Engineering Safety Assurance for Concept Level Submarine Design

R Hemsley* MSc CEng MIMechE

* *BMT, UK*
* Corresponding Author. Email: Richard.Hemsley@bmtglobal.com

Synopsis

In modern surface warship concept development it would be inconceivable to engineer the concept without safety in mind however, to assess the level of safety provided, it is often necessary to mature the design to a fairly advanced stage. Should the level of safety be found to be lacking, any resulting design changes are likely to be extremely disruptive and expensive. This is, in part, why Class Rules exist: to avoid the most fundamental safety concerns of basic designs.

If we then shift focus from surface vessel design to submarines, where the design complexity is an order of magnitude higher and safety requirements are paramount, the impact of a design not meeting safety objectives could be prohibitive and the challenges of operating safely underwater in a three-dimensional domain would mean most surface vessel Class Rules are inappropriate with few submarine-specific notations available. As a result, the customer and designer alike have a vested interest in ensuring the design is working towards, and following, the right safety objectives from as early a stage as possible.

To date early concept design safety assessment has largely been attempted by utilising Fault Tree/Reliability Block Diagram analysis to provide a quantitative assessment of safety. This method is entirely reliant on the accuracy of the core reliability data, using either known part data (thereby limiting innovation) or generalised data from sources such as the Non-electronic Parts Reliability Data (NPRD) where context is lost.

The Naval Submarine Code (NSubC or NATO document ANEP-102) has been developed by the International Naval Safety Association (INSA) to provide a goal-based framework that enables naval submarines to be certified within a navy's safety management system as safe to operate. Effectively providing a high-level safety element of Class Rules.

This paper will discuss an approach, developed by BMT, to employ the NSubC as a base to evaluate concept design engineering safety and put it into the context of key safety events. This has established a process that allows continuous evaluation that matches the expected design maturity and can mature with it.

Keywords: Safety; Submarine; Goal-based; Concept; Safety systems

1. Introduction

In modern naval vessel design there is an increased focus on non-warfighting operations and the focus that brings. While military capability is still critical the wellbeing of the crew in peacetime, which constitutes the majority of the vessels active life, has a significant influence on the design. As a result Safety Engineering has become an essential part of the design journey that no country's procurement agent could afford to ignore However safety engineering is an involved process that requires an understanding of how a system or equipment will operate, and the scenarios it will operate in, to fully address. To ease the burden and allow many key issues to be mitigated in advance, surface ships are largely designed and built to Class Society Rules (e.g. Lloyd's) that lay down rules to be followed for systems and equipment, to provide assurance of a minimum level of safety. These naval rules currently apply to surface ships and submersibles, but the majority do not apply to naval submarines. Applying a prescriptive rules-based assurance system to submarines, with the inherent secrecy associated with each nation's Concept of Operations (ConOps), has had limited application to this point.

This paper explains an approach taken by the author and supporting team to evaluate the Engineering Safety of an early concept submarine design, employing a goal-based designation as criterion or guiding principles. The purpose was to provide early stakeholder assurance that the design follows or approaches good practice, or identify areas where further scrutiny and development may be required.

Naval submarines are incredibly complex vessels, forming not only a weapons platform, but a manoeuvring platform in 3-dimensional space (as opposed to the 2-dimensional space a surface ship operates), a home, a canteen, engine room, workshop, exercise space and an enclosed biosphere for patrol duration. Figure 1 is an example of modern submarine design and the many unique challenges a submarine design needs to address.

Author's Biography

Richard Hemsley is a Principal Engineer at BMT in Bath, UK. A Chartered Engineer, he has a background in Mechanical Engineering and has over 20 years' experience in the submarine and surface ship domains from early design, to development, and in-service support to UK and other navies.

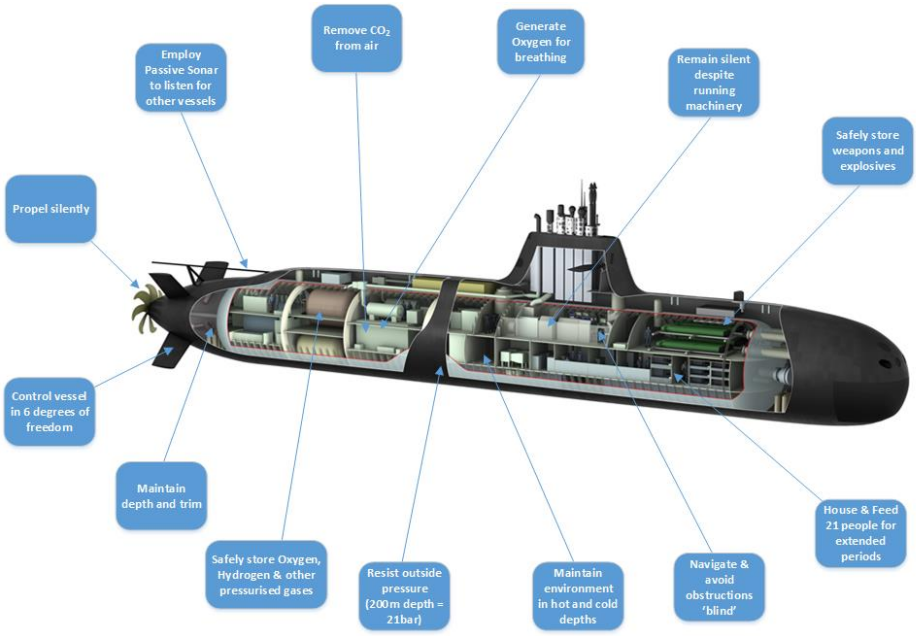

Figure 1 – The Unique Submarine Challenges (BMT)

