest, HMS Vengeance, has been at sea for over 7 years. The long gestation period for submarines means that even the Vanguard Class design goes back to the early 1980s.

Arguably, a nuclear powered submarine is one of the most complex and diverse objects built. It comprises a wide range of functions and technologies, all packed into a steel tube about 30 feet in diameter and 200 feet long. The main issues involved include:

- Propulsion – in addition to the nuclear reactor which provides the power source there is a full set of steam propulsion machinery (rapidly becoming the only remaining example of steam power at sea). This requires an electrical generation and distribution system sufficient for a small town including one of the largest electric batteries produced.

- Underwater operation – The submarine must have the structural strength to survive at great depths. It must also be able to adjust its bodily weight to dive and surface and it must be able to steer, both vertically and horizontally. Amongst other services this requires large volumes of high pressure air to provide buoyancy and powerful hydraulic systems to operate the control surfaces.

- In addition to surviving in its environment the submarine must be able to function as a warship. Its combat systems must be able to detect and track other ships and submarines. To engage the enemy requires weapons and this, in turn, requires large quantities of explosives in torpedoes and missiles to be stored within the submarine hull. The submarine must be able to navigate precisely and remain in communication with its base whilst at depth. To achieve all this requires the most modern technology if we are to have an advantage over any potential opposition.

- The submarine is also a place where people live. It must provide a safe environment for up to 120 human beings to breathe, eat, work and sleep beneath the surface of the sea for several months without a break.

A final, and less obvious, complexity is that of the organisational structure within which the modern submarine operates. It involves many different agencies, companies and military commands to design, build, repair, support, and supply the vessels and to provide and train their crews. As we are reminded all too often, in the modern world the organisation has as great an influence on safety as do the engineering and the materiel.

Risk

From the previous section it will be clear that the operation of submarines involves risk. One of the oldest and simplest statements of this is known as the Submarine Equation – that over the life of the submarine the number of times it surfaces should be equal to the number of times it dives. The submarine safety case must address these functional safety risks but in addition it must cover other some other aspects as well.

The health and safety at work issues of cramming large amounts of machinery and stored energy into a very small space should not be underestimated, particularly when that workplace can roll, dive and climb unexpectedly.

Long term health effects on the ship's company have been a concern since the 1960s when submarines were first able to operate completely out of contact with the atmosphere for long periods. The restrictions on carrying toxic substances on board (or incorporating them into equipment) have to be stringent since some effects may not become apparent for many years.

Finally there is the question of military risk. A warship is designed to go into hazardous situations and get shot at. There is a continuing debate as to what extent this is treated through safety management processes and to what extent design for vulnerability and survivability lie outside the conventional safety case.

What is the Retrospective safety case?

The Royal Navy has a long history of submarine safety management. The first RN submarine was introduced in 1900 and since HMS Dreadnought went to sea in 1963 we have built up nearly 600 boat-years of nuclear submarine operating experience. Submarine safety relied largely on deterministic analysis, robust design, quality control, skilled and experienced people, and (in some cases bitter) experience.

In the early 1990s the Ministry of Defence introduced a risk based approach to safety management at a time when the old concepts of Crown Immunity were coming to an end. Today MOD policy requires safety standards to be at least as good as those required by statute. For ships and submarines this approach was enshrined in Joint Service Publication 430, the MOD Ship Safety Management Policy. One of the key requirements of the JSP was that all vessels should have a safety case. Deadlines were set by the Ship Safety Board for this to be achieved.

The need for a safety case for in-service submarines was established, but what would it consist of? The new Astute Class design was developing a state of the art modern safety case which was able to influence design down to component level. It was clear that the same approach was not appropriate for in-service submarines where the design was often many years old and hard to change in practice, but had been proven by many years of operational experience.

It was also recognised that the safety case would be expensive in a time of scarce resources. A key requirement at the outset of the project was that the safety case must be useful to as wide a range of project stakeholders as possible.

The approach taken was to construct a multi-legged safety case that would take credit for all those processes that have assured submarine safety for so many years

and would build in new concepts as they develop. Fitting these to a Claims – Arguments – Evidence structure would enable the strengths and weaknesses of current practice to be analysed and form the justification for additional work.

The first step was to understand the basic Claims – Arguments - Evidence structure, starting with the fundamental question "What are we claiming to achieve?"

The initial scoping study, carried out by SPMJ Consultants, looked at just what a submarine safety case should comprise. The results are summarised by a simple but important diagram (FIG.1).

