Shipping Safety into the Naval Industry

A Labonté Jones[1], BEng (Hons), MIET,
N Lerigo-Smith[2], BEng (Hons), CEng, MIET

L3 MAPPS Ltd.
Author Emails: Aneirin.LabonteJones@L3T.com; Nicola.Lerigo-Smith@L3T.com

Synopsis

Safety engineering and legislation (IEC-61508, 61511 etc.) has been entrenched in many industries (O&G, process) for years. Although regulation has been progressed by Lloyd's Register, the Marine industry has been inherently slower to accept and adopt functional safety practices employing quantitative analysis. As in other industries, a review of legislation would usually be kick started by a large-scale accident.

With an aim to reducing manning costs, marine vessels are now developed with increasing amounts of automation in their control systems. Incidents resulting from failures of these systems are becoming more frequent due to either poor safety considerations when designing the systems, or operators not understanding interactions with the automated systems. Preferably, before incidents increase in frequency or severity, engineered safety using inherent safety controls will become a more important factor in the Marine sector.

Opposition to functional safety has primarily been due to cost and scheduling purposes. Businesses have to be profitable to survive, and Safety Engineering can be viewed as introducing programme delays and unnecessary costs. In reality, other safety related programmes have demonstrated the benefits of following safety related development programme.

As in most instances of programme delay, poor initial requirements capture causes late changes to be incorporated to products, resulting in escalating delays and costs.

If safety is engaged early in the product lifecycle, then programme delays and unnecessary safety risk can be reduced and managed effectively throughout the lifetime of the ship. In all projects, there can be conflicts between safety and security design, but early integration of safety will allow you to balance safe, secure and reliable operation, ultimately improving the quality of your end product.

Major savings can be made by reducing maintenance on systems that have been proven to have lower integrity due to quantitative analysis and proof testing – provided it has been demonstrated to be As Low As Reasonably Practicable (ALARP). If your company does not embrace safety integrity within its culture, you can run the risk of losing credibility, a competitive edge within the marketplace and incur expensive damage to reputation.

In conclusion, the manufacturer and end user will incur far higher costs of redesign if changes are needed for safety when the product has reached post-development. If left unchanged, consider the following: If a designed system fails and causes an incident, will the company reputation be tarnished and product orders halt? Remember: If somebody is injured or dies in an accident, any company individual can be found liable and prosecuted.

Keywords: IEC-61508; IEC-61511; Functional Safety; Regulation; Engineering Process

1. Introduction

Safety engineering legislation and standards (IEC 61508 [1] etc.) has been entrenched in many industries (automotive, process, rail and aircraft) for years. Although regulation has been progressed by Lloyd's Register [2], the Marine industry has been slower to accept and adopt functional safety practices employing quantitative analysis and evidence-based practices. Typically, an industry is forced to review its safety legislation and / or standards after a large-scale incident has occurred. Needless to say, by this time it is too late leading to improvements in safety culture.

2. What is Safety Engineering?

Safety Engineering is intended to design systems with inherent safety measure i.e. to identify dangerous failures and control their mitigation and recovery to minimise consequences. It includes the management of likely operator errors, hardware and software failures and environmental changes [3]. Safety Engineering helps

[1] Aneirin (Nye) has worked in safety engineering since he joined L3 in 2017. Here, he has worked on Naval projects from surface ships to submarines. Nye has a background in controls and instrumentation previously working as both a technician and an engineer within the nuclear, defence and power generation industries.

[2] Nicola has worked in safety engineering since 2012, specialising in software safety. She has been with L3 for the last five years; working on Naval projects including surface ships and submarines. She is a chartered engineer with the IET and has spent most of her working life as a software and integrated systems developer, team leader and manager.

http://doi.org/10.24868/issn.2631-8741.2018.017

to design a system that can execute specific functions correctly, even under non-intended use (or sometimes even misuse).

Apart from the above, the benefits of safety engineering include:

- Increased system availability – the proportion of time that the equipment or system is able to perform its function.
- Increased system reliability – the probability that the system will perform its required function, in the intended operational environment, for a stated period.
- A quantitative measure of software quality – no more "it's safe, because we have always developed it this way".

Manufacturers are required to identify potential unintended behaviours of the system that could lead to a hazardous event, and perform safety risk assessments [4].

2.1. How are evidence-based Safety Engineered systems developed?

One method is the Goal Structured Notation (GSN). An example of Platform Management System (PMS) development GSN is shown in Figure 1. This GSN displays the overarching goal that the 'PMS is safe', but caveats it within the contexts of a) its intended operational environment and b) required safety target in accordance with Def Stan 00-056 [5]. The GSN breaks down the ways to achieve that top goal via a strategy and subsequent goals beneath that.

For each of the sub-goals, supporting evidence is generated and this is then collated in the Safety Case to substantiate each of the goals / claims. The Safety Case brings together the overarching goal that the system is safe and must be evidence based to stand up to independent audit scrutiny.