Addressing these challenges requires an understanding of the systems involved: a submarine will operate in high pressure environments (e.g. 200m depth = 21bar), while finding its way via inertial navigation for much of its time, immersed in seawater of varying temperature and salinity, employing several potential methods of propulsion (conventional (SSK) submarines), while conducting potentially dangerous missions for weeks, or up to months away from base. To give a better sense of complexity and scale, Figure 2illustrates the number of systems, suppliers, parts, effort, time and cost involved in design and building a submarine in comparison to a Main Battle Tank, a Modern Airliner and a Frigate. From this figure it is clear to see that clear to see that designing and building a submarine is a massive undertaking and important to get right from the early stages to avoid design shortcomings or re-work at a later stage.

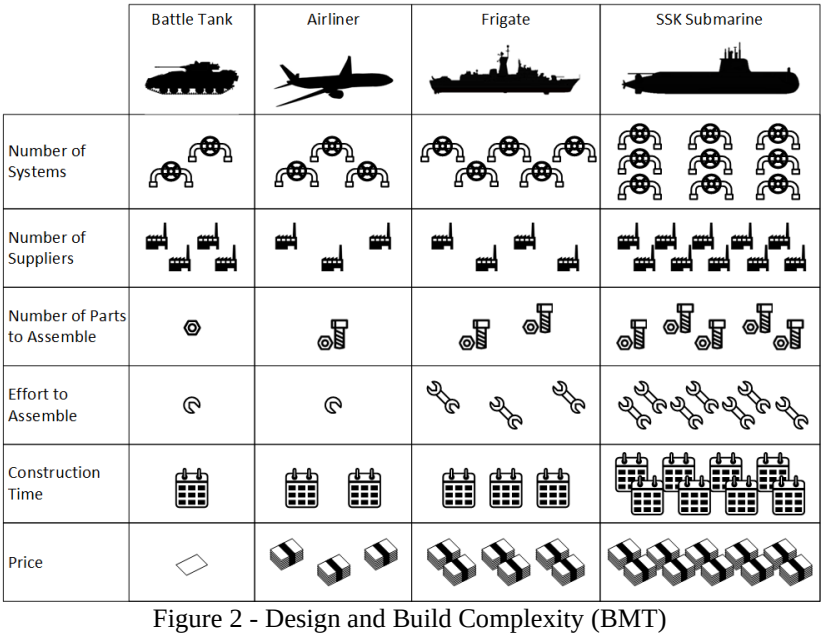

Figure 2 - Design and Build Complexity (BMT)

Among the highest priorities in submarine design is the design's safety. While they are designed for military operations, which carry their own risks, for the majority of their service life most submarines will be operating in peacetime. These submarines can carry complements from 18 to 160 persons and form a home for the crew, providing protection from not only external elements and the heat/cold of the external sea, but also from the hazards inherent in the internal systems to operate the submarine and generate/preserve the environment onboard.

2. Safety in the Submarine Context

What is Safety? Safety is the inherent property of a component, system or the platform as a whole to be safe and to support safe operation. In the unforgiving underwater environment this becomes critical to the survival of the crew and vessel itself when the following key submarine events are considered:

a) **Fire & Damage Control** - Fire in the enclosed environment of a submarine can kill within a short space of time and any fumes produced will continue to circulate within the atmosphere until the submarine ventilates. Additionally any water used to fight a fire will shift the centre of gravity and buoyancy of the submarine potentially unbalancing it. Examples of incidents of fire aboard submarines are HMCS Chicoutimi (Canada) in 2004, Daniil Moskovsky (Russia) in 2006 and K-150 Tomsk (Russia) in 2013;

b) **Management of Explosives** - It must be remembered that a submarine is an instrument of war and as such, will regularly carry weapons and other items with potentially explosive and dangerous consequences. While this must be an tolerated risk to deliver Capability, it is important to minimise and mitigate the risk to personnel and the platform. Examples of explosive incidents are USS Scorpion (United States) in 1968, Kursk (Russia) in 2000 and INS Sindhurakshak (India) in 2013 (following a fire event);

c) **Power and Propel** - Electrical power is the lifeblood of a naval vessel, this becomes increasingly important for a submarine when it is understood that it powers the systems that navigate the submarine, likely turns the propellor, heat, cool and ventilate the submarine as well as generate water, Oxygen and remove Carbon Dioxide from the air among a multitude of other control and support functions. An example of an incident involving propulsion was the K-11 Project 627A (Soviet Union) in 1970;

