A PRACTICE MIGRATION STRATEGY TO FACILITATE IMPLEMENTATION OF BS EN IEC 61508 IN THE UK COMMERCIAL MARINE SECTOR

Edward James Shaw

A thesis submitted in partial fulfilment of the requirements of Liverpool John Moores University for the degree of PhD

December 2022

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

In many engineering sectors with the potential to produce major accident hazards in the event of a failure, accepted good practice for implementing functional safety of Safety-Critical Systems (SCS) is considered conformity to the standard IEC 61508. Major accident hazards may potentially occur in the United Kingdom Commercial Marine Sector (UKCMS) in the event of a collision or capsizing of a large vessel, however IEC 61508 is not implemented sector wide.

In this thesis, the International Maritime Organizations (IMO) Formal Safety Assessment is utilised as the framework for a model that determines a series of objectives required to overcome barriers to the implementation of IEC 61508 in the UKCMS. The typical cost-benefit analysis used during a Formal Safety Assessment is enhanced with a Balanced Scorecard (BSC) that assesses the barriers to the standards implementation from perspectives other than financial. The objectives and measures of the BSC are determined using a survey answered by engineers with a range of backgrounds and experience related both to functional safety of SCS in general, and the UKCMS. The rank in terms of importance of each objective, and of each perspective is determined using a fuzzy variant of the Analytical Hierarchy Process (AHP), then the top 25 ranked objectives are chosen for further investigation. The current success of the objectives are determined by investigating their progress relative to their measures. Afterwards, further actions for progressing measures below a certain score threshold are determined. Recommendations for achieving these actions are derived from a survey with experts, which are then used to form a strategy for UKCMS companies to migrate from current practice for implementing functional safety of SCS, to practice that aligns with IEC 61508.

Objectives used in the BSC align with the typical perspectives of a BSC, however this project's first survey indicated the necessity to address regulatory and cyber-security related barriers as well. The validity of the results is measured against their ability to represent the full breadth of the UKCMS, which is dependent on expert participation. The migration strategy provides actions suitable for the current situation regarding conformity to IEC 61508, however the methods used in this project require iteration for continuous use. The methods used in this project and the current iteration of the migration strategy provides a solution for implementing IEC 61508 without a legislative incentive, and may also be useful should the standard be mandated in the future by IMO or a classification society. This thesis concludes with a proposal for the migration strategies implementation and iteration.

DECLARATION

No portion of the work referred to in the thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning.

ACKNOWLEDGEMENTS

Thanks are given to my Director of Studies at Liverpool John Moores University, Dr Ben Matellini, for his guidance and the performed responsibilities of his role.

Thanks are given to the other members of my supervisory team at Liverpool John Moores University, Prof Jin Wang, and Dr Karl Jones, for their continuous aid and their reviewal of my work.

Thanks are given to Prof. Ron Bell for his extensive aid when learning about IEC 61508, most significantly my inclusion on an ESC Ltd. Safety Instrumented Systems course.

Thanks are given to Kenneth Simpson for donating a signed copy of his book “The Safety Critical Systems Handbook”.

Thanks are given to the administrative staff for the Faculty of Engineering and Technology at Liverpool John Moores University for their performed responsibilities related to my PhD, and aid running my extracurricular activities.

Thanks are given to my parents and friends for their support.

Thanks are given to Liverpool John Moores University for their funding of my PhD via my awarded scholarship.

Final thanks are given to Dr Eddie Blanco Davis and Professor Gerasimos Theotokatos for their examination of my Thesis.

ABBREVIATIONS

AHP	Analytical Hierarchy Process
ALARP	As Low As Reasonably Practicable
BOP	Blow Out Preventer
BSC	Balanced Scorecard
BP	British Petroleum
BPCS	Basic Process Control Systems
BSI	British Standards Institute
CAPECO	Caribbean Petroleum Corporation
CCA	Common Cause Analysis
CEN	Comité Européen de Normalisation
CI	Consistency Index
COTS	Compliant Off The Shelf
CR	Consistency Ratio
DAL	Development Assurance levels
DE&S	Defence Equipment & Support
DWH	Deepwater Horizon
E/E/PE	Electrical, Electronic, and Programmable Electronic
ESC	Engineering Safety Consultancy
EUC	Equipment Under Control
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FSA	Functional Safety Assessment
GSN	Goal Structured Notation
HAZAN	Hazard Analysis
HAZOP	Hazard and Operability
HSE	Health and Safety Executive

HSWA1974	Health and Safety Work Act of 1974
IACS	International Association of Classification Societies
IChemE	Institute of Chemical Engineering
IEC	International Electrotechnical Commission
IET	Institute of Engineering and Technology
IHLS	Independent High Level Switch
IMO	International Maritime Organization
ISO	International Standard Organization
KPI	Key Performance Indicator
LR	Lloyds Register
MAIB	Marine Accident Investigation Board
MASS	Maritime Autonomous Surface Ship
MCA	Maritime and Coastguard Agency
MGN	Marine Guidance Notes
MIIB	Major Incident Investigation Board
MOD	Ministry Of Defence
MSC	Maritime Safety Committee
NASA	National Aeronautics and Space Administration
NGO	Non-Government Organisations
OGSM	Objectives Goals Strategies Measures
OKR	Objectives and Key Results
PC	Programmable Controller
PLC	Programmable Logic Controller
PSSA	Preliminary System Safety Assessment
RAF	Royal Air Force
RI	Random Index
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations

SCS	Safety-Critical System
SFARP	So Far As is Reasonably Practicable
SIS	Safety Instrumented Systems
SOLAS	Safety Of Life At Sea
SQEP	Suitably Qualified and Experienced Person
SRS	Safety-Related System
STS	Socio-Technical System
TBS	Target Barrier Survey
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution
UKCMS	United Kingdom Commercial Marine Sector
UNCLOS	United Nations Convention on Law of the Sea
VPF	Value to Prevent a Fatality
VPI	Value to Prevent an Injury

Chapter 1. Introduction

This project concerns the introduction of IEC 61508 to the United Kingdom Commercial Marine Sector (UKCMS). This chapter provides a background regarding IEC 61508, and the UKCMS, to indicate the necessity for its implementation. Also described are the project's aim and objectives, hypotheses, and structure.

1.1 Background

1.1.1 The conception of IEC 61508

Prior to BS 5304 Code of practice: Safeguarding of machinery, first published in 1975 (BSI, 1988), safety integrity of SCS (SCS) in the manufacturing and process sectors relied on qualitative design methods (Bell, 2017). Qualitative design methods measured safety integrity based on the availability of a system to continue operating safely during a failure, i.e., accommodating redundant channels (e.g., multiple valves or electrical contacts operating simultaneously, or to back up a failed channel) in a system, the lower the number of redundant channels, the lower the safety integrity.

Also considered when designing SCS is the recording and consideration of Fault Criteria. This involves setting targets a systems design must meet to avoid a dangerous mode. Fault Criteria introduced the concept of Failure to Safety, meaning to design the system so that failure of its safety functions did not result in a dangerous failure (Bell, 2017).

These methods provided a basis for subsequent standards to provide guidance against random hardware failure. SCS in engineering sectors such as the manufacturing, process oil and gas, and Nuclear sector, increased in scale; and proportionally, so did the risk of major hazards. As a result, it became increasingly difficult to identify the integrity of systems as a whole. The increased scale of SCS also necessitated increased use of Electrical, Electronic, and Programmable Electronic (E/E/PE) functions, thus also increasing the risk of systematic failure of said SCS.

Quantified analysis of safety integrity therefore became considered accepted good practice for determining safety integrity. Among the first to implement the concept of quantified safety analysis were the Heavy Organic Chemicals Division of the Imperial Chemical Industries (Bell, 2017). They developed the analysis techniques required to design safety functions that could satisfy a safety target based in the Probability of Failure On Demand. Safety of Programmable Electronic Systems developed most notably between 1980 and 1998.

From 1980 onwards, major contributions to the foundational concepts of modern accepted good practice for functional safety included a focus on management of functional safety during a systems lifecycle, qualitative safety targets for systematic error, and the concept of a Safety Integrity Level (SIL). Between 1998 and 2000, the International Electrotechnical Commission (IEC) produced the standard IEC 61508 to centralise all the above methods and concepts, along with further development of setting risk targets to consider not only failure rate, but to also take into consideration risks of fatalities (Bell, 2017).

A suitable definition for accepted good practice describes it as a set of working methods that is officially accepted as being the best to use in a particular business or industry, usually described formally and in detail (in this case, as a standard) (Cambridge University Press, 2022).

1.1.2 UK Commercial Marine Sector industries

The UKCMS is defined as a network of connected industries that work together to provide a wide range of services to UK businesses that rely on sea travel (Carnie, 2011). The industries that the Marine Sector consists of include:

- The Shipping Industry, also known as the Merchant Navy, which consists of:
    - Ships that move material resources and products such as tankers and container ships.
    - People transportation and leisure ships such as ferries and cruise ships (not including private yachts).
- The Port Industry, which involves the operation of UK ports, and acts as the bridge between the Marine Sector and other sectors in the UK.
- The Marine Equipment Manufacturing Industry, which involves shipbuilding and ship repair (currently the UK caters predominately to niche high value markets such as superyachts).
- A Maritime Regulatory Framework.

1.1.3 Failure classification

IEC 61508 concerns the management of E/E/PE SCS at all stages of an overall safety lifecycle. Such systems that exist in the UKCMS are therefore the concern of this project. The standard splits failure of a system into hardware (mechanical and structural faults) and systematic (failure of software to return a system into a safe state), and this project goes further by also considering failure due to cyber-attacks.

1.1.4 Marine Accident Investigation Board

The Marine Accident Investigation Board (MAIB) provides overall statistical data regarding accidents in the UKCMS, as well as summaries of accidents and recommendations for the sector to prevent future similar accidents from occurring. Regarding accident investigations that began in 2020, most of them concern vessels grounding and capsizing, resulting in a 2020 recommendation referring to more stringent measures to improve stability (MAIB, 2021).

The MAIB 2019 annual report includes multiple investigation summaries concerning the failure of functional safety systems and failure of safety management systems (MAIB, 2020a). Among the most notable is the inadvertent release of a ‘FirePro’ condensed aerosol from a fire extinguishing system onboard the fishing vessel ‘Resurgam’ In November 2019 (MAIB, 2020b). The resulting MAIB safety bulletin recommended that safety precautions should be taken to avoid similar hazards in the future, stating:

"Prior to intentional discharge of a condensed aerosol system, there should be visible and audible alarms to alert personnel. Checks should also be made to ensure the protected compartment has been evacuated before the system is activated."

and

"When condensed aerosol free extinguishing systems are being installed or maintained the system should be fully isolated to guard against inadvertent activation, non-essential personnel should be clear of the area and an enclosed space rescue plan should be in place."

These recommendations may have been considered were IEC 61508 implemented by merit of its rigorous investigation of sources of hazards at each stage of an assessed systems lifecycle.

The following is an example of how inadequate safety management systems and safety culture can result in a very serious marine casualty. The Olivia Jean, a vessel equipped for dredging the ocean floor for scallops, uses a series of chain dredges connected to a long tow bar that lowers into the ocean, and is dragged for 2 hours before being hauled (MAIB, 2019a). In June 2019, after replacement of two dredges between hauls, one of two safety chains designed to hold the tow bar steady were mistakenly not removed before raising and realigning the tow bar in preparation for casting. These safety chains connected one end of the tow bar to the side of the vessel, so as the bar was hauled, only one end raised. The skipper who was operating the derrick called for the engineer to be ready to unlatch the safety chain once the tow bar was lowered. The engineer positioned himself so that as the derrick lines were slacked, the tow bar swung into him, resulting in a fatal head injury (MAIB, 2019a). An MAIB investigation identified that:

- The deck operations at the time of the accident were not being properly supervised or controlled. The deck crew were working independently of each other and the skipper and engineer both became task focused after things started to go wrong; neither had a full understanding of the situation as it developed.
- Communication on board Olivia Jean was adversely affected by a lack of a common language and a poor level of English language proficiency among the foreign crew.
- The crew did not re-assess the risks of the work required when an unexpected problem had occurred.
- The controls listed in the vessel's risk assessments were not being followed. Had the crew been wearing head protection while working on deck during dredge gear lifting operations, the severity of the engineer's head injuries might have been reduced.
- The vessel's safety management system was incomplete and was not being used or maintained on board Olivia Jean.
- The safety culture across the fleet of fishing vessels managed by TN Enterprises Ltd was weak.

The Work in Fishing Convention Regulations 2018 covers some of the competency requirements set by IEC 61508 (GOV.UK, 2018). Many of the issues listed above however were a result of a partially executed safety management system, which was also out of date. More frequent assessment of the safety management system may have mitigated some of the risks associated with this accident. A

focus on process over safety can be observed in many other accidents that are a result of inadequate functional safety, as seen in the Buncefield Fuel Depot explosion.

The following final example of a UKCMS accident differs from the previous two. They were a result of failed safety systems, and safety management. The following illustrates the danger of operating systems that were designed with inadequate layers of protection against hazards.

MAIB Accident Report No. 9/2021 states the following (MAIB, 2019b):

"On 28 September 2019, a cargo tank containing styrene monomer on board the Cayman Islands registered chemical tanker Stolt Groenland ruptured causing an explosion and fire. The tanker was moored alongside a general cargo berth in Ulsan, Republic of Korea and the Singapore registered chemical tanker Bow Dalian was moored outboard. The ignition of the styrene monomer vapour resulted in a fireball, which reached the road bridge above. Both vessels were damaged, and two crew suffered minor injuries. Fifteen emergency responders were injured during the firefighting, which lasted for over 6 hours. The rupture of the styrene monomer tank resulted from a runaway polymerisation that was initiated by elevated temperatures caused by heat transfer from other chemical cargoes. The elevated temperatures caused the inhibitor, added to prevent the chemical's polymerisation during the voyage, to deplete more rapidly than expected. Although the styrene monomer had not been stowed directly adjacent to heated cargo, the potential for heat transfer through intermediate tanks was not fully appreciated or assessed. Critical temperature limits had been reached before the vessel berthed under the road bridge in Ulsan. The tanker's crew did not monitor the temperature of the styrene monomer during the voyage, and therefore were not aware of the increasingly dangerous situation."

Among the conclusions drawn from this investigation report were that *"calculations to predict heat transfer during cargo stowage planning were not conducted because they were complex and outside the capabilities of the ship operator and the tanker's crew. They were also outside the scope of the cargo stowage software."* In this example therefore the ship suffered from hardware and software failure, as well as lack of competency to identify the major hazard. Accidents similar to this in other industrial sectors have resulted in greater improvement to practise than that of the UKCMS.

Many of the shortcomings of current practice in the UKCMS stem from the fact that historically more robust practice is prescriptive after major accidents occur. Updating of culture and methods tends to come when mandated, or if incentivised (proven to result in financial gain or for competitive reasons). Some marine engineering companies have begun implementing IEC 61508 without mandate external to the UKCMS such as Wartsila. One barrier this project addresses therefore is the means for incentivising the use of IEC 61508 before its inclusion in legislation.

1.1.5 Legacy practice for safety management

Most standards and legislation implemented in the UKCMS are mandated by the Maritime Regulatory Framework, primarily consisting of rules set by the IMO and the UKs classification society Lloyds Register (LR). LR is one of the International Association of Classification Societies (IACS) and confers with other classification societies and the IMO regarding the overall integrity of ships (LR, 2020). Without classification from one of the IACS, A ship cannot verify among other things, their

safety management practice. Unless LR mandate the use of IEC 61508 or similar practice, then there is no legal incentive for UKCMS companies to implement it. The investigation for strategic methods will therefore include means for encouraging change at a legislative level.

1.2 Justification for research

1.2.1 Purpose of implementing IEC 61508

The purpose of IEC 61508 is to facilitate the implementation of a Functional Safety Assessment (FSA) at certain milestones in a SCS lifecycle. The Safety Critical System Handbook describes FSA as a process for conducting the following 7 steps (Smith & Simpson, 2016).

Step 1 involves the setting and verification of the capability of whoever is implementing the FSA. A FSA may be implemented by an individual, an independent department of a company or organisation, or by an independent company or organisation.

Step 2 involves setting a risk target for the assessed SCS. This is achieved by conducting a Hazard and Operability (HAZOP) study to identify hazards the system in question may pose during failure. HAZOP is defined fully in the standard BS EN 61882:2016 (BSI, 2016). Once each hazard is identified, a maximum tolerable failure rate for the system is determined based on the number of individuals exposed to the hazards, and the number of simultaneous hazards that an individual may be exposed to.

Step 3 involves determining the safety related functions of a system. These are mechanisms to prevent a hazard from occurring, or to return a system to a safe state once a hazard has occurred.

Step 4 involves establishing a Safety Integrity Level (SIL). A SIL represents the relationship between the demand of the safety related system (how frequently it may be relied on), and the consequences of its failure in terms of injury or loss of life. There are 4 discreet SILs, a SCS receiving a level 1 SIL has the lowest reliance on its safety related systems, and therefore the rigor of its risk assessments. A level 4 SIL represents a high reliance on safety related systems and the most rigorous risk assessments to maintain a tolerable level of safety integrity.

Step 5 involves modelling the reliability of the safety related system hardware via a quantitative risk assessment. This is done to determine the rate of failure of the safety related system, known as Failure on demand.

Step 6 involves modelling the reliability of the safety related systems software via a qualitative risk assessment. This is done to mitigate systematic errors.

Step 7 involves measuring the failure rate on demand against a rate of failure reduced to As Low As Reasonably Practicable (ALARP). Once the gap between the two failure rates is established, further failure mitigating measures are called for if the failure rate on demand resides above what is considered a broadly acceptable rate of failure.

Each step of the FSA is not unique to IEC 61508, indicated in section 1.1.1 however, the guidance for the frequency at which each of these procedures are implemented is.

1.2.2 IEC 61508s use in major hazard industries

Most major hazard industrial sectors have already implemented IEC 61508. Reasons for shared interest between the UKCMS and other sectors such as the rail or nuclear are primarily the desire to reduce accidents that result in major hazards from occurring (hazards that result in a cost for recovery disproportionally larger than the amount spent on preventing the accident). Where the UKCMS differs from the others is that its regulatory framework does not necessitate as robust a safety management system as that prescribed in IEC 61508 (which is considered accepted good working practice).

1.2.3 Increased use of E/E/PE technology

Legacy practice for functional safety in the UKCMS naturally lags behind accepted good practice, as the former was established before the relatively recent boom in use of E/E/PE technology. While the use of computer technology was increasing in the UKCMS, ships designed without the use of computers were still in service. Ships retrofitted with programmable controllers (PCs) and other electronic systems are unlikely to have had safety assessments equally rigorous as those conducted during IEC 61508s implementation due to the PCs exclusion during the ships early lifecycle stages (when considering the whole ship as a system).

1.2.4 Rise in cyber crime

When computers are used in any industry, they are subject to risks associated with cyber-attacks. Without cyber security adequately addressed during a safety assessment, Ships are at risk of cyber-crimes such as system manipulation via hacking, or a loss of security integrity. IEC 61508 in its current edition when this thesis is published does not address cyber-security, however future editions of IEC 61508 shall consider cyber-security

1.3 Research aims, objectives, hypothesis, limitations, and novelty

1.3.1 Aim

The aim of this project is to produce a strategy for the UKCMS that facilitates migration from current practice for implementing functional safety of SCS, to practice that aligns with IEC 61508. Early studies performed during this project indicate that: full implementation sector wide, without intervention from the maritime regulatory framework, is unfeasible. Value may be derived from the migration strategy by companies and organisations that wish to implement more robust functional safety practice prior to, or during, the potential future legislated implementation of IEC 61508.

The UK marine sector is among the oldest industrial ones world-wide, and relies heavily on legacy practice. This project therefore investigates the gap between current practice for implementing functional safety in the UKCMS, and the guidelines provided in IEC 61508.

1.3.2 Objectives

The first objective for this project is to identify the gap between the UKCMS current practice for implementing functional safety of E/E/PE SCS, and the practice the methods from IEC 61508 facilitates. It is not feasible to fully define practice within the UKCMS; due to the sectors broad range of industries, each with their own technologies, as this would take a very long time. This objective

therefore considers the practice from the whole sector in a generic sense, which in turn should identify analogues in IEC 61508, being a ‘generic’ standard. Current practice regarded by this project involves practice that is either determined via literature (such as practice mandated by legislation described in standards), and practice described by experts in surveys.

Once the gap in practice is identified, the next objective is to then identify the means for bridging the gap. The process for ‘bridging the gap’ will be what is communicated as the migration strategy, and needs to be executable at all levels of the UKCMS (i.e., it should include actions for individuals, whole companies, and whole industries in order to achieve the standards implementation sector wide). This project utilises a structure similar to the Formal Safety Assessment. The first objective covers identification of the gap between current and accepted best practice (barriers to IEC 61508s adoption by the UKCMS). This objective involves an assessment of the gap to determine what is needed to bridge it. This is achieved with a study that results in objectives and measures for overcoming the most significant barriers from different perspectives.

The third objective of the project is to use the migration strategy to communicate recommendations relevant to any of the stakeholders to facilitate IEC 61508s implementation. The strategy will also therefore benefit from a means of iterative development, as recommendations may need to adapt as a company or industry progresses. A BSC is used to communicate identified perspectives, barriers, objectives, and measures. This is followed up by a study to translate the BSC into a list of recommendations for achieving the BSC objectives.

The final objective is to communicate the strategy using a method that all relevant stakeholders may utilise. Clear communication of the migration strategy aids primarily in its assessment during this project, and secondarily in the event that the strategy is adopted post publication of this thesis. The migration strategy involves a clear list of recommendations to be read in tandem with the BSC, and a success map that illustrates the recommended order of completion of the BSC objectives and how they relate to the recommendations.

In summary, the aim is to:

Produce a strategy that migrates current practice for implementing functional safety of SCS in the UKCMS, to accepted good practice, utilising BS EN IEC 61508 as the datum for accepted good practice.

The objectives are to:

1. Identify the gap between current practice and accepted good practice.
2. Identify how to bridge the practice gap.
3. Produce and communicate a migration strategy for the relevant stake holders.
4. Draw recommendations relating to the standards implementation for any stake holder.

The structure of the technical chapters of this thesis, and how their content achieves the aims and objectives are illustrated in Figure 3.

1.3.3 Hypothesis

The following are a set of hypotheses that define the assumptions made during this project.

The process for developing the migration strategy will first yield a profile of weaknesses in current methods and culture that influence the implementation of functional safety of SCS in the UKCMS. This profile may be utilised for attempts to reduce shortcomings in future research.

In stages of this project that require communication with experts for data collection, identification of gaps and bridges will benefit from a multiple perspective approach. This flexibility may be required as to not restrict an expert's contributing knowledge.

Part of the research done in this project will influence the decision regarding the number of actions or tasks the migration strategy will include (the work required to achieve any strategy becomes more difficult in proportion to the number of tasks or actions it includes). Once a feasible number for actions or tasks for the migration strategy are determined, the top corresponding ranked bridging actions will be addressed in the migration strategy. As mentioned previously, a process for iterative review of the strategy may identify new issues (thus further justifying the multi-perspective approach), or increase the focus of current actions.

1.3.4 Research limitations

1.3.4.1 Sources of risk data

Shortcomings are identified during this project in regard to the current methods and culture in the UKCMS, however they require ranking in order to decide which are tackled in the strategy. One such method for quantifying the shortcomings could be to measure relevant failure data, and make a judgement on which are the most pressing based on related fatalities due to system failure, cost for recovery, frequency of failure, etc. In order to gather this data, companies in the UKCSM must uniformly implement a safety management system that gathers the relevant data and publishes it. The researcher was unable to find many sources outside of statistics published by MAIB and other grey literature. Many issues that the strategy tackles rely solely on qualitative data, and require knowledge from within multiple engineering sectors.

1.3.4.2 Access to knowledge concerning the research topics

When qualitative data is required, the researcher is reliant on the participation of experts with strict inclusion criteria. Among the roles of the literature review is to determine where strategies and studies similar to this project have been implemented previously. With this knowledge, the researcher can judge which individuals internal and external from the UKCMS qualify for inclusion in the data gathering processes.

1.3.5 Novelty

The novelty of this project involves investigating the gap between the identified practice for implementing functional safety of SCS (assumed to be current practice), and practice that complies with IEC 61508 (assumed to be best accepted practice). A practise migration strategy is determined

by utilising Formal Safety Assessment with an embedded BSC. The migration strategy results in a list of recommendations, and the order of their execution is illustrated with a GSN success map.

1.4 Thesis structure

The remainder of this thesis includes:

- Chapter 2. A Preliminary Literature Review that investigates the research topics in a generic sense.
- Chapter 3. A description of the chosen methodology.
- Chapters 4 to 8. Execution, description, and discussion of the methodology. As data collection is iterative in this project, some technical chapters include further primary research in the form of focused literature reviews, or further investigation where Experts have recommended topics for reading.
- Chapter 9. A conclusion and recommendations for furthering the areas of research this thesis concerns.

Chapter 2. Preliminary literature review

2.1 Preliminary literature review Introduction

A system considered safety-critical has the potential to cause harm in the event of failure. Harm is physical injury or damage to the health of people or damage to property or the environment (IEC, 2010a).

Safety is freedom from unacceptable risk whereas IEC 61508 defines Functional safety as part of the overall safety relating to the Equipment Under Control (EUC) and the EUC control system that depends on the correct functioning of the E/E/PE Safety-Related Systems (SRS) and other risk reduction measures (IEC, 2010a).

The purpose of this chapter is to:

- Describe IEC 61508s definition for a risk. When a risk is ever referred to during the remainder of this thesis, it uses the definition given in this chapter.
- Describe how other standards have influenced the writing of IEC 61508 and how they have evolved in response to major accident hazards that have occurred. Risks evolve, and often increase in proportion to the size and complexity of SCS, this chapter investigates a few real life examples to justify why the marine sectors standards address this.
- Provide and describe some examples of major accident hazards that were the result of failures that could occur in the UKCMS. This chapter investigates the causes of major hazards, the risk mitigating safety functions available, and if IEC 61508 was implemented, and how it might have reduced the risk of the hazard if it had been implemented.
- Describe the concept of safety targets and how they are related to safety integrity levels as described in IEC 61508. SILs are how the reliance on a system not failing dangerously are communicated, and therefore are well defined in this thesis for future reference.
- Describe the 7 parts of IEC 61508. The standards first three parts provide the guidance for implementing functional safety, while the other 4 parts provide guidance for conformity to IEC 61508. Each part is given a brief description in this chapter, however only the first three parts are referred to during the proceeding chapters.
- Describe the concept of a SCS lifecycle. IEC 61508 is often communicated in multiple ways. Chapter 1 refers to the standard by its FSA. This chapter provides context for its implementation by describing the lifecycle stages of a SCS at which FSA is implemented.
- Investigate and describe examples of SCS and their functional safety assurance framework used in the UKCMS.
- Investigate alternative functional safety assurance frameworks, and to compare them to IEC 61508.

This thesis implements an iterative approach to researching topics outside of IEC 61508. Once the above topics are covered, with the added context provided in chapter 1, a methodology for introducing IEC 61508 in the UKCMS is proposed. Later chapters shall include their own more focussed literature reviews as the IEC 61508 is better understood, and the challenges to its implementation in the UKCMS are identified.

2.2 Risk

According to Part 4 of IEC 61508, the definition of risk is the combination of the probability of occurrence of harm and the severity of that harm (IEC, 2010a).

The failure rate of a systems physical parts cannot be zero as long as they are in use and the rate of failure due to human error cannot be confidently eradicated without the elimination of human interaction with said system (which itself is impossible as a human must be present at least during installation) (Smith & Simpson, 2016). Physical errors occurring in a system has the potential to cause scenarios that incorporated software is not designed to register. Due to these concepts, risk cannot reach zero.

According to IEC 61508, tolerable risk is a level of risk which is accepted in a given context based on the current values of society (IEC, 2010a). Factors that govern tolerable risk include how manageable the consequence of a risk is, the scale of the consequence and the very nature of the risk (meaning how accepting a person is of the risks existence). When designing SRSs, Target risks are determined to achieve a tolerable risk. IEC 61508 defines target risk as risk for a specific hazard taking into account the EUC risk together with the E/E/PE SRSs and the other risk reduction measures. EUC risk being risk arising from the EUC or its interaction with the EUC control system.

2.3 Standards and Legislation

The 1970s witnessed a culture change towards functional safety of systems that involved massive quantities of potentially hazardous material. Typical safety practice back then used to improve in response to an accident, but as industrial plants increased in size and the use of E/E/PE systems became more common, and increased in complexity, so did the scale of the accidents. Large scale accidents eventually triggered efforts to pre-emptively identify potential hazards and quantify the consequences of failure (Smith & Simpson, 2016). Beginning in 1980, and completed in 1987, HSE published the HSE Programmable Electronic Systems Guidelines which were the first set of safety guidelines written by a safety regulator for industrial E/E/PE SRSs. By 1984, the IEC, under the instruction of the British Standards Institute (BSI) Technical Committee, assembled a work group to produce an international standard for safety-critical software. In 1985, the IEC work expanded to include E/E/PE systems as part of the standard, then in 2000, IEC 61508 Functional safety of Programmable Electronics Systems was published and has continually been updated since 2010 (Bell, 2017). This section of the literature review will briefly cover other relevant legislation that IEC 61508 either passively invokes or provides evidence to regulators under conformity.

2.3.1 Health and Safety at Work Act 1974

The health and safety at work act 1974 is the legislation that enforces occupational health and safety in the UK. Originally published on the 31st of July in 1974 it contains four parts. The first part provides rules for the control of substances and emissions harmful to people and the environment. The second part provides rules for employment in the medical sector, the third section includes regulations for buildings and the final part includes further general rules.

Before the publishing of IEC 61508, formal guidance for hazard assessment and doing all that is reasonably practicable, to address major accident hazards in industrial plants came from interpreting section 6 of the Health and Safety at Work Act 1974, which reads (HSE, 1974):

"It shall be the duty of every employer to consult any such representatives with a view to the making and maintenance of arrangements, which will enable him and his employees to cooperate effectively in promoting and developing measures to ensure the health and safety at work of the employees, and in checking the effectiveness of such measures".

2.3.2 COMAH

On the 10th of June 1976, The Icmesa Chemical Company owned chemical reactor plant suffered a ruptured bursting disk, resulting in the release of toxic material in the atmosphere. The nearby Italian town of Seveso suffered widespread illness and 26 women were forced to abort their children due to the contact with airborne toxic material (Lees, 2012). There were deaths in the thousands of flora and fauna in the surrounding area due to being poisoned, followed by the slaughtering of thousands of contaminated animals to reduce further spreading of the toxic material. To prevent a similar catastrophe, the European Commission initiated the Seveso Directive to control major accident hazards from industrial activities (European Commission, 2018). In 1984, the Bhopal Union carbide factory suffered a toxic gas leak, resulting in the death of 5000 people (Cullinan, 2004); this disaster among others caused the updating of the Seveso directive resulting in Seveso II and the introduction of CIMAH in 1984. In 2012, Seveso III replaced Seveso II, updated again to cover accidents that had occurred since Seveso II. This directive introduced COMAH, originally written in 1999 and last updated in 2015 (HSE 2015a).

COMAH regulations enforce the Seveso III directive and guide emergency planning staff and engineers in and outside of industry where major accidents can potentially happen. The COMAH regulations define which substances are dangerous with the Classification Labelling and Packaging regulations, updated as regularly as possible with the Adaptions of technical Progress (HSE 2015b). Complying with IEC 61508 provides evidence to a regulator for hazard assessment as required in COMAH.

2.3.3 Machinery Directive

Introduced in 1989, updated most recently in 2006, the Machinery Directive introduced documented risk analysis as a regulation. Trading and using machinery within the EU requires the machinery to have the CE mark, which acts as a declaration that the manufacturer has followed the Machinery Directive regulations.

Guidelines present in IEC 61508 align with the regulations above, however none of the mentioned regulations require a tolerable risk being set, assessing the safety of systems at the design stage or mandate 'safety-related features' within a systems design (Smith & Simpson, 2016).

2.3.4 BS EN 1050 Principles of Risk Assessment

The Principles of risk assessment was written by the Comité Européen de Normalisation (CEN) in 1996 to provide a standard for risk assessment procedure (CEN, 1997a). The standard requires that

risk assessment for machinery is conducted in a consistent systematic way by factoring the designer's knowledge and experience, and reported past accidents. The standard also introduces the concept of a machine's life cycle, which plays a significant role in IEC 61508. Principles of risk assessment uses a very simple iterative process for improving the safety of machinery, which involves identifying hazards associated with the machinery via a risk assessment, evaluating the safety of the machine then implementing a risk reducing measure and cycling through the process again. The standard does not provide guidance on when the machine is safe enough, instead resorting to a what if method for deriving possible hazards and eliminating every single one. IEC stands out from Principles of risk assessment because of its requirements for tolerable risk targets, and that it seeks to standardise functional safety systems whereas EN 1050 standardises safety of single machines.

2.3.5 BS EN 954-1 Safety of Machinery

Safety of machinery is very similar to the principles of risk assessment; however, it addresses risk reducing measures for control and safety related systems (CEN, 1997b). Safety of machinery includes Principles of risk assessment as one of its normative references. The process lifecycle for achieving safety using this standard includes more steps than Principles of risk assessment (such as categorisation of safety functions and verification steps), making it more similar to IEC 61508, though it does not include methods for reducing risks for programmable logic controllers and therefore requires other standards used in tandem to achieve this.

2.4 Major industrial accidents

The previous section gave details concerning legislative efforts to reduce industrial hazards before the publishing of IEC 61508. Large-scale accidents that occurred in the past triggered global societies interest in improved safety of industrial systems. This section of the literature review gives examples of major industrial accidents, then explains how improved hazard analysis during their design or operation would have reduced the chance of them occurring.

2.4.1 Buncefield fuel depot

On Sunday 11th December 2005, a fuel tank at the Buncefield Fuel Depot overfilled, spilling petrol into the bunding, which resulted in a cloud of petrol vapour engulfing the site (MIIB, 2008). The cloud ignited causing an explosion and fire that spread to 23 other fuel tanks on site and to residential areas within Hemel Hempstead that lasted 5 days.