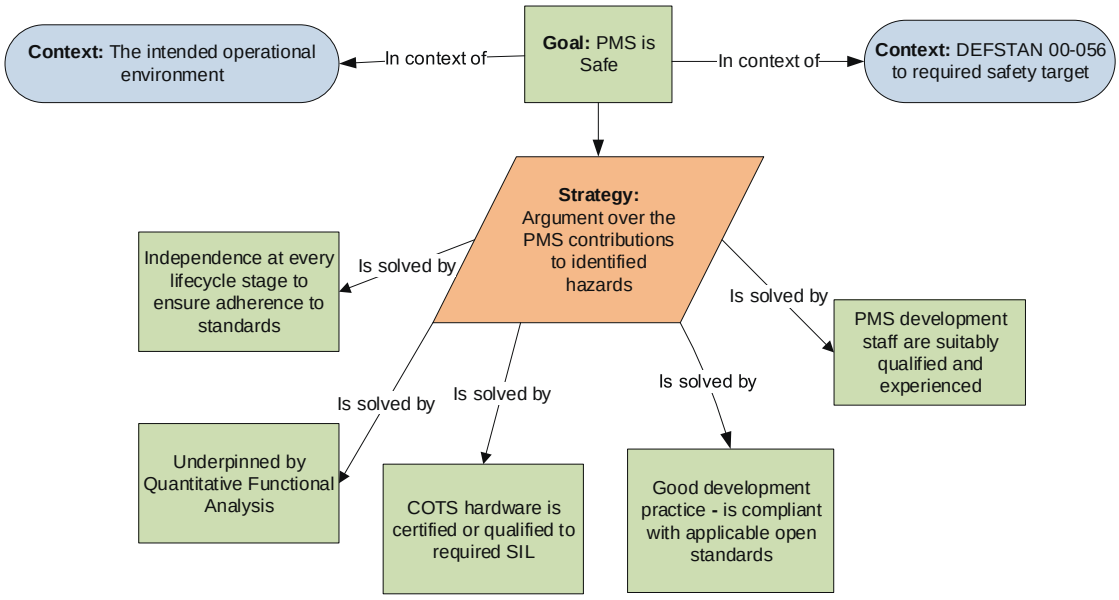

Figure 1 Example of GSN for development of PMS

2.2. Quantitative Functional Analysis & Safety Integrity Level (SIL) Ratings

With appropriate functional analysis, you can determine the SIL required for the system safety-related functions (functions that are required to remove risk of key whole ship hazards). The SIL ratings allow for a function (and all equipment and software involved in that function) to achieve a determined failure rate i.e. when called upon, the system will be available to provide its safety-related function. SIL ratings are based on good engineering practices throughout development and documented testing procedures throughout the life of the system.

2.3. Opposition to Safety Engineering

Opposition to including functional safety in a programme has primarily been due to cost and scheduling purposes. Businesses have to be profitable to survive; managers carry the responsibility for ensuring that the equipment is competitively priced, and that its safety integrity is adequate in operation. Functional Safety

http://doi.org/10.24868/issn.2631-8741.2018.017

engineering can be viewed as introducing delays and unnecessary costs. In reality, although there is a higher initial development cost, the economic value is realised through the life of the programme.

A systematic approach will help to ensure that optimum solutions will emerge in terms of cost and safety (Cost Benefit Analysis). This is achieved by identifying safety requirements early, designing / implementing once, using rigour to reduce change impact.

A general study [6] made by the Health and Safety Executive (HSE) into the cost of accidents showed that the costs of error / accident rectification far exceeded those that would have been incurred if a systematic approach had been employed from the outset (see Figure 2).

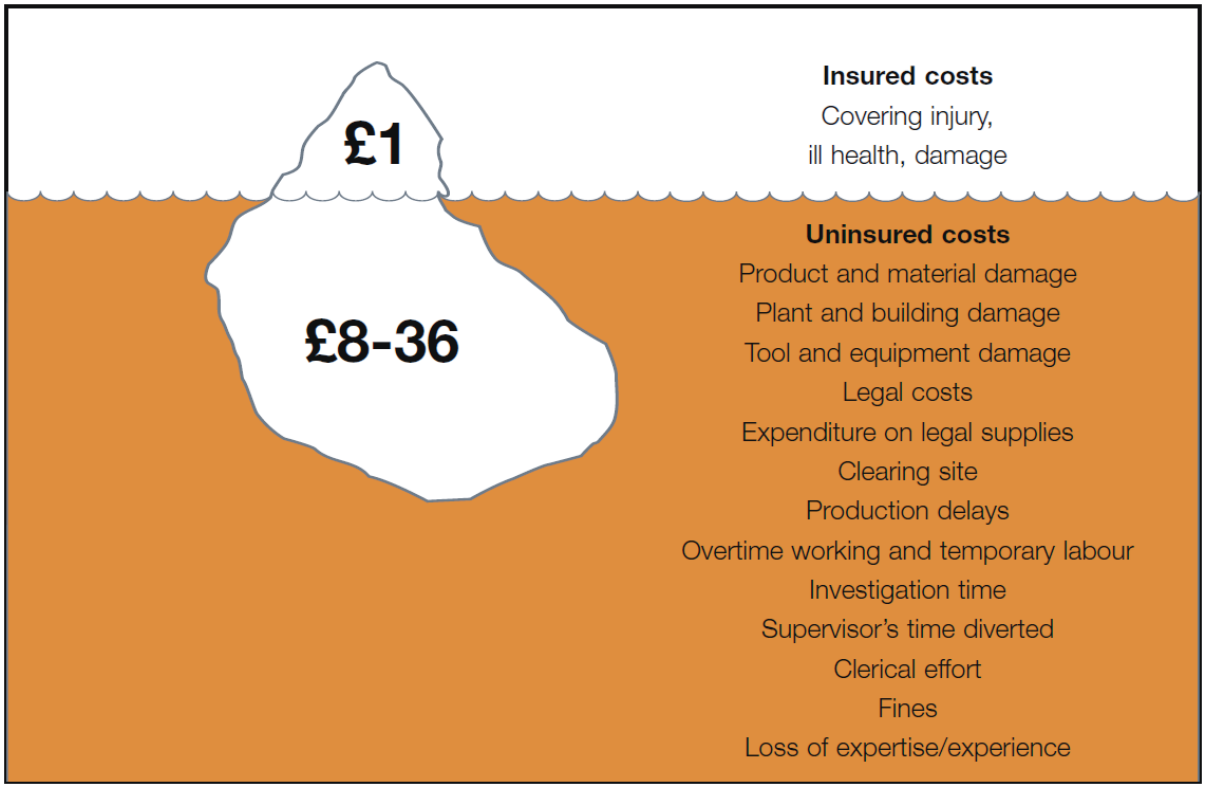

Figure 2 Accident iceberg – the hidden cost of accidents (HSE) [7]

