Safety Critical Items in naval systems

D Gardner CEng MIET[a], C Brooking MEng CEng FIMechE CEnv AIEMA FSP[b], J R Inge CEng CITP MIET MBCS MAPM[a].[1]

[a]*Defence Equipment & Support, UK;* [b]*Occam Group Ltd, UK.*

Synopsis

What components make a ship safe to operate? Many; but not all are of equal importance. Applying a proportionate level of scrutiny and analysis to components and systems during design and safety case development, and then through life is key to the efficient management of the "safe to operate" argument. Applying true proportionality would be individual to every component and system – this would be cumbersome. Categorising safety related items to delineate between those that are essential to the platform safe to operate argument from those that provide a safety function that whilst important is not essential, allows appropriate focus to be placed on those essential items. Many would contend that this rationale has already been incorporated into existing design codes with terms in use such as Safety Critical Functions, Mobility or Ship Systems, Essential Services, Vital Services, Essential Safety Functions. However, these are generally loosely and subjectively defined and so open to interpretation. Furthermore, existing design codes tend to prescribe design outcomes. This leads to safety cases placing considerable emphasis and reliance on code compliance and certification rather than arguments focused on robust control and mitigation of hazards. Taking the lessons from offshore oil & gas, and other regulatory regimes and practices Defence Standard (Def Stan) 02-904, Surface Ship Safety Critical Items, was drafted to provide a consistent definition of Safety Critical Items and how they should be treated. The intent behind this standard is to generate a more risk focused approach to the management of component and system integrity through a platform life cycle and a leaner and more focused set of safety arguments. This paper examines the rationale behind Def Stan 02-904 and the work underway to implement its requirements.

Keywords: Safety; Safety Critical Items; Safety Case; Safety Function

1. Introduction: the problem space

Currently, many UK Naval Surface Ship Safety Cases do not clearly articulate the arguments that the platform is safe to operate. Causes of this are multi-faceted and include the following:

- There is no delineation between platform safety risks and occupational safety risks.
- The Claims, Argument, Evidence trail is not easy to follow.
- Assessment of design suitability and associated evidence is weak or fragmented.

In parallel to the above, it is observed that:

- Safety arguments required to underpin certification submission are developed outside the safety case.
- Existing design codes tend to prescribe design outcomes, and hence platform safe to operate arguments place considerable emphasis and reliance on code compliance and certification.

Instead of relying on code compliance and certification, platform safe to operate arguments should instead focus on robust control and mitigation of hazards; however, a risk-based approach based upon scrutiny and analysis of all components and systems during design and safety case development, and then through life, is impractical.

Categorising safety related items to delineate between those that are essential to the platform safe to operate argument from those that provide a safety function that whilst important is not essential, allows appropriate focus to be placed on those essential items.

Whilst this concept is relatively straightforward, commonly used associated terms, such as Safety Critical Functions, Mobility or Ship Systems, Essential Services, Vital Services, and Essential Safety Functions, have been loosely and subjectively defined to date and hence open to interpretation. This is a significant barrier to any implementation of the concept.

Author's Biographies

Dan Gardner is Deputy Head of Engineering and Chief Marine Electrical Engineer in the Ships Engineering HQ at DE&S. He has a background in the offshore, nuclear and renewables industries, and has been leading the work to develop Def Stan 02-904.

Charles Brooking is a principal consultant at Occam Group Ltd, providing safety assurance services for complex systems in the defence maritime, weapons, land and nuclear domains.

James Inge leads the Ships domain Safety and Environmental Protection Team in Defence Equipment & Support. He is a past chair of the MOD Safety and Environmental Standards Review Committee and is currently part of IEC SC65A Working Group 18, developing the new system safety standard for defence, IEC 63187.

 https://doi.org/10.24868/11194

2. Approach

To enable proportionate, risk based, platform safe to operate arguments to be generated, a Safety Critical Items approach has been developed and will be implemented within MoD Surface Ships Environment. This Safety Critical Items approach is based upon good practice used in the Offshore Industry (SCR, 2015, PFEER, 1995) and the Submarine Domain (MOD, 2015). Importantly, it also aligns with the expected update of the ANEP-77 Naval Ship Code to include the following definition:

> *Essential Safety Function: Those safety functions identified as being of primary importance in the prevention (and/or reduction) of the level of significant risk to the ship or several persons onboard, from Foreseeable Damage events to (at least) a level of safety deemed acceptable by the Naval Administration.*

The approach has been introduced to MoD Surface Ships via Defence Standard (Def Stan) 02-904 Surface Ship Safety Critical Items) which establishes a clear framework for the identification and management of Safety Critical Items for UK Naval Surface Ships (MOD, 2023).