The explosion and fires destroyed most of the fuel depot and surrounding residential and commercial area. 43 people were injured because of the accident, 2000 people had to be evacuated from their homes and a part of the M1 Motorway had to be closed until the fire was controlled. Smoke from the fire spread into the atmosphere and was blown across much of the south of England.

Safety systems intended to shut off the flow of petrol between tanks to prevent an over-filling scenario, failed during the delivery of a petrol and butane mixture from the Thames-Kingsbury pipeline (fuel intended for aeroplanes refuelling at Heathrow Airport). 300 tonnes of fuel spilled into Tank 912's bund wall, approximately 30 tonnes of which then turned into vapour and drifted over the

top. CCTV and eyewitnesses from onsite staff confirm the existence of the vapour cloud spreading throughout the site. While the specific cause for ignition has not been identified, it is determined that the explosion originated from the nearby Maylands Industrial Estate carpark.

The accident caused varying degrees of damage to properties within a five-mile radius outside of the Buncefield Fuel Depot. Economic damage outside of the cost of repairs to damaged property includes the disruption to business conducted by the 630 companies on the Maylands Industrial Estate ran by approximately 16,500 people. The accident cost local businesses a total of £70 million. Environmental damage further to the fires smoke cloud includes the contamination of soil and water (Lake Buncefield primarily) from the spilt fuel. Chemicals such as Perfluoro-octane-sulfonic acid from firefighting foam, and many other harmful compounds present in released fuels stored at Buncefield polluted the surrounding area in large quantities as well.

There were two safety measures to prevent overfilling of the fuel tanks at Buncefield: a gauge for monitoring the level of the fuel in the tanks and an Independent High Level Switch (IHLS), which cuts the flow of fuel automatically should the fuel level in the tank rise too high (HSE, 2011). The gauge for employees to monitor the level of fuel was stuck the night of the spill; therefore, it did not accurately display the true level of fuel. The IHLS was not installed correctly either; the switch was designed to allow an employee to purposefully lift a checking lever into the 'high level' position to simulate a high level of fuel without cutting the flow, for testing purposes. When the IHLS is in use, a padlock is required to hold the checking lever down to prevent the overriding of the blocking of the flow of fuel. The IHLS was obsolete because the switch did not have the padlock on, and presumably the checking lever was left up.

In August of 2005, the level gauge on tank 912 reported to be unreliable as it was reported to get stuck during use. Management staff responsible for rectifying this failure did not respond sufficiently. The night of the spill, tank 912 accepted fuel from three pipelines, two of which the staff in charge of monitoring the level of the tank could not control. The work culture at Buncefield made process operation a higher priority than process safety, this prevented the safety measures getting the attention they required. Many other factors contributed to the overall failure at Buncefield; however, the following conclusions are drawn.

The Major Incident Investigation Board (MIIB) recommended *"Systematic assessment of SIL requirement"* and *"Protecting against loss of primary containment using high integrity systems"* (MIIB, 2008).

The chances of the accident occurring may have been reduced if the risks were better identified and errors identified in the safety-critical equipment's operation were dealt with properly. Had culture at Buncefield perceived safety as a higher priority than process, the management staff would have dealt with the multiple failures that resulted in the petrol spill. Health and Safety Executive (HSE) and the other organisations that make up the Competent Authority recommend further that an auditing system to test how well the fuel tanks are managed should be put in place, and the inclusion of a monitoring system for the IHSL (Herbert, 2010).

These recommendations are in-line with the guidelines set out in IEC 61508, and the process sector specific version IEC 61511, neither of which were reported to be implemented at the time of the incident. Similar oil and fuel pumping procedures are conducted between ports and ships, and a similar spill and explosion occurred onboard a ship (unnamed) in Baytown Texas in 1974 (Stephens, 1997). Baytown has witnessed more recent explosions at presumably the same oil and fuel pumping facility now owned by Exxon in 2019 (Lozano, 2019) and 2021 (Cole, 2021). Since the Buncefield explosion, research has been done specifically regarding the implementation of IEC 61508 and IEC 61511 to Buncefield fuel depot, resulting in recommendations that align with the comments made in this section (Joosten, 2010).

Despite the strides in practice and technology since then, similar accidents are capable of occurring in the UKCMS, as one did in Buncefield, and in the following two examples.

2.4.2 Deepwater Horizon

On April 20th in 2010, the Macondo Well located 50 miles out to sea in the Gulf of Mexico suffered unintentional release of subterranean oil and gas, which ignited, resulting in the sinking of the Deepwater Horizon (DWH) oilrig and the deaths of 11 men (Sutherland, 2016).

The Transocean oilrig company owned DWH; however, British Petroleum (BP) operated it. The events leading to the accident began with ‘temporary abandonment’ procedures going awry. The purpose of a temporary abandonment of the well is so that another company, Halliburton, could return to it later, to continue oil and gas extraction (BP, 2010). The abandonment procedure involves plugging the well bore with cement and then conducting integrity tests to ensure there is an ALARP risk of spilling once the oilrig is disconnected. Should the cement plug fail during its integrity test, the oilrig has a Blow Out Preventer (BOP) stack to prevent oil and gas rising to the wellhead. The oil spill occurred due to simultaneous errors; firstly, a cement barrier at the bottom of the well had failed its integrity test when the DWH operators believed it to have passed. The Macondo well had another cement plug planned for installation; therefore, the BOP stack was opened to allow mud to be removed. During the mud removing operation, the initial cement plug ruptured. For almost an hour, oil and gas rose up the well without detection resulting in the spill. Spilled oil and gas found a source of ignition causing an explosion. During the spill, the BOP activated but failed to reseal the oil and gas. The total results of the accident include the death of 11 people and the evacuation of 115 staff members and colossal damage to the environment due to 4 million barrels of oil spilled into the Gulf of Mexico and further pollution due to the sinking of DWH (Sutherland, 2016).

After the U.S. Chemical safety and hazard investigation board’s investigation into the accident, the technical factors responsible for the sinking of DWH from the wellhead down begins with failure to manually close the BOP before the oil reached the oilrig. The BOP has an automated mode function that closes the oilrigs blind shear ram during a spill. Two control systems operate the blind shear ram, both of which were mis wired, rendering the blind shear ram inoperable. The drill pipe buckled due to the pressure of the rising oil, preventing the BOP from fully sealing the well. Human error responsible for the accident includes poor decision making regarding the timing of closing the BOP and verifying the integrity of the cement plug and availability of the safety related control systems.

The blind shear ram's specifications did not align with the physical conditions experienced during the spill, resulting in its failure. The designers of DWHs SRSs did not consider human factors.

It is not reported whether or not DWH implemented IEC 61508 or one of its daughter standards, however it would have mitigated the similar draw backs present during the Buncefield explosion. Among the recommendations made by the Resources For the Future (RFF) centre for Energy Economics and Policy are (RFF, 2010):

- Provide stronger incentives for industry to invest in safety, risk reduction, and spill response and containment technologies.
- Reform regulatory structures to adapt to deep water drilling risks.
- Strengthen the oversight capacity of institutions involved in offshore drilling.

If IEC 61508 is not mandated (such as in the UKCMS), then this project shall address the requirement to provide incentives further than legislation. Until IEC 61508 is mandated, it may prove worthwhile to address the route for having it reviewed and considered by the appropriate legislative bodies (IMO and IACS). The third of the RFFs recommendations is addressed by IEC 61508s independence assessment.

2.4.3 Caribbean Petroleum Corporation petrol spill and explosion

On October 23rd 2009, the gasoline tanker Cape Bruny over filled tank 409 at the Caribbean Petroleum Corporation (CAPECO) Bayamón facility (U.S.CSHIB, 2015). The above ground storage tank the ship was offloading into pumped a volume of petrol above its capacity of 5 million gallons into a containment dyke. A cloud of hydrocarbon vapour rose out from the containment dyke and ignited in the wastewater treatment section of the Bayamón facility. The resulting explosion caused tremendous damage to 17 neighbouring tanks and 300 nearby homes. The explosion and a fire that burned for 60 hours caused petrol from damaged tanks to leak into the ocean and soil surrounding the facility. Damage to the Fort Buchanan military base cost $5 million; further costs include the loss of business due to interruption to nearby sea and air transportation. In addition, the Puerto Rico fire department was not equipped to deal with a fire of this magnitude.

The reasons for Tank 409 over filling begins with the tanks level measuring systems not working. A float and tape level measuring apparatus did not accurately display the tanks level on its level side gauge. Knowing this, the onsite operators decided to calculate an approximate duration for the filling procedure based on the petrol's flowrate and the tanks known volume. Petrol pumped from the Cape Bruny had an inconsistent flowrate, rendering the calculation invalid. The tank was not fitted with an independent high-level alarm, meaning there was no form of safely monitoring the level of petrol in the tank. There were not enough lights around the tank for the onsite staff to see the petrol flowing out at night.

This accident involved similar causes and consequences as those present during the Buncefield explosion, whilst also involving a ship and occurring near a port. Recommendations are typically implemented in response to major accidents as seen in the timeline for COMAH. This project regards the examples given in this section and chapter 1 as justification for pursuing UKCMS wide pre-legislated implementation of IEC 61508.

2.4.4 Other significant incidents

The UKCMS has in its history implemented regulatory change in response to major incidents. Possibly the world's most famous marine incident, the sinking of the RMS Titanic, resulted in the forming of the Safety Of Life At Sea (SOLAS) convention. The Titanic sunk as a result of the hitting an iceberg in the Atlantic Ocean during its voyage from Southampton to New York in April 1912 (Ballard, 1987). The collision with the iceberg resulted in breaching of the hull. Compartments between bulkheads were not watertight, resulting in the ship taking on enough water to cause it to sink. The bulk heads were not watertight as a result of them not reaching the top deck, to allow larger hospitality areas for passengers on the upper decks. Also mistakenly decided for the convenience of the passengers were the limited number of lifeboats brought for the voyage, to make space on the top decks. Upon review of the causes for the sinking, and the limited capability of the ship and crew to save the lives of the passengers, the SOLAS convention was produced to mandate minimum standards for safety while at sea (IMO, 2019b).

The fire at Grenfell Tower on the 14th of June 2017 demonstrated how inadequate specification of safety targets during initial design (among other causes), lead to the approval of flammable exterior wall cladding (GLA, 2017). This change in the buildings design was not properly considered in relation to the capability of the towers fire suppression systems (being inside the building, not out). An increased risk of fire when attaching exterior wall cladding was communicated by the Environment, Transport and Regional Affairs Committee in 2000, but was not recognised at Grenfell (Potton *et al*., 2017). Implementing FSA before and after the installation of the wall cladding may have resulted in the identification of the new risks the cladding posed.

The Herald of Free Enterprise capsized shortly after leaving Zeebrugge on the 6th of March 1987 due to the bow doors not closing before beginning its voyage, resulting in water flowing into the vehicle deck and the deaths of 193 people (Sheen, 1987). Recommendations implemented since the incident involved the inclusion of more SRSs, specifically those that monitor bow doors, and alerting crew when they are open. These changes were implemented to all UKCMS roro ferries, demonstrating that the sector is willing to implement change when major hazards occur.

2.5 Safety targets

Safety targets for SRSs are either quantitative or qualitative. A quantitative safety target is when the predicted random failure rate of hardware after the implementation of safety measures is within the tolerable risk target. If not then further redundancy is required. Qualitative safety targets lower systematic failures until they meet the tolerable risk target.

Random hardware failures refer to the failure of components within a system. Component failure is numerically recordable, recorded past random hardware failures can be referred back to hence their use in producing quantitative safety targets. Systematic failures occur due to errors in the design of a system, inadequately addressed modifications to a system or a failure in a systems software. This type of error is unique to its specific system and therefore past failure data usually cannot be used, hence its use when determining qualitative safety targets.

Most modern SCS involve hardware and software in some form. SILs provide single numerical values assigning levels of assurance for systems that have both quantitative and qualitative safety targets. There are 4 levels of safety integrity, SIL1 describes safety integrity that is achievable by following ISO 9001 and by successfully demonstrating functional safety capability. SIL2 involves the same requirements as SIL1 but usually with further testing and reviewing of the SRS. The cost of meeting SIL2 is greater than SIL1.

There is a significant increase in assurance when meeting SILs 3 and 4. Meeting SIL3 usually requires increasing system operator competency and redesigning of the system. SIL4 will require formal methods of implementing safety equipment and high levels of Expertise among system operators, making it the most time consuming and costly SIL to implement.

The SIL a SRS should meet depends on its rate of demand along with a relative failure rate. SRSs that have a high demand rate such as a smoke detector need their rate of dangerous failure measured per hour. SRSs that have a low demand however, such as a sprinkler system, has its probability of failure measured per year.

2.6 IEC 61508 parts

IEC 61508 consists of 7 parts; the first 3 parts are guidelines to complying with the standard, and parts 4 to 7 provide information to aid the understanding and carrying out of parts 1 to 3. Briefly summarised; the purpose of IEC 61508 is to establish a SIL target for a SCS, then to provide a strategy of meeting the SIL target by incorporating safety related equipment into the SCS design (Smith & Simpson, 2016). This section of the literature review will state summarise what each part of the standard includes.

2.6.1 Part 1 General requirements

The first part describes the management requirements for safety-critical systems. Procedures required by the manager of a safety-critical system include the carrying out of a risk assessment both during the SCS design and intermittently during operation in order to meet the systems identified SIL target. While part 4 provides the majority of definitions required to understand IEC 61508, part 1 describe what SILs are along with the importance of hazard analysis. The standard considers Human error when determining SILs by defining competency criteria for operators of SCS in order to meet the required level of safety integrity. The higher the SIL, the more independent the safety assessment of SCS needs to be, requirements for which are covered on part 1 of IEC 61508.

2.6.2 Part 2 Requirements for E/E/PE

Modern computerised safety related equipment comprise of hardware and software, part 2 of IEC 61508 covers the requirements for the hardware. Part 2 also describes the hardware lifecycle, the importance of quantitative reliability assessment, and measures for mitigating random and systematic hardware failure. In order to reach higher SIL levels; layers of redundancy may be required such as architectural constraints, guidelines for these come from part 2.

2.6.3 Part 3 Software requirements

In this part, the software requirements of safety related equipment is given. Part 3 describes systematic failures and provides guidelines for qualitative risk assessment. Tables are used to indicate the suitability of techniques used to comply with the required SIL.

2.6.4 Part 4 Definitions and abbreviations

Part 4 provides the definitions of words, terms, and abbreviations used in the earlier parts.

2.6.5 Part 5 Examples of methods

This part of IEC 61508 consists of seven informative annexes labelled A to G. Annex A describes the importance of risk reduction by employing safety requirements. Annex B describes the methods for determining a SIL target. Annex C provides guidelines for applying ALARP. Annex D gives the method for quantitative determination of a SIL, and Annex E gives the method for qualitative determination of a SIL. Annex F describes the semi-quantitative layers of the protection analysis method and Annex G provides a qualitative method for producing a hazardous event severity matrix.

2.6.6 Part 6 Guidelines on the application of Part 2 and 3

Part 6 of IEC 61508 consists of more informative annexes. Part 6's annexes provide examples for calculating low and high demand hardware failure probabilities, common cause failure, diagnostic coverage, and how to apply software requirement tables for SIL's of 2 and 3.

2.6.7 Part 7 Overview of techniques and measures

The final part of IEC 61508 acts as a reference guide for the techniques and measures explained in all earlier parts. The techniques and measures fulfil the following goals: determining SCSs SIL target, assessing possible random hardware failures, ensuring ALARP is met, architectural assessment, meeting life-cycle requirements and ensuring that a system has the functional capability to achieve these.

2.7 Life cycle approach to safety

IEC 61508 uses a Life-cycle approach for achieving functional safety. A safety-critical system can suffer from failure due to negligent risk analysis at periods other than during operation. IEC 61508 segments the generic life cycle of any E/E/PE safety-critical system into the following stages:

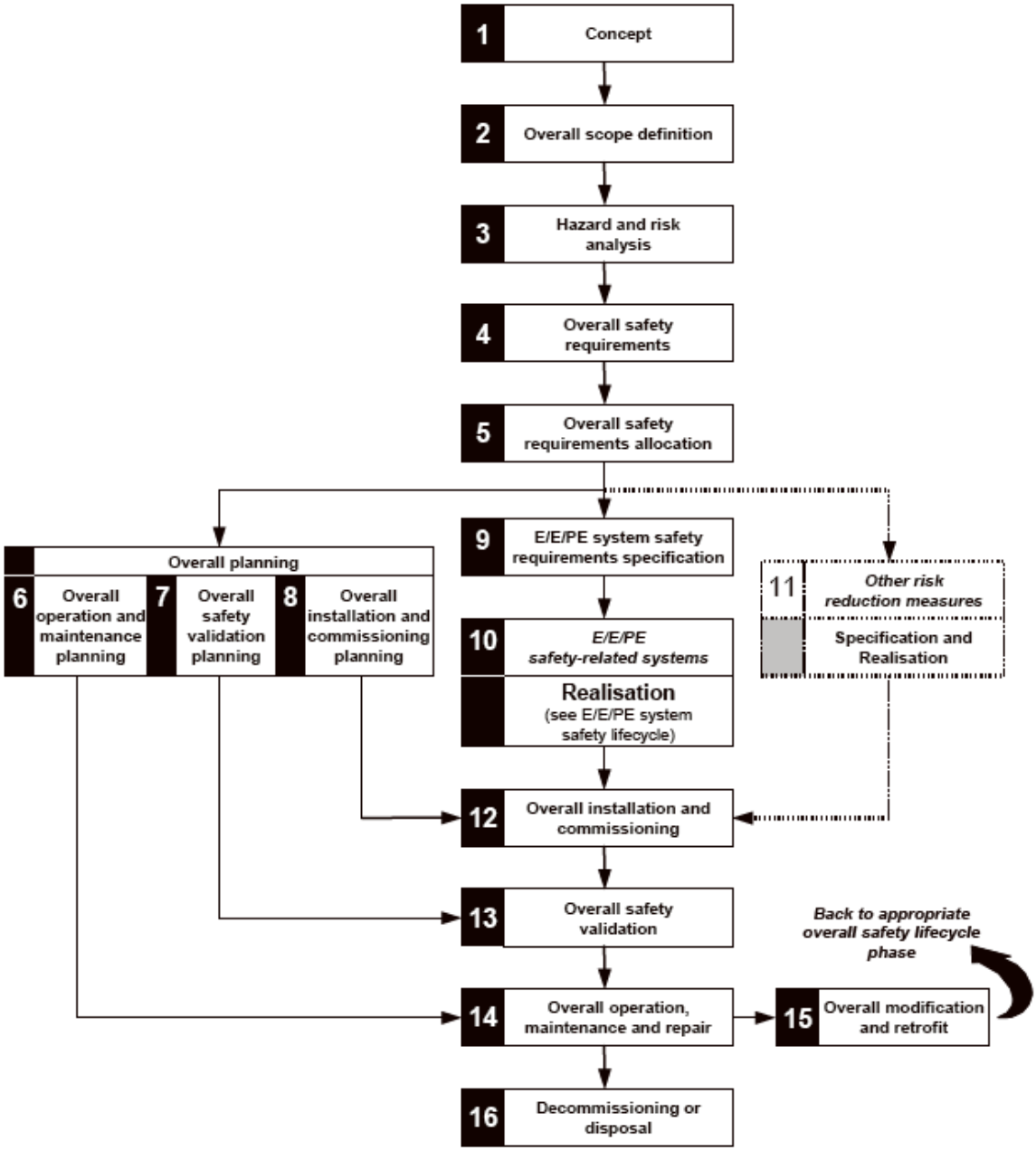


Figure 1 Overall safety lifecycle from IEC 61508 part 1

The concept and scope for a SCS EUC occurs first. At this stage, the concept of a EUCs, boundary and safety requirements are determined as well as the scope for its hazard analysis. Also written at this stage is the safety plan for the EUCs life cycle.

The second main stage of the life cycle is the Hazard and risk analysis, this involves conducting a quantified risk analysis for the EUC.

The Safety requirements and allocations and the Safety specification requirements combined is the next stage of the life cycle. The previous two stages are sequential; however, the third stage addresses or is referred back to for all the following stages of the life cycle. At this stage, the safety functions for the EUC are defined, meaning the hazards that it should protect against (identified

during the hazard and risk analysis stage) are chosen, then a SIL is determined for each safety function depending on its level of risk.

Next come three simultaneous planning activities bound by a single Planning stage, these are the plan for the SCS Operation and maintenance, its Validation, and its Installation and commissioning:

- The operation and maintenance plan revolves around preparing for hazards that occur during an EUCs use. This stage addresses the risks due to Human error and the recording of safety related demands of the system.
- The validation plan accumulates verification evidence to show the meeting of safety requirements for the EUC.
- The installation and commission plan is similar to the operation and maintenance plan due to the human interaction aspect.

Next the safety system physically manifests in the design and build system stage, also known as the Realization stage in IEC 61508.

After the building of the safety system, its Installation and commission stage takes place according to its plan.

An overall validation stage occurs next, just like the previous stage it uses the plan produced in the planning stage. The validation stage requires the successful conducting and recording of tests to prove that the E/E/PE SRSs hardware and software meet their requirements for their target SILs.

The plan for the Operation and maintenance stage gets carried out upon successful validation. Modifications to the SRS if needed occur during this stage as well.

The final stage in a SRSs life cycle is its Decommissioning stage which addresses the hazards involved while disposing the EUC.

There are two stages conducted at multiple points during the safety life cycle. The Verification stage ensures that all previous stages meet their deliverables. The FSA stage tests safety functions to see whether they are meeting the requirements for their specified SIL.

The FSA involves seven steps of its own. Firstly, the assessor is assessed along with the Design organisation if required, this is known as the Functional safety capability step. Risk targets are next set for risks that result in hazards identified from a hazard identification procedure, such as HAZOP. Maximum tolerable failure rates are set after carrying out a quantified risk assessment. The maximum tolerable failure rate is reflective of the maximum tolerable probability of injury due to a hazard.

The next step of the FSA is to choose the safety related functions required to protect against the hazards determined when establishing the SRSs target risk, then the Safety-related functions receive SILs of their own.

Quantitative assessment via reliability modelling for the SRS happens next, followed by a qualitative assessment of the target SILs.

The SRS receives a SIL earlier in the functional safety assessment, however this does not necessarily mean it meets ALARP. Further risk reducing measures get considered in the final step of the FSA to ensure that the risk the assessed SRS is designed to protect against is reduced to an acceptable level.

2.8 Functional Safety Assurance in the UKCMS

The IEEE shares a similar definition for Safety-Critical Systems as the IEC (Knight, 2005), defining them as *"systems whose failure could result in loss of life, significant property damage or damage to the environment."*

Typical examples of a SCS that are found universally in engineering sectors are Fire alarm systems and fire suppression systems. Fire alarm systems involve a device that catches the attention of individuals near by a possible fire using either or both light and sound emitters. Fire suppression systems involve a device that emits a fire suppressant, such as a non-flammable gas or water. Both systems may trigger manually, or automatically by a heat or smoke detector. Should a fire alarm or suppression system fail to activate, the risk of a fire causing harm to a person, or the risk of a fire propagating to cause damage to property or the environment increases, thus they may be considered SCSs.

As ships are large vehicles, most systems related to propulsion and steering may also be considered SCSs. Their failure when the ship is manoeuvring in a busy shipping lane or within a port may result in a collision. A collision may cause harm to individuals should it result in further hazards such as explosions, or capsizing. Most ships carry fuel oil, and other cargo which may be released as a result of a collision and cause damage to the environment. Fires on ships are especially high consequence compared to on-land fires, as the capacity for crew or passengers to retreat from an out-of-control fire and muster at a safe distance requires boarding and launching lifeboats.

Risktec defines functional safety assurance as *"the process by which we ensure that safety-related systems do what we need them to do, when we need them to do it, so that risk is maintained at tolerable levels"* (Risktec, 2022). The HSE states that *"The general benchmark of good practice is BS EN 61508, Functional safety of electrical/electronic/programmable electronic safety related systems"* (HSE, 2022), therefore both Risktec and HSE derive their definitions for Functional Safety from that standard.

The Maritime and Coastguard Agency (MCA) provides *"The safety requirements for systems and equipment that move and control vessels, and make vessels usable for crew, passengers and cargo"* for the UKCMS (MCA, 2012).

The MCA provides guidance for Electrical equipment and installations, Machinery and watertight doors, Boilers, and Propulsion and emergency engines in for form of Marine Guidance Notes (MGN). The MGNs indicate the relevant BSI regulations that a vessel must comply with for the given system.

The HSE, the authority that encourages which standards should be legislated in UK engineering sectors, categorise Safety Instrumented Systems (SIS) (to which functional safety assurance is

applied) into Alarm systems and Basic Process Control Systems (BPCS). The following are the definitions for each type of SIS (HSE, 2022):

"Alarm systems are instrumented systems designed to notify an operator that a process is moving out of its normal operating envelope to allow them to take corrective action."

"BPCS are instrumented systems that provide the normal, everyday control of the process."

The HSE primarily suggest BS EN IEC 61508 as the technical standard to provide functional safety guidance for SISs, however other standards are also suggested such as BS 6739 Code of practice for instrumentation in process control systems: installation design and practice, and BS EN 62682 Management of alarm systems for the process industries. HSE also provides publications relating to Operational guidance, resources, and Information concerning functional safety, among which includes the publication titled Marine risk assessment.

The UKCMS must comply to the regulations set by the IMO when conducting functional safety assurance. IMO uses the Maritime Safety Committee to determine the appropriate safety-related international regulations. The Maritime Safety Committee is divided into Sub-Committees. The Ship Systems & Equipment sub-committee determine the practice for assuring *"life-saving equipment, appliances and arrangements; and fire detection and fire extinguishing systems"* for all types of vessels globally (IMO, 2019).

LR rules and regulations state (LR, 2020):

"It should be appreciated that, in general, classification Rules and Regulations do not cover such matters as the ship's flotational stability, life-saving appliances, and structural fire protection, detection and extinction arrangements where these are covered by the International Convention for the Safety of Life at Sea, 1974".

LR rules and regulations do however state specific standards that conformity to provides evidence that the rules and regulations are satisfied. For E/E/PE SCS, LR consider conformity to ISO 17894, Ships, and marine technology - Computer applications - General principles for the development and use of programmable electronic systems in marine applications as evidence that a ships SCS meet their rules and regulations.

IMO state regarding SOLAS (IMO 2019b):

"The main objective of the SOLAS Convention is to specify minimum standards for the construction, equipment and operation of ships, compatible with their safety."

It is assumed that functional safety practice in the UKCMS complies with practice mandated by SOLAS. SOLAS provides goals for safety, however, is does not specify methods with which to achieve said goals. For example: Chapter II-2, Regulation 5, Section (ii)(1) states *"In passenger ships carrying more than 36 passengers, each of the required fire pumps shall have a capacity not less than 80 per cent of the total required capacity divided by the minimum number of required fire pumps and each such pump shall in any event be capable of delivering at least the two required jets of*

water. These fire pumps shall be capable of supplying the fire main system under the required conditions" (IMO, 1974). Each of the required parameters are provided earlier in the chapter.

Practice for assuring SCS in the UKCMS whilst also complying with all rules and regulations in summary involves:

- Complying with ISO 17894, Ships, and marine technology - Computer applications - General principles for the development and use of programmable electronic systems in marine applications to satisfy the LR Rules and Regulations for Classification.
- Complying with The International Convention for the Safety of Life at Sea 1974 to satisfy the LR Rules and Regulations for Classification set by the IMO.
- Complying with the relevant BSI standards indicated by the Marine Guidance Notes from the MCA.

Further guidance is provided by publications and standards suggested by the HSE such as the Marine risk assessment. This is considered the minimum required practice; however, this does not mean that all UKCMS only follow this practice.

2.9 Other Functional Safety Assurance Frameworks

BS EN IEC 61508 is considered accepted best practice for assuring safety of E/E/PE SCS for its satisfaction of other standards, and the method of setting SIL goals then doing all that is reasonably practical to achieve them during a systems life cycle. This ensures that a system remain tolerably safe throughout its entire life, even if technology and its capability for causing harm during an accident surpasses the consideration of the current mandated standards. The following are alternative safety assurance guidance and standards, and a discussion of what they do and do not provide compared to IEC 61508.

2.9.1 ARP4761

ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment is the guidance recommended by the Society of Aerospace Engineers, for the purpose of assuring aircraft functional safety systems (SAE, 1996). Similar to IEC 61508, It utilises a Safety Life Cycles which involves the following steps:

1. Functional Hazard Assessment (FHA) during aircraft hardware development.
2. System level FHA during development of aircraft software, and a Common Cause Analysis (CCA).
3. Preliminary System Safety Assessment (PSSA) during development of the aircraft architecture, and updating the CCA.
4. Iterate the CCA and PSSA as the system is allocated hardware and software components.
5. Further System Safety Assessments during system implementation, and completion of the CCA.
6. Check to see that the results of the CAA satisfy the standards 14 CFR 25.1309 and CS–25.1309 (airworthiness regulations).

The life cycle above differs from IEC 61508s Safety Lifecycle in multiple ways, notably how it does not include continuous safety integrity checks past implementation, which IEC 61508s FSA does. ARP4761 as a standard differs from IEC 61508 as its focus is identification of hazards, and designing them out, whereas IEC 61508 designs systems to fail at a tolerable frequency or with tolerable consequences. The FHAs determine Development Assurance levels (DAL). DALs classify risk consequences and frequency per flight hour, and are referred to in both Americana and European airworthiness regulations. This is appealing to engineers and aircraft owners who can consequently be clear when demonstrating compliance regardless of the location of the aircraft.

The PSSA and the CCA result in a list of identified and mitigated hazards drawn from the design and implementation of an aircraft, which can be measured against the relevant airworthiness regulations. If an aircraft cannot demonstrate conformity, recommendations may be drawn to bridge the gap. ARP4761 being an aeronautical engineering standard cannot be directly implemented in other engineering sectors, however ARP4761 uses many methods utilised in other engineering sectors and may be used in IEC 61508 such as FTA and FMEA. ARP4761 also does not reduce risks to ALARP as the judgement for which DALs are acceptable, and the budgets for risk reduction are prescriptive, and found in other standards.

2.9.2 ISO 14971

ISO 14971 Medical devices Application of risk management to medical devices is a 9 part standard that lays out a lifecycle involving (ISO, 2021):

1. Risk analysis
2. Risk evaluation
3. Risk control
4. Evaluation of overall residual risk
5. Risk management review
6. Production and postproduction activities

Risk analysis and evaluation involves identification of hazards with a significant focus on human error and misuse of medical equipment. Risk control options therefore apply inherent safety by design to the design and implementation of medical devices, which are often required to maintain or improve the health of patients. Examples of inherent safety designed into medical devices include where possible the removal of elements of a device and its controls that could be misused, and the addition of automated functions to reduce human error. Residual risks once reviewed during production and implementation of a device involves the addition of safety guards around mechanical systems where dangerous interaction could cause injury, and alarms in the event of a fault. These approaches are suitable for systems that are not at risk of damage from environment, and are therefore not designed with the intention of receiving ‘non-sterile’ maintenance. Medical devices differ significantly from SCS on ships as they are more easily replaced, especially compared to a vessel at sea, which needs to be designed with the capability for repair and maintenance designed in (which inherently makes the crew vulnerable to the hazards involved).

ARP4761, ISO 14971, and other safety assurance frameworks provided in standards such as MIL-STD-882E, and the daughter standards to IEC 61508 tend to provide engineering sector specific

practice (Bolbot et al., 2019). Practice that ultimately demonstrates compliance to engineering specific mandated legislation. IEC 61508 is chosen in part as practice for the UKCMS to migrate to as it is applicable to any engineering sector. The existence of IEC 61508s daughter standards could indicate the desire to implement practice that aligns with the original standard in other engineering sectors.

An advantage of implementing an engineering sector specific safety assurance framework is the confidence that they may provide by having prescribed safety goals which may be demonstrated via quantitative analyses. IEC 61508 sets its own goals, and permits multiple routes for meeting those goals, which may cause a lack of confidence by SCS owners.

Chapter 3. Methodology overview

This chapter describes a process of integrating techniques for standard scrutiny, vision communication and implementation, and semi-quantitative data collecting, in order to produce a strategy for aligning the practice for implementing functional safety of SCS in the UKCMS with accepted good practice.

3.1 Methodology introduction

The purpose of this chapter is to provide a description, background information, and justification for each process used for this project's methodology. The project uses Formal Safety Assessment as a foundation for its framework. A BSC is embedded into the Formal Safety Assessment in order to expand upon its assessment stages by including a multi-perspective approach. Decision making regarding the content of the BSC is based on the results of a fuzzy variant AHP, produced using comparison matrices filled in by Experts. Goal Structured Notation (GSN) is used to illustrate the strategy, then Experts are consulted to rate the feasibility for each of the strategies objectives, based on its measures. The final stage of the project involves analysing the validity of the strategy, and drawing recommendations for the UKCMS regarding steps required to implement IEC 61508, and for improving the strategy.

3.1.1 Definition of an Expert

The project methodology requires participation from individuals often referred to as Experts in its interviews and surveys. This thesis defines an Expert as an individual who reached a senior position during a career that provided said individual a professional background and experience relating to one or more of the following areas:

- The UKCMS and or its regulatory framework.
- Functional safety of SCS in other engineering sectors.

For the purpose of personal data protection, individual Experts are referred to with pseudonyms.

3.2 Methodology components

The purpose of this section is to describe the individual methods used in the overall methodology for producing a strategy that facilitates the implementation of IEC 61508 to the UKCMS.

3.2.1 Formal Safety Assessment

The backbone of this project's migration strategy resembles the IMO's Formal Safety Assessment.

IMO describes Formal Safety Assessment in its mission statement as *"a rational and systematic process for assessing the risks associated with shipping activity and for evaluating the costs and benefits of IMO's options for reducing these risks"* (IMO, 2019e). It can be used as a tool to help evaluate new regulations or to compare proposed changes with existing standards. It enables a balance to be drawn between the various technical and operational issues, including the human element and between safety and costs. The IMO states also that *"(Formal Safety Assessment) was originally developed partly at least as a response the Piper Alpha disaster of 1988, when an offshore*

platform exploded in the North Sea and 167 people lost their lives, and is now being applied to the IMO rule making process"

Sections 1.1.1 and 1.1.2 of the 2018 version of Revised Guidelines for Formal Safety Assessment for use in the IMO Rule-making Process state the following (IMO, 2002):

1.1.1 Formal Safety Assessment is a structured and systematic methodology, aimed at enhancing maritime safety, including protection of life, health, the marine environment, and property, by using risk analysis and cost-benefit assessment.