As in most instances of programme delay, poor initial requirements capture causes late changes to be incorporated into products, resulting in escalating delays and costs. These additional delays and costs are increased when left to a later stage in the development lifecycle in fact the cost of correcting a change is increased later in the lifecycle this is implemented [Appendix 1]. This in turn can cause a ripple effect with costs of delays amplified when passed on to your clients where integration is necessary with other suppliers.

Not all safety requirements are determined immediately in the preliminary design phase; most derived safety requirements will become apparent during the detailed design phase from analysis of the intended design. The earlier this safety analysis is undertaken the less rework will be required.

If safety is engaged from the start of the product lifecycle, then programme delays and safety risk can be reduced and managed effectively throughout the lifetime of the ship. Not only does a safe system protect lives, it can also save your company money both in development (by removing the need for additional re-work), as well as in operational service.

2.4. How can involving safety save money?

By using the appropriate functional safety analysis an appropriate integrity level can be determined for a safety function. Completing this analysis allows for mitigations and engineering designs to be implemented that are proportionate to the determined amount of safety risk; provided the residual safety risk has been demonstrated to be As Low As Reasonably Practicable (ALARP)[3].

[3] "A risk is ALARP when it has been demonstrated that the cost of any further Risk Reduction, where the cost includes the loss of defence capability as well as financial or other resource costs, is grossly disproportionate to the benefit obtained from that Risk Reduction." [Def Stan 00-056].

http://doi.org/10.24868/issn.2631-8741.2018.017

Inherent safety development and engineered mitigations (as much as practicable) offer manufacturers a way of improving their productivity and competitiveness in the market. Here, safety becomes an integrated part of functionality, rather than an after-thought added to meet regulations.

Designing appropriate safety controls can reduce the effect of a hazard and it is usually cheaper to *proactively* engineer a mitigation into the design, rather than *reactively* control the consequences of a hazard. This is demonstrated on the bow tie diagram [Figure 3].

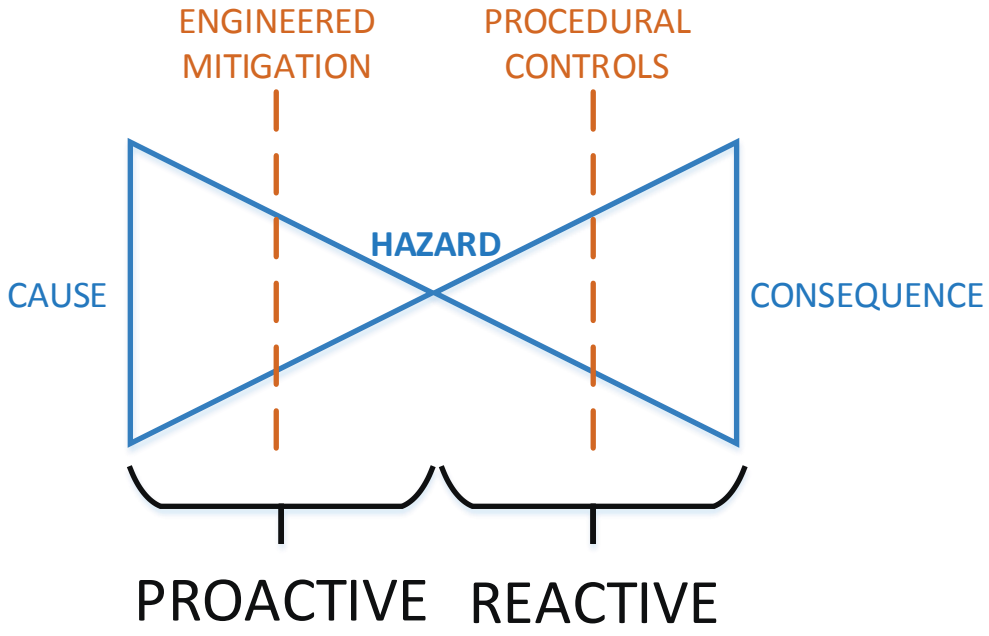

Figure 3 Bow tie diagram displaying interjection of engineered mitigations to avoid hazardous consequences

3. What policies currently influence the Naval industry?

Defence activities are governed by DSA01.1 Defence Policy for Health, Safety and Environmental Protection stating risks should be reduced, ALARP, and managers are to lead by example on Health Safety and Environmental Policy (HS&EP) [8]. In Naval programmes the primary safety management standard is the same as for all defence systems, Def Stan 00-056 [5]. This standard was originally written with a preference for bespoke systems as it was hard to find compliant 'off the shelf' components in the marketplace. In the current version of the standard, the Ministry of Defence's (MOD's) Safety Standards Review Committee realised the benefits of using open standards in the assurance of Commercial Off The Shelf (COTS) items and thus reissued Def Stan 00-056 [5] and Def Stan 00-055 [9] to allow exactly that. Def Stan 00-056 [5] expects that the use of a particular open standard must be appropriate for the contract, the military operational context of use and be in-line with the MOD Safety Management Systems policies and procedures (ASEMS [10], POSMS [11]).