Within this framework, Safety Critical Items are identified as being core to delivering a safe to operate platform as they perform the Essential Safety Functions that are central to the control of key hazards. Def Stan 02-904 specifically defines Safety Critical Items as:

> *Any part of a platform, providing a safeguard or mitigation against, or failure of which could cause or contribute substantially to:*
>
> - *a reasonably foreseeable loss of multiple lives associated with a Key Hazard Area, as defined in DSA03-DMR – Naval Authority Rules for Certification of MOD Shipping.*
> - *the failure of life support systems for diving operations or the trapping of a diver.*
> - *a platform-level effect with the potential to lead to severe damage or loss of platform and multiple fatalities.*
>
> *Safety Critical Items may be structures, systems, equipment, components, or software.*

3. Benefits

Implementation of the Safety Critical Items approach will enable those responsible for the provision of safe platforms to better understand the items they are reliant upon to make the platform safe to operate. Justified arguments that the specified Safety Critical Items are suitable to deliver the platform's Essential Safety Functions enables development of a more compelling and comprehensive argument that the platform is safe to operate. This facilitates an improvement in the utility of Platform Safety Cases, such that they can, for example, directly substantiate requests for certification, and more effectively support pre-sailing seaworthiness assurance reviews.

The approach also supports the prevention of unintentional Essential Safety Function degradation. When Safety Critical Items are clearly identified and tagged, it is possible to introduce prohibitions or controls on the modification or replacement of those items unless an assessment of the potential impact on the Platform Safety Case has been undertaken.

Importantly, the approach also supports assessment of the impact of material state degradation on the Platform Safety Case. In particular, it enables the requirements for live material state data to be focussed on those items and measures of performance associated with the Essential Safety Functions. With the appropriate information available, the safe to operate argument can be updated dynamically, better informing decisions regarding operation of the platform. This is of particular value when considering the cumulative impact of ostensibly unrelated Safety Critical Item degradations.

4. Identification of Safety Critical Items

Def Stan 02-904 requires that:

- *For each platform, the Safety Critical Items associated with that platform shall be recorded.*
- *For each Safety Critical Item, the related safety functions shall be recorded.*

Recording first requires identification of the Safety Critical Items. This is not always straightforward as Safety Critical Items may come in various forms: structures, systems, equipment, components, or software. For example a Safety Critical Item may be an entire system (e.g. fire detection system), or an individual component (e.g. pressure relief valve). In addition, Safety Critical Items do not solely comprise items that must correctly function in emergency situations; they may also comprise items that must correctly function on a continuous basis to enable safe operation of the platform.

 https://doi.org/10.24868/11194

It should be noted that systems (e.g. electrical generation and distribution systems, fuel supply systems, hydraulic systems etc) upon which identified Safety Critical Items are dependent, may also be considered to be Safety Critical Items. This is due to the significant role they play in ensuring that dependent Safety Critical Items can continue to deliver their safety functions.

As a result, application of engineering judgement, by personnel with thorough knowledge of the platform and platform systems, is vital when identifying Safety Critical Items at an appropriate level of system breakdown. Identification at too low a level will result in an unmanageable number of Safety Critical Items. Identification of Safety Critical Items at too high a level may result in important safety functions not being identified.