d) **Sustainment of Life** - This encompasses: providing a safe working environment for crew including maintaining temperature and humidity, controlling contaminants, providing safe food and drink, controlling waste and providing escape, rescue and abandonment facilities. Examples of incidents involving sustainment of life and escape are K-278 Komsomolets (Soviet Union) in 1989, Ming 361 (People's Republic of China) in 2003, HMS TIRELESS (United Kingdom) in 2007 and K-152 Nerpa (Russia) in 2008;

e) **Vehicle Control**[1] - Controlling the submarine in 3 dimensions requires control of buoyancy, weight, ability to steer and dive to avoid objects and return to the surface, control navigation (submarine navigate essentially blind underwater, relying instead on inertial navigation systems), provide stability, provide securing arrangements when alongside. Examples of incidents involving vehicle control are USS Thresher (United States) in 1963, USS San Francisco (United States) in 2005 and HMS ASTUTE (United Kingdom) in 2010;

f) **Watertight Integrity** - The integrity of the metal pressure hull and all of the systems that penetrate it protects the crew and equipment from the outside water pressure and the threats it poses such as flooding, short-circuit and water spray damage. Examples of Watertight Integrity events are USS S-4 (SS-109) in 1977 and HMAS Dechaineux (Australia) in 2003;

g) **Structural Strength** - In addition to watertight integrity, the pressure hull provides the structural strength to resist the deep sea pressure and prevent crushing of the submarine. Examples of Structural Strength incidents are USS Thresher (United States) in 1963 following initiating event or events, USS Scorpion (United States) in 1968 following an explosive event and ARA San Juan (Argentina) in 2017 (cause unknown).

Safety is linked to risk: the likelihood of an incident occurring and the potential harm/damage that could result. In some circumstances, particularly in platforms designed for war-fighting, it is not possible to eliminate all Safety risks, in these circumstances there is a need for those accountable for Safety to define the tolerability of risk based on likelihood and impact.

Safety is driven into the design before the submarine is built, this could be in the form of duplication of systems to ensure redundancy of function; or a higher level of integrity to ensure the equipment functions as intended 100% of the time.

For operational safety it is important that components and systems perform in a safe manner so as not to create a hazardous environment for the personnel on-board or the public. It is also important that they perform their Safety critical roles reliably to support Safety functions.

3. Safety in Early Design

In the early design stages of a submarine, much of the focus is taken up by achieving the platform/operational characteristics (e.g. can it achieve x speed? is it capable of firing y number of torpedoes? etc.), however safety

[1] Vehicle Control addresses three Key Safety Events: Collision/Grounding, Loss Manoeuvring & Control and Loss of Stability.

should also be a key focus, especially from a stakeholder/operator perspective. Recent events (the ARA San Juan and KRI Nanggala) have drawn submarine-operating navies into stark focus, and their duty of care to the operating crew has never been more important. Incidents, even near misses, gain a high profile in the media, bringing unwanted attention and scrutiny to navies. Given the risks Submariners regularly weather, there is an enhanced duty of care that navies are urged to enact when designing submarines to not only avoid unfavourable media coverage and loss of life, but also to encourage future submariners to serve by demonstrating that their lives are valued and that preservation of safety is a priority.

So why is safety in early design so difficult? Design maturity affects the ability to analyse and assess safety in measurable or assurable ways because the level of detail that safety relies on, and indeed often insists on, is usually not there to fully understand safety scenarios and the vessel's response.

In many designs early safety evaluation is based on Fault Tree Analysis (FTA) where the key equipment that prevent/mitigate hazards and support responses are analysed from a statistical reliability standpoint to understand the estimated likelihood of an incident occurring. However these FTAs have their own inherent limitations, principally they are only as good as the reliability information input.

This information is primarily either based on historical data from previous/in-service submarines or obtained from generic Availability Reliability & Maintainability (AR&M) sources such as the Non-Electronic Parts Reliability Data (NPRD). Ideally legacy/existing platform data would be employed, unfortunately, unless the designer was directly involved supporting the platform, or has received this information from the operating navy, this will be sparsely populated and limited in its application to a new design. Catalogues such NPRD may be freely available however, due to the security classifications of submarine information, and navies reticence to release much information, submarine-specific information is relatively rare.

This is key as reliability data is context-specific: e.g. a ball-valve on a main battle tank will not experience the same conditions as a those on a submarine, where differences in humidity, salinity and chemical make-up, or even routine operating patterns could be at different extremes. Even surface ships and submarines rarely share comparable operating contexts; indeed, there are very few environments that share similar conditions to those experienced underwater at depth.

Equally, utilising reliability data from legacy/existing platforms, while more reflective of context, offers little coverage of new technology/innovation. FTAs may give some assurance that critical elements of safety events have been considered in the design, however the detail is not presented and the statistical value of the likelihood could be misleading in terms of giving a sense of accuracy.

This type of initial safety analysis can lead designers to make early decisions which have significant impact on the design as a whole, but require significant time, effort and money to reverse if it transpires they are ill-founded.

Figure 3 is the MacLeamy curve, which illustrates that the designers influence diminishes throughout a design project, while the cost to change the design increases exponentially on the same timeline.