Relating specifically to software (applicable to both surface ships and submarines), the Naval Authority Group has released a Naval Authority Notice (NAN) entitled Software Integrity Policy [12]. The Policy's goal is that for each activity where equipment containing software is used, the duty holder has managed the risks associated with the software and provided assurance that it is safe to use for its intended purpose. NAN 06/2018 [12] stipulates that all equipment and systems that contain and / or are controlled by software, have to deliver their function without causing / impairing recovery or mitigation from a Key Hazard.

Areas of concern with software or systems containing software include the successful integration of hardware and software. For example, in an embedded system 'client' compatible layers have to be developed starting from hardware Basic Input / Output System (BIOS) level, through the operating systems up to the top level applications [Figure 4]. These different layers can create the risk of incompatibility if not developed together. Safety assurance applies to the entire embedded system not just the application software.

http://doi.org/10.24868/issn.2631-8741.2018.017

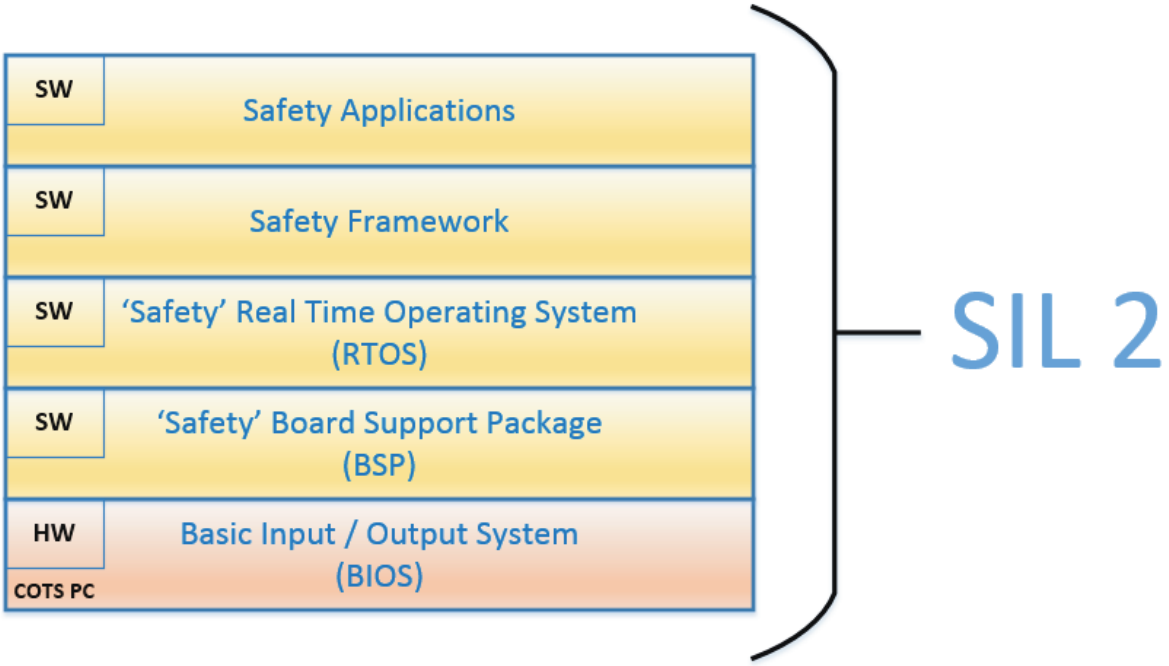

Figure 4 Example 'Client' hardware and software levels to be integrated (separate to Programmable Logic Controller (PLC) based SIL 2 assured / identified components)

Due to the size and complexity of software it is not always practical to completely test every possible permutation of its behaviour within a distributed integrated system, such as a PMS with upwards of 30,000 individual signals. Consequently, should the operating environment change and the software enter a state that has not previously been tested there is a potential that latent errors may be unearthed. To minimise this, recognised good practice should be adhered to.

Finally, control measures should be applied to assess safety impact of modifications to maintain the integrity of modified software, while also managing change through effective configuration management and preserving traceability.

From Def-Stan 00-056 [5] allowing the usage of open standards, alongside NAN 06/2018 [12] advocating the use of recognised good practice for software systems, it can be argued that implementing a commercial safety standard is a viable option to assure the integrity of safety-related systems aboard a Naval vessel. This can be particularly effective where COTS items are used.

4. Why is a safety standard necessary?

Many industries (process, rail and aircraft) have made the move towards having increased levels of automation for greater efficiency, consistency and reduced man-power needed to control systems. Due to the high risk of injury to the public these industries have developed their own standards (IEC 61511 [13], EN 50126 [14] and DO-178C [15]; some from the IEC 61508 [1] parent standard [Figure 5] to design and assure the integrity of safety systems.