The process of identification is shown in Figure 1. It draws heavily on the risks recorded in the Platform Hazard Log, and comprises:

1. Review of platform hazards to identify 'major accidents'; i.e. those that align with '*a reasonably foreseeable loss of multiple lives associated with a Key Hazard Area*' etc.
2. Application of engineering judgement to identify Safety Critical Items:
    a. That provide a safeguard or mitigation against the accidents; or
    b. The failure of which could cause or 'contribute substantially to' the accidents[2].
3. Recording of each Safety Critical Item within a Schedule of Safety Critical Items, together with the safety function(s) delivered by the Safety Critical Item (in relation to the hazard). Recording the safety functions at this stage ensures that Performance Standards (discussed below) are focussed on the safety functions of interest, not other functions that the Safety Critical Item may deliver. In each case, the boundary of the Safety Critical Item must be defined, as not all of a 'system' may be performing the safety functions of interest.

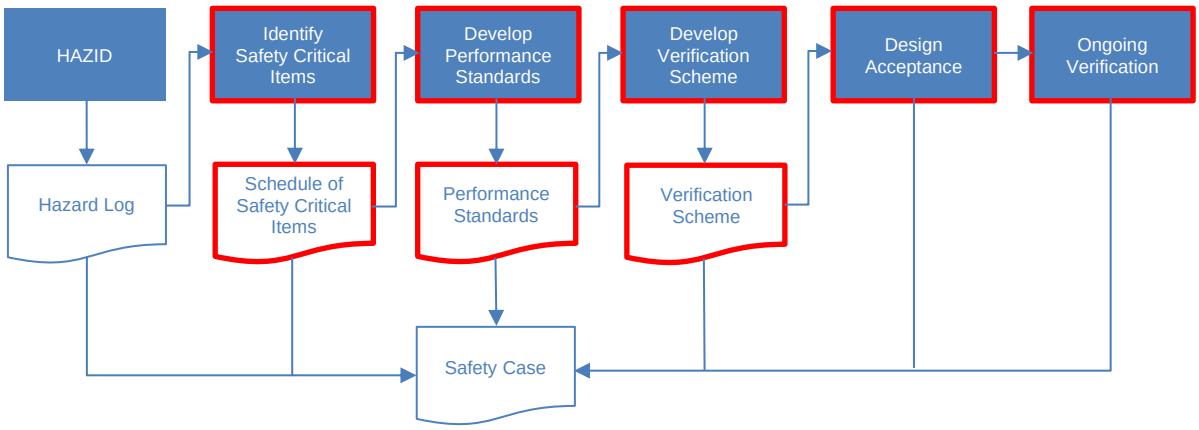

Figure 1. The Platform Hazard Log as an input to the Safety Critical Item identification process.

To support thorough identification of Safety Critical Items, it is recommended that hazards and Safety Critical Items are portrayed together in bowtie diagrams. An example of a bowtie developed for a Landing Craft hazard of Broaching is presented in Figure 2. This shows both Safety Critical Items that directly perform a safety function (Kedge Anchor and Winch), and those that have been defined as Safety Critical Items given the dependencies upon them (Hydraulic System etc).

[2] 'Contribute substantially to' is used to ensure that those Safety Critical Items, whose failure would make a significant contribution to a chain of events that could result in or aggravate the defined accidents, are included.