1.1.2 Formal Safety Assessment can be used as a tool to help in the evaluation of new regulations for maritime safety and protection of the marine environment or in making a comparison between existing and possibly improved regulations, with a view to achieving a balance between the various technical and operational issues, including the human element, and between maritime safety or protection of the marine environment and costs.

Regarding Formal Safety Assessments application, section 1.3.1 states:

The Formal Safety Assessment methodology can be applied by a Member State or an organization in consultative status with IMO, when proposing amendments to maritime safety, pollution prevention and response-related IMO instruments in order to analyse the implications of such proposals.

Section 3.1.1.1 states the 5 steps of Formal Safety Assessment:

3.1.1.1 Formal Safety Assessment should comprise the following steps:

1. *Identification of hazards.*
2. *Risk analysis.*
3. *Risk control options.*
4. *Cost-benefit assessment; and*
5. *Recommendations for decision-making.*

The identification of hazards may be replaced with an investigation into reasons why IEC 61508 currently is not implemented. The corresponding analysis and control options stages shall be enhanced using the BSC process. The cost benefit analysis shall accommodate all perspectives of the BSC, and recommendations for decision making will remain comparable to a standard Formal Safety Assessment.

3.2.2 Balanced Scorecard

Dr Robert Kaplan and Dr David Norton devised BSC in 1992 as a means for introducing changes to management (Bourne & Bourne, 2007). The basic principles of the BSC begins by determining a specific 'vision' a company wants to see completed, then translating this vision into a number of easy to understand goals. Each goal, referred to as an objective, has a series of measures to measure its success. A company's reason for making changes are typically due to financial incentives, however the chances for successful implementation improve when other non-financial factors are considered. These are the company's relationship with their customers, its internal processes and the company's

future learning and growth (Kaplan & Norton, 2007). Therefore, a BSC balances measures for accomplishing its goals between the following four perspectives:

- Financial
- Customer
- Process
- Learning

The purpose of embedding a BSC into the Formal Safety Assessment method is that Formal Safety Assessment measure control options are based on a cost benefit analysis.

The feedback from the first survey of this project suggested that organisations in the UK marine sector do not conform to IEC 61508 chiefly because there is no legislative incentive to do so, therefore business owners do not wish to spend the money and resources doing so. This however suggests that there are further under lying issues to overcome before proposing a means for the standards implementation, including knowledge of the standard and its benefits (such as the potential for saved costs in the future should an accident occur and improved safety for E/E/PE systems).

A BSC is a multi-perspective vision implementing tool that typically consists of three tiers. The top tier represents the vision, which is a goal an organisation wishes to accomplish. This project's BSC includes four tiers, the second of which does not normally feature in a BSC, necessitated by the barriers to the vision. The third tier defines objectives to satisfy the vision, from the perspective of overcoming each barrier. The fourth tier defines methods for measuring the success of an objective. Users of the BSC may assess the objectives via their measures, and identify actions required to satisfy the vision.

The advantages of embedding a BSC for implementing a standard is that it simultaneously measures not only the financial impact, but also the effects to customer reputation, the internal processes and the learning and growth of an organisation or sector. Using a BSC facilitates the non-financial challenges for implementing IEC 61508 to the UKCMS. This framework proposes using the BSC method to replace the typical 3rd and 4th stages of Formal Safety Assessment, resulting in the 4th stage to expand by considering 4 or more perspectives rather than just financial.

Formal Safety Assessment is chosen to address the barriers to IEC 61508s implementation in the UKCMS as IMO utilises Formal Safety Assessment when introducing new standards to its rules and regulations (IMO, 2019e). Step 4 of a Formal Safety Assessment is a cost-benefit analysis. The scope and method for conducting a cost-benefit analysis for a Formal Safety Assessment are provided in chapter 8 of The Guidelines for Formal Safety Assessment for use in the IMO rule-making process. Implementing Formal Safety Assessment as described in its April 2018 revision measures the costs of control options against the ability of a given assessed standard to protect an interested entity (IMO, 2018). As the argument of this projects assessment concerns barriers to a standards implementation, rather than its cost, an alternative to the traditional cost-benefit analysis is proposed.

BSC is proposed as it can address the barriers from multiple different perspectives other than the relationship between finance and risk, and extracts from the chosen perspectives Key Performance Indicators (KPI). These KPIs can be translated into objectives and measures, which in turn facilitate

goals that a strategy can work towards. As a result of BSC using multiple perspectives, it is not straight forward to measure the significance of barriers observed from different perspectives. It is also unfeasible to quantify every KPI. A BSC requires continuous monitoring and updating, which may be unfavourable by some organisations to invest time and resources into (Wright, 2022).

Since the creation of BSC in 1992, many other strategic planning methods have come about, such as methods named after their stages like OGSM (Objectives Goals Strategies Measures) (Archpoint, 2019) and OKR (Objectives and Key Results) (Van Der Pol, 2018). These both align with BSC as they determine objectives based on indicators of a vison's success, however they take different routes to determine these. Companies such as Anheuser-Busch, Panasonic Eco Solutions, and the Centres for Disease Control and Prevention (CDC) have used OKR for its direct approach to determining objectives to achieve a vision by merit of its speed and ease of comprehension (this is important for communicating strategies to the layman, such as the general public). OGSM was a potential option as it also provides concise strategic goals for a vision, and facilitates long term planning. Similar to OKR, it does not draw objectives from set perspectives, which aids in its comprehension of results by others unfamiliar with the process.

BSC is chosen over these alternatives still, as they both represent an amendment to the core BSC process in order to make it faster and easier to understand the results to individuals unfamiliar to the process. These qualities are not as necessary in this projects context as its strategy is for use by individuals in an engineering sector who are likely to understand the process better than the general public. Similar to the example alternatives, this project does adapt the BSC also by adding two more perspectives, which addresses a criticism of BSC provided when comparing its base process against further, tailored alternatives such as Triple Bottom Line Scorecards (Ndzomga, 2020). The desirable quality of a traditional Balanced Scorecard is its multi perspective that most alternatives aim to design out for the sake of brevity.

An alternative method that does include the multi perspective that was not considered until too late into the project is the socio-technical system.

A socio-technical system is a system regarded as two parts, or sub-systems: a social sub-system and a technical sub-system. Each part is sub divided into two parts. The social sub-system concerns the structure of the system (the organisations culture and goals), and the people or actor in the system (human resources and the efficacy of their communication and relationships). The technical sub-system concerns the systems physical capability or technology (hardware, software, and knowledge and skills of operators), and the systems tasks (procedures, workflow, rules). Understanding a sociotechnical system means acknowledging that each of the technical and social components of the entire system influence each other.

The classic BSC and the STS share a four pointed structure, and that each point influences change in the others. A typical BSCs focus is driving financial growth whilst observing the other perspectives. The focus of this project however is driving change to process (implementation of functional safety systems). Monitoring of people comes under the 'People' system, and concern for regulations would feature in the 'Tasks' system.

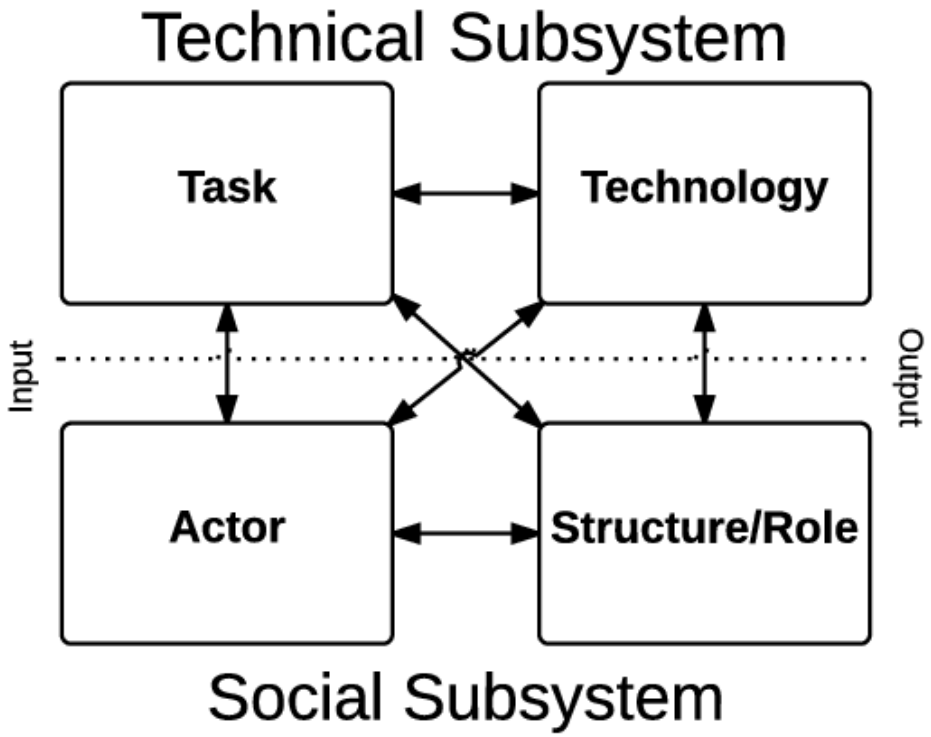


Figure 2. Socio-technical system (Brauner, 2016).

3.2.3 Analytical Hierarchy Process

The AHP is a method for prioritising elements of a multi-variant argument by providing weights for each element.

The AHP involves the following steps (Saaty, 2008):

1. Define the problem and determine the kind of knowledge sought.
2. Structure the decision hierarchy from the top with the goal of the decision, then the objectives from a broad perspective, through the intermediate levels (criteria on which subsequent elements depend) to the lowest level (which usually is a set of the alternatives).
3. Construct a set of pairwise comparison matrices. Each element in an upper level is used to compare the elements in the level immediately below with respect to it.
4. Use the priorities obtained from the comparisons to weigh the priorities in the level immediately below. Do this for every element. Then for each element in the level below, add its weighed values and obtain its overall or global priority. Continue this process of weighing and adding until the final priorities of the alternatives in the bottom most level are obtained.

The first stage of the project involves determining the barriers to the standards implementation, however the BSC has a maximum capacity of barriers to tackle if it is indented to be feasible. The AHP is employed during as a means to determine which barriers represent the most friction to IEC 61508s implementation to the UKCMS. The barrier identification stage serves to satisfy the first stage of the AHP as defined by Saaty. The elements of this project's AHP are determined via a literature review and structured interviews with Experts whose backgrounds range from engineers from various companies from within the marine and naval sectors, as well as engineering safety consultants and legislators.

There exists an inconsistency between the definition of words used when talking about BSCs and the AHP. An objective in the BSC refers to a measurable procedure towards accomplishing the vision, however the objectives in the AHP refer to the identified barriers.

Nomenclature aside, the hierarchy of the decisions in Saaty's definition of the second stage of the AHP aligns with the hierarchy of the BSC. Under the vision, the AHP exists to rank the perspectives used in the BSC, then rank the barriers under each perspective. No intermediate levels are used in the AHP, as they would manifest as the objectives as defined in the BSC. The BSC and the AHP cease to align at this point, and it is here that the results of the AHP serve to determine barriers that require objectives for the BSC.

The pare wise comparisons referred to in step three consist of a matrix for the BSC perspectives definitions, and a separate matrix for each set of barriers categorised by each perspective. The method for accomplishing step four is described in the context of the barrier measures results and discussion.

The AHP has been used in the past to produce a model that ranks the cost effectiveness of safety measures to combat vessel collisions, mainly by combatting human error (Wang *et al.,* 2012). The AHP is used here to supplement a Bayesian network with semi quantitative data, so that the model user may best judge which safety intervention methods to implement. A similar model provides a decision route for investigating human organisation factors using the same method (Wang *et al.,* 2011a). The similarities of these models, and the methodology of this project, is that the AHP is integrated into another modelling technique in order to feed it semi-quantitative data that is usually difficult to obtain.

An alternative multiple-criteria decision-making method to AHP is the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) method. The following is a brief description of the TOPSIS method (Yatsalo, 2020):

1. Produce a decision matrix measuring multiple options for a decision, against criteria concerning the benefits or costs of a decision. These are normally assigned a single value; however, a set of fuzzy values may be inserted.
2. Normalize the criteria values using a value normalizing equation.
3. Calculate a weighted normalized decision matrix.
4. Determine the ideal and anti-ideal solutions.
5. Calculate the distance between the ideal and anti-ideal solutions.
6. Determine a relative coefficient of closeness between each decision option.
7. Each decision option may then be ranked based on their relative coefficient of closeness. The highest ranking decision may be considered the best option.

In summary, TOPSIS ranks decision options by comparing them against weighted criteria. Decision options that satisfy the most or the higher weighted criteria ultimately receive the higher ranks when their coefficient of closeness is calculated (Ayag, 2021). TOPSIS is therefore a useful multiple-criteria decision-making method when the criteria for which decisions to make are predetermined.

AHP ranks decision options by comparing the decision options between each other and choosing which is more important or preferred. Fuzzy number sets can be implemented by changing the binary decision of which option is better, into a subjective preference communicated via a linguistic term (such as a strong or weak preference when comparing two options). AHP is as a result vulnerable to inconsistent answers, however the consistency of answers can be calculated. AHP is a preferable method for use in the TBS as the criteria for options for implementing IEC 61508 to the UKCMS was not investigated. Instead, barriers to the standard are chosen for adoption by the BSC. The TBS AHP requires comparison of barriers within a BSC perspective, however the perspectives themselves were also ranked. The relative simplicity of AHP compared to TOPSIS is also preferred for the purpose of easier repetition of the whole project's methodology.

Other alternative multiple-criteria decision-making methods such as Grey relational analysis, and Preference ranking organization method for enrichment of evaluations, share the criteria ranking quality of TOPSIS. Application of these methods are therefore not desired in this project for the same as TOPSIS.

3.2.4 Fuzzy set theory

AHP translates linguistic terms of importance into numerical values, converting a qualitative date set to a semi-quantitative data set. The difference between a linguistic term and a number however is the range of values each represent. A number has a single set value, but a linguistic term is subjective, and could equal different numerical values of a scale depending on its perceived magnitude. Without some means for collating the perceived magnitudes of each linguistic term, two equal answers provided for pairwise comparisons may not correctly reflect the opinions of the two respondents.

Saaty suggests extending the AHP method by collecting a fuzzy set of data pertaining to the value of each linguistic term, unique to each answerer (Saaty, 1983). Using their triangular membership function; an upper, lower, and most probable numerical value for each linguistic may be found. The averages of each answerers triangular membership function may then be used as a conclusive numerical value for each linguistic term. This fuzzy extension of the AHP has become standard practice among researchers. While other methods for normalising the fuzzy numerical values of linguistic terms exist (e.g., the alpha cut method, centroid technique, trapezoidal fuzzy set theory), the triangular fuzzy set theory is used for its implementation of the Pythagorean theorem (which is simpler to use than the functions required for the other commented methods).

Sii and Wang use fuzzy set theory as an element in their design–decision support framework for evaluation of design options and proposals that uses a composite structure methodology (Sii & Wang, 2002). In their study, fuzzy set theory is used to describe criteria that have vital importance in a Delphi method iterative survey. By merit in part of fuzzy set theories implementation, the study resulted in a framework that provides powerful tools for comparing alternatives under subjective and uncertain evaluation procedures.

An alternative to using triangular fuzzy numbers would be the use of trapezoidal fuzzy numbers. Triangular fuzzy numbers use three values on a scale, and uses a centre of gravity approach towards

defuzzification. Trapezoidal fuzzy numbers require four numbers in the fuzzy set, and a more complicated process for defuzzification. The results of an assessment of a student's skills that used trapezoidal fuzzy numbers demonstrated that the process was fit for purpose (Voskoglou, n.d.). Trapezoidal fuzzy numbers are used also for optimal transportation theory, or for decision making and defuzzification of uncertain data produced by artificial intelligence (Mitlif, 2022). Little argument for its use can be made in this project when triangular numbers will suffice and require fewer calculations.

3.2.5 Goal structured notation

Kelly defines the purpose of safety case is a means to *"communicate a clear, comprehensive, and defensible argument that a system is acceptably safe to operate in a particular context"* (Kelly & Weaver, 2004).

Different standards define the safety case slightly differently, universally however they consist of three stages. At the core of any safety case are safety requirements and objectives, followed by a scrutiny of the objectives progress, which is based on some form of gathered evidence. Safety objectives are drawn by some form of safety analysis, or from requirements. Evidence for each objectives progress may be interpreted from Failure Modes and Effects Analysis (FMEA), Fault trees, or other quantitative, semi quantitative, or qualitative method. In the past, the argument process has represented a cause in quality of safety cases due to poor communication.

GSN is defined as *"a graphical argumentation notation that explicitly represents the individual elements of any safety argument, and the relationships that exist between these elements"*. GSN is a useful method for communicating a safety case as it illustrates how its three stages connect to one another. GSN uses nodes with shapes that signify goals, solutions, strategies, etc in a network similar to a Fault tree analysis. GSN is a successful communication tool by merit of its clarity, achieved by breaking down the goals of a strategy into separate components that can subsequently be disseminated to the appropriate authorities. GSN has seen notable use by (Kelly & Weaver, 2004):

- Eurofighter Aircraft Avionics Safety Justification
- Hawk Aircraft Safety Justification
- U.K. Ministry of Defence Site Safety Justifications
- U.K. Dorset Coast Railway Re-signalling Safety Justification
- Submarine Propulsion Safety Justifications
- Safety Justification of UK Military Air Traffic Management Systems
- London Underground Jubilee Line Extension Safety Justification
- Swedish Air Traffic Control Applications
- Rolls-Royce Trent Engine Control Systems Safety Arguments

In the UK Naval sector, L3 marine has utilised GSN to communicate the strategy for ensuring conformity to DEF STAN 00-56 by their Platform Management Systems (Labonté Jones & Lerigo-Smith, 2018).

The nodal network structure of GSN aligns with the hierarchy of the BSC. This project therefore utilises GSN to communicate its sector wide migration strategy. This project benefits from the clarity of communication provided by GSN during its final stage where Experts are relied on to understand what the BSC is communicating. With the objectives and measures (which represent the methods for evidence gathering) displayed clearly, Experts may communicate their feasibility, and progress, which facilitate the actions and recommendations that make up the migration strategy.

An alternative approach to illustration of the migration strategy considered was the use of multiple modified Bowtie diagrams. Bowties usually illustrate an event that results in a hazard at its centre, flanked by means for managing its risks and consequences. By placing each BSC objective at a bowties centre, the diagram could illustrate the UKCMSs current practice on its left, and the work required to for conformity to IEC 61508 on the right. A network of bowties could illustrate overlapping shortcomings of the UKCMS, and solutions to these addressed by multiple objectives, however it would result in a very complicated diagram that could not clearly differentiate between the different perspectives, and could cause further confusion if the reader were already familiar with bowtie diagrams.

3.3 Methodology stages

The following are brief descriptions of the methods utilised in the following chapters of this thesis. Each stage of the methodology is given in greater detail in its respective chapter.

The project methodology described in this thesis was written and implemented beginning 2019, despite the project beginning 2017. This project's initial methodology was designed to investigate the gap between current practice for implementing functional safety in the UKCMS in general, and practice as described in IEC 61508. To specify the methods that are and are not used in the standard in the first stage of the project for the purpose of then strategizing the implementation of the missing methods. Little was found in terms of literature indicating the gap, plus a series of interviews with Experts, lead to the realisation that the UKCMS was most likely fully capable to implement IEC 61508 already, or capable of hiring consultants to introduce the standard. The project therefore changed its perspective to instead address the barriers preventing standards implementation, achieved via the following project stages.

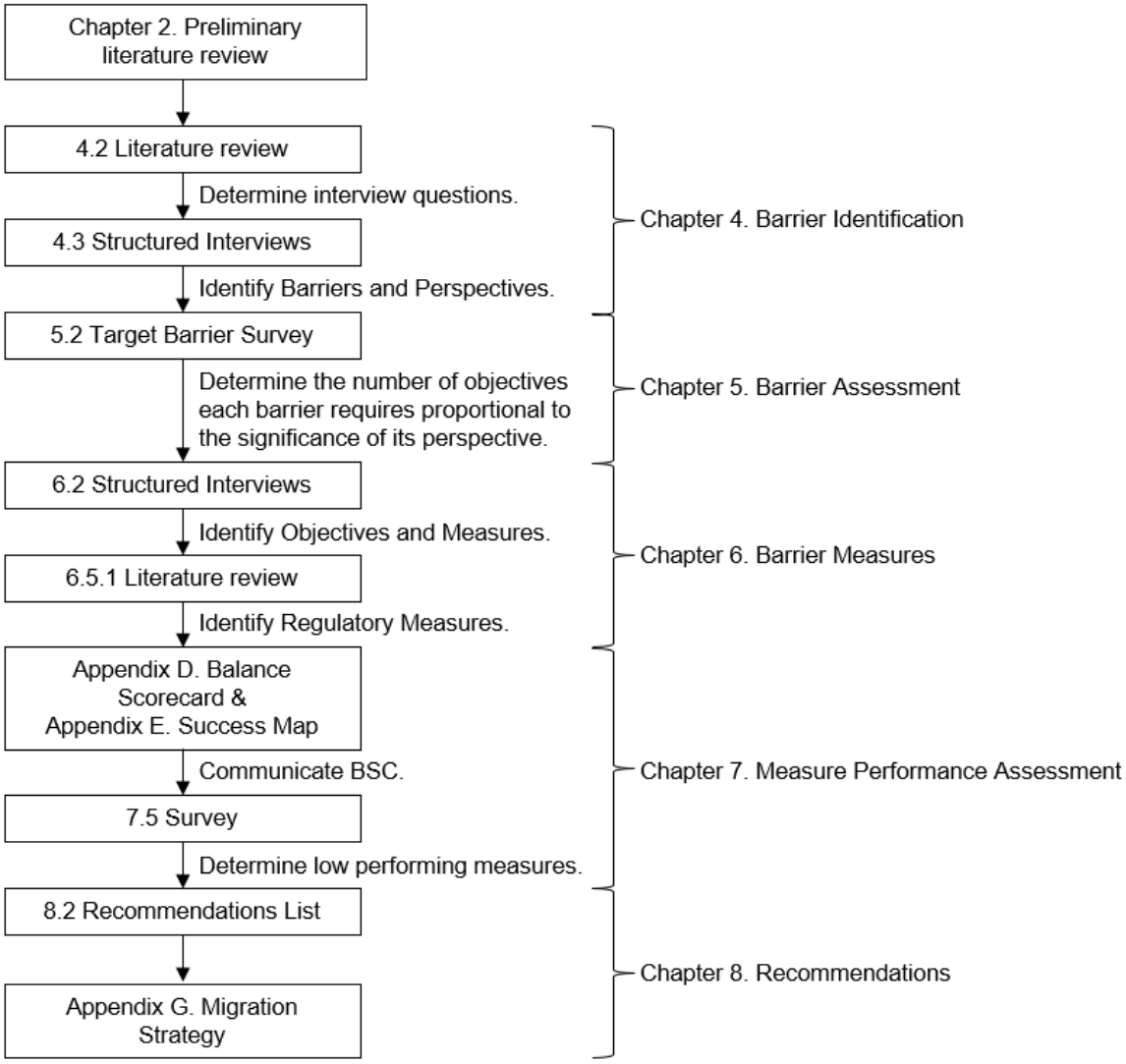


Figure 3. Project Methodology Flowchart

3.3.1 Barrier identification brief

The purpose of the barrier identification chapter is to investigate and define the barriers to the implementation of IEC 61508. First a literature review is conducted focussing on the implementation of the standard in other sectors, and any grey literature that refers to any past attempts at the standards implementation in the UKCMS.

The literature review provides a foundation of knowledge on the topic of the barriers to IEC 61508s implementation. This is used next to design a structure for interviews held with Experts. This structure consists of questions and areas of interest related to practice for implementing functional safety, and which perspectives should feature in a BSC that's vision is the implementation of IEC 61508 in the UKCMS. This stage also involves recruitment for participants, and acquiring appropriate ethical approval.

The result of the barrier identification methodology is a list of barriers preventing the UKCMS from implementing IEC 61508, and perspectives for objectives that address the barriers.

3.3.2 Barrier assessment brief

The purpose of the barrier assessment is to determine which barriers to IEC 61508s implementation will feature objectives in the BSC. The assessment involves the use of a fuzzy variant of the AHP to determine which barriers are the most important.

Experts were surveyed to provide the pairwise comparisons required for the AHP for both barriers and perspectives. The results of the AHP indicates which 25 objectives should feature in the BSC, and how heavily each perspective needs to be represented by objectives in the BSC.

3.3.3 Barrier measures brief

The purpose of the Barrier measures methodology is to define objectives and measures for each barrier. This is achieved by conducting another structured interview with Experts, followed by a chapter dedicated literature review.

The number of objectives and measures applied to each barrier is proportional to its magnitude of importance determined in the Barrier assessment.

The barrier measures methodology results in all the components required to produce the BSC.

3.3.4 Measure performance assessment brief

The Measure performance assessment is prefaced by the production of the project's BSC, as well as the illustrated component of a BSC in the form of a GSN map.

The methodology for the measure performance assessment involves conducting another survey with Suitably Qualified and Experienced Persons (SQEP) participants to provide numerical ratings to each measure regarding their progress, as well as a written statement providing a description of each measures progress in the UKCMS. These methods chapter also reviews literature in its discussion, focusing on practice and technology relating to the processes similar to those that feature in the migration strategy that have been achieved in other engineering sectors that conform to IEC 61508.

3.3.5 Recommendations for decision-making brief

The migration strategy this project repeatedly refers to is a series of recommendations produced in this part of the overall methodology. Recommendations are drawn from another study with Experts to determine how to improve the scores of the BSC measures.

3.4 Migration strategy hierarchy

This thesis will occasionally refer to a migration strategy hierarchy. The migration strategy hierarchy is the concept that the 5 main stages of this project occur in their specific order because the results of each stage influence the method of the proceeding stage. This project's overall methodology could be repeated for a different engineering sector, or a different standard, resulting in possible changes to how each of the 5 stages are conducted, however they would still have to be completed in the correct order.

The Migration strategy hierarchy is the list of project stages in given in the following order:

1) Determination of the vision (specify the engineering sector in focus, and the standard requiring conformity).
2) Identify barriers to the standards implementation (assuming the engineering sector in focus is capable of conformity).
3) Determine the perspectives from which to address barriers; then objectives that align with the perspectives, the achievement of which, overcome the barriers.
4) Determine measures for each objective and produce a BSC.
5) Assess the BSC, then derive recommendations from the BSC assessment.

The 5th level in the migration strategy hierarchy is the migration strategy communicated to the engineering sector in question.

Chapter 4. Barrier identification

This chapter identifies the barriers to IEC 61508s implementation, categorised into different perspectives; technical, cultural, financial, social, regulatory, and cyber security. Other challenges and drivers to the standards implementation are identified, and serve to bolster a profile of barriers, and justify the pursuit of a migration strategy. The barriers are identified via a literature review, and a study that involves conducting structured interviews with Experts whose backgrounds are relevant to the research topics.

The technical barriers highlight the differences between the technological capabilities of the marine sector, and the process sector (for which IEC 61508 was originally written). The cultural barriers indicate that despite the marine sector being one of the oldest engineering sectors in the UK, it has one of the least mature safety cultures. The social and financial barriers are relatively generic, and could easily be identified in other engineering sectors. As IEC 61508 addressed functional safety of E/E/PE SCS, it was deemed necessary to include barriers related to cyber security. The regulations and rules a ship must abide by changes during a voyage, therefore it was necessary also to investigate the barriers to the standard related to the maritime legal framework, and the benefits its implementation may provide.

4.1 Barrier identification introduction

The purpose of this chapter is to describe the processes for identifying the barriers that currently impede implementation of IEC 61508 in the UKCMS.

The method for identifying the barriers to IEC 61508s implementation in the UKCMS involves:

- Conducting a literature review that highlights challenges the UKCMS and the relevant challenges non-marine engineering sectors face when implementing IEC 61508.
- Conducting structured interviews with Experts familiar with IEC 61508 or the implementation of SCS in the UKCMS. The interview consists of questions that ask about the practical problems of migrating from current practice in engineering sectors with increasing complexity of technology, to conforming to the guidelines set in IEC 61508 from multiple business perspectives.

Barriers to the implementation of IEC 61508 feature as the second level of the migration strategy hierarchy. The desired results of the aforementioned literature review and structured interviews is a profile of barriers that currently prevent IEC 61508s implementation to the UKCMS.

The structure of the remainder of this chapter includes:

- The literature review.
- The interview process and its results.
- A discussion of the methods and their results.

4.2 Barrier identification literature review

This section consists of a literature review that identifies the challenges of implementing IEC 61508 to the marine sector, and other engineering sectors. Little is written that directly identifies the barriers to IEC 61508; however, some are indicated when the costs of its implementation are discussed.

There is little impetus for an industry to review its safety standards and legislation unless a major accident occurs (Labonté Jones & Lerigo-Smith, 2018). The HSE identified long ago that almost half of avoidable causes of accidents related to the failure of control systems were a result of their inadequate specification (HSE, 2003). Engineering sectors such as the rail, automotive, process, nuclear etc. responded in part by implementing IEC 61508, or one of its daughter standards (indicated by their existence). The standard defined and provided guidance for improving rigor of functional safety for 16 discreet stages of a SCS lifecycle.

The safety culture in the UKCMS sector often places process and finance above safety (Labonté Jones & Lerigo-Smith, 2018). Functional safety engineering requires an unattractive initial financial investment, and represents a strain to scheduling that engineering businesses would rather avoid for market purposes. Despite LR improving its regulations over the years, it is yet to set requirements for the implementation of IEC 61508. Engineers are at risk of solely considering the costs of compensation for staff injury, and damages to ships and their systems when determining whether a disproportional amount has been spent in the pursuit of reducing risks to ALARP (HSE, 2003). In reality, for every £1 spent on the insured costs mentioned before when dealing with an accident, between £8 - £36 may be spent on a plethora of damages to products, tools, and industry plants. In addition, legal costs, site clearing, delays, and the costs affiliated with a possible loss of staff Expertise (HSE, 2003). The National Aeronautics and Space Administration (NASA) came to a similar conclusion in an investigation that tallied the costs of fixing systematic errors that arose after the requirements of a system were specified (Boehm, 2003). Boehm quoted: *"early detection of errors is highly important to the success of any project."* Granted the costs to fix errors to US military aircraft and communications satellites are incomparable to commercial ships, both share the concept that a lifecycle approach to safety can save significant costs.

In regard to integrating systems on ships in the marine sector, *"The challenges that the marine sector faces in the 21st century are going to require solutions borrowed from other industries"* according to Pomeroy. Considering the conclusions drawn by Charles Haddon-Cave in his review of the 2006 Royal Air Force (RAF) Nimrod crash, the marine sector would benefit from safety assurance maintenance throughout a systems lifecycle (Pomeroy *et al.,* 2009).

Implementing cyber-security measures may fulfil functional safety requirements, as they often align (Wilkinson, 2019). Issues that arise when integrating cyber-security and functional safety typically involves over-engineered solutions, or problems surrounding retrofitting. It is beneficial to integrate cyber-security and functional safety early in a systems lifecycle in order to reduce cost, and optimise operability.

One notable example that demonstrates how cyber security and functional safety are linked is the Triton malware attack on a Saudi Arabian petrochemical plant in 2017. Triton malware targets the safety instrumented systems of the plant, and is designed to give hackers remote control of them (Giles, 2019). The malware potentially allowed hackers to use shut off and pressure release valves

to release hydrogen sulphide gas into the atmosphere, or cause an explosion. Fortunately, the malware was detected, resulting in a full shut down of the plant. Another similar example of cyber-attacks effecting SCS is the 2010 Stuxnet worm attack on the Natanz uranium enrichment facility in Iran. The Stuxnet worm is a highly complex virus that successfully sabotaged gas separation centrifuges, causing them to fail catastrophically (Karnouskos, 2011).

One example of a cyber-attack on global shipping is the June 2017 NotPetya malware attack on A.P. Moller Maersk. The malware infected Maersk through an email, and encrypted files, demanding $300 million worth of bitcoin paid for decryption (Greenberg, 2018). Maersk is responsible for 15% of global sea freight; however, the attack forced Maersk to close down its 76 terminals around the world, costing an estimated $10 billion dollars globally (Cyber Security, 2018). Among the lessons learned by Maersk after recovery from the attack, developing response and recovery plans that are tested and updated frequently in order to include new mitigation actions potentially protect against potential future cyber threats. Additionally, being proactive and investing in the organisation's protection and employees' awareness may mitigate the financial loss due to a possible future cyber-attack. Considering the potential for compromising functional safety cyber-attacks pose; the commercial marine sector should strongly consider integrating cyber security into functional safety implementation.

Recently IMO have begun drafting legislation that addresses the possibility of similar attacks. Such attacks could potentially release ballast water, or cargo at dangerous times causing catastrophic damage to a ship, the environment, and risking the lives of crew members. The IMO Guidelines on Maritime Cyber Risk Management state (IMO, 2017):

"The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management."

IMO have identified that cyber-attacks may lead to vulnerabilities for the following systems:

- Bridge systems
- Cargo handling and management systems
- Propulsion and machinery management and power control systems
- Access control systems
- Passenger servicing and management systems
- Passenger facing public networks
- Administrative and crew welfare systems
- Communication systems

IMO speculate that (IMO, 2017):

"Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber-discipline."

The introduction of integration of cyber security with a lifecycle approach to implementing functional safety could reduce the risk of hazards that are a result of cyber-attacks.

4.3 Barrier identification structured interviews

This section describes the process for conducting structured interviews to identify the barriers to IEC 61508, and their results. The purpose of the structured interviews are to compliment the literature review regarding data gathering concerning barriers to IEC 61508s implementation. The premier advantage of speaking with Experts and safety regulators in person is that; data gathered regarding the standard and the marine sector represents their most recent opinions. It is possible that data collected using structured interviews does not feature in published literature. Repetition of barriers identified via the literature review during an interview serves as verification for said barriers legitimacy (on the condition that the author and the Expert are not the same person). Another advantage of speaking with Experts in person is that it facilitates other comments made by participants into the data (recommendations for further research, other possible participants, etc.) The barrier identification stage requires quantitative data. Allowing participants to speak their answers alleviates the restrictions present in a written response.