http://doi.org/10.24868/issn.2631-8741.2018.017

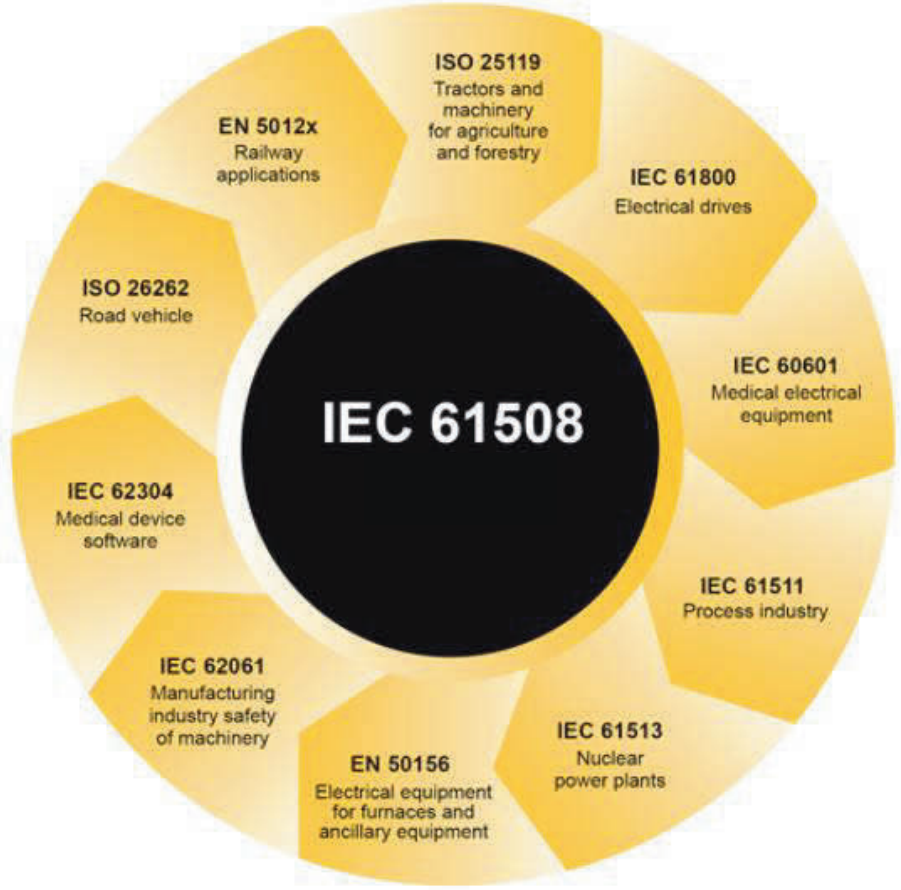

Figure 5 Industrial safety standards derived from IEC 61508 [1][4]

The promise of increased efficiency and cost saving through automation has been applied to many Navies around the globe where there has been a push towards the concept of 'lean manning'. Lean manning involves reducing the contingent of sailors needed to safely crew a ship to increase efficiency, reduce staffing costs (training and maintaining personnel to crew ships is one of the largest expenses facing Navies [16]) and in the case of the Royal Navy, crew more ships with the limited personnel employed. New Royal Navy vessels are designed with this in mind; a modern example being the HMS Queen Elizabeth aircraft carrier which has less than 700 sailors to man the vessel, whilst an American carrier of a similar size needs around 3000 sailors [17].

To achieve these reduced staffing levels, increasing levels of automation with thousands of sensors distributed around the ship give operators based in the control room real time information about the ship's status. They use integrated intelligent systems employing software control and monitoring to process tens of thousands of incoming and outgoing signals for various ship functions such as steering and propulsion. Failure of such may contribute to whole ship hazards. Incidents resulting from failures of these systems can arise from poor safety considerations when designing the systems, or operators not understanding interactions with the automated systems.

Preferably, before incidents increase in frequency or severity, engineered safety using inherent safety controls will become a more important factor in the Marine sector.

5. How is functional safety to be applied in a PMS context?

It is not unusual for a Naval submarine to have a SIL 2 safety-related PMS. These vessels are utilised in dangerous environments with difficult scenarios such as dive operations. For example the hover function is normally an automated operation because it is difficult to control manually. The integrity of such systems aboard a submarine are paramount; especially those denoted as safety-critical. Due to the environment it is utilised in, any failure aboard a submarine could result in a catastrophic[4] accident [18].

[4] Submarines have different Risk Classification Matrices to surface ships for this very reason.

http://doi.org/10.24868/issn.2631-8741.2018.017

Naval vessels can be utilised in harsh environments and with the increasing levels of automation used aboard these vessels, creating a safety-related PMS is a logical progression.

Safety-related systems on these vessels provide an unprecedented challenge in the industry. Some of the trials faced are a complex PMS architecture, managing tens of thousands of signals across a huge platform, keeping data in sync and maintaining high performance of the system.

Automation is ever increasing [Figure 6], so it stands to reason that increased safety engineering is necessary [Figure 7] as marine control systems have a hand in such essential ship services, the integrity of the software and system components involved needs to be adequately assured against functional failures.