 https://doi.org/10.24868/11194

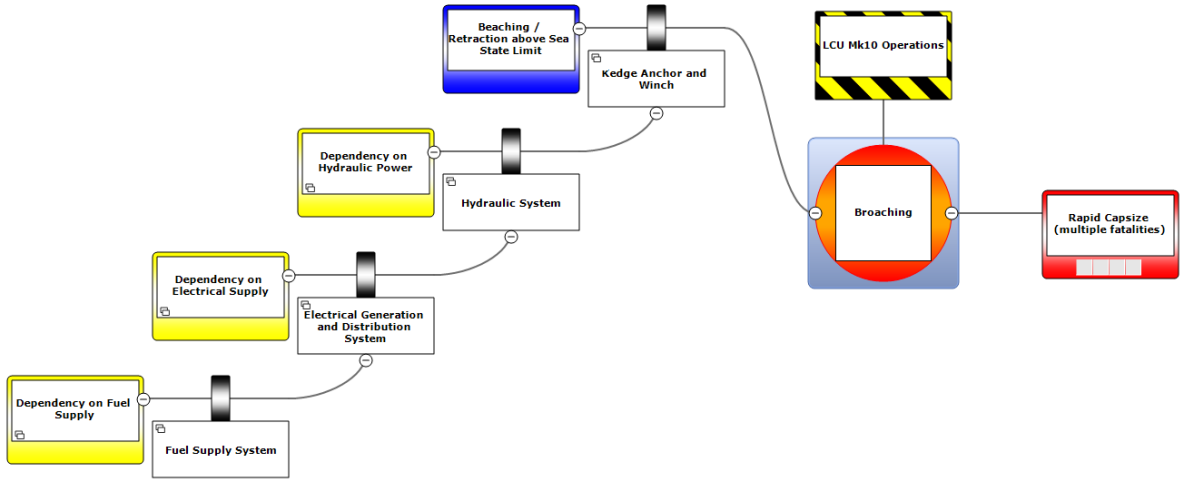

Figure 2. Bowtie showing Safety Critical Items in relation to the Landing Craft hazard of Broaching.

5. Performance Standards

Performance Standards define clear Safety Critical Item performance requirements, compliance with which prevents major accidents from occurring or escalating.

Def Stan 02-904 requires that:

> *For each related safety function, the Safety Critical Item shall have a record of its required Performance Standard.*

Def Stan 02-904 also provides the following definition:

> *Performance Standards are statements which can be expressed in qualitative or quantitative terms. A performance standard shall contain sufficient information against which to assess the suitability and condition of the items to which they apply and cover functionality, reliability, availability, survivability, reversionary modes, and interdependence where appropriate.*

To meet the above requirements, Performance Standards should developed against the following FARSI criteria:

Functionality – What safety functions must the Safety Critical Item be able to deliver? Functionality refers to what the Safety Critical Item must do to prevent, detect or mitigate hazards that may lead to a major accident. It can be expressed as the overall goal of the Safety Critical Item against the specific major accidents to which it relates. This may be qualitative or quantitative, but either way must be verifiable. Functionality requirements may include reference to applicable standards, if their applicability is justified. A Safety Critical Item may relate to more than one major accident and may be performing slightly different functions in each case; the specific functionality requirements in each case must be clearly recorded.

Availability – When must it be ready and able to perform? Availability refers to the scenarios in which Safety Critical Item are required to perform. This may differ between different operating conditions of the platform, e.g. some Safety Critical Items will not be required to be available when a platform is alongside, some may not be needed if no munitions are embarked, etc. Availability should be expressed in quantitative or semi-quantitative terms and must be verifiable.

Reliability – What level of reliability is required? Reliability refers to how likely the Safety Critical Item is to perform on demand. Required reliability may differ between different operating conditions of the vessel. Reliability may be achieved by redundancy or alternative back-up systems. The full benefit of Performance Standards will be realised during acquisition, when they are used to assess candidate Safety Critical Items. Quantitative derivation of reliability requirements is likely to be required to support this. For in-service platforms, taking a quantitative approach may not be proportionate; a semi-quantitative or qualitative approach may be more suitable. Either way, reliability requirements must be verifiable.

Survivability – What kind of events does it need to survive and for how long? Survivability refers to how the Safety Critical Item will perform after a major accident has occurred, i.e. how well it will survive a fire, flood, etc. Required survivability may differ between different operating conditions of the vessel, as discussed further below. Survivability may be achieved by redundancy or alternative ‘reversionary’ or fragmented or fall-back operating modes. Survivability should be expressed in qualitative terms against the various threat levels. As for other criteria, survivability performance must be verifiable.

 https://doi.org/10.24868/11194

Interdependence – What other systems does the Safety Critical Item interact with? Interdependence refers to the way that the Safety Critical Item:

- Is dependent upon other Safety Critical Items to operate.
- Is dependent upon other systems or equipment to operate.
- Otherwise interacts with other Safety Critical Items.

Where Safety Critical Items are reliant upon common systems, e.g. electrical power, an assessment should be made of the impact of common cause failure. As noted above, systems that do not directly perform a safety function may themselves be identified as Safety Critical Items due to their high levels of interdependence. Interdependence must be considered when determining availability, reliability and survivability.

6. Operating Conditions

Unlike other industries, e.g. Oil & Gas, where assets operate in a single, defined, operating scenario, Naval Surface Ships are required to operate in multiple scenarios ranging from peacetime operations, through maritime security, to combat operations. The Performance Standards for Safety Critical Items may vary between these scenarios.