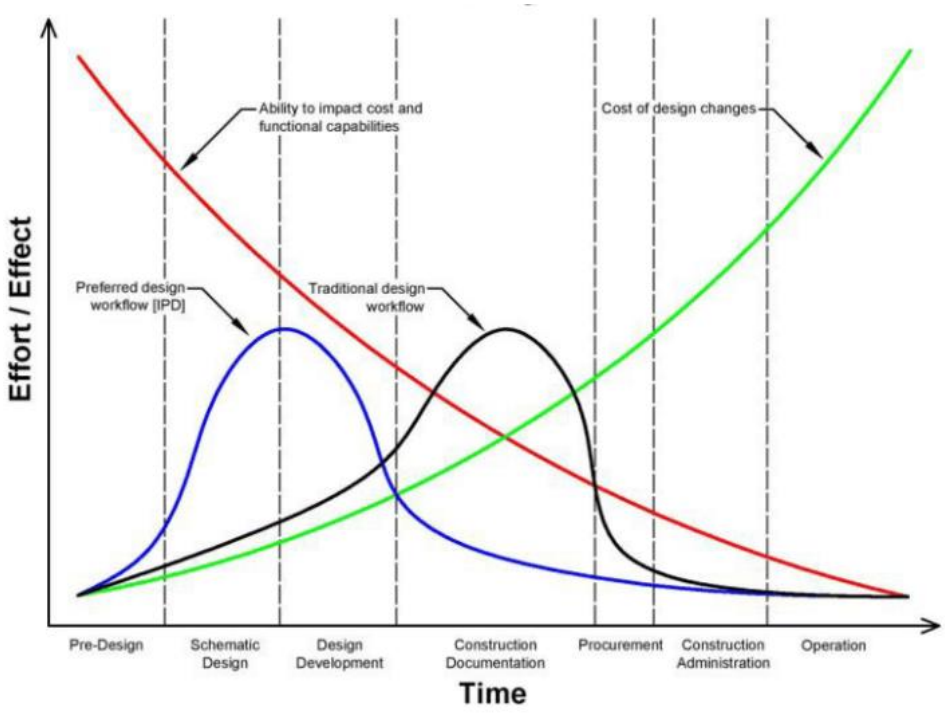

Figure 3 - The MacLeamy Curve (Davies, 2013)

4. An Alternative Approach

In the surface ship world, an element of safety assurance is gained by following Class Society Rules (e.g. Lloyd's Naval Rules), which specify design rules and specific features that vessels of certain classes should incorporate to demonstrate a consistent levels of 'safe design'. These rules have developed from previous design and operating experience to mitigate common design hazards. Unfortunately, due to the inherent secrecy involved in submarines, this accumulated knowledge and experience has not been compiled into a Class Rules for submarines.

So how does a submarine designer approach gaining assurance of safety without relying on either restrictive, or potentially misleading statistical data? One opportunity is to use established submarine community 'good practice' but in a more open, goal-based manner. Until recently this would not have been possible, for the reasons noted in the previous paragraph, however the International Naval Safety Association established a project to compile a Naval Submarine Code (NSubC, also known as ANEP-102). This compiled contributors' established experience and Learning from Experience (LfE) to arrange a goal-based standard specifically for key submarine safety aspects. A goal-based approach describes the intended end result and is generally not prescriptive on how it is achieved, which provides design freedom, enables innovation and avoids restricting designs to certain products and/or manufacturers.

The NSubC breaks down the submarine design into key themes/areas that contribute significantly to submarine safety:

- Structure
- Buoyancy, Stability and Controllability
- Engineering Systems
- Seamanship Systems
- Fire Safety
- Submarine Escape, Rescue, Abandonment and Survival
- Communications
- Navigation
- Dangerous Goods
- Integration of Platform, Combat and Navigation Systems
- Atmosphere Control

As a result, the NSubC provides goals and limited context that can support a review of a design at any stage. This can be employed by the shipbuilder to design the vessel, however for the buyer to gain early confidence in the design there may be benefit in obtaining Independent Technical Assurance (ITA).

ITAs are conducted by an experienced submarine engineering third parties (i.e. not the buyer or the shipbuilder) that are independent of commercial interest in the project (i.e. not a competitor or supplier). This enables them to provide an assessment of the design purely on its merits, as they align to goal-based objectives of the NSubC, and provide recommendations relevant to the problem. This activity can take place at any time and be continuous or periodic, coinciding with key milestones such as technical assurance or design maturity reviews when the design documentation is likely to be in a more presentable form.

5. The NSubC Independent Technical Assurance – an approach

The approach described here is based on an early concept submarine design review focussing on Engineering Safety. The submarine buyer desired an independent view on the engineered safety of the design and, as they were in the process of adopting the NSubC and its principles, the logical approach was to use this standard as the basis of good practice safety goals. These goals were employed as prompts to conduct an evidence-based review of the documented design (as provided by the shipbuilder) along with a review of the principal safety requirements to identify any contradictions.

The aim of such a review is to provide the buyer with an independent assessment of the Engineering Safety of the design at the developing concept stage, providing confidence that key safety aspects have been considered and are being progressed in line with good practice. It is not a statement, or opinion, that the design was safe, or an assessment of the tolerability of the of risks arising from identified hazards. Nor is it an opinion whether any risks were As Low As Reasonably Practicable (ALARP), as this is subjective to priorities and limits of an individual nation and its naval operator. Instead the reviews are more a measure of coverage of safety areas, as will be described below.