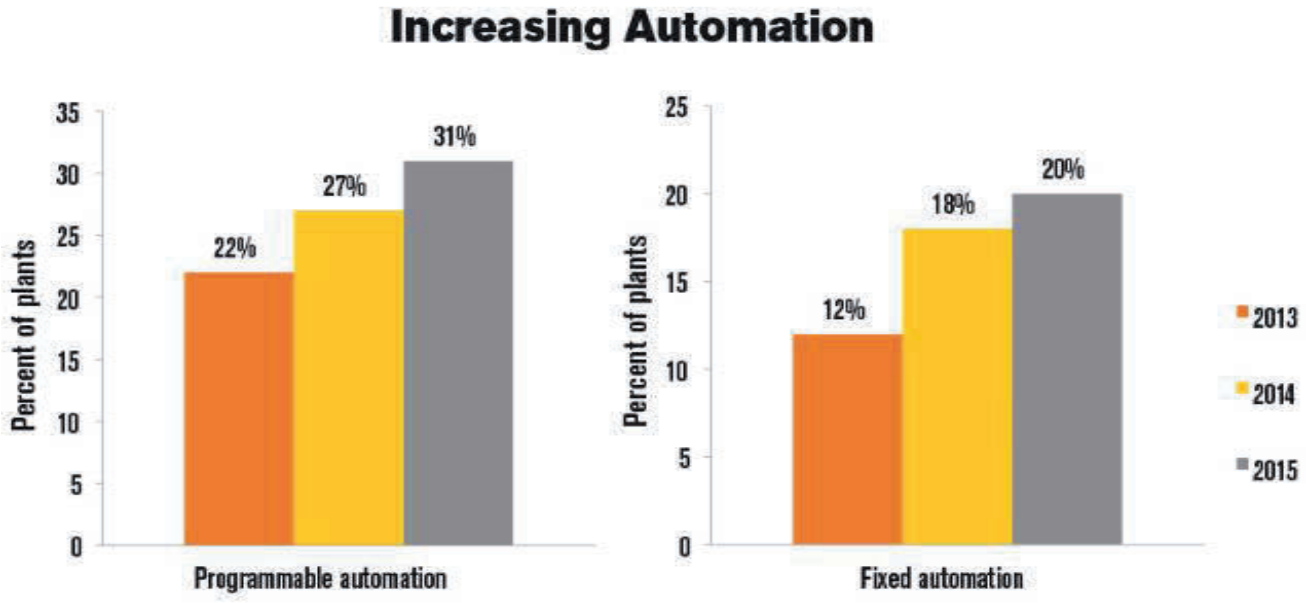

Figure 6 Increased programmable and fixed automation on US assembly lines [19]

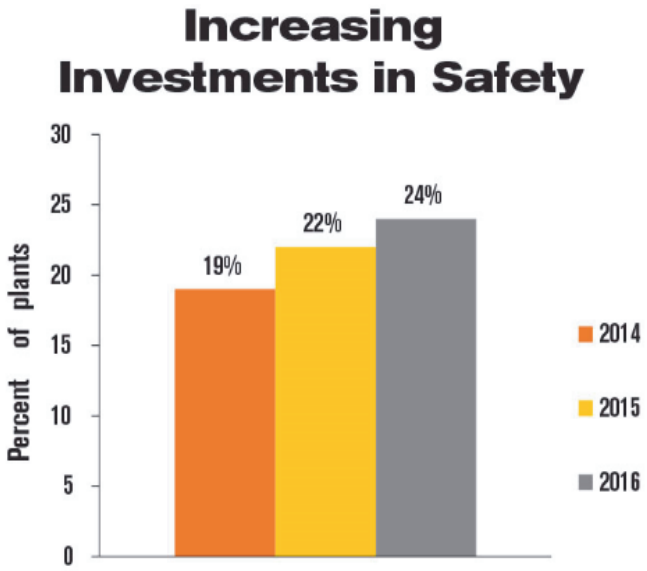

Figure 7 Increasing purchases of equipment to improve safety on US production lines [19]