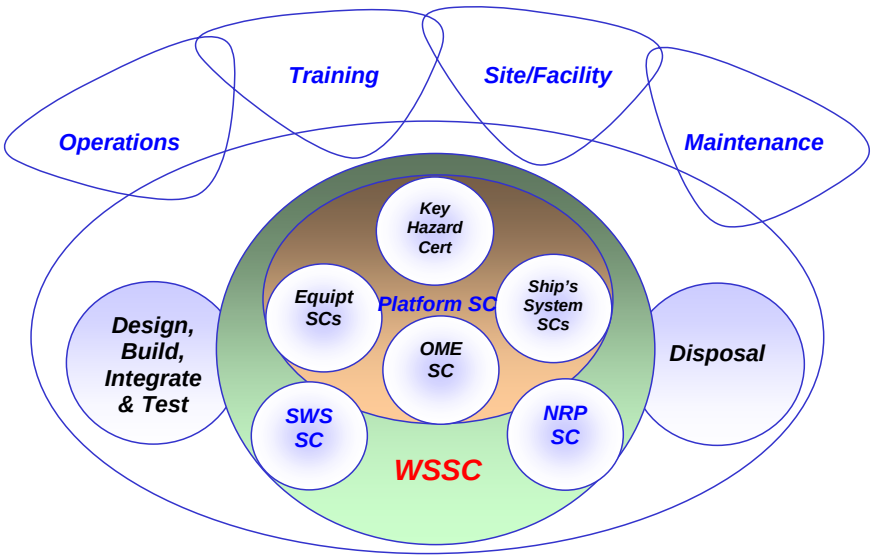

FIG.1 - WHOLE SUBMARINE SAFETY CASE CONTEXT

In the Platform section of the overall safety case the main elements would be:

- The management of the Key Hazards[1]: Structural Strength, Stability, Watertight Integrity, Fire Safety, Manoeuvring and Control, Propulsion, Atmosphere Control, and Explosives;
- The management of other hazards including personnel health, safety and environment issues;
- Regular certification of the submarine as fit for service for a further period;
- The hazard log and active management of new and existing hazards;
- An effective and well developed safety management system.

Presenting the safety case

With the size of the safety case and the number of organisations involved it was recognised early on that a soft copy safety case would be desirable. SSMG chose the ASCE (Assurance and Safety Case Environment) tool created by Adelard for the task.

A key feature of ASCE is its ability to show a graphical representation of the Claims, Arguments and Evidence structure of the safety case. This was central to our first task of identifying exactly what the structure of claims in our safety case was to be. (FIG.2) shows the claims structure taken from a notional version of a vessel safety case.