It must be understood that, due to time and cost pressure during bid and concept development stages, it is unlikely that the design evidence provided by the shipbuilder will be assembled in a format directly conducive to NSubC review (i.e. there are unlikely to be direct answers/solutions to the goals as they are described in the

standard). Therefore it is a fundamental requirement of the ITA team to consist of Suitably Qualified and Experienced Personnel (SQEP) proficient in understanding and interpreting the design articles (documentation and drawings) to allow analysis and formation of conclusions and recommendations.

For the project in question, the SQEP team was focussed onto the key individual themes/areas through preparatory work, which involved a review of the NSubC regulations and selection/assignment of 110 of those that were deemed particularly relevant. The individual reviewers utilised their wealth of experience and knowledge to interpret the design information/evidence presented and assessed whether the specific goals are fulfilled, in part or in full, by the design. To assess degree of goal fulfilment, a grading system was incorporated (see Table 1) to ensure a consistent process for the review. Any shortfalls would be clearly identified and recommendations for action, or suggestions for change, were identified as part of each regulation review.

Table 1 - Regulation Grading

Grade	Description
Grey	Insufficient information provided to conduct review.
Red	Direct evidence of inconsistency with the regulation, or non-fulfilment.
Amber	Evidence to indicate that some areas of the regulation are fulfilled (in general) but additional information would likely resolve any uncertainty.
Green	Sufficient evidence to conclude the regulation fulfilment by the design as described.

6. Regulations and WBSOs

It was recognised that the selected NSubC regulations contributed directly to Whole Boat Safety Objectives (WBSOs). While all regulations are likely to play a part in safety, and they are important, it is clear that at a whole boat/platform level there are circumstances where groups of regulations work together to achieve safety objectives, but they might not come from the same NSubC area. An example of a WBSO might be an objective to 'Control Fire' (see Figure 4). The NSubC contains a chapter with regulations directly related to Fire (Fire Safety), however these are not the only requirements applicable to controlling fire as both the submarine structure and the operational information and control system assist in controlling a fire.

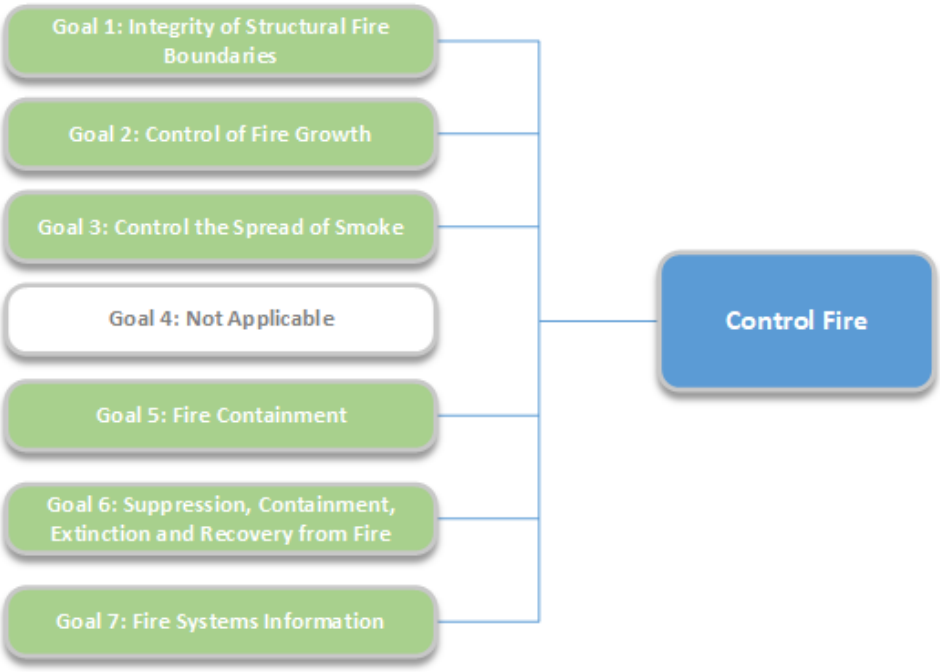

Figure 4 - Example NSubC Goals to WBSO

This is the concept of WBSOs, in relation to the NSubC, where relevant regulations that work together to support an objective are grouped together to present a more holistic view of an objective to support whole boat safety. 29 WBSOs were identified and shown in Figure 5 below.

Figure 5 - Whole Boat Safety Objectives[2]

At this stage, it might be asked 'what do these regulation reviews mean in the context of whole submarine safety?'. We attempt to provide this picture by looking at Key Submarine Safety Events (KSEs) for threats at a whole boat level, the KSEs are shown in Figure 6 below.