http://doi.org/10.24868/issn.2631-8741.2018.017

6. How can commercial safety standards be applied?

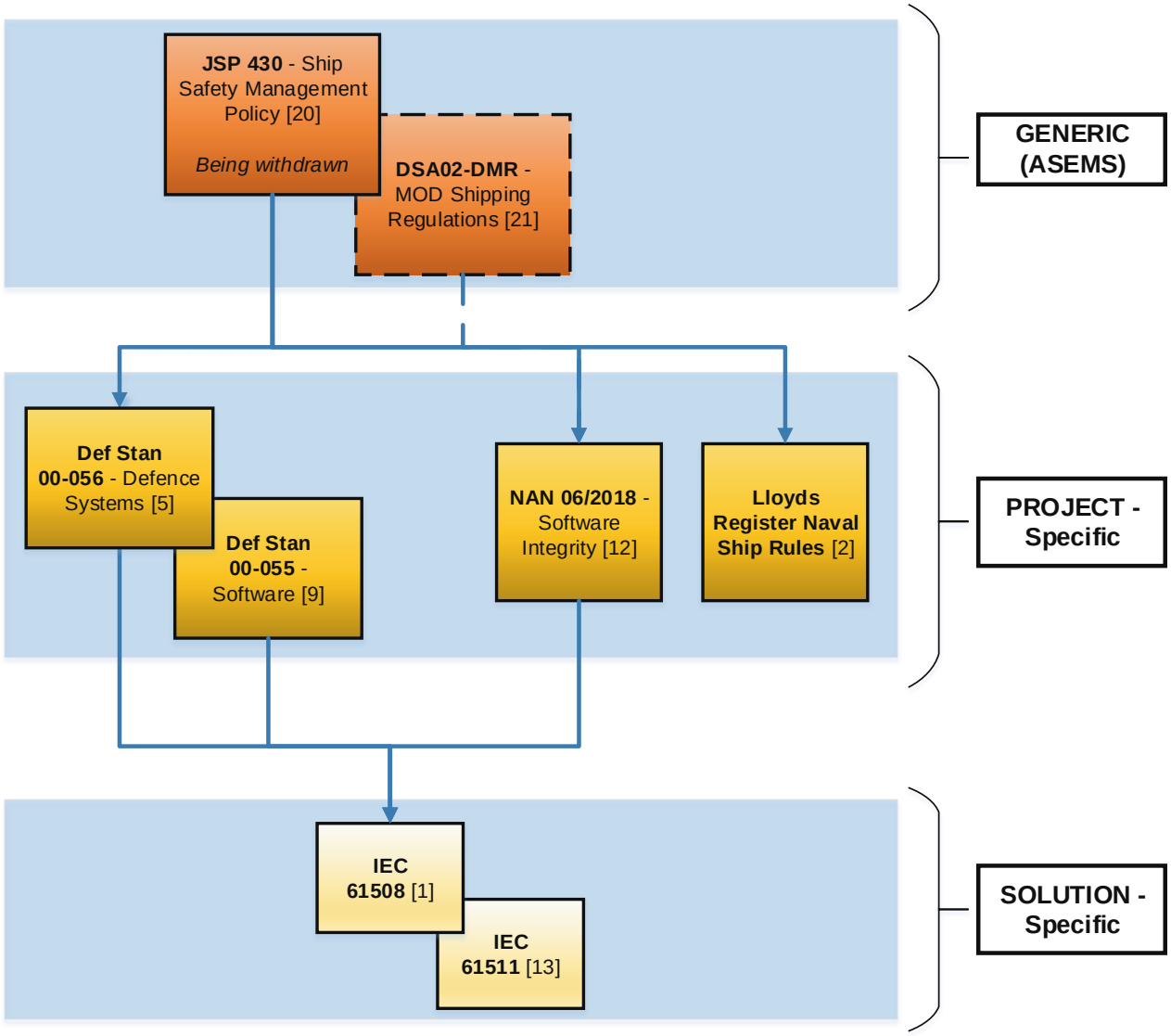

Figure 8 Application of safety standards to a Naval project which includes automation

It is not all plain sailing though. As in all projects, there can be conflicts between safety and security design. This is most simply demonstrated in a fire system for a building. A *safe* system would be one where when the fire alarms are sounded all the fire doors will unlock, but a *secure* system would keep the doors locked at all times.

The continuing move towards utilising COTS equipment and software in safety-critical systems has led to the creation of common vulnerabilities and consequently more well-known weaknesses exist. Due to the common nature of these weaknesses, once one is exposed (e.g. zero-day exploit in windows, exposed by Stuxnet [22]), the system flaw can then be sold online with details of how to initiate an attack, meaning more people can now possess the knowhow and skills to identify and exploit a weak spot in safety-critical systems [23].

Attacks can range from malicious code unknowingly hidden on a Universal Serial Bus (USB) flash drive, which can then compromise a system when plugged into a computer. Other threats can be caused by seemingly helpful actions that have unintended consequences, for example a system component that can be updated remotely from shore. This could potentially halt a ship operation if an update is carried out on the fly without any warning. Generally, remote connections increase the vulnerability for attacks whether intentional or not.

Ultimately, safety is the priority of most systems, but a system cannot be safe without being secure so there is always a trade-off. This usually needs to be carried out on a case-by-case basis between security and safety Subject Matter Experts (SMEs). Early integration of safety and security will allow effective trade-off of safe, secure and reliable operation, ultimately improving the resilience of the end product.

http://doi.org/10.24868/issn.2631-8741.2018.017

7. So what does all this mean?

With ever increasing levels of automation in the Naval industry what will happen when failures occur in the future?

IEC 61508 [1] has birthed subsequent standards for the process, rail and automotive industries who have recognised the increased levels of automation in their industries. For people who are unaware of Marine practices, the common exclamation is “But Naval vessels are dispersed when out at sea so collisions are unlikely!”. This is untrue in busy ports and shipping lanes where there is a large amount of traffic and the relatively fast speeds, but slow manoeuvring capabilities of ships can cause serious accidents [24]. Other infrequent, but dangerous scenarios include Replenishment At Sea (RAS) (transferring fuel, munitions and stores from one ship to another) and helicopter operations.

In conclusion, the manufacturer and end user will incur far higher costs of redesign if changes are identified for safety when the product has reached post-development. If left unchanged, consider the following: If a designed system fails and causes an incident, will the company reputation be tarnished and product orders halt? Remember: If somebody is injured or dies in an accident, any company or individual can be found liable and prosecuted.

If your company does not embrace safety integrity within its culture, you can run the risk of losing credibility and a competitive edge within the marketplace. Consider that your product, a PMS, is being marketed against another. The competitor has developed their system to achieve an appropriate SIL to prevent dangerous or undetected failures in the system. Your product does not offer this qualification and justification. Which one is the customer likely to choose when brand reputation, the environment and ultimately human life can be negatively impacted should a failure occur?

http://doi.org/10.24868/issn.2631-8741.2018.017

8. References

1 IEC 61508:2010, Functional Safety of electrical/electronic/programmable electronic safety-related systems;

2 Lloyd's Register Naval Ship Rules, 2006;

3 Functional Safety, TÜV SÜD. Accessed at: https://www.tuv-sud.com/activity/focus-topics/functional-safety;

4 The Importance of Functional Safety, Lattice Semi-Conductors, Accessed at: http://www.latticesemi.com/en/Blog/2018/02/02/00/07/ImportanceofFunctionalSafety

5 Defence Standard 00-056 Safety Management Requirements for Defence Systems, Issue 7, 28 February 2017;

6 The costs of accidents at work, HSG96 (Second edition) HSE Books 1997, ISBN 0 7176 1343 7.

7 Out of control, HSE, HSG238 (Second Edition), 2003, ISBN 978 0 7176 2192 7.

8 DSA01.1 - Defence Policy for Health, Safety and Environmental Protection Accessed at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/548060/DSA01_Defence_Policy_for_Health_Safety_and_Environmental_Protection-20160804.pdf;

9 Defence Standard 00-055 Requirements for Safety of Programmable Elements (PE) in Defence Systems, Issue 4, 29 April 2016;

10 Acquisition Safety and Environmental Management System (AESMS), Defence Equipment and Support (DE&S). Accessed at: https://www.asems.mod.uk/about-asems;

11 Project Oriented Safety Management System (POSMS), Defence Equipment and Support (DE&S). Accessed at: https://www.asems.mod.uk/about-asems;

12 NAN 06/2018 – Software Integrity Policy, Naval Authority Group, Issue 2.0, February 2018. Accessed at: https://www.nakmo.co.uk/Library;

13 IEC 61511 Functional Safety – Safety instrumented systems for the process industry sector. Series (parts 1 to 3), 2004.