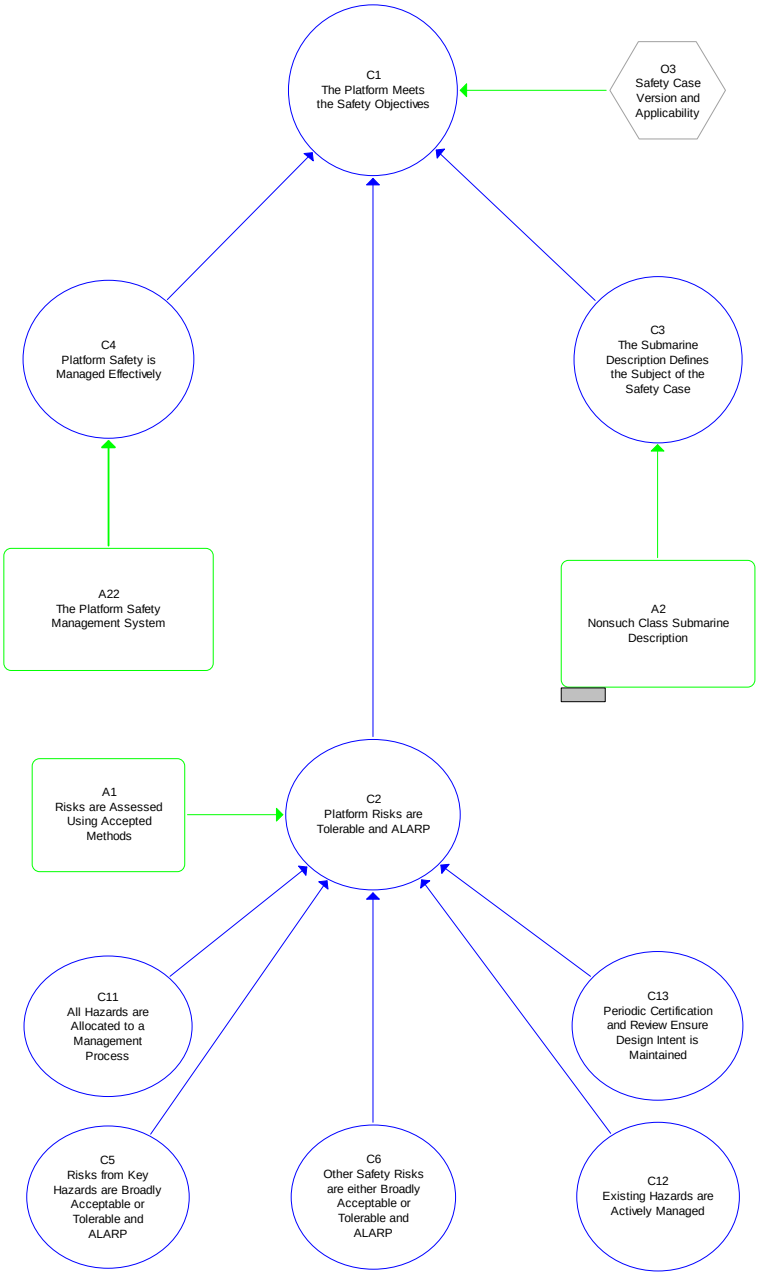

FIG.2 - TOP LEVEL STRUCTURE OF THE SAFETY CASE

Having identified the claims other ASCE 'nodes' were added to build up the structure of the supporting arguments and evidence. ASCE allows the text to be contained within the node. With linkage between the nodes it is possible to follow a particular line of argument though the network. (FIG.3) shows an example of a node contents for a major safety case claim.

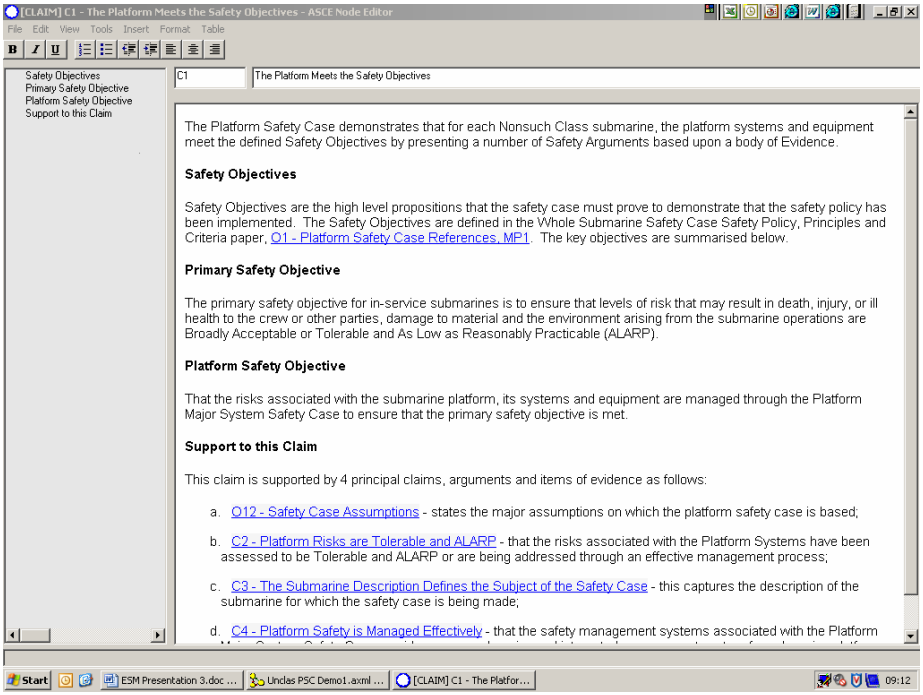

FIG.3 - EXAMPLE OF A SAFETY CASE NODE TEXT

After much thought and analysis we arrived at an ASCE model describing the structure of our whole safety case as a hierarchy enabling a simple graphical display.

Managing the evidence

Evidence to support the submarine safety case comes from many sources. With vessels over 25 years old, much original information has become 'lost'; not in the sense that it does not exist but that, being stored by many organisations, on many sites, and in many formats, no one person knows where it is all to be found. Gathering together the significant evidence in a way that would make it visible to all users was seen as one of the great advantages of the safety case. To help achieve this we were able to use the features of ASCE to exploit the Ministry of Defence's extensive Wide Area Network (known as RLI) and SSMG's electronic Library Document Management System (LDMS).