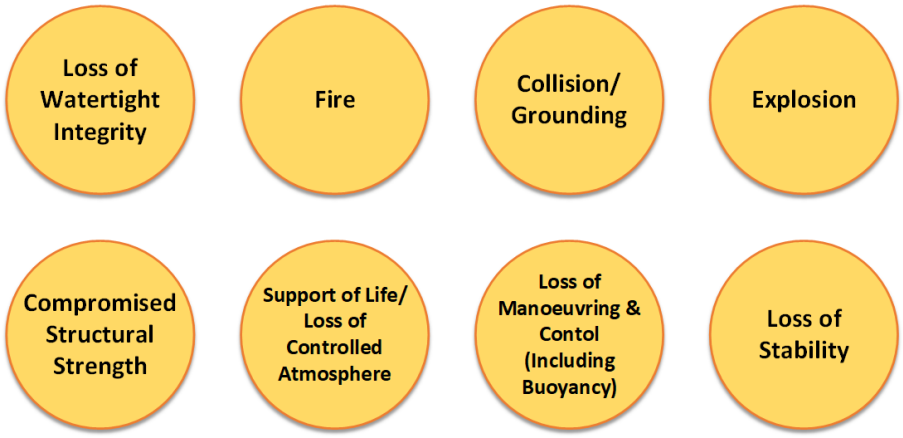

Figure 6 - Key Safety Events

At this level, the WBSOs come into context to form barriers to threats/hazards that might initiate an event and mitigations that might lessen the impact, or end consequence, of the event. For example, for the KSE of Collison/Grounding there are several acknowledged hazards that could lead to this event, such as 'Underwater terrain', illustrated in Figure 7. To prevent this hazard leading to an event the designer introduces barriers such as the WBSO 'Control Safe Navigation' which would look to the submarine design to provide sufficient navigation

[2] OME – Ordnance, Munitions and Explosives

systems, and redundancy, to reduce the likelihood of this event occurring to a minimum. Conversely, should the event already have occurred (despite the designed-in barriers) there are consequences that a submarine operator would want to avoid such as 'Inability to Surface'. For these the design is looking for the WBSOs to mitigate the outcome/consequence of the event to reduce its impact, in this case it would be addressed by the 'Control Buoyancy' WBSO.

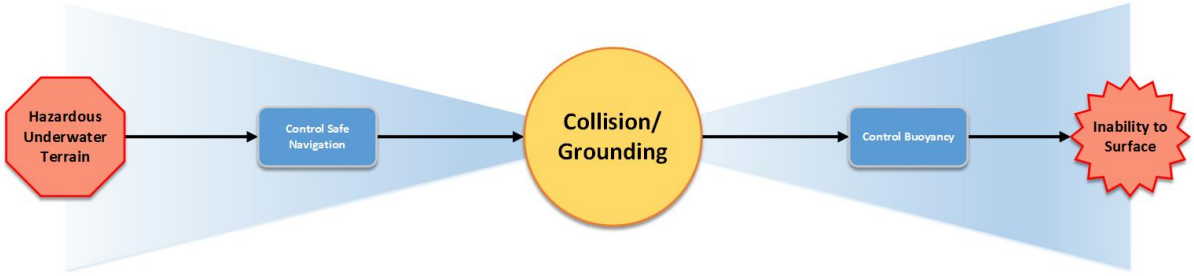

Figure 7 - Simple Hazard-KSE-Consequence Example

Repeating this process, identifying all hazards and consequences together with their related barriers and mitigations builds up a familiar picture of a safety "Bow-Tie" diagram, as shown in Figure 8. A Bow-tie is a graphical depiction of pathways from the causes of an event or risk to its consequences in a simple qualitative cause-consequence diagram. When used for detailed safety/risk analysis, it is a simplified combination of a fault tree that analyses the cause of an event or risk (the left-hand side of the diagram), and an event tree that analyses the consequences (the right hand side). When used in this way the bow-tie illustrates multiple layers of barriers and mitigations (and gates) on both sides of the central event.