4.3.1 Barrier identification structured interviews method

The method for organising and conducting the structured interviews involves:

- Participant recruitment.
- Organisation of interview.
- Conducting interview.
- Formal recording of data.

Participant recruitment primarily relied on contacting Experts known by the researcher's external advisor. Participants received an email briefly describing the project. Attached to the email was a structured interview template that elaborated on the project background, the purpose of the interview, and provided the interview questions (see Annex A.1). By revealing the questions beforehand, participants could prepare their answers ahead of time. The researcher and participant communicate via email to agree on a time and location for the interview. The researcher offered to conduct the interview via telephone call, video call, or accept answers to the questions via email should meeting in person prove unfeasible.

The time span for the Barrier Identification literature and structured interviews began on October 1st 2019 and concluded on November 30th 2019. The Migration strategy does not acknowledge sources indicating unaccounted barriers to IEC 61508s implementation to the UKCMS received after November 2019. Once the process for deciding which barriers to target concludes, new barriers cannot be included.

The researcher acts as scribe during the interview to record all spoken responses made by the participants. The researcher produces a profile for the barriers to implementing IEC 61508 using the literature review and the transcripts from the structured interviews.

The structured interview template asked the following:

Regarding the practical problems of migrating from current practice in engineering sectors with increasing complexity of technology, to conforming to the guidelines set in IEC 61508:

1. What are the technical issues?
2. What are the cultural issues?
3. What are the social issues?
4. What are the financial issues?
5. What are the drivers for IEC 61508s implementation?
6. What are the challenges whilst dealing with cyber security and functional safety simultaneously?
7. What are the other challenges that the industry is facing that affects the implementation of IEC 61508?
8. Do you know of any other Experts with knowledge or experience relevant to the research topics?
9. Do you have any recommendations regarding the research topics, aims, objectives, and methods?

Questions 1 to 4 address the traditional perspectives of the BSC. Objectives for barriers drawn from the answers to the first four questions allude to undesirable changes to current practise in the opinions of ship owners/ship builders. Question 5 facilitates the identification of desirable changes to current practise as a result of migration to IEC 61508. Cyber security represents multiple challenges that span multiple domains within the UK marine sector. Question 6 addresses these. Question 7 serves as a safety net that allows interviewees to speak freely about any further issues the migration strategy could address. Questions 8 and 9 were optional questions that aided the researcher by expanding the pool of participants and breadth of the literature review.

Technical issues represent the barriers to IEC 61508 that concern the technological capability of the UKCMS. These may highlight the differences between systems in the marine sector and other engineering sectors that currently implement IEC 61508.

Cultural issues correspond to how safety culture in the UKCMS may cause friction to a stakeholder's willingness to conform to new standards or practise. The marine sector is one of the UKs oldest engineering sectors, and may have difficulty adapting.

Social issues relate to how society or other forces external to the UKCMS may influence functional safety practise. Such forces may include customers, politics, and the UK public.

Financial issues represent the barriers that revolve around the costs required for implementing IEC 61508. Without a financial or legislative incentive, stakeholders will have difficulty justifying the costs for conformity.

Functional safety of E/E/PE systems connected to the internet should not be addressed without considering Cyber Security. Any system controlled by programmable controllers with an input is at risk of cyber-attacks.

Regulatory issues correspond to barriers that arise while complying with the maritime legal framework. UKCMS companies tend to align with the rules and regulations set by classification societies, flag states, IMO, maritime nation states, and company stakeholders.

4.3.2 Barrier identification structured interview results

The following is the profile of barriers to, and drivers for, IEC 61508 determined via the literature review and the barrier identification structured interviews.

4.3.2.1 Technical issues

1. The marine sector has a lower technical capability compared to other engineering sectors.

2. IEC 61508 is not generic enough for use in all engineering sectors.

3. The standard currently is not suitable for assigning SILs to automated systems.

4. Competency issues may arise without specific training for standard conformity.

5. Gathering Safety insurance evidence for high numbers of PC and PLC signals is difficult and time consuming to acquire.

6. Customers of marine sector systems might not fully specify all safety functions.

7. Difficulties arise when separate stakeholders share the budget to achieve a target SIL.

8. It is often difficult to derive value from quantitative risk assessment data for systematic failures.

9. Due to complexity of AI algorithms, hardwire backups are often used to relieve reliance on software.

4.3.2.2 Cultural issues

1. There is a general lack of awareness of IEC 61508 within the marine industry.

2. There is poor communication between different engineering sectors.

3. The marine sector relies heavily on legacy systems and practise; it is not agile in regard to changing practise.

4. Small numbers of accidents in the marine sector results in an underdeveloped safety culture.

5. More automated systems are wanted but require human interaction, therefore; SCS require safety built in.

6. It is difficult for a company to understand the importance of risk based, life cycle approach to functional safety.

7. Failing into a safe state is increasingly hard to design with complex software systems.

4.3.2.3 Social issues

1. The marine sectors perception of safety mirrors societies.

2. Customers and external users of SCS broadly assume robust practise when designed, due to small numbers of accidents.

3. Companies looking to implement IEC 61508 from the beginning of a SCS life cycle look at technology in a different way.

4. IEC 61508 does not use the concept of completely failure safe; one must comply with the standard to prove failure safe for specific modes of failure, the standard avoids loose language.

4.3.2.4 Financial issues

1. Shipping companies generally accept some risk of loss of cargo for reduced costs in safety due to insurance.

2. The initial investment required bringing old systems to acceptably safe levels, and the cost of maintaining safety throughout the entire lifecycle is off putting by ship owners.

3. GDP and safety costs increase proportionately. (It is difficult to improve safety without growth.)

4. There is a lack of investment to safety as a whole due to lack of understanding in the marine sector.

5. If IEC 61508 requirements are decided after a contract award, based on risk assessment, then the cost is taken by the builder.

6. Costs for independent analysis for higher SIL safety functions.

7. Other costs may arise for the initial tweak in standard alignment effort.

4.3.2.5 Cyber security issues

1. Safety managers are reluctant to accept safety measures blindly.

2. Cyber security can undermine Hazard Analysis (HAZAN), as cyber security threats can result in further consequences of hazards.

3. Cyber security is a recent shock to engineering sectors.

4. Engineers do not want address cyber security risks.

5. Plants connected to office IT networks are at risk to cyber-attacks if connected to the internet.

6. Independent cyber security and functional safety Experts may not achieve the target SIL if integration occurs late into a project.

7. Cyber security is way behind functional safety in regard to Expertise.

8. There is a trade-off between security requirements and safety requirements.

9. A system needs in built Cyber security, or cyber security integrated as early as possible to avoid issues during operation.

10. The need to meet requirements for functional safety and cyber security, whilst complying with normative requirements for both.

11. IEC wants functional safety engineers to work with cyber security Experts, but separately.

4.3.2.6 Regulatory challenges

1. Without consistency for fundamental terms used by different maritime regulatory frameworks regarding functional safety practise, the different tiers of the regulatory framework cannot agree where the baseline for equivalent level of safety is.

2. Inconsistency between, or lack of, legal definitions for safety-critical systems, and an understanding of accepted good practise for functional safety between different legal frameworks, further increases the complexity of deciding where the baseline for equivalent level of safety exists.

3. Sprawling duty holders required for evidence gathering already causes friction for IEC 61508s implementation, increasing numbers of stakeholders as a result of increased automation on ships means increasing the number of evidence gathering procedures.

4. The IMO does not provide a definition for ALARP.

5. No general understanding of what acceptable means.

6. Engineers can only claim dangerous failure rates with appropriate rigor.

4.3.2.7 Other challenges

1. Despite having comparatively less complex technology, the marine sector faces most of the same non-technical issues as other engineering sectors, such as environmental protection and emissions goals.

2. Engineers fear increasing requirements for proven in use arguments when implementing IEC 61508.

3. Restrictions in technology to balance conformity may not be feasible.

4. Political changes may potentially cause deregulation, or dilution of standards.

5. Technical staff involved in functional safety may have the skills to implement IEC 61508, but cannot easily convince managers they need to do so.

6. Using IEC 61508 restricts the use of ‘off the shelf’ systems without modification for its environment.

4.3.2.8 Other drivers

1. There is an inevitable merging of classifications regarding functional safety frameworks.

2. All engineering sectors want a single framework for conform to regarding functional safety. As more people become aware and trained to use IEC 61508, it will become easier to implement the standard sector wide.

3. IEC 61508 is a basic safety standard, which is why it has daughter standards for specific sectors. The marine sector may receive a daughter standard of its own in the future.

4. The Ministry of Defence uses rules that are as least as good as statute. The Naval ship software rules states process requirements for engineering systems, software producers, and classification. Processes out of scope of the software rules align with early steps of IEC 61508s overall safety life cycle.

5. IEC 61508 edition 3 is in the active development stage, and strongly considers cyber security for integration. A breech of cyber security can compromise power or safety of a plant and lead to an accident. Cyber security is getting increased attention by standard bodies.

6. Most sectors are adopting a risk-based approach when implementing functional safety; theoretically it would not be difficult to adapt to conform to IEC 61508.

7. New off-the-shelf systems and hardware may be compliant to IEC 61508. Companies can sell Products certified to IEC 61508 at a higher price to gain a market advantage. Effort invested into certification pays off.

8. A HSE inspection requires risks lowered to ALARP under the Health and Safety at Work etc. Act 1974 (HSWA1974), which is why IEC 61508 is benchmark for accepted good working practise.

9. When a hazardous accident occurs, a duty holder who can demonstrate compliance to IEC 61508 can discharge duty of care under The Corporate Manslaughter and Corporate Homicide Act 2007 (GOV.UK, 2007).

10. Big accidents usually have multiple small precursors. Small improvements made and sustained during the lifecycle of a system using FSA can help prevent a hazard from occurring.

12. In other engineering sectors, IEC 61508 is chosen because it is prescriptive nature. Engineers like to use annex A, B part 3 as it is well laid out (IEC, 2010b).

13. It is difficult to develop safety without high levels of reliability proportional to complexity of technology.

14. Work is required to; illustrate that the likelihood of accidents and/or their consequences would reduce, and equipment reliability would increase. This is a benefit to both the regulators, in terms of improving safety, and owners and operators. It is not a benefit to the shipbuilders and designers. Hence, the regulators, owners, and operators need convincing of the benefits.

15. Many industrial companies likely already employ most of the practise required for conformity to IEC 61508. Independent Expert consultancy may be required to tweak and reiterate practise for all life cycle stages, and conduct hazard identification so that hazard data fits the standard model.

16. There may be a significant cost for an initial compliance effort; however, many organisations may already employ the underpinning processes for compliance. Recouping of costs occurs in the end due to improved reliance of functional safety.

17. Raising of the cost of products and services due to conformity is unjustified.

18. Engineering sectors with poor insurance evidence gathering methods would benefit greatly by communicating with engineering sectors with good insurance evidence gathering methods.

19. IEC 61508 provides a holistic view of safety-critical systems, and provides answers for companies that ask, “Do we have what I need, when I need it” in regard to functional safety failures.

20. People want complex technology. IEC 61508 facilitates adoption of complex technology for safety systems at accepted good practise within a legal framework.

4.4 Barrier identification discussion

The following is a discussion of the barrier identification process, and the identified barrier profile.

4.4.1 Discussion of barrier identification method

The structured interview method was straightforward to execute. In one instance the researcher was unable to visit an Expert at their place of work, however the flexibility of the method allowed for reorganisation of an in person interview, to a telephone interview. The Experts all responded well to the process, and expressed their interest and willingness to participate in the future stages of the project.

Regarding the multi-perspective questions, the technical, cultural, and financial perspectives yielded 8 barriers each on average, whilst the social perspective only yielded half as many. The Experts were given details concerning the research topics, and the interview questions a month prior to the interview, and the contact details of the researcher for asking questions if they did not understand precisely what was asked of them. None of the Experts claimed to misunderstand what the researcher meant by ‘social issues’ therefore it is possible that there are fewer social issues surrounding the implementation of IEC 61508 compared to other issues.

The flexibility of questions 7, 8, and 9 facilitated one Expert to provide information about the regulatory challenges to implementing the standard. It is possible that had more Experts been included in this study, more categories of barriers may have been identified.

The Experts identified many issues surrounding cyber security, more so than each of the multi-perspective categories individually. Cyber security received its own question in the interview due to its connection with functional safety. For the purpose of the barrier assessment, the barriers under the ‘other challenges’ category will be distributed among the preceding categories.

4.4.2 Discussion of barrier list

In regard to the technical issues, multiple Experts claim that friction would arise when implementing IEC 61508 on the basis that there are fewer SCS compared to sectors that currently conform to IEC

61508. Also, that there may be issues related to SCS in the marine sector that the standard does not address. Engineers from the process sector originally wrote IEC 61508 to manage control systems and protect workers, and manage the safety of automated systems (Bell, 2017). The marine sector has different additional systems to the process sector such as propulsion and manoeuvring. These may require as robust safety integrity as required by systems in the currently conforming engineering sectors due to their environments.

When considering insurance data gathering required for conformity, a ship wide computer system may have a small number of PCs at the top layer of a computer hierarchy. Each top layer PC may have multiple second level PCs. Progressively lower PCs will have multiple tributary PCs, PLCs, and machinery. This results in thousands of signals to gather safety evidence data. Industries with highly complex SCS involve many people in a systems design, development, operation, maintenance, and decommissioning. IEC 61508 provides guidance for all life cycle stages; however, difficulties may arise when gathering evidence based assurance data consistently for FSA from all domains (IEC, 2010b).

In regard to the cultural issues, one Expert pointed out that from their experience, the shipping industries shipbuilders, system designers, rule makers and class societies are qualified primarily in naval architecture, and secondly in mechanical engineering. A narrow pool of engineers reduces interest, understanding, and uptake of IEC 61508.

Poor communication between different engineering sectors results in the marine sector not recognising solutions to similar engineering problems employed in other engineering sectors. In a similar vein, the extensive use of legacy systems and software restricts practise agility (Loughran *et al.,* 2002). The majority of builders and designers have little appetite to build or design beyond established practices that use easy to follow and well-defined ‘do this’ type rules. In addition, there is little awareness and no current encouragement from IMO, IACS and national administrations to adopt IEC 61508. Improving Functional safety management-practice is difficult for currently used functional safety systems; IEC 61508 requires use throughout the systems whole lifecycle. It is difficult to justify to marine safety engineers the use of increasingly complex safety systems when old precautions for low frequency hazards worked in the past. In reality, engineers may ask themselves: why not use a single fire extinguisher for a low frequency fire hazard area instead of lowering the risk of a fire to ALARP.

Accidents are what drives society’s perception of safety, and insurance. It is difficult to make the argument for IEC 61508s implementation when existing standards and practise yields acceptably safe enough functional safety. In industries that are not, as agile in regard to changing practise, why do more work for what seems to yield the same results? It is a challenge to convince the value of compliance of IEC 61508 to managerial duty holders.

In the marine sector, stakeholders want more automated systems, decreasing human interaction. Engineers must ask themselves: with humans in the loop, how do you ensure automated safety systems?

Without Expert advice, it is difficult for a company to understand the importance of a risk based, life cycle approach to functional safety. An Expert could break the standard down into smaller manageable parts. In industry, increased dependence on evidence of competency requires independent assessments. This requires greater amounts of time to complete projects waiting for evidence; however, current safety culture calls for as little delay as possible.

Traditional safety involved designing inherently safe systems (Singh *et al.,* 2010). For example, wooden water towers on the top of buildings in America. During a fire, they could potentially fail safely and put the out fire. General safety involves reducing the risk of a hazard from occurring, and including mechanisms for preventing or reducing consequences by failing into a safe state. The term *"inherently safer"* is now used. An example of a ship operating inherently safer would be reducing inventory on a ship that would cause damage or harm upon unintentional release.

Concerning the social issues, the marine sector's perception of safety mirrors societies. This means it improves at thresholds. For example, a major accident causing outrage among the public driving the reassessment of regulations. One notable example of this is the route the original Seveso 1 directive took to become the Control of Major Accident Hazards COMAH regulations.

One Expert pointed out that customers and external users of SCS broadly assume robust practise when designed, due to the low numbers of accidents in the marine sector. As a result, internally, duty holders may consider current functional safety practise, without the use of risk-based standards, 'accepted good practise'.

Another issue that highlights the possible redundancy of the standard is that users risk restraining the complexity, or novelty, of technology in order to conform to IEC 61508. Companies may wish to find a trade-off between conformity and novelty in order to avoid technological stagnancy. If any standard restricts a company's growth, one questions its relevancy.

The Experts pointed out that IEC 61508 does not use the concept of completely failure safe; you must comply with the standard to prove failure safe for specific modes of failure. Responsible stakeholders may make promises with loose or inaccurate language to do what it takes to ensure an accident will not happen again for public acceptance. The term completely failure safe is often misused this way.

In regard to the financial issues, the Experts explained conformity to IEC 61508 involves significant costs; these include training for staff, and documentation and insurance evidence gathering. Complying with IEC 61508 increases project completion time. Stakeholders see that costs to implement standards requires an initial unattractive investment, but engineers may see that it pays off in the long term.

One Expert pointed out that GDP and safety costs increase proportionately, specifically that it is difficult for a company to improve safety without growth.

The lack of understanding, and not knowing precisely what hazards arise from failure of E/E/PE systems, result in a weak argument for their defence in a cost benefit analysis. Engineers may ask; how do we know when we have done enough? There are extra costs spent to satisfy independent

safety auditors. Little financial gain may be observed when paying to reach and sustain integrity for higher SILs.

The profile states that if IEC 61508 requirements are decided after a contract award, based on a risk assessment, then the builder takes on the cost. Typically, the shipbuilder and designer proposes a fixed-cost and assumes the financial risk after the contract award, unless the buyer requests a change. Therefore, if a change is identified after the contract award, because of a risk assessment for example, this comes at the builders or designers' expense. Not knowing before the contract award what IEC 61508 requirements are needed, and the impact this might have on equipment choices, is a strong reason for builders and designers not to want to embrace the standard. If they do, they either take a financial risk or raise the fixed cost. With few in the industry aware of IEC 61508, and its benefits, this may make a bid uncompetitive.

In regard to cyber security, Experts stated that safety managers are reluctant to accept safety measures blindly. Cyber security is usually addressed via 'acceptable means of compliance', and uses risk mitigation measures outside of what a standard calls for, meaning there would be reliance on procedures outside of the safety framework.

Cyber security can undermine HAZAN because cyber security potentially increases hazard consequences and risk for hazards. Cyber security is a recent shock to engineering sectors, therefore risks to cyber-security are usually 'worked around'.

In order to address cyber security risks, engineers require different areas of Expertise. Addressing cyber security risks are often considered 'not agreeable to the market' for this and financial reasons. Cyber security becomes more important the more connected a physical system is to an IT system. There is a lot of disagreement in regard to regulations required for cyber security among engineers.

One Expert identified that in general, ships must comply with the regulations set in SOLAS, however the Non-compliance against SOLAS requirements grant a means for exemption. One such exemption comes in the form of 'Equivalent Level of Safety' which states (IMO, 1974):

"An exemption will only be granted where compliance with the regulations is unreasonable (whether on grounds of practicability or for some other reason) and the signatory is satisfied that alternative steps are taken so as to achieve an equivalent level of safety".

The definition of equivalent set in the context of the non-compliance requirements is (IMO, 1974):

"Compliance with a regulation but using the substitution of a particular fitting material, appliance, apparatus, or operational procedure which the Administration deems to be at least as effective as that required by regulation".

The maritime regulatory framework comprises of three main tiers: The IMO, the Flag States, and the Classification societies. Neither SOLAS nor IMO have a set definition for a SCS and different flag states and classification societies have different views regarding what constitutes a SCS. Without consistency for fundamental terms used in functional safety practise, the different tiers of the regulatory framework cannot agree where the baseline for equivalent level of safety is. Implementing IEC 61508 in the marine sector however could serve as this baseline.

The different tiers of the maritime regulatory framework define their own legal frameworks. Maritime nation states have their own legal frameworks as well, and ports and rivers may have their own set of rules too. The 1982 United Nations Convention on Law of the Sea (UNCLOS) specify the boundaries for each legal frameworks jurisdiction by splitting the oceans into five zones (UN, 1982). Inconsistency between, or lack of, legal definitions for safety-critical systems, and an understanding of accepted good practise for functional safety between different legal frameworks, further increases the complexity of deciding where the baseline for equivalent level of safety exists.

The UKCMS looks to increase its automated systems capability. Doing so requires the inclusion of a new 'branch' of stakeholders. The typical stakeholders involved in a ships lifecycle could broadly be categorised into regulator bodies, classification societies, Insurers, shipyards, ship owners, and other stakeholders (these would include crew and operators of systems external to the ship such as refuelling system operators and other dockworkers). The new branch that categorises stakeholders involved with automated systems would require those involved with the lifecycle of automated systems design and operation, these include remote operating centres, satellite communication companies, data analysists, and other communications and insurance duty holders. Sprawling duty holders required for evidence gathering already causes friction for IEC 61508s implementation, increasing numbers of stakeholders means increasing evidence gathering procedures.

Among IMO original mission statements, the purpose of the organisation is (IMO, 2019a):

"to provide machinery for cooperation amongst Governments in the field of governmental regulation and practices relating to technical matters of all kinds affecting shipping engaged in international trade; to encourage and facilitate the general adoption of the highest practicable standards in matters concerning maritime safety, efficiency of navigation and prevention and control of marine pollution from ships"

IMO maritime safety committee agreed to introduce a Regulatory scoping exercise for the use of Maritime autonomous Surface Ships in June 2017 (IMO, 2019c). A Maritime Autonomous Surface Ship (MASS) is a ship, which to a varying degree can operate independent of human interaction. The scoping exercise involves conducting trials to determine to which degree a ship is autonomous. There are four discreet levels of autonomy, level 1 being a ship with automated processes and decision support systems, but also has crewmembers on watch to supervise these systems. The other levels categorise thresholds of independence and remote operability up to level 4, which defines a fully autonomous ship.

Clause 2.1.1 of the Regulatory scoping exercise for the use of Maritime autonomous Surface Ships states (IMO, 2019d):

"Among other things, the guidelines say that trials should be conducted in a manner that provides at least the same degree of safety, security, and protection of the environment as provided by the relevant instruments. Risks associated with the trials should be appropriately identified and measures to reduce the risks, to ALARP and acceptable, should be put in place."

An Expert makes the three following observations:

1. The IMO does not provide a definition for ALARP (just calls for it, same as the HSWa1974)
2. It would be necessary to say what acceptable means as there is no general understanding of this.
3. Given the standard definition of ALARP, no third party without access to the underlying data can assess cost disproportionality.

Requirements for conformity to IEC 61508 by all maritime legal frameworks would provide them with the consistent legal definitions required to conduct the regulatory scoping exercises.

Finally, as a driver for IEC 61508s implementation, an Expert brought to the researcher's attention the Provisional Rules and Regulations for Software to be used in Naval Ships. The Ministry of Defence uses rules as least as good as statute. The Naval ship software rules states process requirements for engineering systems, software producers, and classification. Processes out of scope of the software rules align with early steps of IEC 61508s overall safety life cycle (LR, 2016).

In regard to the other challenges to implementing IEC 61508, engineers would prefer to use off the shelf legacy systems where possible. Their ability to do so is limited when using high SILs. If facilitated by political changes, manufacturers may relax functional safety regulation for a market advantage.

The other drivers for implementing IEC 61508 are self-explanatory. They serve no immediate purpose for the migration strategies actions, but may help with its justification.

4.4.3 Limitations to barrier identification

The barrier identification structured interview process aims to produce a profile that represents current barriers to IEC 61508s implementation in the UK marine sector based on Expert consensus. Each Expert involved with the study increases the accuracy of study. An initial limitation of the study is that only seven Experts were recruited for inclusion. Experts accepted for inclusion need knowledge regarding IEC 61508 and knowledge of at least one of the bodies that make up the Maritime legal framework, or a company from the UK marine sector. The small number of Experts recruited supports the first of the cultural issues *"There is a general lack of awareness of IEC 61508 within the marine industry"*. Fortunately, the Experts recruited had a diverse range of backgrounds. The barrier profile uses multiple perspectives. The greater the diversity of backgrounds and experiences the Experts have, the more likely the consensus will identify barriers in each issue category.

The researcher did not consider regulatory issues initially as its own category. It was strongly recommended by one of the Experts who had extensive knowledge regarding the maritime legal framework. The inclusion of more Experts may have resulted in more specific categories. Barriers in the Other issues category need to be distributed into the other categories before the barrier assessment.

4.5 Barrier identification conclusion

The methods used in this chapter have facilitated the writing of interview profiles for each Expert. The individual Experts' profiles, and the literature review, were combined to produce the barrier

profile in section 4.3.2. The other issues eluded in the barrier profile require distribution among the proceeding issue categories. The barrier profile also needs to be analysed for repetition, redundancy, and have issues that simply cannot be dealt with filtered out before use in a barrier analysis.

The purpose of this chapter is to describe the processes for identifying the barriers that currently impede IEC 61508s implementation in the UKCMS. The methods for doing so were completed within a specific time span that would not compromise the theses' submission deadline. The accuracy of the barrier profile could be improved if a greater number of Experts were used, and a longer amount of time spent researching the topics related.

Chapter 5. Barrier assessment

This chapter specifies which of the barriers to IEC 61508s implementation will feature objectives in the BSC. The methodology in Chapter 4 resulted in identification of barriers impeding conformity to IEC 61508 by the UKCMS. This chapter describes how a fuzzy variant of the AHP is used to determine which barriers were the most important to address, and which perspectives were most important, so that a proportional number of objectives may be assigned.

The results of the AHP indicated that the regulatory, financial, and cultural barriers represent the most friction, and the technical, social, and cyber-security barriers represent the least friction to IEC 61508s implementation. With this data, an informed decision may be made in regard to the route taken to efficiently investigate which objectives are required for a feasibly sized migration strategy featuring 25 objectives.

One criticism of the data is that the Experts had difficulty keeping their comparison matrix answers consistent. This is difficult for any comparison matrix with more than 3 factors, however when matrices with a CR of greater than 20% are not considered in the objective count calculations, a similar array of objective allocations are observed. This is likely a symptom to the small number of Expert participants.

5.1 Barrier assessment introduction

This chapter aims to determine what objectives will feature in the BSC by conducting a study, titled the Target Barrier Survey (TBS), that uses Experts' opinions to allocate numerical values to linguistic terms that describe thresholds of importance, and then use these to rank the barriers.

The TBS indicates which barriers shall feature in future studies to converge on a migration strategy. The project's initial research question exists as the top level of the migration strategy hierarchy. The second layer consists of the identified barriers, and the processes demonstrated in this chapter indicates the route to producing the third layer. The results of the above method include a decisive list of barriers that require objectives for the migration strategy, which shall be specified in the following chapter.

The remainder of the Barrier assessment chapter includes:

- Demonstration of the TBS, and how the AHP serves as a decision making tool for choosing which barriers to tackle in a feasible BSC.
- A discussion regarding this chapters' content, and a verification of its outcomes.

5.2 Target barrier survey

5.2.1 Target barrier survey introduction

The purpose of the TBS is to determine the priority of barriers to the implementation of IEC 61508 to the UKCMS. As the architects of the BSC, Kaplan and Norton (Kaplan & Norton, 2007) recommend each BSC should feature no more than 25 objectives, typically distributed among 4 perspectives (Mackey, 2005). There are examples of greater numbers of perspectives in successful BSCs used

in the past by other organisations (Guerra *et al.,* 2016), however as the number of objectives and corresponding measures grow, the larger the scope of the BSC vision grows, making it harder to realise. The focus on specific objectives and measures using a BSC has proven to be beneficial when implementing and appraising standards (Hristos, 2009) (Kopia *et al.,* 2017).

The overall methodology featured in this thesis may be repeated by engineering companies once most or all of the objectives are achieved to determine new objectives tailored to the needs of the company or organisation implementing the migration strategy.

The barrier identification structured interviews revealed 27 barriers to IEC 61508s implementation. Collectively the barriers are incomparable in regard to the effort required to overcome them, therefore it is unwise to assume each can feature as an objective in a single BSC. There is also the question of which barriers currently provide the most friction to IEC 61508s implementation? In order to tackle this, the TBS asks Experts to provide pairwise comparisons between the barriers, and comparisons between the types of barriers, referred to as perspectives. After ranking the barriers and perspectives, each barrier may receive a number of objectives for overcoming them, proportional to their importance. If a single barrier takes high precedence over the others within its perspective, it receives multiple objectives, whereas low ranking barriers may be disregarded (for the first iteration of the BSC).

Additionally, as multiple Experts are contributing to the AHP matrices, the methodology integrates a fuzzy element so that data processing may mitigate inconsistencies between the Experts understanding of linguistic terms.

The researcher distributed the survey among Experts who participated during the barrier identification structured interviews study. The remainder of this section covers the method, and results of the TBS.

5.2.2 Target barrier survey methodology

The following is a summary of the TBS and fuzzy AHP method. The TBS asks Experts to do the following:

1. Allocate numerical values to linguistic terms of importance.
2. Provide pairwise comparisons of barriers and barrier types to IEC 61508s implementation in the UKCMS.

Previously, the researcher conducted structured interviews with Experts to determine the barriers to IEC 61508s implementation in the UKCMS. The TBS asks Experts to allocate linguistic terms that best describe the importance of the barriers when compared one another. Prior to this, the Experts allocated a range on a numerical scale from 1 to 9 for each linguistic term. The closer to 9 the highest possible value for where a linguistic terms range resides, the greater the importance that term represents.

It makes sense to consider the numerical values of the linguistic terms equidistant from one another on a scale, and in logical order (equally important closer to 1 and extremely more or less important

closer to 9). Participants were required however to allocate the numerical ranges for linguistic terms in order to account for possible inconsistency between the Experts' personal definitions.

Once all the participants returned their answered surveys, Microsoft Excel was used to input the results into AHP matrices to determine the barriers priorities.

The initial barrier profile featured other challenges and other drivers, each do not succinctly fit into the typical BSC perspectives, nor the regulatory or cyber security perspectives. There were many similarities between several of the barriers. The number of comparisons made in the survey for each perspective increases geometrically with each barrier included, therefore the researcher produced the following summarised version of the barrier profile (27 Barriers) for use in the TBS. Each barriers number code corresponds with the code used in the AHP matrix tables. These codes in chapter 16, indicated by Table 15:

Technical perspective barriers

T1. Differing technical capabilities in the commercial marine sector compared to the process sector for whom IEC 61508 initially provided guidance.

T2. Lack of competency required for IEC 61508s implementation from within the commercial marine sector.

T3. It is highly time consuming to gather insurance evidence for high numbers of PCs and PLCs on ships.

T4. Low reliance of customers' ability to define all safety functions required by safety-critical systems.

T5. Using IEC 61508 restricts the use of 'off the shelf' systems without modification for its environment, It is hard or sometimes costly to ruggedize a system.

T6. It is very difficult to assign SILs to automated SCS and artificial intelligence with hardwire back-ups and human interaction to relieve reliance on software.

Cultural perspective barriers

C1. Lack of awareness of IEC 61508, and the significance of a risk based, life cycle approach to functional safety of safety-critical systems.

C2. Poor communication between different engineering sectors prevents recognition of solutions to similar challenges the commercial marine sector faces.

C3. The commercial marine sector relies heavily on legacy systems and practise, and is not agile to adapt or update.

Social perspective barriers

S1. The marine sectors perception of safety mirrors societies, and improves in thresholds rather proportionally to gradually increasing risk because of increasing complexity of technology. Until a major accident occurs, users of SCS broadly assume robust practise when designed.

S2. Engineers looking to implement IEC 61508 from the beginning of a SCS life cycle, they risk restraining the complexity or novelty of technology in order to conform to IEC 61508.

S3. IEC 61508 does not use the concept of completely failure safe; the standard avoids loose language that the commercial marine sector likes to use.

S4. The marine sector faces most of the same non-technical issues as other engineering sectors, such as environmental sustainability and emissions goals.

S5. Political changes may potentially cause deregulation, or dilution of standards.

Financial perspective barriers

F1. The initial investment required bringing old systems to acceptably safe levels, and the cost of maintaining safety throughout the entire lifecycle is off putting by ship owners.

F2. GDP and safety costs increase proportionately; it is difficult to improve safety without growth.

F3. Typically, a systems designer proposes a fixed-cost and assumes the financial risk after awarding a contract unless the buyer requests a change. If a risk assessment called for a change to a SCS design, this is at the builders or designers' expense.

F4. The costs for independent analysis for higher SIL safety functions and other costs for the initial tweak in alignment effort is off putting by ship owners.

F5. Companies typically split the budget to achieve safety functions between different stakeholders, compromising a company's ability to achieve a target SILs.

Cyber security perspective barriers

CS1. Safety managers are reluctant to accept risk mitigation measures that reside outside of acceptable means of compliance.

CS2. Cyber security can undermine HAZAN, as cyber-attacks can result in additional causes and consequences of hazards.

CS3. Cyber security is way behind functional safety in regard to Expertise.

CS4. Indecisiveness regarding the trade-off between security requirements and safety requirements.

Regulatory perspective barriers

R1. Without consistency for fundamental terms used by different maritime regulatory frameworks regarding functional safety practise, the different tiers of the maritime regulatory framework cannot agree where the baseline for an equivalent level of safety is.

R2. Inclusion of stakeholders relating to increased automation on ships means increasing evidence-gathering procedures.

R3. The IMO does not provide a definition for ALARP, given the standard definition of ALARP, no third party without access to the underlying data can assess cost disproportionality.

R4. Inconsistent understanding of what acceptable means between the different legal frameworks.

The following is a summary of the data processing method after all participants either return answered surveys, or withdraw from the study:

1. Determine the averages of the allocated numerical values for the linguistic terms.
2. Produce a pairwise comparison matrix for each barrier type.
3. Input the fuzzy values into the pairwise comparison matrices.
4. Determine crisp numbers for each fuzzy relationship.
5. Determine the priority vectors for each barrier.
6. Conduct a consistency check.
7. Determine the rank and magnitude of importance for each the barrier.

The AHP is a decision-making technique that facilitates the prioritization of many different options (Saaty, 2008). The result of an analytical hierarchy is a rank and magnitude of preference for each option. The AHP has been employed in the past in an effective means for determining the magnitude of importance for proposed safety measures (albeit safety measures initially determined using a quantitative analyses rather than via interviews) (Wang *et al.,* 2011b).