The submarine safety case divides evidence into three types:

- Major documents that are central to the safety case. Most of these are produced by the SUBIPT or their contractors. Master copies are held in the

SSMG LDMS and are hyperlinked to the safety case in ASCE. In this way we can be certain that a reference will always be at the correct issue state for the safety case version in use.

- Documents owned by other organisations and available across the RLI can also be hyperlinked to the safety case. This gives access to an enormous range of reference material, but it does have the disadvantage that we cannot control the issue state of the document being viewed.

- Lastly the safety case also calls upon conventional paper document references, either because of their security classification or because they are too bulky to be worth scanning into LDMS.

Obviously there is a significant overhead to maintain all these references up to date but, provided it is done regularly and consistently this is more than balanced by the value of having immediate access to so much relevant information.

Generating reports

One of the great revelations of creating an electronic safety case was the way that it exposed the difference between the safety case and the safety case report. In the past it has been easy to confuse the paper safety case report with the whole of the safety case, not least because access to the safety case documents themselves was often limited to a few safety engineers.

With an electronic safety case it is possible to make the full safety case available to anyone with a PC and a network connection. Very powerful tool as this is, at first it obscured the importance of producing safety case reports that analyse all or part of the safety case at a point in time. There is a temptation to give the Duty Holder or user the entire safety case and expect him to pick the items of interest. In fact the ASCE system allows us to make any number of different selections from the safety case contents to address different requirements. These can include a class-wide overview of safety, an analysis of the status of a particular vessel, or a brief for the submarine's Commanding Officer.

Because the safety case itself is kept up to date continuously in electronic form it is possible to produce reports whose information may be only a few days old.

However, despite the many advantages of electronic documents, it is a fact that when presented with a safety case report for review most users (and particularly senior managers) prefer a paper version. "Give me something I can read on the train". SUBIPT and SSMG have developed the export functions of the safety case tool to produce tailor-made MS Word documents in the SUBIPT's standard format. We have been able to reduce the time it takes from pressing the button for a Word export to having a fully formatted document ready for review down to a few hours.

Putting the safety case to work

Safety cases for new projects have a clear goal in mind – achieving acceptance. Once the equipment is in service there is a danger that the safety case report will

be little used between infrequent reviews. At the beginning of our safety case development we set a goal that it should be useful – so what has been achieved?

- Has the safety case process found dramatic new hazards that no one had thought of before? No, but it has raised the standard of hazard management, together with the introduction of a web based hazard log tool. Formal hazard management is now established as a routine activity in the SUBIPT and the results are regularly published to the submarine community through the safety case reports.

- The safety case has identified areas of the management system that need to be formalised. Arguably for legacy vessels it is the management system, its ability to find and resolve emerging safety issues, that is the most important part of the safety case. The process of formally recording the management systems of the many organisations involved leads to greater clarity and the ability to challenge interfaces and assumptions. Additionally the safety case provides the auditor with a clear view of what is being claimed and helps him to assess whether it is being delivered.

- The safety case enables users to understand the relationships between safety processes. The graphical presentation helps users to follow the 'legs' of the safety case and to trace the development of an argument. It is possible to show how one set of evidence (for example a group of equipment safety cases) can support several areas of the safety case. It can also allow an engineer who is assessing the significance of a request to deviate from a design requirement to establish quickly the safety functions and performance required from the equipment.

- The safety case has created a powerful reference library that is available to anyone on the Ministry's RLI. This has great potential to provide an essential information service for a complex group of interrelated organisations where historically much knowledge has been held in a very compartmentalised way.

- Above all the ability to make the live safety case visible at the user's desktop creates a very powerful common resource across the user community.

Conclusion

The development of submarine platform safety cases is still at an early stage but already much has been done. The first versions of the safety case have been accepted by the responsible authorities, yet this should be seen not as crossing the finishing line but as the first of a number of steps that will enable the safety case to become a useful resource for all those involved in the operation and support of submarines.

Although we have not been able to produce a safety justification of all the design details integrated to the whole submarine level (as will be done for the Astute Class) we believe that we have achieved:

- A clear understanding of the claims and arguments;

- A set of priorities for further work to develop the safety case;
- The ability to publish reports targeted at particular user groups;
- Easy access to the safety case evidence;
- A means of making the whole safety case visible to those who can benefit from it as an on-line resource.

References

1. The concept of Key Hazard Certification, introduced by JSP430, applies an independently regulated approach to those 'Key Hazard Areas' of a vessel that represent a significant danger to the lives of several people, loss or severe damage to the platform, or significant damage to the environment.