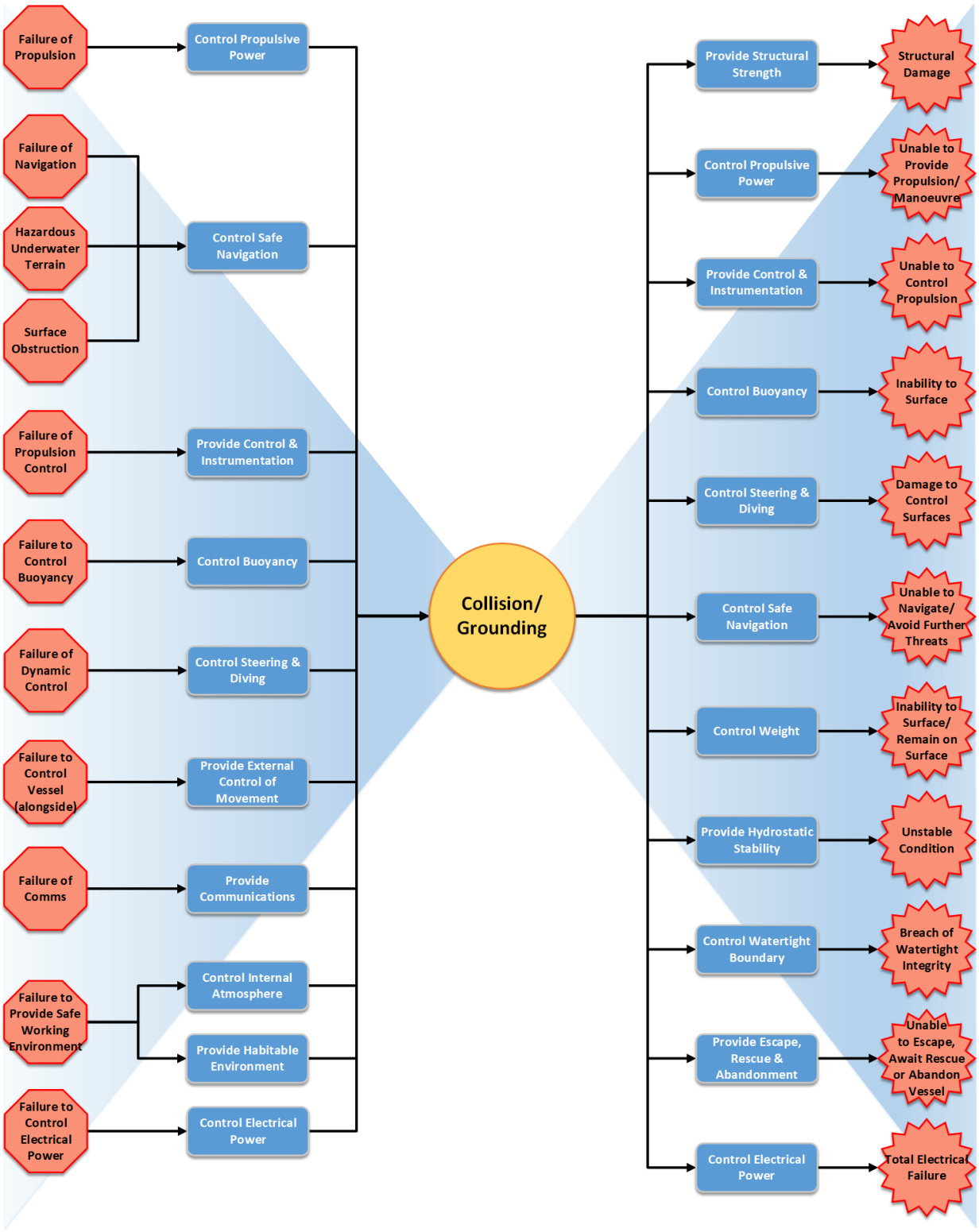

Figure 8 - Bow-Tie Diagram

The Bow-tie diagram presented in Figure 8 does not follow the standard format as described above, as it is focused on threats to achieving particular WBSOs and the associated confidence of the review team in the design evidence presented in relation to the effectiveness of the WBSOs in providing the multiple barriers and mitigations as described above. However, this type of Bow-tie diagram is quite powerful in graphically presenting the results of an NSubC assessment and an overall feel for the cohesiveness of KSE arguments can be grasped (as shown in

the Collision example in Figure 9) and identify areas for further focus. It could also be that the customer considers certain hazards inapplicable, given their Concept of Operations (ConOps), and therefore certain shortfalls can be discussed and omitted from future reviews. By employing the Grey/Red/Amber/Green of WBSO grading system for NSubC regulations (as shown in Table 1), Figure 9 presents this overall picture. It must be noted that WBSO grading would be at the discretion of the reviewer whether aggregation (of the contributing regulations/goals) is appropriate or there are pre-dominate regulations that hold a significant impact over the WBSO, and therefore determine the grade.