The cognitive psychologist Blumenthal (Saaty, 2003) wrote that:

"Absolute judgement is the identification of the magnitude of some simple stimulus. whereas comparative judgement is the identification of some relation between two stimuli present to the observer. Absolute judgment involves the relation between a single stimulus and some information held in short-term memory, information about some former comparison stimuli, or about some previously experienced measurement scale. To make the judgement, a person must compare an immediate impression, with an impression in memory of similar stimuli."

Objectivity normally drives decision making, which brings the use of judgements into question. When using numbers to represent an objective linguistic scale, their interpretation can be subjective. This subjectivity may be addressed by using a triangular fuzzy set to represent the collective opinions of the Expert participants. Other types of fuzzy set theory methods exist, such as Trapezium fuzzy sets, however triangular is chosen in this project due to its simplicity (Mokhtari, 2012). More complex methods may have been utilised had the researcher collected a larger data set.

The linguistic terms used expresses the Experts' preference range from equal importance between two barriers, and Extreme importance. Table 1 is an empty graph for inputting the opinion based numerical values.

Table 1. Numerical values for linguistic terms judgement table

Linguistic term	Term symbol	Lower value	Most possible value	Upper value
Equal importance	E			
Equal to Weak importance	EW			
Weak importance	W			
Weak to Strong importance	WS			
Strong importance	S			
Strong to Demonstrated importance	SD			
Demonstrated importance	D			
Demonstrated to Extreme importance	DEx			
Extreme importance	Ex			

Triangular fuzzy set theory is utilised by finding the lower, most probable, and upper value for the above linguistic terms in each Expert's opinion (Saaty, 1983). The averages of every Experts lower, most probable, and upper values are found discreetly, after which, the average of all three are found for each linguistic term to determine their crisp values.

After assigning values to each linguistic term, the Experts were asked to provide pairwise comparisons between each barrier within their barrier types, and to compare the barrier types themselves.

Experts were given two ways of providing pairwise comparisons, either a written comparison, or a scale to illustrate how important one barrier is compared to another. Figure 4 is an example pairwise comparison survey interface.

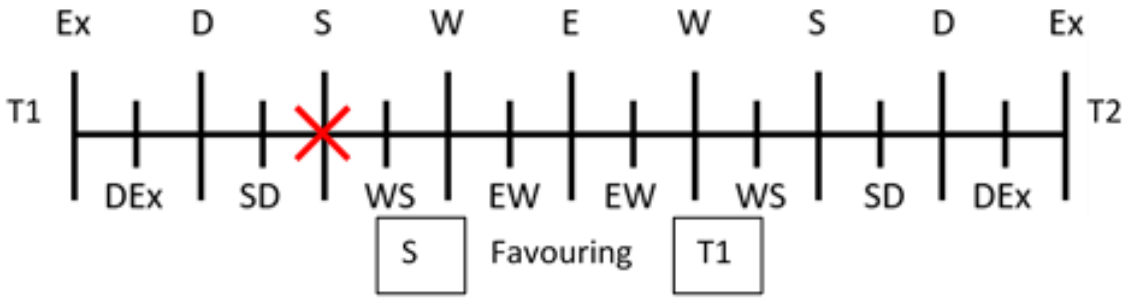


Figure 4. Example pairwise comparison survey interface

By inputting S Favouring T1, barrier T1 is strongly more important than barrier T2 in regard to implementing IEC 61508. Experts input the answers that represented their opinion in the text boxes, or clearly marked the pairwise comparison scale using a Word processor. Alternatively, they could print the survey, use a pen to mark the scale, scan the answered survey, and email it back to the researcher if they wished.

Each barrier type has between three and six barriers that represent the consensus among Experts. The following equation describes the relationship between the number of barriers (n) and the number of comparisons required to compare all the barriers in a specific category (C).

$$C = (n(n-1))/2 \quad (1)$$

At n = 3, C = 3 (2)

At n = 6, C = 15 (3)

The mathematical stages of the AHP were completed using Microsoft Excel, the following is an explanation of each stage of the AHP. Five Experts from a diverse range of backgrounds were able to complete the survey, however all Experts had a good understanding of IEC 61508 and the challenges that the UKCMS faces. The Experts were allocated a number from 1 to 5 as their pseudonym. The AHP will be demonstrated using Expert 5's survey results.

Firstly, the Experts were instructed to provide upper, most probable, and lower values for the linguistic terms of importance. Table 2 presents Expert 5's answers.

Table 2. Expert 5's numerical values for linguistic terms judgement table

Participant pseudonym	5		
Term symbol	Lower value	Most possible value	Upper value
E	1	1	2
EW	1	2	3
W	2	3	4
WS	3	4	5
S	4	5	6
SD	5	6	7
D	6	7	8
DEX	7	8	9
EX	8	9	9

Next the upper, most possible, and lower values of the linguistic terms from all 5 Experts are averaged to produce Table 3:

Table 3. Average numerical values for linguistic terms

Term symbol	Lower value	Most possible value	Upper value	Crisp value
E	1.00	1.00	1.33	1.11
EW	1.00	1.67	2.33	1.67
W	1.33	2.33	3.33	2.33
WS	2.33	3.33	4.33	3.33
S	3.33	4.00	5.33	4.22
SD	4.33	5.33	6.33	5.33
D	5.33	6.33	7.33	6.33
DEX	6.67	7.67	8.33	7.56
EX	7.67	8.67	9.00	8.44

The crisp value represents the average of the lower, most probable, and upper values for each linguistic term. The crisp values are used to represent the linguistic terms in the pairwise comparison matrices.

In the TBS, the Experts provided pairwise comparisons between each barrier within its type, Table 4 presents the comparison matrix for Expert 5's comparison of the Technical barriers:

Table 4. Expert 5's comparison of the Techincal barriers

Technical	T1	T2	T3	T4	T5	T6
T1	1.00	0.24	0.43	3.33	4.22	0.43
T2	4.22	1.00	4.22	6.33	6.33	2.33
T3	2.33	0.24	1.00	2.33	2.33	0.43
T4	0.30	0.16	0.43	1.00	1.00	0.24
T5	0.24	0.16	0.43	1.00	1.00	0.24
T6	2.33	0.43	2.33	4.22	4.22	1.00
Column sum	10.43	2.22	8.84	18.22	19.11	4.66

In a pairwise comparison matrix, barriers on the left hand column are compared with the barriers on the top row. T1 to T6 represent each of the 6 Technical barriers described earlier. Figure 5 presents Expert 5's answer for the comparison of two technical barriers:

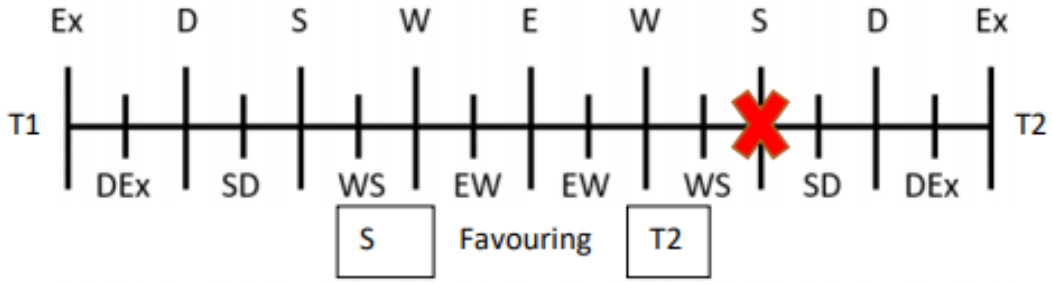


Figure 5. Expert 5's comparison of T1 and T2

By stating that technical barrier T2 is strongly more important that T1, the inverse of the S value is input in T1's row, T2's column. The excel matrix automatically inputs the inverse of (T1,T2) into (T2,T1). The rest of the matrix is filled using the remaining survey answers. The sum of each column is found for use in the barrier weight calculation.

Table 5 presents the results of the pairwise comparison of all technical barriers:

Table 5. Technical barriers comparison matrix

	T1	T2	T3	T4	T5	T6	w	λ
T1	0.10	0.11	0.05	0.18	0.22	0.09	0.124	1.298
T2	0.40	0.45	0.48	0.35	0.33	0.50	0.419	0.929
T3	0.22	0.11	0.11	0.13	0.12	0.09	0.131	1.158
T4	0.03	0.07	0.05	0.05	0.05	0.05	0.051	0.931
T5	0.02	0.07	0.05	0.05	0.05	0.05	0.050	0.957
T6	0.22	0.19	0.26	0.23	0.22	0.21	0.225	1.048
Column sum	1.00	1.00	1.00	1.00	1.00	1.00		

Each cell in the above table equals its equivalent in the technical barrier comparison matrix divided by its corresponding column sum.

T1's row, T2's column = 0.24 / 2.22 = 0.108 = 0.11

W is the weight of each barrier. W is determined by finding the average of all values in each row. In the opinion of Expert 5, barrier T6 is the most important with a weight of 0.2247. T5 is the least important with a weight of 0.0501.

Each set of comparisons are also subject to a consistency check. If for example T2>T1, and T1>T4, logically then T2>T4. When making large numbers of comparisons, it is reasonable to question an Expert's ability to sustain logical answers.

The process for checking the consistency in a pairwise comparison matrix begins by determining the principle eigen vector.

Principle eigen vector λmax equals the sum of each barriers eigen vectors. Each eigen vector λ equals the product of the column sum for its corresponding barrier in the pairwise-comparison matrix, and the weight of each barrier.

For a consistent reciprocal matrix, the Principle eigen vector should equal the number of barriers, λmax = n.

The consistency of a matrix is indicated by its Consistency Ratio (CR). The CR is determined by dividing a Consistency Index (CI), with a Random Index (RI). CI is calculated using the following formula:

$$CI = \frac{\lambda \max - n}{n-1} \qquad (4)$$

The RI is indicated on a random CI chart.

Table 6. Random CI chart

n	3	4	5	6
RI	0.58	0.9	1.12	1.24

For comparison matrices with 6 barriers, RI = 1.24.

The comparison matrix ratio CR is determined using the following formula:

$$CR = \frac{CI}{RI} \qquad (5)$$

Due to the difficulty for Experts to complete each comparison matrix consistently, a CR of 20% or less is considered acceptable, where normally it would be as low as 10% (Saaty, 2008).

5.2.3 Target barrier survey results

This section describes the results of the AHP. The pair-wise comparison matrix consistency checks will be analysed in the chapter 5 discussion.

The purpose of the AHP is to find the weights of each barrier type, and to determine the number of objectives each barrier type should have so that the migration strategy includes 25 objectives in total. The AHP also measures the weights of each barrier within each barrier type to determine how many objectives should be allocated to each barrier. 25 is chosen as the total number of objectives in the

migration strategy as architects of the BSC, Kaplan and Norton, recommended that a feasible BSC includes no more than 25 objectives.

Table 7. Barrier type weights

Barrier type weights							
Type	**1**	**2**	**3**	**4**	**5**	**Average**	**Number of objectives**
B1	0.115	0.062	0.064	0.023	0.051	6.33%	2
B2	0.183	0.135	0.221	0.125	0.110	15.49%	4
B3	0.118	0.104	0.035	0.062	0.114	8.65%	2
B4	0.132	0.281	0.154	0.250	0.220	20.73%	5
B5	0.094	0.038	0.178	0.068	0.046	8.48%	2
B6	0.358	0.380	0.349	0.471	0.458	40.32%	10

Table 7 displays the weight for each barrier type. The columns 1 to 5 represent the weights given by each Expert for each barrier. The number of objectives each barrier type gets is determined by finding the product of the average of each barrier type's weight, and 25.

B6 receives 25 × 0.4032 = 10.08 = 10 objectives. (6)

The regulatory barriers, represented by B6, will receive 10 objectives. The Financial barriers, represented by B4, will receive 5 objectives. The Cultural barriers will have 4 objectives, and the Technical, Social, and Cyber-security barriers will each receive 2 objectives.

Table 8. Barrier weights

Technical barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
T1	0.147	0.086	0.122	0.202	0.124	13.61%	0.2154	0
T2	0.338	0.399	0.047	0.065	0.419	25.34%	0.4011	1
T3	0.192	0.247	0.066	0.081	0.131	14.33%	0.2268	0
T4	0.198	0.080	0.300	0.140	0.051	15.38%	0.2435	0
T5	0.063	0.158	0.403	0.096	0.050	15.39%	0.2437	0
T6	0.063	0.030	0.063	0.417	0.225	15.95%	0.2526	1
Cultural barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
C1	0.572	0.333	0.732	0.057	0.231	38.50%	1.4907	2
C2	0.274	0.333	0.191	0.696	0.231	34.51%	1.3362	1
C3	0.154	0.333	0.077	0.248	0.538	27.00%	1.0453	1
Social barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
S1	0.261	0.199	0.213	0.351	0.483	30.15%	0.6522	1
S2	0.298	0.204	0.415	0.092	0.157	23.35%	0.5051	1
S3	0.312	0.394	0.171	0.091	0.069	20.74%	0.4486	0
S4	0.086	0.147	0.065	0.344	0.203	16.89%	0.3654	0
S5	0.043	0.055	0.136	0.122	0.088	8.87%	0.1919	0
Financial barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
F1	0.402	0.120	0.079	0.154	0.362	22.33%	1.1568	1
F2	0.085	0.144	0.040	0.073	0.085	8.53%	0.4419	0
F3	0.161	0.244	0.206	0.242	0.150	20.05%	1.0390	1
F4	0.273	0.187	0.532	0.502	0.266	35.18%	1.8229	2
F5	0.079	0.305	0.144	0.030	0.138	13.91%	0.7209	1
Cyber-security barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
CS1	0.129	0.312	0.045	0.185	0.234	18.09%	0.3834	0
CS2	0.542	0.361	0.119	0.196	0.184	28.02%	0.5938	1
CS3	0.082	0.277	0.254	0.091	0.429	22.67%	0.4804	0
CS4	0.247	0.051	0.582	0.527	0.154	31.22%	0.6615	1
Regulatory barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
R1	0.197	0.095	0.127	0.312	0.502	24.66%	2.4855	2
R2	0.057	0.222	0.325	0.334	0.087	20.51%	2.0675	2
R3	0.355	0.572	0.062	0.333	0.126	28.97%	2.9205	3
R4	0.391	0.110	0.486	0.020	0.285	25.86%	2.6073	3

The weights for each barrier based on each Expert's survey results are given in Table 8. The final weight for each barrier equals the product of the average weight of the barrier, and the number of objects the barrier type was allocated. For example, the sum of the final weights for the Technical barriers equals 2, and the sum of the final weights for the Cultural barriers equals 4.

The objectives are distributed proportionally between the barriers based on the final weights. For the Technical, Social, and Cyber-security barriers, the two barriers with the greatest weights were allocated 1 objective. The 3 Cultural barriers were allocated at least 1 objective each, and the greatest weighted barrier received 2. The other barriers were allocated objects using the same judgement pattern.

The regulatory barrier weights are all relatively close to 25%, but required 10 objectives shared among them. 3 objectives were allocated to the 2 barriers with the greatest weight, and 2 objectives

were allocated to the 2 barriers with the slightly lower weights. This distribution may appear to show that barriers R3 and R4 are 150% the weight of barriers R1 and R2, despite not being so.

5.3 Barrier assessment discussion

The results of the TBS AHP indicate that the Experts considered the Regulatory barriers to IEC 61508s implementation significantly more important than the other barrier types. Barriers R3 and R4 each received 3 objectives. These barriers stated: the IMO does not provide a definition for ALARP, given the standard definition of ALARP, no third party without access to the underlying data can assess cost disproportionality, and that there existed an inconsistent understanding of what acceptable means between the different legal frameworks.

HSE's definition of ALARP states (HSE, 2022):

"ALARP is short for "as low as reasonably practicable". Reasonably practicable involves weighing a risk against the trouble, time and money needed to control it. Thus, ALARP describes the level to which we expect to see workplace risks controlled".

The remainder of this discussion includes comments made by some of the Experts. These are reiterated from either notes taken during conversation, or copied from emails verbatim.

The maritime legal frameworks are a set of legal requirements whose jurisdictions are bound within different sections of the ocean set by UNCLOS (UN, 1982). A country has State rules for the territorial ocean immediately surrounding their borders. The classification societies reign over the economic parts of the ocean, while the high seas share regulations set by IMO. The results allude to a need for consistent definitions for vocabulary, specifically acceptable and for IMO, ALARP, for ships conforming to legislation as they pass through different ocean zones. One of the Experts claimed that *"The definition of "acceptable" and implementation of ALARP equivalent concepts are deterministic, so very unlikely to be resolved separately."* Only one Expert articulated this, however the other results indicate the other Experts may have had similar opinions.

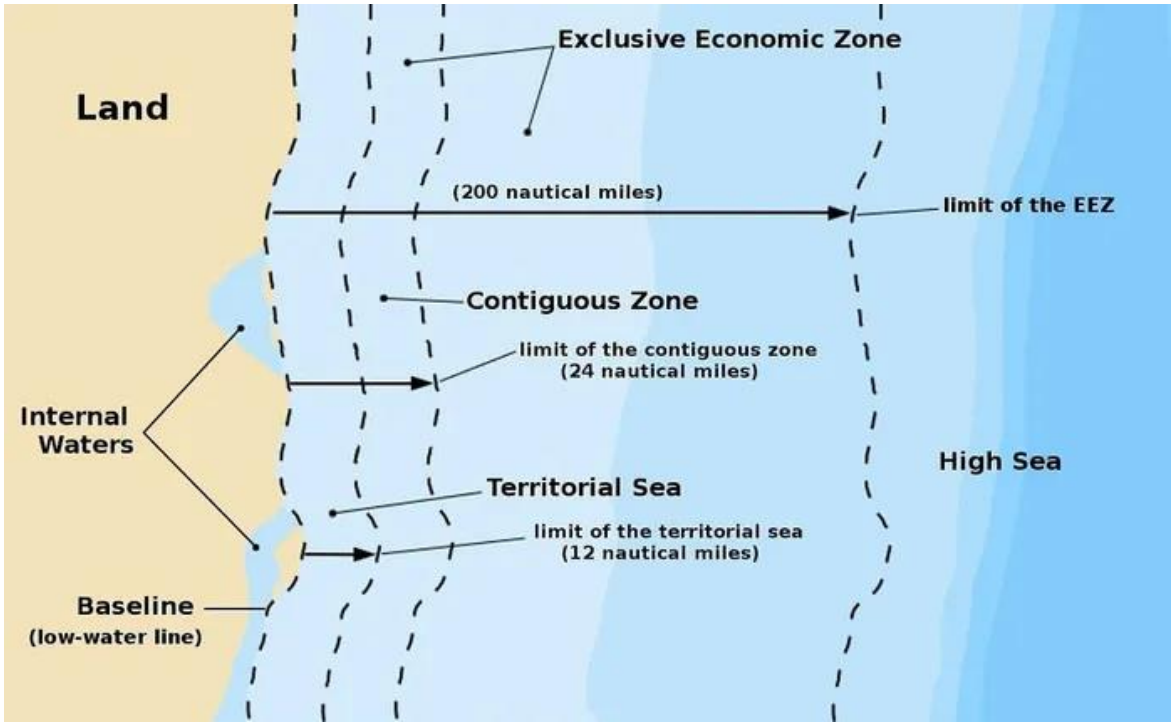


Figure 6. UNCLOS ocean zones (Sailors Insight, 2016)

No other barriers received a weight that allocated greater than 2 objectives. The remaining two Regulatory barriers include: Without consistency for fundamental terms used by different maritime regulatory frameworks regarding functional safety practise, the different tiers of the maritime regulatory framework cannot agree where the baseline for an equivalent level of safety is. Inclusion of stakeholders relating to increased automation on ships means increasing evidence-gathering procedures. The first of these two barriers further indicates a need to address the diversity of language used in regulations between the UNCLOS ocean zones. The second of these two barriers suggests that the Experts believe increasing automation in the sector will result in the reliance of increased dependence of stakeholders to aid with insurance information gathering.

Expert 4 emphasized that if companies in the maritime sector do not follow a process for identifying the criticality of a system, then how can they demonstrate that the system is safe in a defined operating condition? There are barriers mainly due to the lack of a mandatory requirement to carry out a risk assessment in commercial marine applications. An anecdotal example Expert 4 provided from a conference they attended; *"they (UKCMS company owners) meet all regulatory requirements and are insured"*. Unless it is a mandatory requirement, they will not do it. No-one will do something that will cost them money, even if they know the benefit of carrying out a risk assessment. These points support the necessity for the BSC to allocate 40% of the total objectives to overcoming the Regulatory barriers.

The second most significant barrier type is Financial, despite being only half as significant as the Regulatory barrier type, indicated by the allocation of half as many objectives. Most significant of the Financial barriers stated: The costs for independent analysis for higher SIL safety functions and other costs for the initial tweak in alignment effort is off putting by ship owners. This mirrors the comments made by Expert 4. The only Financial barrier that did not require a barrier states: GDP and safety costs increase proportionately; it is difficult to improve safety without growth. Expert 1 explained that

GDP and safety costs may not grow together, as regulation (and in fact de-regulation) may reverse one of the trends to support the other.

The CR results indicate that the Experts had difficulty sustaining the consistency of their comparisons. Saaty states that a CR of 10% is normal (Saaty, 2008). 20% is used in this project as most comparison matrices yielded a CR between 10% and 20%. Procedure for remedying inconsistent answers involves asking participants to produce a new judgement, however due to the method used for submitting answers, this was not feasible. This discussion therefore tests the matrices at different consistency ratios to determine the impact of tightening and loosening this factor. The Technical barrier comparison matrix for instance, only Expert 5 was able to produce a consistent pair-wise comparison matrix with CR = 0.05. The objective allocation array derived from Expert 5's answers aligned with the average of the inconsistent answers when comparing Table 8, which features all objective weights, against Table 9, which features only Experts 5 weights for the Technical barrier objectives. This phenomena is observable with most of the averages of the other barrier types as well.

Table 9. Techical barrier weights considered with <10% CR

Technical barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
T1					0.124	12.45%	0.2591	0
T2					0.419	41.88%	0.8717	1
T3					0.131	13.10%	0.2726	0
T4					0.051	5.11%	0.1063	0
T5					0.050	5.01%	0.1042	0
T6					0.225	22.47%	0.4676	1

Table 10. Social barrier weights considered with ≥20% CR

Social barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
S1	0.261	0.199	0.213	0.351	0.483	30.15%	0.6522	1
S2	0.298	0.204	0.415	0.092	0.157	23.35%	0.5051	1
S3	0.312	0.394	0.171	0.091	0.069	20.74%	0.4486	0
S4	0.086	0.147	0.065	0.344	0.203	16.89%	0.3654	0
S5	0.043	0.055	0.136	0.122	0.088	8.87%	0.1919	0

Table 11. Social barrier weights considered with <20% CR

Social barrier weights								
Barrier	**1.000**	**2.000**	**3.000**	**4.000**	**5.000**	**Average**	**Weight**	**Number of objectives**
S1			0.213		0.483	34.83%	1.0098	1
S2			0.415		0.157	28.63%	0.8303	1
S3			0.171		0.069	11.99%	0.3476	0
S4			0.065		0.203	13.38%	0.3881	0
S5			0.136		0.088	11.17%	0.3239	0

Table 10 displays the averages of all 5 Experts pairwise comparisons for the Social barriers. Table 11 presents the same data with Experts 1, 2, and 4's weights removed, as they had consistency ratios of greater than 20%. Expert 3 has a CR = 0.2 and Expert 5 has a CR = 0.07. Both tables display the same barrier objective allocation array regardless.

Table 12. Regulator barrier weights considered with ≥20% CR

Regulatory barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
R1	0.197	0.095	0.127	0.312	0.502	24.66%	2.4855	2
R2	0.057	0.222	0.325	0.334	0.087	20.51%	2.0675	2
R3	0.355	0.572	0.062	0.333	0.126	28.97%	2.9205	3
R4	0.391	0.110	0.486	0.020	0.285	25.86%	2.6073	3

Table 13. Regulator barrier weights considered with <20% CR

Regulatory barrier weights								
Barrier	**1.000**	**2.000**	**3.000**	**4.000**	**5.000**	**Average**	**Weight**	**Number of objectives**
R1	0.197	0.095			0.502	26.46%	2.6989	3
R2	0.057	0.222			0.087	12.20%	1.2441	1
R3	0.355	0.572			0.126	35.11%	3.5805	4
R4	0.391	0.110			0.285	26.24%	2.6758	3

The Regulatory and Cultural barriers were the only barrier types that received at least 1 objective for each barrier. Table 13 disregards the inconsistent results. The lowest weighted and highest weighted barriers sustain their ranks, however barrier R1 and R4 have swapped ranks (R1 has swapped from being the 3rd most important regulatory barrier, to being the 2nd most important). The lowest ranking barrier lost an objective, and the highest ranking barrier gained an objective. This was the only example where a barrier type received a different array of objectives after inconsistent results were disregarded.

This chapter has described the process for conducting the TBS, and processing the results using a fuzzy extension of the AHP. The TBS was designed to be as simple to understand, and easy to execute as possible, however it could have been improved in the following ways.

Firstly, the greater the number of participants, the more accurately the results would have reflected the opinions of Experts from the UKCMS. The study relied solely on the inclusion of Experts that were contacted through the researcher's supervisor team, and then those the Experts recommended, resulting in 2 tiers of participants. Despite receiving rejections from many contacted Experts, the researcher initiated the survey with only 5 due to time constraints.

The use of a fuzzy variant of the AHP presented a variety of issues. The advantage of using fuzzy set theory is that Experts may communicate their opinions in regard to the magnitude of each linguistic term before applying them to their pairwise comparisons. A problem with this is that if an Expert does not understand the method of the fuzzy variant of the AHP, then their answers may not make sense. One example of this is the magnitude allocation for the linguistic terms given by Expert participant 2 in Table 14.

Table 14. Expert 2's numerical values for linguistic terms judgement table

Participant pseudonym	2		
Term symbol	**Lower value**	**Most possible value**	**Upper value**
E	1	1	
EW	1	2	
W	1	3	
WS	1	4	
S	1	5	
SD	1	6	
D	1	7	
DEX	1	8	
EX	1	9	

While the allocation of most possible answers illustrated this Experts understanding that the EX symbol for extreme importance should receive the highest magnitude, and the E symbol for equally important should receive the lowest magnitude of 1, the Experts written answer also suggested that every term could have a lower value of 1 also. Because the calculation for determining the actual weight of each linguistic term involves finding the average between the lower, most possible, and upper values (which were left blank), the final results would not reflect what the Experts appears to be trying to communicate. In this instance, the study only used the most possible value column for this Expert as it is clear that the Expert perceived the different linguistic terms to be equidistant on a scale of importance (this was also confirmed with the Expert via email).

The survey itself would have benefited from a more advanced interface. The researcher wished to incorporate a sliding scale that allowed participants to drag a bar under the term symbol for each comparison. This is more intuitive and faster than asking Experts to write the answer and or draw a cross on the scale, however the researcher did not have the technical capability for accomplishing this.

The difficulty of keeping one's answers consistent is proportional to the number of comparisons required. Little could be done to reduce the number of comparisons required in the TBS, however.

The difference between the acceptably and unacceptably consistent answers manifested as different objective arrays in the Regulatory and Financial barrier types. The next step of the project is to determine objectives and measures for each of the barriers that received objectives. The process for this will include conducting further interviews with Experts to record their ideas, and to conduct a literature search to identify past solutions for overcoming the barriers, then to make a judgement for which objectives and measures should be used in the BSC. Regardless of which set of AHP results used, they both indicate the same barriers to address.

5.4 Barrier assessment conclusion

Out of the initial 27 barriers assessed, 17 were prioritised. The Regulatory and Financial barriers accounted for 8 of the 17 barriers that will feature in the BSC. While accounting for approximately half the barriers addressed, they have 2/5th of the allocated objectives. From this we can conclude

that the Regulatory and Financial barriers are the most significant barrier types to IEC 61508s implementation in the UKCMS.

The next step of the research is to determine what the objectives and measures will feature in the strategy for implementing IEC 61508 to the UKCMS. The result of the TBS allows the researcher to design an interview structure that asks Experts to determine and efficiently allocate the finite number of objectives in the BSC.

Chapter 6. Barrier measures

The prior steps in the formal safety assessment structure this project utilises identified and assessed barriers to IEC 61508s implementation. This chapter translates each barrier into a number of objectives and measures proportional to the barriers significance in impeding the UKCMS adoption of the standard in question. Experts were interviewed to determine their opinions, advice, and experience regarding how barriers may be overcome. Further research was required to achieve a proportional response to the regulatory barriers; therefore, a focussed literature review is included. This chapter concludes with a list of objectives and barriers, which are used to produce the migration strategy hierarchies fourth tier. The next stage of the BSC is to determine the actions that will satisfy the objectives, and provide data via the measures, or if reconsideration of the objectives and measures are necessary.

6.1 Barrier measure's introduction

This chapter describes the process for determining objectives and measures for the barriers to IEC 61508s implementation in the UKCMS. A typical BSC includes 3 main tiers; a vision an organization wishes to see realised, objectives to accomplish the vision, and measures for monitoring the progress of the objectives. In this project, the vision was initially to migrate current practise for implementing functional safety, to accepted good practise, and the chosen method for this is to implement IEC 61508. An initial investigation indicated that the UKCSM was probably capable of implementing IEC 61508 from a technical perspective, however, significant cultural, financial, and regulatory barriers existed, resulting in the elaboration of the vision to overcome said barriers.

6.2 Barrier measures structured interview method

This section describes the methodology and results of the barrier measures structured interview. Interviews with Experts were chosen as a means of data acquisition and validation when identifying objectives and measures for the barriers to IEC 61508. The researcher is limited regarding options for data gathering methods and validation techniques outside of reading literature, and asking those with industry experience to contribute their knowledge.

The purpose of the interview is to record the opinions and suggestions of Experts regarding objectives and measures for facilitating the implementation of IEC 61508 in the UKCMS. These questions were given in the context of the identified barriers selected for consideration in the migration strategy.

The researcher conducted a series of structured interviews described in the previous chapters that asked Experts to identify barriers to IEC 61508s implementation in the UK marine sector. Afterwards, the researcher conducted a survey with the same pool of Experts to provide pair-wise comparisons between the barriers.

The Researcher approached the same Experts used in the previous studies with an invitation to participate in this structured interview. Upon confirmation of their intention to participate, a phone interview was organised to ask Experts:

“In your opinion, please describe and discuss with the researcher; objectives for overcoming the following barriers, and if possible a means for measuring their progress”.

5 Experts participated in this study. The interviews were strictly conducted remotely due to the 2020 COVID 19 pandemic lockdown.

The Experts were provided an opening letter, information sheet, and an additional supporting document to ensure they were fully informed regarding the interviews purpose.

The researcher hand wrote notes while the Experts verbally communicated the answers to their questions. The flow and topics of the interview were flexible to allow the Experts to communicate any useful information relating to the barriers.

6.3 Barrier measures structured interview results

Appendix C.2 provides a summary of the notes taken during the interviews. Where Experts provided a method but no specific measure, the researcher made an assumption as to what quantifiable data may be extracted.

Upon concluding communication with Experts and the LR Affairs Team, objectives and measures were derived from the written notes, which are described and discussed in the following sections of this chapter.

6.4 BSC objectives derived from the interviews

Presented in Table 16. Each Barrier is abbreviated to ‘B.(barrier number)’. Using this system, the barrier that states “a lack of competency required for IEC 61508s implementation from within the commercial marine sector”, formally referred to as T2 in the Barrier Assessment, is represented by B.1.

Table 15. New barrier code

Old code	New code	Number of Objectives
T2	B.1	1
T6	B.2	1
C1	B.3	2
C2	B.4	1
C3	B.5	1
S1	B.6	1
S2	B.7	1
F1	B.8	1
F3	B.9	1
F4	B.10	2
F5	B.11	1
CS2	B.12	1
CS4	B.13	1
R1	B.14	2
R2	B.15	2
R3	B.16	3
R4	B.17	3

Below are the total number of objectives suggested by the interviewed Experts to overcome their respective barriers. Each objective is coded by the barrier number, then an objective number (e.g., the first objective suggested for B.1 is coded with B.1.1, the second objective is coded with B.1.2, etc):

B.1.1 Training and education regarding conformity to IEC 61508, advocated by regulators.

B.1.2 Increasing awareness of IEC 61508 among UKCMS stakeholders for the purpose of increasing customer demand of the standards conformity.

B.1.3 Use of in-house Experts.

B.1.4 Use of consultation.

B.1.5 Conducting a technical review of compliance in the UKCMS to define the technical requirements, and produce a UKCMS specific daughter standard of IEC 61508 (similar to IEC 61511 for the process oil and gas sector).

B.2.1 Recording and development of case studies referring to failure rate of automated SCS and artificial intelligence in the UKCMS.

B.3.1 Training and education regarding risk based safety and safety life cycles.

B.3.2 Increase publicity of IEC 61508 withing the UKCMS.

B.3.3 Increased membership to the SCS Club by staff in the UKCMS.

B.3.4 Increased awareness of IEC 61508 at management level of UKCMS companies.

B.4.1 Cross sector forums between The marine sector and other engineering sectors that comply to IEC 61508, and increased attendance of relevant conferences.

B.4.2 Production of a UKCMS specific daughter standard of IEC 61508.

B.5.1 Development of proven-in-use data for compliant safety-critical systems.

B.5.2 Pressure to conform to IEC 61508 based on sector internal competition.

B.6.1 Training and education regarding risk based safety and safety life cycles to override societal perception.

B.7.1 Use of Compliant Off The Shelf (COTS) technology.

B.8.1 IEC 61508 compliance between SCS suppliers and customers.

B.8.2 Development of proven-in-use data for compliant safety-critical systems.

B.9.1 Implementation of tailored risk assessments.

B.10.1 Provide guidance to ship owners and builders regarding the potential cost of failure of SCS conformity to IEC 61508 reduces.

B.10.2 Recording and development of case studies referring to the failure rates of compliant safety-critical systems.

B.11.1 Use of specified safety functions when designing safety-critical systems.

B.11.2 Cross industry reviews for the purpose of determining financial solutions for implementing IEC 61508 in the UKCMS.

B.12.1 Reduce connection to the internet onboard ships and onshore control systems.