14 BS EN 50126 Railway Applications, the Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), 2017;

15 RTCA/DO-178C Software Considerations in Airborne Systems and Equipment Certification 05 January 2012

16 Optimized Surface Ship Manning, Naval Research Advisory Committee Report. April 2000.

17 'An American carrier of a similar size needs 3000 sailors, HMS Queen Elizabeth will have less than 700', Britain's Biggest Warship – Episode 1, Documentary, BBC, 2018.

18 Argentina's navy searches for missing submarine with 44 crew on board, The Guardian (UK). Accessed at: https://www.theguardian.com/world/2017/nov/17/argentinas-navy-searches-for-missing-submarine-with-at-least-40-on-board

19 ASSEMBLY Capital Spending Report: Capital Spending to Increase, John Sprovieri for Assembly Magazine. Accessed at: https://www.assemblymag.com/articles/93144-assembly-capital-spending-report-capital-spending-to-increase;

20 JSP 430 Ship Safety Management Policy Guidance (to be superseded by [21]);

21 DSA02-DMR – MOD Shipping Regulations for Safety and Environmental Protection, Defence Maritime Regulator (DMR), September 2016. Available from: https://www.nakmo.co.uk/Library

22 An Unprecedented Look at Stuxnet, the World's First Digital Weapon, Kim Zetter, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/;

23 Why We Cannot (Yet) Ensure the Cyber-Security of Safety-Critical Systems, Chris Johnson, University of Glasgow. Developing Safe Systems – Proceedings of the Twenty-fourth Safety-Critical Systems Symposium, Brighton, UK. Feb. 2016;

24 USS John McCain, MEMORANDUM FOR DISTRIBUTION, Enclosure (1) Report on the Collision between USS FITZGERALD (DDG 62) and Motor Vessel ACX CRYSTAL, Enclosure (2) Report on the Collision between USS JOHN S MCCAIN (DDG 56) and Motor Vessel ALNIC MC; Office of the Chief of Naval Operations. Accessed at: http://s3.amazonaws.com/CHINFO/USS+Fitzgerald+and+USS+John+S+McCain+Collision+Reports.pdf;

25 Error Cost Escalation Through the Project Life Cycle. Accessed at: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100036670.pdf

 http://doi.org/10.24868/issn.2631-8741.2018.017

9. Appendix 1

A study carried out by the National Aeronautics and Space Administration (NASA) Johnson Space Centre [25] showed the escalating cost of initial requirements errors found at different stages of the project lifecycle.

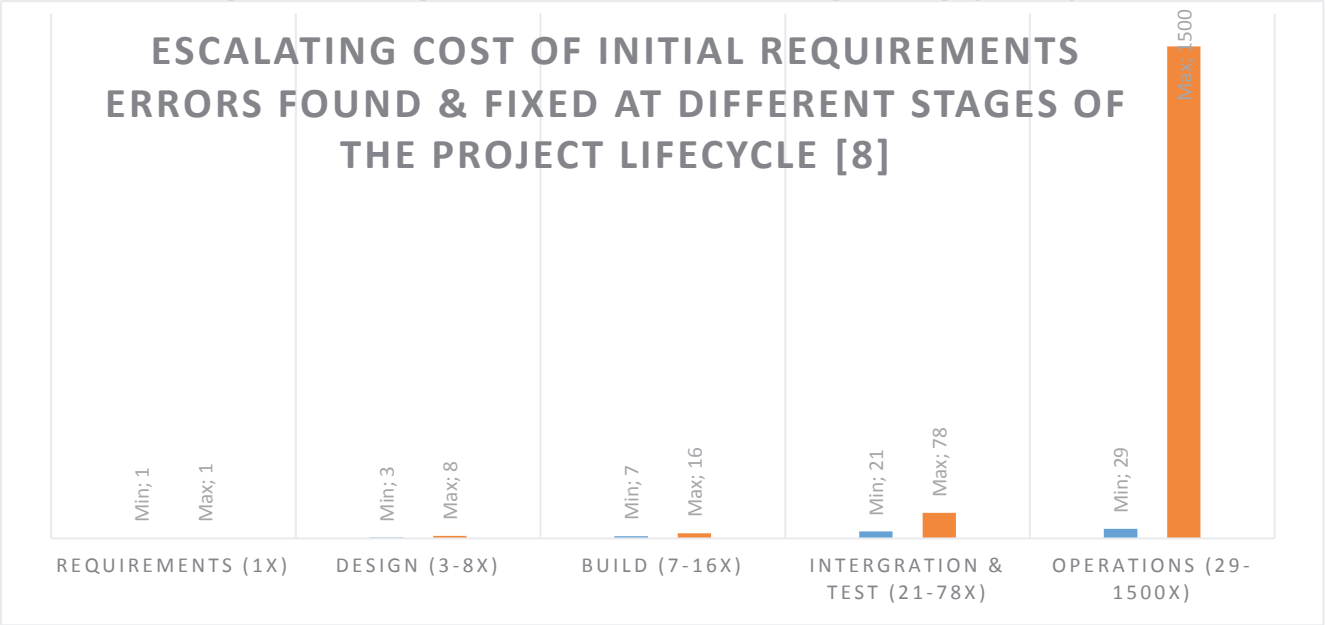

Figure 9 Escalating cost of initial requirements errors found & fixed at different stages of the project lifecycle [25]

http://doi.org/10.24868/issn.2631-8741.2018.017