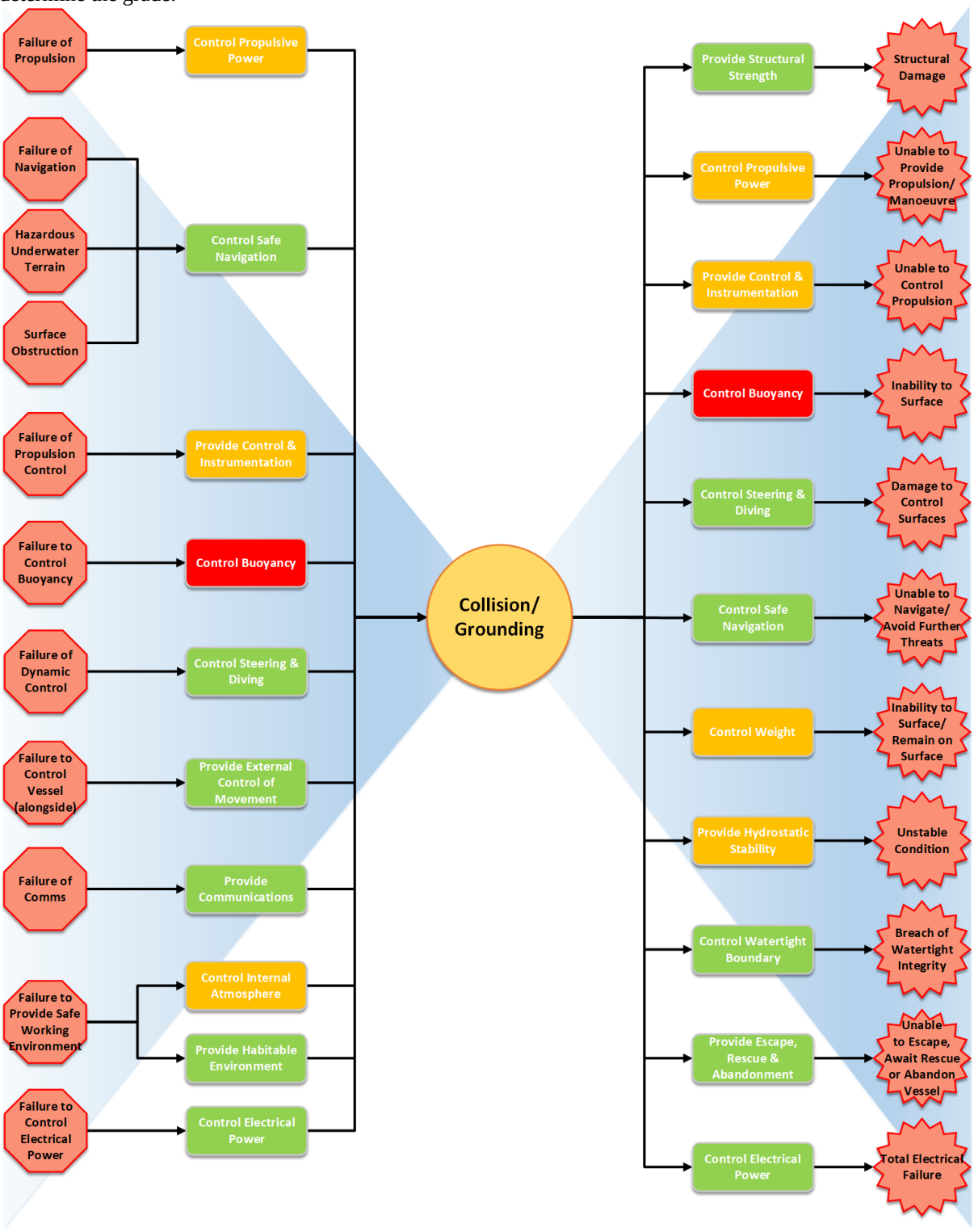

Figure 9 - Bow-Tie Diagram with Review Status

7. Overcoming the challenges

The challenges in a review, such as this, are fundamentally about information. Without information at sufficient depth and breadth to understand the approach it is very difficult to assess alignment. Given that design information grows throughout the design process, this type of assessment could be considered much simpler at a later stage, but is much more impactful at the earlier stages when this type of analysis can influence decisions and change focus to enable Engineering Safety. With close cooperation and an agreement of understanding with respect to Intellectual Property Rights (IPR) etc. the designer and the ITA team can work together to not only provide assurance to the customer, but also benefit from the outside review. Utilising the ITA as a 'second opinion', which may include innovation and LfE from other spheres of submarine design [3], and considering the recommendations/suggestions made there can help understand the issues and refine the design itself. Reviewing the engineering safety aspects earlier in the design (i.e. concept stage) is also beneficial to both the customer (to build confidence) and the designer to ensure any points of disagreement are resolved early when they are less costly/onerous to address.

It is also incredibly important to identify the relevant stakeholders in the design and ITA review, and ensure all those identified are briefed and engaged before, during and after the project to maximise the usefulness to all parties.

8. Conclusions

Ultimately design requirements are specific and measurable (or should be) and therefore assessing the fulfilment of a requirement is straightforward: it's either a yes or a no, but for safety engineering it is difficult to set requirements that can be analysed and assured in the early stages of design. For goal-based objectives, for which the line is less well-defined, significant knowledge, experience and understanding of the subject matter are required to make a judgement on the matter. Given sufficient design information and a responsive designer, it is possible for an ITA to employ goal-based criteria to build assurance that safety engineering is being considered, and aligns to good practice, at an early stage.

The approach described here (using the NSubC as a base of good practice) has presented a logical framework for an independent review to provide a submarine design customer with a holistic view of the submarine's safety approach, identifying strengths and weaknesses for consideration and prioritisation of design focus. Confidence can be drawn from the review that key safety events and their barriers and mitigations are being considered and are being monitored. It can also provide a submarine designer with a valuable external perspective and confidence that engineering safety philosophical conflicts can be identified and addressed early in the design stage.

However, it is clear that there is a minimum amount of design information needed to assess the degree of goal fulfilment and this requires close relationships with stakeholders to ensure this is available in the quantity and quality required.

Acknowledgements

The author would like to acknowledgement the efforts, organisation and refinement of ANEP-102 by the International Naval Safety Association (INSA) to compile submarine lessons learned and experience into this goal-based framework.

References

North Atlantic Treaty Organization Allied Naval Publication: "ANEP-102 Part 1 Naval Submarine Code: Foals, Functional Objectives and Performance Requirements", Edition A Version 1, 2021.

R. Davies, C. Harty, "Implementing Site BIM: A Case Study of ICT Innovation on a Large Hospital Project", Automation in Construction 30 (2013) 15-24

[3] Subject to the boundaries of export control and classified material.