B.12.2 Consideration of cyber security during each life cycle risk assessment.

B.13.1 Employment or consultation of Experts experienced in both safety and security.

B.13.2 Consideration of safety and security in a daughter standard.

B.14.1 Consistent language employed by regulatory frameworks.

B.14.2 Definitions for quantitative safety parameters.

B.15.1 Employment of safety measures and data gathering techniques tailored for automated safety-critical systems.

B.15.2 Use of modified COTS systems to aid compliance effort.

B.16.1 Implementation of D ships risk classification matrices.

B.17.1 Use of SFARP universally in the UKCMS.

Other objectives suggested by interviewed Experts:

S.1 Implementation of functional safety audits.

S.2 Use of pre-certified systems (similar to use of COTS systems).

S.3 Inclusion of IEC 61508 in LR in the Rules and Regulations for the Classification of Ships. This may require interventions by IACS (three routes for this).

The following steps are taken next to complete the objectives list:

1. For barriers that have the correct number of objectives determined, no further action is required.
2. For barriers with a number of determined objectives greater than the amount allocated in the results of the Target Barrier Analysis (TBS), select objectives for elimination.
3. For barriers with a number of determined objectives fewer than the amount allocated in the results of the TBS, add to the appropriate objectives list.

One method for ensuring the objectives list aligns with the allocation array from the TBS involve transferring matching objectives from a barrier that has too many, to a barrier that has too few, depending on their significance. Further research required for barriers with too few objectives is described in section 6.5

Repeated objectives need to be eliminated, and similar objectives may be merged.

Once the objectives list is finalised, measures need to be designed that represent the observable effects of each objective that combats its affiliated barrier.

Table 16. Objective difference list

Old code	New code	Number of Objectives	Objectives determined after SI	Difference
T2	B.1	1	5	-4
T6	B.2	1	1	0
C1	B.3	2	4	-2
C2	B.4	1	2	-1
C3	B.5	1	2	-1
S1	B.6	1	1	0
S2	B.7	1	1	0
F1	B.8	1	2	-1
F3	B.9	1	1	0
F4	B.10	2	2	0
F5	B.11	1	2	-1
CS2	B.12	1	2	-1
CS4	B.13	1	2	-1
R1	B.14	2	2	0
R2	B.15	2	2	0
R3	B.16	3	1	2
R4	B.17	3	1	2

Table 16 identifies the barriers that require attention in order to complete the objectives list. Barriers with no difference between the number of objectives required, and the number of objectives determined, require no further investigation (green rows).

All remaining barriers except B.16 and B.17 need to have objectives eliminated, whereas B.16 and B.17 require 2 extra objectives each. Table 16 does not include the important tertiary objectives that do not relate directly to the barriers.

Several of the determined objectives are very similar. Most objectives exist with the following shared themes:

- Training and education (internal knowledge).
- Guidance and consultancy (external knowledge).
- Increasing awareness of IEC 61508.
- Production of a UKCMS specific daughter standard of IEC 61508.
- Use of COTS.
- Development of proven-in-use data.
- Consistency of language between different legal frameworks/ organisations/ etc.

Objectives that reside within these themes could be merged to reduce repetition. In reality, training and education provided on IEC 61508 would be holistic to the whole standard (see ESC courses) and not restricted to the knowledge required to overcome a single barrier. Similarly, a consultant would not necessarily limit his or her service to the tackling of one barrier, but possibly to one barrier type. Awareness of IEC 61508 may occur passively and actively, by attending conferences and seminars, or by having knowledgeable people within a company spread the news.

It is possible to conduct a new AHP to determine the weights of the objective themes, however this was not done to conform to the project's time plan at the time, and to prevent over complication of the methodology. Balancing equally was therefore decided to be most appropriate.

The process to determine which objectives shall feature in the BSC migration strategy involves:

1. Merging objectives for a given barrier that share the same theme.
2. Eliminating objectives that share the same theme between different barriers within the same perspective, and eliminating objectives to balance theme preference.
3. Repeating the first two steps to converge towards the required number of objectives based on the results of the TBS.
4. Include all important additional suggested objectives.
5. Determine questions to achieve difference calculated in previous table.

Table 17. Initial Objective themes table

			Objective themes							
Perspective	**Barrier**	**Objective**	**Education**	**Guidance**	**Awareness**	**Daughter standard**	**COTS**	**Proven-in-use data**	**Language**	**Other**
Technical	B.1	B.1.1	✔							
		B.1.2			✔					
		B.1.3		✔						
		B.1.4		✔						
		B.1.5				✔				
	B.2	B.2.1						✔		
Cultural	B.3	B.3.1	✔							
		B.3.2			✔					
		B.3.3			✔					
		B.3.4			✔					
	B.4	B.4.1			✔					
		B.4.2				✔				
	B.5	B.5.1						✔		
		B.5.2								✔
Social	B.6	B.6.1	✔							
	B.7	B.7.1					✔			
Financial	B.8	B.8.1							✔	
		B.8.2						✔		
	B.9	B.9.1								✔
	B.10	B.10.1		✔						
		B.10.2						✔		
	B.11	B.11.1							✔	
		B.11.2								✔
Cyber-security	B.12	B.12.1								✔
		B.12.2								✔
	B.13	B.13.1		✔						
		B.13.2				✔				
Regulatory	B.14	B.14.1							✔	
		B.14.2							✔	
	B.15	B.15.1						✔		
		B.15.2					✔			
	B.16	B.16.1								✔
	B.17	B.17.1							✔	
Other suggested objectives		S.1								✔
		S.2					✔			
		S.3								✔
		Tally	3	4	5	3	3	5	5	8

Table 17 illustrates each objective, and which theme it represents. Table 4 satisfies the first step by merging similar objectives given by different Experts (e.g., B.1.3 and B.1.4 both suggest objectives concerning guidance and consultation to combat a lack of competency required for IEC 61508s implementation from within UKCMS).

Table 18. Objective themes table with similar objectives merged

			Objective themes							
Perspective	**Barrier**	**Objective**	**Education**	**Guidance**	**Awareness**	**Daughter standard**	**COTS**	**Proven-in-use data**	**Language**	**Other**
Technical	B.1	B.1.1	✔							
		B.1.2			✔					
		B.1.3, B.14		✔						
		B.1.5				✔				
	B.2	B.2.1						✔		
Cultural	B.3	B.3.1	✔							
		B.3.2, B.3.3, B.3.4			✔					
	B.4	B.4.1			✔					
		B.4.2				✔				
	B.5	B.5.1						✔		
		B.5.2								✔
Social	B.6	B.6.1	✔							
	B.7	B.7.1					✔			
Financial	B.8	B.8.1							✔	
		B.8.2						✔		
	B.9	B.9.1								✔
	B.10	B.10.1		✔						
		B.10.2						✔		
	B.11	B.11.1							✔	
		B.11.2								✔
Cyber-security	B.12	B.12.1								✔
		B.12.2								✔
	B.13	B.13.1		✔						
		B.13.2				✔				
Regulatory	B.14	B.14.1							✔	
		B.14.2							✔	
	B.15	B.15.1						✔		
		B.15.2					✔			
	B.16	B.16.1								✔
	B.17	B.17.1							✔	
Other suggested objectives		S.1								✔
		S.2					✔			
		S.3								✔
		Tally	3	3	3	3	3	5	5	8

Merging similar objectives within a barrier has resulted in convergence towards the correct number of objectives required for B.1, and the correct number of objectives met by B.3. Rows highlighted in green indicate barriers with the correct number of barriers as determined in Table. 16. The tally indicates a preference towards the development of proven-in-use data, and the alignment of language between different organisations. Objectives that reside in the 'Other' column are not included when balancing the themes.

Table 19 eliminates the objectives that share themes within the same perspective.

Table 19. Objectives with shared themes within the same perspective are eliminated.

			Objective themes							
Perspective	**Barrier**	**Objective**	**Education**	**Guidance**	**Awareness**	**Daughter standard**	**COTS**	**Proven-in-use data**	**Language**	**Other**
Technical	B.1	B.1.1	✔							
		B.1.2			✔					
		B.1.3, B.14		✔						
		B.1.5				✔				
	B.2	B.2.1						✔		
Cultural	B.3	B.3.1	✔							
		B.3.2, B.3.3, B.3.4			✔					
	B.4	B.4.2				✔				
	B.5	B.5.1						✔		
		B.5.2								✔
Social	B.6	B.6.1	✔							
	B.7	B.7.1					✔			
Financial	B.8	B.8.1							✔	
	B.9	B.9.1								✔
	B.10	B.10.1		✔						
		B.10.2						✔		
	B.11	B.11.2								✔
Cyber-security	B.12	B.12.1								✔
		B.12.2								✔
	B.13	B.13.1		✔						
		B.13.2				✔				
Regulatory	B.14	B.14.1							✔	
		B.14.2							✔	
	B.15	B.15.1						✔		
		B.15.2					✔			
	B.16	B.16.1								✔
	B.17	B.17.1							✔	
Other suggested objectives		S.1								✔
		S.2					✔			
		S.3								✔
		Tally	3	3	2	3	3	4	5	8

Table 19 converges Barriers B.4, B.8. and B.11. Further investigation is required to determine which remaining objectives should be prioritised for each barrier

The barriers that require further investigation to determine which objective(s) to neglect, and their suggested objectives are:

B.1 Lack of competency required for IEC 61508s implementation from within the commercial marine sector.

B.1.1 Training and education regarding conformity to IEC 61508, advocated by regulators.

B.1.2 Increasing awareness of IEC 61508 among UKCMS stakeholders for the purpose of increasing customer demand of the standards conformity.

B.1.3 & B.1.4 Use of in-house Experts/consultation

B.1.5 Conducting a technical review of compliance in the UKCMS to define the technical requirements, and produce a UKCMS specific daughter standard of IEC 61508 (similar to IEC 61511 for the process oil and gas sector).

B.5 The commercial marine sector relies heavily on legacy systems and practise, and is not agile to adapt or update.

B.5.1 Development of proven-in-use data for compliant safety-critical systems.

B.5.2 Pressure to conform to IEC 61508 based on sector internal competition.

B.12 Cyber security can undermine HAZAN, as cyber-attacks can result in additional causes and consequences of hazards.

B.12.1 Reduce connection to the internet onboard ships and onshore control systems.

B.12.2 Consideration of cyber security during each life cycle risk assessment.

B.13 Indecisiveness regarding the trade-off between security requirements and safety requirements.

B.13.1 Employment or consultation of Experts experienced in both safety and security.

B.13.2 Consideration of safety and security in a daughter standard.

The two remaining regulatory barriers require two more objectives each in order to receive focus proportional to their significance as a barrier to IEC 61508s implementation.

B.16 The IMO does not provide a definition for ALARP, given the standard definition of ALARP, no third party without access to the underlying data can assess cost disproportionality.

B.16.1 Implementation of D ships risk classification matrices.

B.17 Inconsistent understanding of what acceptable means between the different legal frameworks.

B.17.1 Use of SFARP universally in the UKCMS.

Regarding B.1, two Experts suggested the use of guidance and consultancy to overcome a lack of competency required for IEC 61508s implementation, indicating a bias towards this approach. The migration strategy provides options for moving towards the implementation of IEC 61508, objectives not included need not be neglected long term. Organisations may wish to train engineers once use of IEC 61508 is established through the use of consultants. Daughter standards of IEC 61508 are less generic, and tailor parts of the standard for their respective sectors/industries. The barrier refers to competency regarding IEC 61508 specifically. In the past, demand for implementation of more rigorous safety practice came as a reaction after a major hazard occurred. Increasing awareness of the lack of competency for implementation of the standard from within the sector may be neglected, as systematic errors are universal to all industrial sectors that use software operated safety-critical systems. Safety consultants are available to provide the Expertise required.

Regarding B.5, relying on data from IEC 61508 compliant systems contradicts the purpose of the migration strategy. Failure data is generated continuously over time, and results in a more precise understanding of the risks involved with E/E/PE systems as compliant systems are increasingly used.

B.5 would therefore benefit more from internal competition driving improvement of safety practice within the UKCMS. Internal competition in any engineering sector drives progress as long as changes made to practice/product/service/etc result in increased performance/profit/etc relative to competitors.

Regarding B.12, isolation of systems connected to the internet from other software on a ship may result from consideration of cyber security during each life cycle risk assessment.

Regarding B.13, future editions of IEC 61508 shall include cyber-security according to Expert 2 from the Barrier Identification study. A future daughter standard for the UKCMS may reflect this, and the writing of which may involve Experts in both the fields of safety and cyber-security. Implementation of IEC 61508 or a daughter standard may passively result in the satisfaction of B.13.2.

Taking the above into consideration, the objectives adopted by the migration strategy are indicated in Table 20.

Table 20. Final Objective themes table

			Objective themes							
Perspective	**Barrier**	**Objective**	**Education**	**Guidance**	**Awareness**	**Daughter standard**	**COTS**	**Proven-in-use data**	**Language**	**Other**
Technical	B.1	B.1.3, B.14		✔						
	B.2	B.2.1						✔		
Cultural	B.3	B.3.1	✔							
		B.3.2, B.3.3, B.3.4			✔					
	B.4	B.4.2				✔				
	B.5	B.5.2								✔
Social	B.6	B.6.1	✔							
	B.7	B.7.1					✔			
Financial	B.8	B.8.1							✔	
	B.9	B.9.1								✔
	B.10	B.10.1		✔						
		B.10.2						✔		
	B.11	B.11.2								✔
Cyber-security	B.12	B.12.2								✔
	B.13	B.13.1		✔						
Regulatory	B.14	B.14.1							✔	
		B.14.2							✔	
	B.15	B.15.1						✔		
		B.15.2					✔			
	B.16	B.16.1								✔
	B.17	B.17.1							✔	
Other suggested objectives		S.1								✔
		S.2					✔			
		S.3								✔
		Tally	2	3	1	1	3	3	4	7

Next, measures are derived for the selected objectives featured in Table 6, followed by further investigation to determine options for overcoming barriers B.16 and B.17.

6.5 Measures derived from the interviews

Table 21 indicates which objectives feature in the migration strategy.

Table 21. New Objective code

Barrier	Objectives (old code)	Objectives (new code)
B.1	B.1.3, B.1.4	O.1
B.2	B.2.1	O.2
B.3	B.3.1	O.3
B.4	B.3.2, B.3.3, B.3.4	O.4
	B.4.2	O.5
B.5	B.5.2	O.6
B.6	B.6.1	O.7
B.7	B.7.1	O.8
B.8	B.8.1	O.9
B.9	B.9.1	O.10
B.10	B.10.1	O.11
	B.10.2	O.12
B.11	B.11.2	O.13
B.12	B.12.2	O.14
B.13	B.13.1	O.15
B.14	B.14.1	O.16
	B.14.2	O.17
B.15	B.15.1	O.18
	B.15.2	O.19
B.16	B.16.1	O.20
		O.21
		O.22
B.17	B.17.1	O.23
		O.24
		O.25

The following is a reiteration of the barriers, their respected objectives, and how their progress can be measured. The migration strategy requires iterative review, and the most efficient way to measure progress for some objectives may change, depending on the company implementing it. The measures featured in this strategy can be considered the initial measures. The B.16 and B.17 objectives are identified following further research.

B.1: Lack of competency required for IEC 61508s implementation from within the commercial marine sector.

O.1: Use of consultation (or in-house Experts, see O.3).

The strategy could measure for O.1 the inclusion of consultants, or number of IEC 61508 certified individuals proportional to an FSA's independence (systems SIL). At least 1 consultant or in-house Expert per FSA. The same certified individual can be included on all FSAs for a single systems lifecycle (this is preferable).

B.2: Assigning SILs to automated SCS and artificial intelligence, with hardwire back-ups and human interaction, to relieve reliance on software.

O.2: Recording and development of case studies referring to failure rate of automated SCS and artificial intelligence in the UKCMS.

Engineers will implement hardwired back-ups and assign 'humans in the loop' to software driven systems predominantly because they are not confident determining the failure rate of software. To overcome this, IEC 61508 provides a qualitative method for assigning a SIL target to software, however an understanding for the (approximate) frequency of failure is still required. O.2 addresses this by formally producing some form of database to provide engineers with the data required to assign software SILs. Measuring of this objective would require ship owners to implement a system for formally recording and reporting software related failure. SIL determination requires record of the factors that lead to the calculation of a systems maximum tolerable failure rate, these include a profile of time at risk, unavailability of separate mitigation fails, probability of a scenario developing, probability of the scenario escalating (e.g., ignition of a released flammable substance), and the number of fatalities likely to occur. Judgement for each of these require justification, which this objective should result in.

B.3 Lack of awareness of IEC 61508, and the significance of a risk based, life cycle approach to functional safety of safety-critical systems.

O.3 Training and education regarding risk based safety and safety life cycles.

B.3 relates to all other barriers. If engineers and managers of companies in any engineering sector that manages the safety of SCS knew the benefits of a lifecycle approach, it would improve IEC 61508s adherence. The UKCMS suffers in part from legacy practice, and the migration strategy aims to raise the quality of functional safety practice in part by raising awareness of IEC 61508 and the benefits of a risk based approach at the beginning of a sea going systems life cycle. O.3 achieves this by suggesting education at least regarding IEC 61508, and possibly training in its implementation if consultation is less preferable. Training and Education comes in the form of attending courses and achieving certifications for implementing IEC 61508.

B.4 Poor communication between different engineering sectors prevents recognition of solutions to similar challenges the commercial marine sector faces.

O.4. Increase publicity of IEC 61508 within the UKCMS via increased memberships to the SCS Club by UKCMS staff and managers.

The SCS club provides literature and hosts events that can facilitate increased communication of relevant topics between engineers from different sectors. Measuring and increasing membership by

UKCMS staff and managers should reduce friction from different levels of a company when implementing IEC 61508.

O.5 Production of a UKCMS specific daughter standard of IEC 61508.

This objective concerns the writing of a daughter standard to IEC 61508 that caters directly to the management of systems found on commercial ships. Measuring this process involves monitoring of the procedure for writing daughter standards of IEC 61508.

B.5 The commercial marine sector relies heavily on legacy systems and practise, and is not agile to adapt or update.

O.6 Pressure to conform to IEC 61508 based on sector internal competition.

Societal perception of engineering sectors have in the past driven change in safety practice (such as the Grenfell Tower fire triggering a removal of cladding from buildings considered prior to be safe for installation) (Hackitt, 2018). As the benefits of implementing IEC 61508 (or the lack of conformity in the event of a major hazard(s)) becomes apparent to customers, business may be drawn to conforming UKCMS companies. Companies would have to measure their own profits and customer 'adhesion' in comparison to other companies that do and do not advertise the fact that they conform to the standard. If possible, the cost saved due to reduced risk of failures should be recorded. Sector competition is measured by profits and customer preference.

B.6 The marine sectors perception of safety mirrors societies, and improves in thresholds rather proportionally to gradually increasing risk because of increasing complexity of technology. Until a major accident occurs, users of SCS broadly assume robust practise when designed.

O.7 Training and education regarding risk based safety and safety life cycles to override societal perception.

As O.6 concerns observation of safety cultural change in the UKCMS, O.7 concerns observation of actions taken by companies individually to pre-emptively tackle societal concerns (and ultimately potentially saving money and lives). O.7 is similar to O.3 in of that they both involve the same process of training UKCMS staff. The measure for O.7 however regards the implementation of IEC 61508 before a major accident has occurred (which typically drives societal perception, and by extension, a regulator reaction).

B.7 Engineers looking to implement IEC 61508 from the beginning of a SCS life cycle, risk restraining the complexity or novelty of technology in order to conform to IEC 61508.

O.8 Use of COTS technology.

Limitations to a systems design an engineer may face due to conformity to IEC 61508 may be overcome by replacing any systems they need to design or incorporate into another with an already COTS system. Measurement of this involves recording which proportion of systems within a larger system (i.e., separate systems that form to make a ship) include COTS systems.

B.8 The initial investment required bringing old systems to acceptably safe levels, and the cost of maintaining safety throughout the entire lifecycle is off putting by ship owners.

O.9 IEC 61508 compliance between SCS suppliers and customers.

Conformity by customers (ship owners) and suppliers (ship and system manufacturers) may reduce the costs of conformity to IEC 61508 at all stages of a systems lifecycle. It facilitates companies individually spending less when compensating for organisations involved in a systems lifecycle. Measurement involves monitoring alignment of conformity between the previously mentioned stakeholders.

B.9 Typically, a systems designer proposes a fixed-cost and assumes the financial risk after awarding a contract unless the buyer requests a change. If a risk assessment called for a change to a SCS design, this is at the builders or designers' expense.

O.10 Implementation of tailored risk assessments.

IEC 61508 is most efficiently implemented from the very beginning of a systems lifecycle. A source of change to a contract can come from more rigorous risk assessment mandated in an FSA. Tailoring the risk assessment to account for this at the beginning of a systems life, or at it earliest possible stage, can reduce the cost by builders or designers of said systems.

B.10 The costs for independent analysis for higher SIL safety functions and other costs for the initial tweak in alignment effort is off putting by ship owners.

O.11 Provide guidance to ship owners and builders regarding the potential cost of failure of SCS conformity to IEC 61508 reduces.

O.11 improves the chance of success of O.7. O.7 aims to implement IEC 61508 specifically before its implementation is legislated, or demanded by society. O.11 approaches this same goal from a different perspective, by educating UKCMS companies specifically about the potential costs saved via IEC 61508s implementation. The measure would target the specific understanding of cost-benefit for IEC 61508s implementation, rather than its implementation methodology.

O.12 Recording and development of case studies referring to the failure rates of compliant safety-critical systems.

Experts questioned about this barrier suggested that a non-theoretical approach is required also. Measures for O.12 would include case studies internal and external to the UKCMS, however as conformity to IEC 61508 increases, so shall the number of more relevant case studies.

B.11 Companies typically split the budget to achieve safety functions between different stakeholders, compromising a company's ability to achieve a target SILs.

O.13 Cross industry reviews.

The eleventh barrier requires foundational change to how some companies finance a project or job. Review of how sectors such as the rail, automotive, naval etc that implement IEC 61508 managed to migrate their practice in the past, then mirroring the process.

B.12 Cyber security can undermine HAZAN, as cyber-attacks can result in additional causes and consequences of hazards.

O.14 Consideration of cyber security during each life cycle risk assessment.

HAZAN is a process that occurs very early in a systems lifecycle. Software driven systems are often retrofitted to old ships that did not consider cyber-attacks at the design stage. UKCMS companies will need to consider their vulnerability to cyber-attacks at the earliest FSA possible.

B.13 Indecisiveness regarding the trade-off between security requirements and safety requirements.

O.15 Employment or consultation of Experts experienced in both safety and security.

Measures for O.15 would require recording the relevant qualifications of individuals involved with FSA. Individuals with both measurable qualifications or experience conducting FSAs and managing cyber security.

B.14 Without consistency for fundamental terms used by different maritime regulatory frameworks regarding functional safety practise, the different tiers of the maritime regulatory framework cannot agree where the baseline for an equivalent level of safety is.

O.16 Consistent language employed by regulatory frameworks.

This requires measuring the efforts of regulatory organisations to align language with each other.

O.17 Definitions for quantitative safety parameters.

Several standards and guidelines external to the UK marine sector set thresholds for the factors of a risk. IEC 61508 used 4 levels of frequency and four levels of severity. The MODs SMP06 for defining risks prescribes 4 levels of severity, but 6 levels of frequency. The currently defined factors of risks used by the UKCMS need to be identified, aligned with IEC 61508s, then implemented sector wide where possible.

B.15 Inclusion of stakeholders relating to increased automation on ships means increasing evidence-gathering procedures.

O.18 Employment of safety measures and data gathering techniques tailored for automated safety-critical systems.

The number of individuals involved in a systems lifecycle increases proportionally to its complexity. The IMO already implements a scale for how automated a ship is ranging from no automation whatsoever, to a fully automated (crewless) ship. The existence of the extreme end of the scale is indicative of the direction the sector is heading towards. Most automated systems rely on software as a component; therefore, foundations need to be laid for the gathering of data that will support risk

assessment for these future systems. Measures may borrow first from similar systems in other engineering sectors, and eventually migrate data gathering to the current most relevant source (eventually from other ships when appropriate).

O.19 Use of modified COTS systems to aid compliance effort.

Bespoke automated systems require highly complex individual risk assessments. Using a COTS system that is already compliant will help ship builders conform to IEC 61508. Increased rigor of risk targets are required as COTS are modified to be automated, and relied on more independently for functional safety.

B.16 The IMO does not provide a definition for ALARP, given the standard definition of ALARP, no third party without access to underlying data can assess cost disproportionality.

O.20 Implementation of D ships risk classification matrices.

In place of an IMO specific definition of ALARP, the migration strategy implements a method for achieving a risk reduction to ALARP used by the Naval sector called D Ships risk classification. The method involves 9 steps that result in the consideration of a risks factors, cost to implement safety measures, and whether the costs are grossly disproportionate. In its current form, the method is suitable for naval vessels, and adjustments may be required to align the factors. Measurement involves recording the documents included in a risk's safety case, and the inclusion of the documents required to implement D Ships risk classification.

O.21 Inclusion of D ships risk classification as part of the LR Rules and Regulations (and consultation to IMO).

LR is the United Kingdom's International Association Classification Society representative. As an organisation, it is the duty holder for setting the rules and regulations for classified ships in the UK. The IACS provide consultation when for the organisations that generate IMO international rules and regulations. This project does not specifically concern the changing of international practice, however it recognises that international laws influence the UKCMS. Measuring this objective involves waiting for the IMO to recognise the issues related to the lack of definition for ALARP, and actions taken to address this.

O.22 Education and training in D ships risk classification matrices use within the UKCMS.

The necessity to implement training and education for IEC 61508 indicates the same is likely required for other currently unimplemented processes in the UKCMS. The researcher is unaware of formal education in the d ships classification matrices method, it may be learned from the Ministry of Defences (MOD) Defence Equipment & Support (DE&S) Leaflet Ships Operating Centre Safety Risk Review. Adoption relies on awareness also.

B.17 Inconsistent understanding of what acceptable means between different legal frameworks.

O.23 Use of SFARP universally in the UKCMS.

Despite reducing risks to SFARP is mandated by the Health and Safety Work Act of 1974, Experts when questioned about the UKCMSs regulatory issues stated that the use of SFARP should be monitored.

O.24 Definition for acceptable established by the appropriate regulatory duty-holder.

R2P2 lays out the concept that *"the law should provide a statement of principles and definitions of duties of general application, with regulations setting more specific goals and standards"* (HSE, 2001) This should be practiced facilitating the identification of the appropriate duty holder for defining what acceptable is, and then defining the term for the UKCMS.

O.25 Awareness for definition of acceptable increased within the UKCMS.

In order to ensure the barrier does not resurface, it is important that only one duty-holder defines the term acceptable.

6.5.1 Regulatory Objectives and Measures literature review

The purpose of this part of chapter 6 is to review relevant literature, and address information and advice provided by Experts during phone interviews (held after conclusion of the Barrier measures structured interviews) regarding the two remaining barriers included in the IEC 61508 migration strategy. Experts spoken to express their wishes to be contacted should elaboration or further discussion be required during the Barrier measures structured interviews.

Barrier 1 states: The IMO does not provide a definition for ALARP, given the standard definition of ALARP, no third party without access to underlying data can assess cost disproportionality.

Barrier 2 states: Inconsistent understanding of what acceptable means between different legal frameworks.

Fundamental concepts the researcher needs to understand, and map is the route for duty holders when following rules and regulations in the UKCMS. One boundary for the migration strategy is that its implementation considers the fact that conformity to IEC 61508 is not mandated by any UK shipping regulating authority. One such authority is the IMO, which governs internationally. Efforts to change rules at an international scale is not the concern of the project (just UKCMS practice). The IMO influences the rules set by classification societies; therefore, the researcher needs to find the 'top level' authority for regulations in the UK, and designating them (or other organisation that is best suited) the duty holder for term definitions.

In 2001, the HSE introduced the R2P2 document. R2P2 states that (HSE, 2001): it describes *"HSE's philosophy for securing the health, safety and welfare of persons at work and for protecting others against risks to health and safety arising from work activities, and the procedures, protocols and criteria underpinning the philosophy"*.

R2P2 also states: "*criteria by which HSE, in complying with its functions, decides upon the degree and form of regulatory control that it believes should be put in place for addressing occupational hazards. It considers the way scientific evidence (or the lack of it) and uncertainties are taken into*

account and how the balance is struck between the benefits of adopting a measure to avoid or control the risks, and its disadvantages."

One Expert indicated that the R2P2 includes rational for the use of terms in health and safety regulations, and how these terms are defined. Such methodologies and philosophies may indicate objectives for introducing universal uses of the terms ALARP and acceptable in the UKCMS.

R2P2 consists of three parts, part 2 Reviews some of the developments in the UKs health and safety legal framework that influenced the approach to decision-making since the HSW Act was enacted.

The HSWA1974 states that an employer's duty is (HSE, 1974): *"to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees" and "to conduct his undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not exposed to risks to their health and safety"*.

The HSWA1974 calls for lowering risks to So Far As is Reasonably Practicable (SFARP). The HSE includes in its definition of ALARP that: *""ALARP" is short for "as low as reasonably practicable". "SFAIRP" is short for "so far as is reasonably practicable". The two terms mean essentially the same thing and at their core is the concept of "reasonably practicable"; this involves weighing a risk against the cost needed to control it. Thus, ALARP describes the level to which we expect to see workplace risks controlled."*

R2P2 part 2 addresses the above by indicating how values, preferences, and expectations of society advances industries views on risk, and how changes are made to regulations.

The 'review of developments that have influenced our decision-making approach' discussed in R2P2 part two identify the following three points:

- Health, safety, and welfare at work could not be ensured by an ever-expanding body of legal regulations enforced by an ever-increasing army of inspectors.
- Primary responsibility for ensuring health and safety should lie with those who create risks and those who work with them.
- The law should provide a statement of principles and definitions of duties of general application, with regulations setting more specific goals and standards.

The third point provides a rational for objectives that overcome the remaining barriers. The barriers exist because no single organisation is considered the arbiter for the definitions in question. R2P2 describes HSEs definitions for 'hazard' and 'risk' and states their distinctions. The route for having these definitions universally accepted may be applied for the term 'ALARP' and acceptable.

Australian Risk advisers R2A considers ALARP & SFAIRP to have different legal interpretations (R2A, 2022). Whereas in the UK, ALARP is a legal requirement and is based on the concept of residual risk being Broadly Acceptable or Tolerable and ALARP, that is not recognised in Australia and risk has to continue to be reduced by any means that are reasonably practicable. The grossly disproportionate concept that is widely used in the UK may not be acceptable internationally and Cost Benefit Analysis may not apply.

The Australian Work Safety Act states the following (GOV.AU, 2011):

"What is reasonably practicable is determined objectively. This means that a duty-holder must meet the standard of behaviour expected of a reasonable person in the duty-holder's position and who is required to comply with the same duty.

There are two elements to what is reasonably practicable. A duty-holder must first consider what can be done, that is, what is possible in the circumstances for ensuring health and safety. They must then consider whether it is reasonable, in the circumstances to do all that is possible. This means that what can be done should be done unless it is reasonable in the circumstances for the duty-holder to do something less."

This approach is consistent with the objects of the HSWA1974 which include the aim of ensuring that workers and others are provided with the highest level of protection that is reasonably practicable.

The term fail safe can be contentious for many industries, particularly where the safe state may leave the system inoperable and thus unavailable. In some cases, it may mean that services cannot operate (such as grounded planes) and in other cases it can introduce a new unsafe state (such as a battleship or fighter aircraft for example which cannot carry out essential operations). Applied to the UKCMS, a cargo ship rendered inoperable in a shipping lane poses a hazard to other ships.

The term inherently safe poses the following challenges:

- Unless developers are familiar with the requirements of (all parts of) IEC 61508, this can be misunderstood. For example, how safe is SIL 2 developed software if it is housed on a single channel PC (i.e., hardware fault tolerance = zero)? Other open standards do not address this issue as well as IEC 61508.
- Non-deterministic situations can occur in a large and complex distributed network where real-time software is affected by delays and can exhibit unpredictable behaviour. These situations make the application of IEC 61508 difficult to achieve as there can be a large number of safety functions. Developers then tend to apply a particular SIL to the whole system rather than individual safety functions.
- It may be difficult to effectively partition safety and non-safety functions where legacy and/off the shelf elements are used. This often limits the extent of quantitative analysis applied and more qualitative analysis is carried out as justification of a safe system. Phrases such as "following the intent of IEC 61508" are used. Rather than adhering to parts 2 and 3 of the IEC 61508 standard, good practice may be followed against compliance to part 3 for software but due to use of COTS hardware it is difficult to apply IEC 6158 part 2 so a qualitative argument may be used based on analysis of specific safety functions.

In the defence sector, accident/mishap severity is often assessed as the effects to personnel and also damage to equipment, a definition borrowed from US MIL-STD-882E. Thus, Cost Benefit Analysis is widely used to assess if safety measures are proportionate to the benefit gained. In the UK, ALARP statements against identified safety hazards must undergo approval by the relevant MOD authority. At Risk Class A and B this is often 1 or 2 star level.

Taking the above into consideration, the following actions need to be taken to determine the overcoming of barriers B.16 and B.17:

- The hierarchy of regulatory duty holders, laws from whom UKCMS companies comply with.
- Where in the partition between international and UK law makers exist in the hierarchy.
- How UK regulatory duty holders get their laws (and definitions for terms) introduced into the regulatory framework.

The researcher must also consider the regard of SFARP in UK safety law, and its possible use as a steppingstone between current risk reduction philosophy in the UK commercial mariner sector, and reduction of risks to ALARP.

To summarise the other challenges related to the barriers:

- The migration strategy should address the use of SIL 2 risk targets on single PCs.
- Nondeterministic situations relating to the failure of complex systems.
- The consequences of regarding a whole ship as a system, and determining the SIL target.
- How safety and non-safety functions are separated for bespoke and COTS systems.

The IACS are organisations that provide guidance and interprets international statutory regulations for the IMO by its member states. Commercial marine sector companies from the member states adopt the classification society interpretations, and receive classification as a mark of conformity to the IMO rules. IACS provide consultation for IMO regarding the application of technical rules that satisfy IMO conventions.