For example, multiple simultaneous compartment fires may be a credible risk during combat operations; however, during peacetime operations it may be that the credible risk is limited to a single compartment fire. As a result the Performance Standard associated with the fire-fighting system Safety Critical Item may be more demanding for combat operations (e.g. require higher levels of functionality and greater redundancy). Peacetime operations may not require such a stringent Performance Standard.

It is noted that ANEP-77 already defines the following scenarios:

Foreseeable Damage – which includes damage that could be caused by one's own cargo or weapons, navigational hazards (collision, grounding), naval exercises (certain types of navigational exercise, replenishment at sea, landings, boat operations, etc), system failures or maloperation.

Extreme Damage – which includes damage that could be caused by freak waves or typhoons.

Extreme Threat Damage – which includes damage that could be caused by weapon attacks and extreme acts of aggression.

To maintain alignment with ANEP-77, it is recommended that requirements for each of these scenarios are included within the Performance Standards. Recording variation of requirements in this way enables safe to operate assessments to be made in the context of the planned platform operations.

7. Verification Schemes

Once Performance Standards are in place, Safety Critical Items can be managed, with proportionate rigour and scrutiny, via the use of Verification Schemes.

Def Stan 02-904 requires that:

> *For each platform, a verification scheme shall be established for ensuring that the Safety Critical Items will be suitable and remain in good repair and condition, such that the required Performance Standards will continue to be achieved.*

Importantly, Verification Schemes cover both the initial suitability of the Safety Critical Item design (via Design Acceptance), and its ongoing ability to meet the required Performance Standard (via Ongoing Verification).

7.1. Design Acceptance

Before any Safety Critical Item is brought into operation on the platform, Safety Critical Item suitability must be demonstrated. The Verification Scheme should detail the design acceptance activities to be undertaken to assess the suitability of the Safety Critical Items. It is expected that these activities will predominantly focus on the review of design disclosure reports (or similar), which, for each Safety Critical Item, substantiate how the Safety Critical Item design meets the requirements of the associated Performance Standard. The substantiation should demonstrate how the design, and associated support solution (considering aspects such as maintenance schedule and provisioning of spares), will address all the FARSI criteria.

7.2. Ongoing Verification

Ongoing verification will ensure that the Safety Critical Items continue to deliver the Essential Safety Functions throughout the platform's life. Discovering weaknesses by having a near miss or accident is too late and too costly. Early warning of dangerous deterioration within Safety Critical Items provides an opportunity to avoid associated accidents.

 https://doi.org/10.24868/11194

The determination of ongoing Safety Critical Item suitability should involve ongoing verification of Safety Critical Item performance through review of suitable reports or key performance indicators (KPIs). The Verification Scheme must therefore align the maintenance / inspection routines and the records made by Ships Staff / Industry Participants (e.g. within the maintenance management system) with the Performance Standards.

8. Material State Monitoring

When a Safety Critical Item fails to meet its Performance Standard, measures must be taken to assess and mitigate the risks to the platform. If the Safety Critical Item is operable but in a degraded state, a risk assessment should be undertaken to determine if the platform continues to be safe to operate. Temporary mitigating measures should be implemented to reduce the risks to As Low As Reasonably Practicable (ALARP) and help support the justification for continued use. Appropriate limitations of use should be set and the mitigating measures monitored until a permanent repair has been carried out.

Use of live material state data will enable Safety Critical Item degradation to be monitored, and the impact on the Platform Safety Case to be assessed. In support of this, linkages should exist between digital systems to facilitate the timely provision of required information. Ideally, these linkages would support Safety Critical Items material state reporting on demand.

With the appropriate information available, the safe to operate argument can be updated dynamically, better informing decisions to stay on the wall, sail, or sail with suitable operating limitations in place.

9. Trial Implementation

While the Safety Critical Items approach is common practice in offshore Oil & Gas and many onshore process industries, it is new for UK Naval Surface Ships. Adoption of the approach therefore requires development of suitable guidance, which, to be effective, needs to be based on lessons learned from real-world implementation of the approach. As a result, trial implementation of the approach on the Landing Craft Utility (LCU) Mk10 has been undertaken. LCU Mk10 was selected on the basis that this was a comparatively simple platform (compared to other complex warships).