LR is the classification society representative for the UK. LR are responsible for defining the LR Rules for Ships, which govern safety standards for the UKCMS. LR states that (LR, 2020):

"A ship is known as being in class if she meets all the minimum requirements of LR's Rules, and such a status affects the possibility of a ship getting insurance. Class can be withdrawn from a ship if she is in violation of any regulations and does not maintain the minimum requirements specified by the company".

Alterations to a ship need to be approved by LR. LR are also responsible for annual inspections of a ships safety features and systems. Classified ships receive a load line certificate.

6.5.2 D class ships risk classification

So far, the Experts provided one objective for each barrier. For barrier 1, the Experts recommended the implementation of D ships risk classification matrices. This objective synergises well with other objectives that call for greater communication between other engineering sectors.

The implementation of D ships risk matrices comes from the UK defence sector. The barrier states that the IMO does not provide a definition for ALARP. Expert 5 stated that the D ships risk reviewing process provides a *"consistent and proportionate approach when reviewing Safety Risks to demonstrate that ALARP judgements are robust"*. If adopted by the UKCMS, an IMO legislated definition for ALARP is not required.

The process involves 9 steps, illustrated in Figure 7.

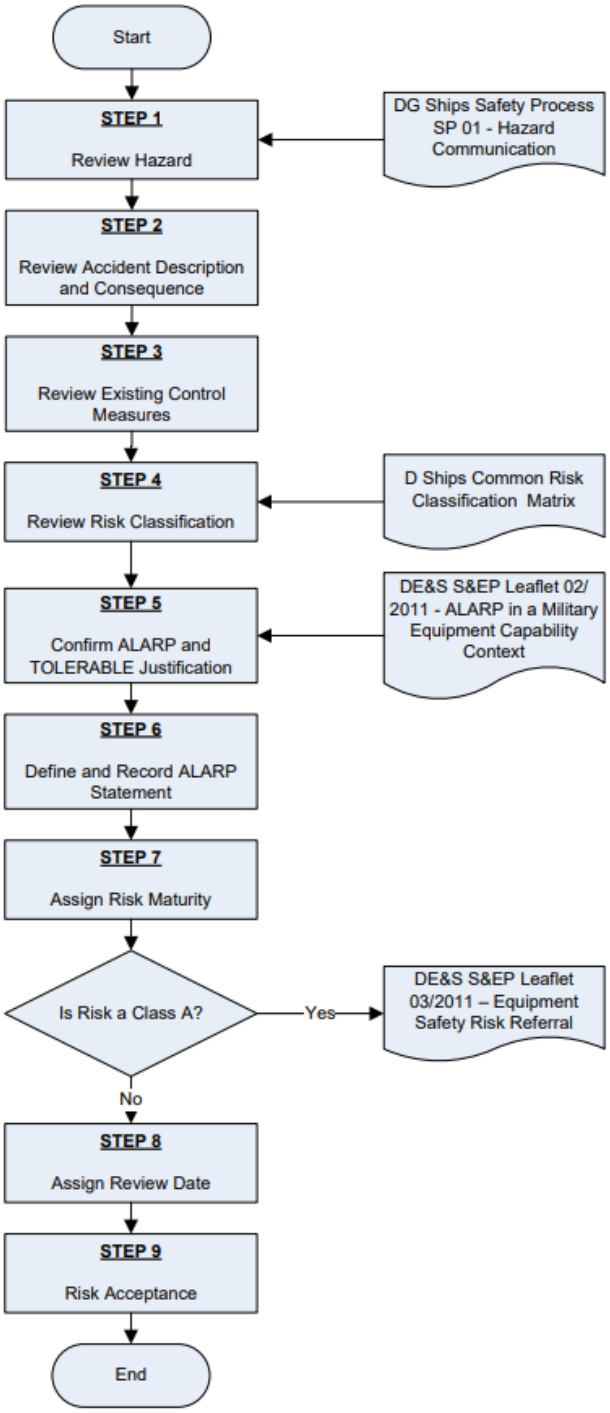


Figure 7. D ships risk matrix flow chart

Each step is satisfied by answering related key questions. Step 1 requires the Hazard in question to be described correctly (measured against the DEF STAN 00-56 definition), and checks that the correct authority is managing the risk.

Step 2 involves identifying the worst case scenario likely to occur as a result of the hazard. A risk is considered the product of a hazard's frequency and consequence, step 2 includes in the safety case an investigation regarding how harm from a hazard is related to its level of risk (i.e., is harm from high frequency low consequence risks easily mitigated).

Step 3 involves ensuring that legislated requirements regarding risk management met, that control measures align with good practice, and that all that is reasonably practical is done to lower the risks associated with the hazard in mind (ALARP). In order to determine whether a risk has been reduced to ALARP, it is first assigned a risk classification via Table 22.

Table 22. D ships risk matrix risk classification table

Risk Classification	Factor to Justify not Making the Safety Improvement
Class A	If the cost exceeds **10 times** the benefit in terms of VPF/VPI and time the hazard is exposed to the user, the sacrifice is judged to be grossly disproportionate to the benefit gained.
Class B	If the cost exceeds **6 times** the benefit in terms of VPF/VPI and time the hazard is exposed to the user, the sacrifice is judged to be grossly disproportionate to the benefit gained.
Upper Class C	If the cost exceeds **4 times** the benefit in terms of VPF/VPI and time the hazard is exposed to the user, the sacrifice is judged to be grossly disproportionate to the benefit gained.
Lower Class C	If the cost exceeds **twice** the benefit in terms of VPF/VPI and time the hazard is exposed to the user, the sacrifice is judged to be grossly disproportionate to the benefit gained.
Class D	If the cost exceeds **the benefit** in terms of VPF/VPI and time the hazard is exposed to the user, the sacrifice is judged to be grossly disproportionate to the benefit gained.

The VPF and VPI refer to Value to Prevent a Fatality (VPF) and Value to Prevent an Injury (VPI).

Expert 5 stated: *"R2P2 introduced the concept of Value to Prevent a Fatality for attributing a sum of money to the reduction in probability of a fatality from a hazardous event"*. There is no central Departmental policy in the defence sector (nor is there for the IMO) on the figure to be used, therefore the Department for Transport published figure for 2007 is used. D Ships mandated in 2009 that a VPF of £2M should be used to calculate the proportionate cost of a risk reduction option. The Value to Prevent an Injury (scaled down from VPF) are shown in the below.

Table 23. Value to Prevent an Injury table

Level of Harm	VPF / VPI[10]
Individual Death resulting from accident	£2,000,000
Individual Permanent RIDDOR Injury	£200,000
Individual Recoverable RIDDOR Injury	£20,000
Individual Non-RIDDOR Injury	£2,000

The risk classification is reviewed in step 4. First a risks frequency of harm and risk classification are used to determine the risk's appropriate location on a D Ships Common Risk Classification RIDDOR Matrix.

The frequency of harm reduction by control measures is then verified using available data. Used data comes in the form of quantitative analyses, exercise of experience and personal judgements from SQEP individuals, and accident data.

The remainder of the D ships classification matrix methodology revolves around the confirmation of the definition for a risk's tolerability, assigning a risk maturity, and reviewing the data before accepting the measures taken to address a risk.

Implementation of this process uses many methods and sources of data that are not relevant to a single engineering sector, and already feature as methods included in IEC 61508. Evidence already collected suggests that in order for the UKCMS to adopt this method, it may require intervention from the ICASs.

LR makes use of classifications for technology qualifications in their Rules and Regulations for classification. In chapter 6, tables provide minimum safety requirements for technology based on certain criteria (e.g., minimum lighting levels for areas based on their operation, permitted inclination of a ship based on the number of essential electrical and safety systems and their position on the ship, the viewing distance of warning labels, insulation classifications, etc). These tables are similar in structure to D class ships risk classification tables; however, decisions are not made based on risk in LR Rules and Regulation for Classification as these are delegated to SOLAS. LR Rules and Regulations for classification could integrate D class ships risk classification as a way to satisfy the 9 steps of the D ships risk matrix flow chart, by merit of its structural similarities. Alternatively, a version that classified UKCMS ships could be referenced; however, this requires the production of a generic ships version of the D class ships risk classification to be produced. The benefit of conducting this work may result in a means of determining SIL levels of SRSs in the UKCMS using familiar methods and communication.

In order to overcome the second barrier which states: Inconsistent understanding of what acceptable means between different legal frameworks. The Expert's interviews resulted in the suggestion that companies reduce risks to SFARP universally in the UKCMS.

The HSE states (HSE, 1974): *"The Health and Safety at Work etc Act 1974 is the primary piece of legislation covering occupational health and safety in Great Britain. It is sometimes referred to as HSWA, the HSW Act, the 1974 Act or HASAWA"*. The HSWA1974 calls for lowering risks to so far as is reasonably practicable, therefore it can be inferred that this objective is essentially satisfied (or that no further work from a regulatory perspective can be done to achieve this objective).

When interviewing the Experts previously, they emphasised the inclusion of the following objectives.

- Implementation of functional safety audits.
- Use of pre-certified systems (similar to use of COTS systems).

- Inclusion of IEC 61508 in LR in the Rules and Regulations for the Classification of Ships. This may require interventions by IACS (three routes for this).

Functional safety audits are included in the process of implementing IEC 61508, and use of certified COTS is suggested in Objective 8 (O.8).

The remaining two objectives for barrier B.16 should involve the intervention of ICAS's to regulate the elements of IEC 61508 that UK marine sector companies have challenges implementing (such as conforming to the concept of ALARP without a current IMO definition).

These objectives would state:

O.20: Implementation of D ships risk classification matrices.

O.21: Inclusion of D ships risk classification as part of the LR Rules and Regulations (and consultation to IMO)

O.22: Education and training in D ships risk classification matrices use within the UKCMS.

Objectives for B.17, regarding the definition of acceptable used universally within the UKCMS:

O.23: Use of SFARP universally in the UKCMS.

O.24: Definition for acceptable established by the appropriate regulatory duty-holder.

O.25: Completion of process that results in regulatory duty-holders definition overriding other definitions for acceptable.

6.5.3 Inclusion of rules to the IMO or LR

When there exists demand for new rules set by the IMO, safety committees are established internally called Maritime Safety Committees (MSC). Each MSC comprises of individuals with knowledge, qualifications, and backgrounds that tailor the focus of Expertise the MSC represents (relevant to the proposed rules). MSCs propose rules for the IMO, which are discussed in plenary sessions. Plenary sessions facilitate discussion between MSCs, representatives from flag states, and representatives from Non-Government Organisations (NGO). Flag state representatives provide details regarding if and how the proposed rules may be implemented by each flag state, then vote to decide whether or not they should be implemented. NGO representatives include industry leaders, and provide a practical perspective outside of the flag state representatives more legislative perspectives. NGOs are not granted a vote, as they do not represent a legislative authority, however the flag state representatives consider their input. The plenary sessions conclude with a vote regarding if rules, or amendments to current rules should be included in IMO rules and regulations. The UKs flag state representative is the Maritime and Coastguard Agency (MCA).

LR may propose and implement rules independently when IMO are lacking rules that adhere to the HSE. Similarly, to IMO, LR will produce a committee of Experts to propose rules, and vote on their implementation internally after meetings analogous to IMO plenary sessions. LR must consider however how new rules effect their competitiveness with other classification societies. Implementing

more rules that improve safety will likely increase the cost of classification, increasing the risk of customers seeking classification with other classification societies. If a major hazard occurs on a classified vessel, the classification society are responsible in part for permitting the conditions for the hazard to propagate, and suffer costs to reputation.

6.6 Barrier measures discussion

Most of the methodology is discussed throughout chapter 6, identification of another tier of categories (Education, guidance, awareness, etc) was necessary for deciding which objectives to carry forward, and which to merge or eliminate. What it achieved was a balanced approach towards addressing the new categories, whilst maintaining the proportionate response to the BSC perspectives as identified in the previous studies. Migration from current practice to accepted good practice will require an iterative review of the objectives and measures, reviewed using the same methods previously used, with gradual inclusion of quantitative data as it becomes more available. The objectives and measures arrived at in this project should address the most pressing approaches towards overcoming the identified barriers. Other objectives and measures identified in this thesis could act as a starting point for the development of the BSCs future iterations.

The method used to arrive at the objectives and measures suffered from many limitations. The number of Experts interviewed was quite low, at only 5. The inclusion criteria for the study was very rigorous to ensure Experts contacted where suitably qualified to provide as valid an opinion as possible, at the cost of a larger pool of participants. Evidence to suggest that some of the opinions given in the interviews were well informed is evident where different Experts repeated suggested objectives and measures. Experts were interviewed independently, and could not influence the answers of other Experts.

Elimination of objectives from the full list was conducted primarily by the researcher using judgement. In most cases, decisions for which objectives to merge or eliminate were trivial, and a full explanation for the researcher's logic was given. Others conducting this stage in the research may have different opinions to the researcher, resulting in a different array of objectives. The opinions of the researcher however are influenced by discussion with multiple industry Experts and literature reviews at the time of conducting this stage of the methodology. Full protection from subjectivity is impossible, however the methodology is designed for iteration, and more important objectives may be determined in the future. Time limitations for the project did not permit a more thorough investigation in this regard. A long term commitment to the BSC and migration strategy that results from the next chapter, involves iterative review of the objectives and measures considered (as mentioned above). Changes to the UKCMS independent to this strategy (e.g., in the event of organic inclusion of IEC 61508 into the Lloyds Registers Rules and Regulations) may partially invalidate the decisions made in this project. As stated before, it is the intention of the research to represent the most important barriers and perspectives in this project's migration strategy.

Experts could not apply bias towards one another, however bias in for form of the application of methods from the organisations the Experts came from was unavoidable. Expert 2 provided knowledge from the Naval sector, hence the recommendation of a method that aligns with the D ships classification matrices. The Experts represented a diverse range of backgrounds however,

which helped to rapidly determine the method for inclusion of IEC 61508 as a topic in an IACS plenary meeting, and identification of other regulatory documents that provided routes for the BSCs implementation that the research did not know about.

The study that is the focus of this chapter would benefit primarily from a larger pool of Expert participants. Cross sector interaction was identified as a useful approach early in this project. The barriers so far align with the typical perspectives of a BSC, plus cyber-security and regulatory. The requirement of further perspectives makes 'balancing' the BSC more difficult, but necessary. If the method is deemed useful for a future project, but use of the BSC perspectives is insufficient, the researcher suggests the use of the perspectives that represent a socio-technical system, described in section 9.3.5.

6.7 Barrier measures conclusion

The two studies conducted in this chapter (the structured interviews, and post interviews literature review) yielded data to produce a list of objectives, and an approach to measure the successful completion of each objective. Data is discussed as it is presented, and means for improving the study's methodology are presented in the discussion of this chapter should the experiment be conducted again.

Chapter 7. Measure performance assessment

This chapter concerns a survey that asks Experts to rate the progress made towards completion of 25 objectives on a BSC whose vision is to implement IEC 61508 in the UKCMS. The results of the study indicate that technical requirements for adopting IEC 61508 guidance are relatively straight forward to achieve, as per hypothesised after the amendment of the methodology. Cultural, social, and adapting for future developments in cyber security pose moderate obstacles to the standards implementation, however these may be mitigated effectively with increased education. Long term committal to IEC 61508 guidance in other engineering sectors proves changing safety culture takes a lengthy period of time, implying that cultural change probably cannot occur in the short term. Financial and Regulatory barriers to IEC 61508s implementation are indicated as the most difficult factors to address indicated by their low ratings in the survey. Results from the survey verified observations made in previous studies, that financial and regulatory issues are linked. Ship owners and managers within the marine sector are reluctant to make the required financial investment without regulatory incentive. The current frequency of functional safety accidents in the UKCMS do not incentivise the standards implementation from a social perspective. The discussion of the results highlights the necessity to adapt the BSC in order to provide a more effective strategy for the Engineers who participated, this being a symptom of the BSCs genericity.

7.1 Measure performance assessment introduction

The product of the previous chapters include the components required to generate a BSC that identifies the barriers that may impede the implementation of IEC 61508 by the UKCMS. Measures for each objective are determined, and the number of objectives per barrier are proportional to the barriers significance in the opinion of a group of engineers and engineering sector safety regulators with a diverse range of relevant backgrounds and experience.

The purpose of this chapter is to construct a BSC using the components made in the previous chapters as well as visualising the BSC. The BSC in this project represents the fourth stage of an IMO Formal Safety Assessment. Typically, a cost benefit analysis is conducted for control options that concern a risk or implementation of a new standard. This projected replaces a normal cost benefit analysis with an analysis of the measures proposed in the BSC (as they are derived from objectives which are analogous to accepted risk options typically derived during the third step of a Formal Safety Assessment).

After the BSC is constructed, the progress of measures are determined, from which, actions may be derived to satisfy the BSC objectives via the identified measurement methods. The implementation of a BSC is iterated until the vision is achieved. Each iteration should review the methods that objectives are measured by, and amend if inadequate. This process is demonstrated in the next chapter.

7.2 Migration strategy BSC

As mentioned section 7.1, the purpose of the previous three stages of the FSA structure of this project was to produce the information to be inserted into the 3 tiers of the BSC below the vision. This project's BSC is communicated via an excel spreadsheet (see Appendix D). The columns

header the Perspectives, Barriers, Objectives, and Measures sequentially. Each Barrier, Objective, and Measure are also labelled with a code number for prompt reference. Each row encapsulates all Barriers, Objectives, and Measures within their respective Perspectives, and this pattern is repeated for multiple objectives bound by a single barrier, and multiple measures bound by a single objective.

The benefits of formatting the BSC this way includes ease of referencing and clarity of information. The code numbers for each component of the BSC allow for prompt reference during assessment and illustration.

7.3 BSC visualisation

The methodology chapter describes the process and structure of GSN. GSN typically features the same components as a BSC in the form of a flow chart; therefore, it is trivial to insert the barriers, objectives, and measures into a GSN style success map flow chart. There does not exist a normal format for success maps as they are tailored to satisfy their respective vision. This project's success map stands out from typical success maps by utilising the GSN context nodes. Context provided relates to the objective types identified in Chapter 6. The success map is provided in Appendix E.

7.4 Measure performance assessment methodology

After the BSC and success map were produced, a survey was used to assess the progress of the objectives, and determine actions for satisfying the measures. The survey consists of three key stages. Participants were asked to:

1. Provide a statement concerning background, achieved qualifications, and knowledge relevant to the topics of the project.
2. Provide scores that represent progress made towards the completion of 25 objectives.
3. Provide their opinion regarding actions/tasks/methods for improving the progress, or achieving the successful completion of each objective if/where possible.

Participants were recruited from the pool of participation in past studies conducted for this project, individuals recommended by the principal investigators supervisory team, and individuals delegated by confirmed participants. The participation criteria involved achieved qualifications and or a background related to the following topics:

- UKCMS, and or UK marine sectors regulatory framework.
- IEC 61508, its daughter standards, and or functional safety of SCS in general.
- Cyber Security in the UKCMS.

Such narrow criteria resulted in a small number of participants initially, however individuals that qualify were likely to know of others who also qualify.

Appendix F provides the survey literature and results in full.

7.5 Measure performance assessment results

Only 1 Expert provided numerical ratings representing the progress made for each objective. The far right column indicates the score for each objective. Experts were provided the option to either place

a cross in the corresponding scores column, or write the score in the far right column Expert 1 provided both.

Table 24. Expert 1 Measure success ratings

	Score											
Objective	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
O.1								X				7
O.2									X			8
O.3								X				7
O.4							X					6
O.5							X					6
O.6							X					6
O.7							X					6
O.8							X					6
O.9								X				7
O.10									X			8
O.11					X							4
O.12					X							4
O.13						X						5
O.14				X								3
O.15				X								3
O.16								X				7
O.17							X					6
O.18			X									2
O.19			X									2
O.20				X								3
O.21				X								3
O.22	X											0
O.23				X								3
O.24	X											0
O.25	X											0

7.6 Measure performance assessment Discussion

This section discusses the points made by survey participants, whilst the next chapter derives recommendations for improving the progress of measures, or how to adapt the objectives and measures to better represent solutions for combatting each barrier. Whilst the survey asked for comments for each measure individually, the following section separates the BSC into its perspectives, as some objectives within their perspectives required similar or related methods of measurement.

The small number of survey participants suggests that the results may not reflect the UKCMS as a whole. An assumption made during the following discussion is that decisions made by companies

and organisations that the participants come from or have worked with are widespread (meaning that they are more likely to be implemented by other companies and organisations than decisions required to progress the poorer scoring measures).

7.6.1 Technical measures

The technical measures scored very well, aligning with one of the initial assumptions of the project that technical requirements for implementing IEC 61508 are achievable with relative ease, and that the more significant obstacles would be the those relating to the other perspectives. Expert 1's company hired a number of engineers to implement IEC 61508 suitable for the level of independence required. In anticipation of companies and organisations having no issues hiring the engineers required as long as the other barriers to the standards implementation are addressed, the recommendations should address Expert 1's concern relating to disagreements between engineers regarding required independence. This may actually be a cultural issue, rather than technical.

Expert 2 stated that the level of consultant support for IEC 61508 is already significant, and it would take little effort to align with the marine sector requirements. They suggested therefore to engage consultants to initiate mapping against a real life system and start documenting findings.

The second measure from the technical perspective is impeded primarily via data protection and a lack of past data. Objective 2 is mostly circumvented by using high quality COTS systems, possibly necessitating a re-evaluation of how to combat Barrier 2. If finding evidence to base quantitative risk assessments off is unfeasible, then high quality COTS may be a suitable alternative.

Expert 2 suggests engaging a stakeholder wishing to improve safety system performance, and to collaborate to develop a case study.

Case studies are mentioned multiple times during the remainder of this thesis. A case study in the context of this project is defined as a research strategy that investigates the implementation of change in an engineering environment. A case study results in literature describing the process of implementing the change, and the result of the change. A case study demonstrating the implementation of IEC 61508 requires observation of an organisation conforming to the standard, and recording the benefits and shortcomings long term.

7.6.2 Cultural measures

The cultural measures revolved mostly around awareness of IEC 61508, and communication.

Engineers that received qualifications for implementing IEC 61508 at Expert 1's company were resistant to the idea at first, but realised the necessity over a long period of time. Long term education appears to be the obstacle, as engineers were also reported to be resistant to the use of the guidance when 'timescales were tight'.

Expert 2 states how Training and education regarding risk based safety and safety life cycles is already available. The UKCMS should therefore only need case studies relevant to the sector to provide context.

Expert 1's company provided funding for engineers that wished to attend functional safety seminars, however the underlying issue of desirability to attend needs to be addressed in the recommendations.

The recommendations could address the use of steppingstones or other standards that are similar or inspired by IEC 61508.

Use of professional institutions like the Institute of Engineering and Technology (IET), the Institute of Chemical Engineering (IChemE) and others to start elevating the profile of the marine industry requirements in safety-critical system development may aid the achievement of objective 4. Expert 2 suggests identifying relevant conferences and publishing routes to transmit case studies and papers.

Adapting company culture cannot happen without the appropriate architecture for safety-critical systems. Use of legacy systems perpetuates legacy practise; therefore, emphasis should be put on updating functional safety capability. The question must be asked however, is this necessary for companies and organisations that deal with low risk systems? Referring to companies with technology that does not qualify for SIL2 and above possibly?

An option for achieving objective 5 involves engaging British committees to understand if the commercial marine sector has specific requirements not already catered for within the existing standards. If so, then the group will raise the need to develop guidance under the BSI system which will then be communicated to the international committee for discussion.

Expert 2 emphasises the need for case studies, as sector pressure will only exist when there's demonstration of compliance and non-compliance.

7.6.3 Social measures

The short term benefits largely effect the social perception of the concept of implementing IEC 61508. Improving societal awareness requires empirical data regarding the long term effects, and committal to the guidance in IEC 61508. Expert 1 suggested monitoring of lifecycle metrics, which could be communicated graphically to aid awareness.

For older and current vessels, use of COTS technology appears to be unavoidable. Widespread availability for recertified systems should be addressed in the recommendations.

Compliant products already exist in the market; therefore, work is needed to contextualise to the sector, done by producing the case studies mentioned earlier.

7.6.4 Financial measures

Despite being a financial measure, M.9 actually measures rate of educated individuals rather than a fiscal variable. This may be indicative of the fact that if a cost must be spent, then a shipowner is unlikely to proceed without making the required financial investment. The customers' requirements are fundamental to business in any sector. Expert 1 rated M.9 quite highly, due to customers of theirs ordering certified systems. There are many opportunities for customers from any sector to learn

about good practice for functional safety (such as the SCS club seminars, and other similar talks and events).

Current implementation of IEC 61508 is one of the justifying factors for this research, therefore the rating for M.10 is understandably low. Measurement of effective risk management should be considered as a recommendation to improve the rating.

Expert 2 states risk assessment methodologies are already well established in all industries, and IEC 61508 makes use of known techniques. As a result, Expert 2 suggests no action for objective 10.

Based on the surveyed Experts, measuring the number of ship owners who actually attend talks and seminars related to accepted good practice for functional safety is possibly the most difficult task. LR advises ship owners to use robust control systems, and this will increase in necessity as automation onboard ships increases. Further guidance is already being considered by LR (imo.org/en/MediaCentre/HotTopics/Pages/Autonomous shipping) for implementation of Automated systems, and how safety should be approached. Other sectors such as the defence sector should be observed when determining how to accomplish O.11.

A current lack of major accidents relating to failure of E/E/PE systems specifically in the UKCMS has resulted in reluctance to improve the rigor of their functional safety of safety-critical systems. Observations made previously in this thesis have indicated that increasing sophistication of safety-critical technology without a proportional increase of safety rigor has caused major accidents to occur in the past in sectors that had not previously implemented IEC 61508. M.12 scored poorly as a result; however, the Experts did not comment on the efficacy of the measures method. Changes have been made to practice in other sectors prescriptively rather than before major accidents have occurred (see COMAH).

M.13 relies heavily on experience within the UKCMS. Knowledge may be taught or imported via experienced engineers. Expert 1 has worked within multiple engineering sectors and has provided Expertise across.

7.6.5 Cyber-security measures

Little progress is estimated to be made towards O.14 due to the relatively recent introduction of systems susceptible to cyber-attack. Maersk has suffered a major cyber-attack, which indicates the importance of cyber security, and its consideration early in a systems design stages. Actions for improving progress towards O.14 and O.15 will likely be similar, focusing on means to improve cyber-security capability of engineers.

Expert 1 states that Cyber security is considered in a systems design when it is included as a requirement, or if a major infringement has occurred in the past. Marine sectors globally were affected by the previously mentioned attack on Maersk. Any software driven system that is also connected to the internet, or can be accessed via second hand connections (i.e., viruses brought aboard via a USB stick) are at risk of cyber-attacks. While Expertise in cyber-security may not be necessary for smaller vessels, or vessels that do not qualify for much consideration at the design stage (i.e., systems that are completely isolated from the internet), future versions of IEC 61508 will include

guidance for implementing more robust cyber security. By recommending some form of increased awareness or training prior, it will make later adoption easier.

7.6.6 Regulatory measures

The regulatory measures were the lowest scoring of the measures, aligning with the assumption that lack of regulatory incentive is a reason for poor adoption of safety practice more costly than what is legally required. Increased flexibility in IEC 61508s implementation may be required in order to account for the 'rigidity' of the language used within, and facilitate the quantitative data collection necessary. This may be addressed in future versions of IEC 61508, or a marine sector daughter standard. Using currently implemented standards as stand ins for IEC 61508 may aid in its compliance. Where gaps do not exist in between current practice, and IEC 61508 guidance, it is likely that a standard or piece of legislation currently implemented within the UKCMS already partially aligns with accepted good practice, and adaptation of such standards could be the next step in improving the score of M.17. Expert 1 suggests a fourth route in IEC 61508 for achieving systematic integrity. Section 7.4.2.2 General requirements in part 2 of IEC 61508 currently provides 3 routes for achieving systematic integrity (IEC, 2010c), these are known as:

- *Route 1S: compliance with the requirements for the avoidance of systematic faults (see 7.4.6 and IEC 61508-3) and the requirements for the control of systematic faults (see 7.4.7 and IEC 61508-3).*
- *Route 2S: compliance with the requirements for evidence that the equipment is proven in use (see 7.4.10).*
- *Route 3S (pre-existing software elements only): compliance with the requirements of IEC 61508-3, 7.4.2.12.*

Each route represents solutions for achieving systematic integrity with decreasing levels of compliance to IEC 61508 followed 'from scratch'. A theoretical route 4S could require even less work to be done to achieve systematic integrity that still aligns with IEC 61508. If Route 3S used pre-existing software (COTS) that conform to the requirements of IEC 61508 part 3, then Route 4S could require COTS that meet a required SIL using more flexible means, such as use of pre-existing standards that converge towards IEC 61508.

Consistent language employed by regulatory frameworks, and defining quantitative safety parameters represents a broader issue, and effects not just the marine sector.

Little is suggested thus far in regards for actions to satisfy O.18. IEC 61508 will have to account for variables in functions that result from machine learning in future versions. LR have explored means for classifying automated and unmanned vessels already (Maxwell, 2018).

COTS are used in SCS in other sectors under certain provisions which will still apply to marine sector. O.19 is not achieved in the marine sector yet according to Expert 2 due to the lack of case studies, but other techniques are available.

Utilisation of D class ships risk assessment techniques provides a fundamental process for extracting the qualitative data required for determining criticality of functional safety systems. Further credibility

may be granted to the use of D class ships risk assessment as it is not normally applied to the most safety-critical of naval vessels (being submarines). As it currently exists; Expert 1 suggests that it may be too onerous for the UKCMS to adopt. Just as this project's aims are to produce a means for migrating strategy for the UKCMS, another project could be dedicated to producing the commercial equivalent of a D class ships style risk assessment, capitalizing on the suggestions made by Expert 1's feedback for M.20, M.21, and M.22. Until this work is done, understandably progress towards the previously mentioned measures is very low.

Actions for O.20 could include mapping and aligning risk concepts based on consistent risk parameters.

O.23 and M.23 may not align, as the HSWA1974 calls for companies to work to ALARP rather and SFAIRP. This should not deter implementation of SFAIRP, as the UKCMS caters not only to UK business, but other international businesses as well. Quantitative risk assessment as a whole is unlikely to be understood to a degree that it could be universally utilised by ship owners in the UKCMS, therefore focus should be put on suppliers.

The final two objectives are concerned with a universal definition of the term acceptable. Early in this project Experts stated that this was a major barrier when 'knitting' regulations from abroad with the UKs. A necessary process considering the functions of SCS may occur within the waters of any given coast.

A restriction of the strategy is its limited influence. It concerns only the UKCMS. A marine sector by definition has elements that must interface with industry from other countries. This necessitates shared standards and legislation between different marine sectors and ports, however Experts queried on this topic stated the rigidity of IEC 61508 may result in marine sectors of different countries following the guidance differently because of inconsistent definitions for terms, such as acceptable. Little is provided in regard to a means for bridging gaps in term definitions abroad, however Expert 1's recommendations involve the increased communication between LR and representatives of companies in the UKCMS.

7.7 Adaptation of BSC

Timescales for this project restricts the researcher from proceeding with the steps required to keep the BSC up to date. The BSC suffers from stagnancy as objectives are met and barriers become less and less significant, or are mitigated satisfactorily. The BSC as it exists in this project combats what is assumed based on the results of the previous chapters studies, the most significant barriers to IEC 61508s implementation. It is unlikely that any measure will ever score a maximum grade, representing satisfaction of an objective and mitigation of a barrier for the whole sector. Future studies should establish an acceptable threshold for these scores, which once met triggers a process for reassessing the barriers. If a barriers objectives are accomplished, then it is possible a barrier is mitigated to the extent that it no longer impedes the implementation of IEC 61508 (for some barriers, complete mitigation may not be required).

There are several conditions that require reassessment of the constituents of the BSC.

If measure scores never meet the required threshold, or scores decrease over time, then the measures need to be reassessed to ascertain whether or not they represent success conditions for their respective objectives.

If measure scores meet the passing threshold, then the objectives need to be checked. It is possible that the measure does not represent the objectives success conditions, thus they incorrectly signify success of an objective.

If measure scores correctly indicate the satisfaction of the objective, then its respective barrier needs to be investigated for its continued impeding of IEC 61508. If the objective has failed to overcome the barrier, then a new objective must be determined to replace it. The barrier may have transformed, or issues that necessitated the objective may have been displaced and resurfaced in another perspective (e.g., Technical requirements are met at the cost of social or financial integrity).

Should a barrier be satisfactorily dealt with, then it may be stricken from the BSC. Continued measurement may be required to ensure ‘standards to not slip’. The vision as a whole is measured by the total adherence of IEC 61508 by the UKCMS. The BSC as it exists now may not facilitate the vision entirely, as it focuses on a ‘manageable number of issues’ to deal with. Repetition of the project methodology may be required to determine or reintroduce barriers that in comparison to the currently identified barriers, were less significant but pose a sufficient gap in current practice to demand attention.

Overall, this project’s results provide a basis for recommendations that will bridge the most significant gaps between current and accepted good practice for implementing functional safety of safety-critical systems. So far, this project has indicated how total satisfaction of the BSC cannot be accomplished in a single ‘push’. Conversion towards satisfaction of the BSC may be asymptotic until all its vision is made a legal requirement in the UKCMS, as it is in other engineering sectors prone to major hazards.

7.8 Methodology shortcomings and alternatives

Many challenges arise when measuring the performance of the objectives using such a small number of survey participants. It is rare that an individual who works in the UKCMS will be confident in providing an informed opinion relating to all perspectives. The generic nature of the BSC means that it requires a pool of participants that represent the full breadth of the sector (as many Experts were approached as possible with this in mind however very few were interested in participation). The necessity of this research is indicative of the lack of knowledge regarding some of the objective’s topics, thus a small number of Experts qualified to answer all elements of the survey is expected.

Chapter 9. discusses the use of alternative means of communicating the types of barriers the BSC addresses, such as use of a socio-technical system.

An alternative approach to completing the survey involves splitting it into sections (e.g., splitting into sections relating to perspectives, or to objective types as described in the previous chapter), then asking Experts to focus their answers on sections they are confident their opinions are well informed

on. It is possible however that this may not improve participation, as it was not specified that Experts needed to answer all parts of the survey as it exists currently.

7.9 Validity of the recommendations

The recommendations given by the Experts provides a basis for producing the actions of the migration strategy. The validity of the recommendations providing a strategy that is representative of the issues the whole UKCMS faces is fairly low due to the low number of participants in the survey. Individuals invited to this project's studies however required qualifications and experience to permit the consideration of their representation of the concerned stakeholders of the migration strategy.