To date, the trial has identified LCU Mk10 Safety Critical Items and associated bowtie diagrams, and has developed a number of Performance Standards and Verification Schemes. Work to create to linkages between digital systems to facilitate the timely provision of material state data is ongoing.

Overall, the trial implementation, conducted with the support of the LCU Mk10 platform engineering team, has been successful. Observations / Learning from Experience, obtained from conducting the trial, and from wider briefings on the introduction of Def Stan 02-904, include:

- A lack of recognition of the need for, and benefits of, the Safety Critical Items approach. This has resulted in resistance to implementation of the standard. It is hoped that this paper, together with outputs of work seeking to provide on-demand material state data for Safety Critical Items, will help to demonstrate the overall benefits of the approach.
- Difficulties in defining reliability requirements for Safety Critical Items on in-service platforms. This is predominantly due to a lack of reliability data. Item failure rates are not recorded, and hence it is difficult to set informed, quantitative reliability requirements. Work is currently ongoing to determine whether Failure Modes, Effects and Criticality Analysis (FMECA) undertaken as part of Reliability Centred Maintenance (RCM) may contain data that could support the setting of reliability requirements.
- Incomplete design acceptance information associated with the original design. Substantiation was only undertaken against the requirements set at the time; however, as Performance Standards were not generated, these requirements did not cover all FARSI criteria.
- Variation in data storage locations. Whilst technical documentation is held centrally, records of ongoing verification activities are sometimes only held by the organisation who has conducted that activity. This limits the ability to create digital linkages required to support material state monitoring.
- Configuration control issues. Design changes have been embodied through life (e.g. to meet modern standards); however, supporting technical documentation and equipment databases are not always updated.
- Determination of critical components within a Safety Critical Item. Whilst equipment databases identify all the components that make up a Safety Critical Item, it is not clear which of these are critical for the Safety Critical Item to deliver its safety functions. Classifying all components as critical could result in unduly stringent requirements (e.g. spares requirements) for those components that do not support delivery of the safety function of the Safety Critical Item. Again, it is hoped that RCM FMECAs will have identified which components are critical, and which are not.

 https://doi.org/10.24868/11194

10. Conclusions

Implementation of the Safety Critical Items approach enables those responsible for the provision of safe platforms to better understand, and proportionately focus effort on, the items they are reliant upon to make the platform safe to operate. Justified arguments that the Safety Critical Items are suitable to deliver the platform's Essential Safety Functions enables development of a leaner, but more focused, compelling and comprehensive argument that the platform is safe to operate.

The approach also supports assessment of the impact of material state degradation on the Platform Safety Case. With live material state data available, the safe to operate argument can be updated dynamically, better informing decisions regarding operation of the platform and providing continuous assurance.

The LCU Mk10 trial showed the Safety Critical Items approach to be effective, but also identified some issues associated with implementation on in-service platforms. It is anticipated that following the approach will be easier and more beneficial if implemented early in the platform lifecycle. Notably, the following benefits would be realised:

- Increased value in undertaking more detailed analysis, such as quantitative analysis to support setting of reliability requirements. This increased value is based upon being able to enjoy the benefit over the full platform life (c.f. remaining life for an in-service platform).
- Use of Performance Standards and Verification Schemes to influence and assess candidate Safety Critical Items during the design phase, thereby ensuring that they will be suitable for delivery of the required Essential Safety Functions.
- Ability to develop data requirements to ensure that all required information is recorded and is easily accessible, in support of material state monitoring.

References

MOD, 2015. *Def Stan 02-207—Quality Management Framework and Requirements for Materiel Safety in Submarines*. Glasgow: Ministry of Defence, Defence Standard No. 02-207 Part 1.

MOD, 2023. *Def Stan 02-904—Surface Ships Safety Critical Items*. Glasgow: Ministry of Defence, Defence Standard No. 02–904.

SCR, 2015. The Offshore Installations (Offshore Safety Directive)(Safety Case etc) Regulations 2015.

PFEER, 1995. The Offshore Installations (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995, (SI 1995/743).

 https://doi.org/10.24868/11194