7.10 Measure performance assessment conclusion

The results imply that objectives for barriers 1 – 9 are already in part satisfied by the UKCMS, having scores that equal or exceed 6. Barriers 1 – 11 are bound by the typical BSC perspectives, validating further the necessity for the other two perspectives to cover other significant barriers to IEC 61508s implementation. Barrier 10s objectives both scored 4, requiring ship owners and other suitable stakeholders to invest in the education and resources required to push implementation of IEC 61508. While only scoring just below half the possible score, the cause for friction for the respective objectives is solved by the objectives themselves, thus requiring a different approach. Barrier 11 requires increased communication between UKCMS companies, and companies with similar technology and practice, the feasibility of which is unlikely due to the sensitivity of the information required with little benefit to the latter party. For the objectives with the typical barriers of a BSC, Barriers 10 and 11 will require recommendations that approach the measures from a different direction (i.e., not just a continuation of work currently being done in the sector).

The remaining barriers, represented by Objectives 14 – 25 scored far lower than the objectives that came before (with the exception for the Objectives that represented Barrier 14). The Cyber security barriers were significant enough that Experts in previous studies to suggested they should be represented in the migration strategy. The regulatory barriers were allocated the most objectives, which received most of the lowest scores, validating the necessity for the relatively large number of objectives (meaning more work is required in the regulatory perspective to overcome its barriers). Almost no progress has been made towards the tackling of barriers 16 and 17, therefore these should receive significant representation in the migration strategy.

Chapter 8. Recommendations

The purpose of this chapter is to satisfy the final stage of the Formal Safety Assessment structure this project utilises. The previous stages of the project structure have expanded on the normal Formal Safety Assessment structure by implementing a BSC to determine and analyse options for implementing IEC 61508, whilst also providing a means for communicating a strategy for migration from current practice, to accepted good working practice. This project places emphasis on strategy feasibility, however the studies have resulted in several objectives of the BSC not having straight forward methods for completion.

8.1 Recommendations introduction

This chapter represents the final stage of both this project and a traditional Formal Safety Assessment by deriving recommendations for satisfying the vision of the BSC (or overall objective of an Formal Safety Assessment). Recommendations are drawn from the results of the previous chapters study, measures performance assessment. Previous stages of the project restricted objectives and measures to a manageable number. This stage differs in that it presents all derived recommendations to provide the most options for individuals or whole companies and organisations in the marine sector to drive migration of functional safety practice.

8.2 Recommendations list

The following are recommended courses of action for progressing the success of one or more of the objectives of the BSC. Recommendations are drawn from the results of the BSC measure performance assessment.

R1. Hire enough engineers to satisfy the level of independence required for the systems a given company produces.

Expert 1 stated how this is something that already occurs within their company, but would be good practice for all UK commercial marine engineering companies that conduct Functional Safety Assessments with systems that regularly qualify for SIL2 or above. R1 could be circumvented via the use of consultants (determine options). Knowledge may be taught or imported via experienced engineers and or consultants.

R2. Prepare for disagreement between engineers in regard to required independence levels.

How this recommendation is addressed depends on the company implementing it. One way may involve emphasising the method provided by IEC 61508 for determining the appropriate independence. This may require implementation of a cultural change to the company assuming arguments against recommended levels of independence are a result of undesirable but attainable process and cost. Evidence of failure as a result of unsuitable independence for safety management could be presented to engineers to provide awareness and context to a given level of independence arrived at.

R3. Engage consultants to initiate mapping against a real life system and start documenting findings.

The results of the Measure Performance Assessment indicated that multiple objectives that had little progress made towards success because of the lack fundamental context provided to engineers if attempting to implement IEC 61508. Multiple recommendations are therefore likely to require a contextual steppingstone for engineers attempting to implement IEC 61508 in the future, such as for R2. R3 could be conducted for UKCMS SCS in general, or specific companies could have their specific systems assessed. The result of R3 provides case studies for UKCMS companies regarding failure whilst implementing, or not implementing IEC 61508.

R3.5. Hiring consultants to conduct the work for R3, or for implementing IEC 61508 in place of in-house Experts.

R.4 Integration of high quality COTS systems that comply to IEC 61508.

Many challenges associated with the Migration Strategy BSC may seemingly be avoided by implementing systems that already comply with IEC 61508 instead of adapting legacy systems. This recommendation is best suited for companies that are struggling to procure quantitative data for risk assessments because of a systems age or novelty, or due to the company's capability, or if a company does not wish to take that route.

For older and current vessels, use of COTS technology appears to be unavoidable. Compliant products already exist in the market; therefore, work is needed to contextualise this to the sector by producing the case studies mentioned in R3.

R5. Engage stakeholders to initiate wider spread desire for implementation of IEC 61508, and to collaborate with development of case studies.

UKCMS companies are more likely to implement IEC 61508 upon communication of the desire from stakeholders for compliment. Such safety management procedures are desired in other engineering sectors where failure may result in a major accident hazard. Stakeholders may address their desire to companies willing to implement IEC 61508, or action can be taken for legislative change by approaching LR or IMO.

R6. Determine and implement non-financial incentives for engineers to attend functional safety related training and seminars.

Companies may need to facilitate the means for engineers to receive the education required for implementing IEC 61508 beyond providing payment. Factors related to the desirability for an engineer to attend training and seminars may be unique to each company, so this should be investigated internally.

R7. Commitment to IEC 61508 conformity regardless of timescale.

This may be addressed when the previously mentioned case studies are produced and provide the engineers using the standard the required context.

R8. Determination and implementation of steppingstones between current and accepted good practice.

The BSC provides a route for implementing IEC 61508 and monitoring the UKCMS to ensure its sustained use, and this project addresses the barriers to its use. Further research could be conducted to determine alternative routes between nodes in the strategy, from different perspectives. One of the Experts in the previous chapter stated that “Use of professional institutions like IET and the IChemE to elevate the profile of the marine industry requirements in safety-critical system”

An option for this recommendation is to determine elements of IEC 61508 currently implemented in standards and legislation used in the UKCMS, or other standards that have elements of IEC 61508 that may be easier for the sector to implement, and determine guidance between these.

R9. Assess necessity to update functional safety capability.

R9.5. Update functional safety capability.

A UKCMS company should assess the necessity of implementing IEC 61508, or to what degree they may require. Implementing the FSA for SCS indicates the SIL demand, afterwards the necessity to implement some or all of the recommendations given can be judged (lower risk, thus demand, may require only few of the recommendations to be addressed, or little updating of capability). Assessment may require consideration toward cyber security, rather than hardware or software capability.

R10. Place pressure on the UKCMS to demonstrate compliance to IEC 61508.

This may be achieved partially from demonstrating non-compliance via the R3 case studies. Informative aid (specifically graphical illustration) may aid the implementation of R10.

R11. Widespread availability for recertified systems

R12. Measurement of effective risk management.

R13. Measure the number of ship owners who attend talks and seminars related to accepted good practice for functional safety.

LR advises ship owners to use robust control systems, and this will increase in necessity as automation onboard ships increases. Further guidance is already being considered by LR for implementation of Automated systems, and how safety should be approached.

R14. Monitor how other sectors implement IEC 61508 continuously.

R15. Increase awareness for accepted best practise regarding cyber-security of E/E/PE systems.

This recommendation is especially valid for companies that would suffer significant costs resulting from a temporary loss of systems capability.

R.16 Development of sector specific daughter standard for IEC 61508, emphasising the use of language compatible with the UKCMS.

As stated before, the UKCMS in general is likely to be technically capable of implementing IEC 61508. One of the main obstacles this project does not address is the language used in the standard

not being flexible enough for engineers to migrate from the legacy practice currently used. Engineers may find it too challenging to collect quantitative data for risk assessments initially.

R.16.5 Adaptation of D class ships risk assessment matrix for use in Commercial marine sector specific daughter standard for IEC 61508.

This project does not recommend the use of D class ships risk assessment techniques in their current form, future research could address this, however.

8.3 Recommendations discussion

8.3.1 Online learning resource options

Part of the migration strategy relies on the development of engineer's knowledge and skills regarding IEC 61508s implementation. Experience has shown that when managers send engineers to take or attend courses, they will choose between competing options. In this discussion one example is provided for the benefit of those looking for an online learning resource (IET, 2022).

The Institution of Engineering and Technology has recently launched an Introduction to Functional Safety course, teaching specifically the implementation of IEC 61508 for *"technical staff, and managerial staff managing functional safety, or involved with, the specification, design, system integration and maintenance involving complex E/E/PE SRSs".*

8.3.2 Who are the recommendations for?

This project considered barriers to the implementation of IEC 61508 to the UKCMS in general. The recommendations do not specify precisely who must address them, however they accommodate for interpretation. For example, R1 is a recommendation for a manager or employer. R2 involves responsibility shared between engineers and managers, whereas R5 relies on intervention by stakeholders to a UKCMS company or service requiring amendment to practice. Further research may involve a multi perspective investigation for each recommendation to determine how each stakeholder is affected or involved in each recommendations execution (see discussion on socio-technical systems in section 9.3.5).

8.3.3 Feasibility of recommendations?

To determine each recommendations feasibility, its costs must be determined. Costs in this case refer to time, resources, financial, and for some recommendations there may be underlying costs in the form of effort required by engineers or managers to make the appropriate professional cultural changes. Feasibility for each recommendation is determined by the ability of those implementing the recommendations to satisfy the costs. It is not required that all recommendations need to be implemented by all individual companies, or by each individual in the UKCMS, therefore the total costs are spread out.

The recommendations are drawn from an iterative set of investigations to determine a strategy for migration for the whole sector. Feasibility was considered at the very beginning, implied by the use of a BSC (due to its limited number of objectives).

The ambiguity of R3, and the reliance on several of the proceeding recommendations represents a significant challenge to feasibility.

Feasibility and necessity of the recommendations will dictate their acceptance by different stakeholders in the UKCMS. This project has highlighted the costs of implementing IEC 61508, therefore certain factors are likely to be considered by ship owners before adoption of the practice voluntarily. These factors are likely to be perceived reliance on functional safety. Small vessels with few watertight compartments, and quick access to lifeboats or hazard mitigating technology (such as handheld fire extinguishers and sound emitters), may see little benefit by further assuring the technology used. Small vessels (such as fishing or river boats) may have fewer E/E/PE SCS than large vessels (such as bulk cargo carriers and oil tankers) which may deter the owners of the former. Owners of very large vessels however may have crew that rely on functional safety far more, and may also be far more vulnerable to cyber-attacks (such as Maersk Line). These stakeholders could therefore be more likely to accept IEC 61508.

8.3.4 Future iterations of the Migration strategy

A useful immediate step for the migration strategy includes defining the boundaries and implementation of R3 in detail. The requirement of case studies and failure data related to the implementation of the standard provides an important foundation for the current and future iterations of the migration strategy. Further academic work should be done to provide support to producing case studies. These will aid both companies in the UKCMS, and regulatory bodies justifying the inclusion of the standard as a legal or classification requirement (both a possibility with the increasing interest in automation at sea).

The BSC objectives and measures need to be assessed regularly to determine the progress made by the sector to satisfy the BSC vision. Objectives may require varying frequencies of assessment, depending on the rate of data collection, and appropriate intervals. An amendment to recommendations based on updated measures should be produced based on regular time intervals, rather than based on the rate of progress, as stagnation in progress may result in stagnation of assessment.

Future academic work may involve updating this project’s BSC.

8.4 Recommendations conclusion

This chapter resulted in a series of recommendations based in the results of the previous chapters assessment. A response to the recommendations are provided, however direct actions are not provided in this project (instructions for implementing the recommendations).

Those responsible for implementing the recommendations are primarily managers of UKCMS companies that have a demand for IEC 61508s implementation independent from legislation. Individuals in a managerial position will be interested in satisfying requirements, however actions for achieving the recommendations are likely to initially require great intervention from consultants with knowledge regarding IEC 61508.

The recommendations seem to reflect the challenges overcome by other engineering sectors during their initial sector wide standard integration stage. It may therefore be in the best interest of companies wishing to increase their reliance on E/E/PE SCS in the marine sector (regardless of environment) to consider the recommendations discussed in this chapter.

Chapter 9. Conclusion

Each chapter of this thesis features a discussion of its technical contents, therefore there is no dedicated discussion chapter. The purpose of this chapter is to summarise the previously addressed points of discussion, evaluate the results of this project, and describe further work and useful areas of research in the authors opinion.

9.1 Evaluation of project aims and objectives

The aims of this project may be summarised as: producing a strategy for UKCMS companies to migrate from current practice for implementing functional safety of safety-critical systems, to practice that aligns with IEC 61508. The chosen approach for this task was to design a strategy to address the barriers to IEC 61508s implementation.

The objectives of this project influenced the approach for producing the strategy by calling for an investigation concerning the gap between current practice and practice that aligns with IEC 61508. The findings from such an investigation were then used to identify the required contributions of diverse types of stakeholders in the UKCMS. The final object involves using the migration strategy to determine recommended courses of action for the different stakeholders to actualise this project's vision.

The migration strategy this project results in satisfies each of its aims and objectives. This chapter describes in detail how each aim and objective was addressed, identifies shortcomings in the project, and describes how any obstacles they posed were negotiated.

Chapters 1 and 2 investigate how IEC 61508 achieves functional safety for safety-critical systems, and identifies the gap in its practice, and practice for achieving functional safety in the UKCMS.

Chapter 3 Determines the method for bridging the gap in practice, specifically by identifying the barriers to the standards implementation, and addressing a feasible number of them in a migration strategy.

The migration strategy is developed via a BSC with 5 tiers: the vision, the barriers, the objectives, the measures, then the actions (for which recommendations are produced. It can be considered that the vision is determined in chapters 1 and 2. Chapter 4 identifies the barriers. Chapter 5 sets the scope of the BSC by assessing the significance of the identified barriers, and deciding which are addressed in the BSC. Chapter 6 identifies the objectives and their corresponding measures for each barrier selected for the BSC in the previous chapter. Chapter 7 measures the performance of the barriers to determine the appropriate actions required to improve their factors of success. Chapter 8 describes these actions in the form of recommendations, thus achieving a strategy for migrating current practice to practice that aligns with IEC 61508.

The entire process is designed to be iterative as is necessary for industry application.

9.2 Migration strategy effectiveness

This project utilises the Formal Safety Assessment format for assessing the feasibility of implementing IEC 61508. FSA's five steps provided a logical sequence for generating the migration strategy, and synergised with the process for producing a balanced score card. FSA's 5 steps provided milestones at which to conduct research in the form of literature review where necessary, and a study to gather data from industry Experts. Each of these studies provided the sequential data required to generate an analytical hierarchy at the stage of the project where options for objectives for the UKCMS to implement the standard needed to be chosen.

Preliminary research indicated the sector in general has the technical capability to implement IEC 61508. The fourth stage of a typical FSA results in options for satisfying the vision from a financial perspective, thus the BSC facilitated further perspectives. Later research indicated the most important perspective was a legislative one, and that cyber security required objectives separate from technical capability, thus the BSC was adapted to include these extra perspectives.

No negative feedback provided in the final studies of this project was directed towards the structure of the migration strategy. The following are shortcomings determined via the experience of the researcher, and how they may be mitigated for future iterations of the migration strategy, or if a similar project is attempted.

9.3 BSC drawbacks

As mentioned in the methodology chapter, the BSC technique was designed in the 1980s. It remains an effective business management tool 40 years after, however the environment in terms of how business in general is conducted has changed in ways that highlight the shortcomings of the BSC. The following is a discussion of the shortcomings and if and how they are combatted in execution of this project.

9.3.1 People

The traditional perspectives of a BSC are internal process, financial, customer, and learning. These perspectives regard the monitoring of inputs and outputs of the contributions of a company or organisations workforce. This project has highlighted the importance of people as a factor of IEC 61508s implementation. Poor safety culture promotes a culture that places procedure and progress above safe working conditions. The customer perspective looks at people external to the company or organisation working towards the BSC vision, however several of the objectives from this project's BSC could fit into a 'people' perspective.

This project has acknowledged the shortcomings in terms of safety culture in the UKCMS by adding a culture perspective. The accidents described in the thesis introduction can all be attributed towards a lack of safety culture rigorous enough to prevent their occurrence.

9.3.2 Suppliers

Output of an organisation is typically monitored via the financial growth. Variables of financial growth however include both profits made by customers, and the costs to processes. Consider also how to monitor the outsourcing of processes, such as software writing or conducting independent safety assessments (a requirement of FSA at certain levels of system safety criticalities). Suppliers in the

past may have been addressed passively in the financial and process perspectives. The marine sectors reliance on legacy systems results in the reliance of outsourced labour for skills that do not reside in legacy practice. Experts that contributed to this project's studies considered the use of suppliers as fundamental in the UKCMS, as far as suggesting they whole standards implementation requires outsourcing the labour required. Suppliers' contribution is acknowledged in every perspective as a result.

9.3.3 Regulators

It appears there is input for objectives that monitor regulatory bodies in a typical BSCs perspectives. Implementation of any practice in the marine sector is influenced fundamentally by the maritime regulatory framework., thus warranting its own perspective. The lack of a regulatory perspective is a current weakness of a typical BSC when considering the leap regulations played in any industrial sector between now and the 1980s (see literature review for timeline).

9.3.4 Society, environment, and competition

Without a regulatory or 'direct' financial incentive, organisations require incentives that drive change from other external perspectives. Mentioned in previous chapters is the importance of a company to monitor its effect on society and the environment. An organisation cannot expect the regular flow of customers if it is responsible for a major accident hazard that effects large groups of people or the environment. An example of such an accident is Arconics role in the Grenfell Tower fire, being the supplier of the cladding that ignited the accelerated the risk to the people inside and the environment (Potton *et al.,* 2017).

9.3.5 Use of a socio-technical approach

Many of the above shortcomings of the BSC are rooted in its scope in terms of what it is used to monitor. How business is conducted has evolved as rapidly as technology has advanced. Implementation of a BSC should include iterative review of the objectives and measures, however one option for ensuring coverage of the previously mentioned shortcomings is use of a socio-technical approach when deciding which perspectives to use.

This project may have benefited from a BSC that uses perspectives drawn from a STS, plus a success map that reflects the STS network illustrated in Figure 2. Future iterations or reuse of this project should consider this method.

9.3.6 Lack of comparable quantitative data

The approach for decision making in this project relied in part on the judgement of the researcher after conducting literature reviews, and via extraction of knowledge of Experts in several ways. These data collection routes yielded mostly subjective data, therefore there is little in the form of objective or numerical data to provide a datum for validating. The merit in this project's data collecting techniques consists of having data that is subject to the bias of SQEP individuals, rather than the researcher. Should the migration strategy be implemented to an actual UKCMS company, or sector wide, quantitative measurements for each BSC measure may be collected. Among the findings of this project is the difficulty posed for the UKCMS to gather quantitative data, therefore qualitative

data gathering routes were suggested, with the recommendation to gradually move to quantitative data collection. It is apt therefore for this project to use mostly qualitative data, as it relied on involvement from individuals facing the previously mentioned obstacle. This project was originally planned to gather quantitative data in the form of iterative analytical hierarchy processes for use in determining how to proceed after each step of the formal safety assessment this project's framework uses. The findings of the first assessment indicated the barriers to this approach, and resulted in qualitative data collection until the assessment of the barriers.

9.4 Areas of further research

9.4.1 Further iterations of the migration strategy

The migration strategy requires long term commitment by a company, multiple iterations are required to ensure the strategy does not stagnate. Further research should be considered to determine what future iterations of the strategy should involve. The recommendations included movement towards quantitative measurement of objectives, therefore means for achieving this should be considered simultaneously.

Should the methodology in this project be iterated in academic work, effort should be made to increase the number of participants in the studies, and to include participants representing a broader range of stakeholders. In this thesis, stakeholders representing LR legislators, IEC safety consultants, and manufacturers of UKCMS and Naval technology participated in the interviews and surveys. Stakeholder representatives that should be sought after for future iterations are implementers of cyber-security, ship owners, representatives from other parts of the UKCMS legal framework (such as IMO and the MCA), and users and installers of current SCS on ships and ports if possible.

9.4.2 BSC objective changes

A major shift of the objectives is likely to be required when two things occur:

- As the number of case studies indicating, with quantitative data, functional safety before and after IEC 61508 is implemented.
- Conformity to IEC 61508 is legislated by IMO or for a classification from a desired society.

Objectives determined in this project, but not included in the first iteration of the BSC may be considered in future iterations as objectives are satisfied.

9.4.3 Steppingstones between current and accepted good practice

The recommendations suggested an investigation into steppingstone practice for implementing functional safety to incrementally adopt IEC 61508 via the implementation of other standards that align with elements of IEC 61508. This method would not apply to managers not interested in conforming to standards that are not mandated, however IMO or LR could consider this route if issues arise should IEC 61508 be mandated in the future. Research in this field could involve cross referencing requirements made by LR against the guidance set in IEC 61508. Eliminate any overlapping practice, then investigate the existence of standards that conform to the remainder of

IEC 61508. Determined standards already mandated by LR may be eliminated, then following the methods in this thesis, determine the barriers to the implementation of the remaining identified standards. This method aligns with this project's original methodology.

9.4.4 How other sectors implement IEC 61508 continuously

Use of a BSC requires continuous monitoring of the progress of the objectives. Implementation of FSA also required intermittent review of risks associated with a safety-critical system. Methods for achieving both may be drawn from other engineering sectors.

9.4.5 Adaptation of D class ships risk assessment matrices

A project could be designed for drawing techniques required to conduct a D class ship risk assessment matrix suitable for commercial marine sector vessels, then producing novel guidance that results in data useful for conducting a FSA in the UKCMS. This could contribute to efforts made in determining steppingstone practice.

9.4.6 Future Studies

Future utilisation of this projects work may involve the implementation of the Project Model to advertise and aid sector wide conformity to IEC 61508 while implementing functional safety systems. It is the authors opinion that research regarding the integration of a STS into the BSC should first occur, as this may improve the model's cohesion with the UKCMS. The benefits of using a STS are explained in chapter 3. The following is a description of the project model, how it may be implemented in the context of how it would affect the life cycle of a commonly used SCS, a fire alarm or suppression system, and a comment is given regarding the use of a STS in the model.

The following are descriptions of the steps required to apply the project model, meaning the methodology for UKCMS companies to adopt and iterate the work done in this project until IEC 61508 is implemented sector wide. The project model is illustrated in Figure 8. Project Model.

1. Communication of Migration Strategy to UKCMS. For the project model to be adopted by Organisations and companies in the UKCMS, awareness needs to be raised regarding the benefits of implementing IEC 61508, and how the project model may provide the means of doing so. Prior to a mandated implementation of IEC 61508, communication of the project and or model may happen at conferences relevant to the UKCMS, or via published articles from the Safety Critical Systems Club.

2. Adoption of Migration Strategy by an Organisation or Company. Once an Organisation or Company accepts the project model, the model's methodology and this projects migration strategy recommendations are communicated among individuals whose responsibilities will involve performing the required actions to implement the model.

3. Addressing relevant recommendations. The model requires iteration; however, this project has produced a starting point for the migration strategy that considers the barriers to implementation of IEC 61508 sector wide. As a single Company or Organisation does not represent the entirety of the UKCMS, judgement must be made to select which recommendations the given company or organisation can address.

4. Assessment of BSC. The recommendations communicated by the migration strategy represent the bottom of the BSC hierarchy. Performing the required actions to address the recommendations may result in the achievement of the BSC objectives, observable as via the measures. Organisations and Companies may observe the magnitude of their contribution towards sector wise implementation of IEC 61508 via their achieved BSC objectives.

5. Iteration of BSC methodology. Once a given company or organisation reaches a point of stagnancy in regard to the number of recommendations it can address, then it may consider iterating the methodology used in this project to produce the BSC in the first place. The following steps provide a sequence of checks to make as a path of decision making.

6. Determine Objective completion progress. This is done by measuring the progress of each objectives. Some objectives may be partially completed; however, some may not be affected at all by currently addressed recommendations, this may be the case for objectives that require specific action by the IMO or LR, or by the sector collectively.

7. Determine new Objectives. It may occur that certain objectives do not contribute towards a given company or organisations progress towards IEC 61508 conformity, this may be a result of change of technology or practice in the future. If this is the case, the concerned company or organisation should repeat the methods used in this project to determine new objectives that achieve the BSC vision.

8. Determine new Recommendations. It may occur that certain recommendations do not result in the achievement of objectives. In this case, the methods used to draw recommendations from the BSC objectives should be iterated to generate new recommendations for relevant for the given company or objective.

9 .Consultation or academic aid. Some companies and organisations may not have the capability to conduct the methods required for the steps above, therefore consultation or academic aid to achieve the above steps may be required.

10. Iteration until barriers to sector wide conformity to IEC 61508 are overcome. Iteration of the above steps should result in the future achievement of the BSC vision.

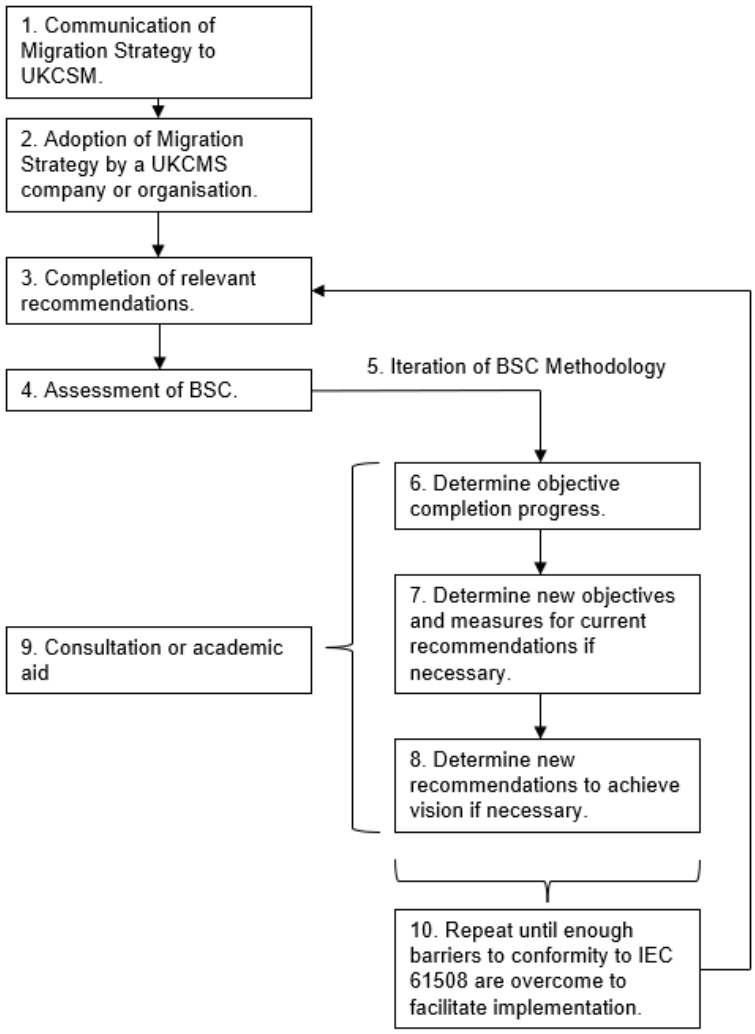


Figure 8. Project Model

9.4.6.1 Comments regarding Project model feasibility and influence

The following are assumptions made regarding applicability of the project model in its current version, they also discuss how the model's implementation may influence the implementation of a common SCS such as a fire alarm or suppression system.

Communication to small independent companies and organisations may be unfeasible if their staff do not interface with the chosen methods for communicating the project model.

The necessity to implement the project model likely correlates with the reliance of SCS, which is not likely to be consistent among all UKCMS companies and organisations (however hesitation of adoption due to other reasons such as an unattractive financial investment has been addressed).

Implementation of new SCSs would involve following the life cycle stages required to comply with IEC 61508, as well as ensuring the requirements set by SOLAS and part 6 of the Rules and regulations for Classification (if the ship owner receives classification from LR) are met. For Fire alarm and suppression systems, section 2 of part 6 of the Rules and regulations for Classification state (LR, 2020):

"Systems complying with ISO 17894, Ships and marine technology – Computer applications – General principles for the development and use of programmable electronic systems in marine applications, may be accepted as meeting the requirements of this Section, in which case evidence of compliance is to be submitted for consideration."

Already installed and currently operational SCSs would only require an appropriate FSA.

Assessing the BSC, and measuring the progress towards overcoming the barriers to IEC 61508s implementation, may become gradually more manageable as individuals tasked with implementing the model improve their understanding of IEC 61508. The means for organisations and companies to tailor the BSC and recommendations so far relies on help be those that understand the BSC methodology. It is possible some organisations and companies already have sufficient knowledge, or are willing to learn before resorting to consultation. Future studies could include the determination of a more streamlined process for this.

9.4.6.2 Amendment of methodology to include the Socio-Technical System

Future studies should consider the use of a STS when determining the perspectives used in the BSC. Modern usage of the 1974 BSC methodology is acknowledged in chapter 3. The pairwise comparison of barriers and objectives is useful for determining the priority of objectives to tackle, however the perspectives used in a typical BSC are vague. The BSC used in this project had to be expanded to accommodate two extra perspectives, Cyber-security and Regulatory, in order to address all the barriers determined. These perspectives would have been implied had a STS implemented rather than the typical four perspectives (Technical, Cultural, Financial, Social). This change would reflect the modern usage of the BSC as well.

9.5 Objectiveness of Results

The strict participation criteria for the studies requiring experts resulted in gradually decreasing participation at each stage of the project (it is possible that the COVID 19 Pandemic had an effect also). The results reflect the opinions communicated by the experts via their answers in the studies, therefore the ability to present answers that accurately refer to real life decreased proportionally.

The communicated opinions between experts did not vary significantly regarding their observations of the UKCMS, and the barriers to IEC 61508 in a generic sense. Higher participation of the Target barrier survey such that a difference between 10% and 20% consistency of answers could be observed is desirable, however. This would have indicated higher accuracy, but requires higher participation.

Should this project or parts of it be repeated, greater effort should be placed on expert recruitment. In this project a single expert was expected to answer all questions. This was decided so that the projects future studies may be designed sequentially. Now that studies are all defined, experts may be selected based on more specific knowledge and experienced, rather than their generic knowledge of the UKCMS, its regulator system, or SCS. Use of a STS may aid this.

REFERENCES

Archpoint (2019), 6 Popular strategic planning frameworks, Accessed at: https://archpointconsulting.com/strategy/6-popular-strategic-planning-frameworks, [Accessed: 31/10/2022].

Ayag, Z. (2021), *A comparison study of fuzzy-based multiple-criteria decision-making methods to evaluating green concept alternatives in a new product development environment*, Emerald Insight, Istanbul.

Ballard, R. (1987), *The Discovery of the Titanic*, Warner books, New York.

Bell, R. (2017), *Safety critical systems - A brief history of the development of guidelines and standards*, Safety-Critical Systems Club, Engineering Safety Consultants Ltd, London.

Boehm, B. W. (2003), *Error Cost Escalation through the Project Life Cycle*, NASA Johnson Space Center.

Bourne, M., Bourne, P. (2007), *Balanced Scorecard*, Chartered Management Institute, Hodder Education, London.

BP (2010), *Deepwater Horizon Accident Investigation Report September 8, 2010*, British Petroleum.

Brauner, P. (2016), Figure 1 from Preparing Production Systems for the Internet of Things The Potential of Socio-Technical Approaches in Dealing with Complexity, Accessed at: https://www .researchgate.net/figure/Adapted-Socio-Technical-System, [Accessed: 26/07/2022].

BSI (2016), *Hazard and operability studies (HAZOP studies) - Application guide*, BS EN 61882:2016, British Standards Institution.

BSI (1988), *Code of practice for safety of machinery*, BS 5304:1988, British Standards Institute.

Cambridge University Press (2022), Meaning of best practice in English, Accessed at: https://dictionary.cambridge.org/dictionary/english/best-practice, [Accessed: 05/07/2022].

Carnie, P. (2011), *A strategy for growth for the UK Marine Industries*, Marine Industries Leadership Council, UK Marine Alliance.

CEN (1997a), *Safety of machinery - Principles for risk assessment*, BS EN 1050:1997, British Standards Institution.

CEN (1997b), *Safety of machinery - Safety related parts of control systems*, BS EN: 1997, British Standards Institution.

Cole, B. (2021), ExxonMobil Baytown Explosion Declared ‘Major Industrial Accident’ As Multiple Injuries Reported, Accessed at: https://www.newsweek.com/texas-exxon-baytown-explosion-harris-county-1662506, [Accessed: 06/07/2022].

Cullinan, P. (2004), *Case study of the Bhopal incident*, Department of Occupational and Environmental Medicine, Imperial College (NHLI), London.

Cyber Security (2018), *Maersk Line: Surviving from a cyber-attack*, Accessed at: https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/, [Accessed: 23/01/2020].

European Commission (2018), *Major accident hazards*, Accessed at: http://ec.europa.eu/environment/seveso, [Accessed: 14/02/2018].

Giles, M. (2019), *Triton is the world's most murderous malware, and it is spreading*, Accessed at: https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/, [Accessed: 21/01/2020].

GLA Oversight committee (2017), *Subject: The Grenfell Tower Fire*, London Assembly, London.

GOV.AU (2011), *Work Health and Safety Act 2011*, Australian Government.

GOV.UK (2018), *The Merchant Shipping (Work in Fishing Convention) Regulations 2018*, Maritime and Coastguard Agency, Essex.

GOV.UK (2007), *Corporate Manslaughter and Corporate Homicide Act 2007*, The Stationery Office Limited, UK.

Greenberg, A. (2018), *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Accessed at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, [Accessed: 23/01/2020].

Guerra, J., Garcia, J., Lima, M., Barbosa, S., Heerdt, M., Berchin, I. (2016), *A proposal of a balanced scorecard for an environmental education program at universities*, Journal of cleaner production 172, Elsevier, pp. 1674 – 1690.

Hackitt, D. (2018), *Building a Safer Future - Independent Review of Building Regulations and Fire Safety*.

Herbert, I. (2010), *The UK Buncefield incident - The view from a UK risk assessment engineer*, Journal of Loss Prevention in the Process Industries, pp. 913 – 920, Elsevier, Aberdeen.

Hristos, K. (2009), *A Risk Based Appraisal of Maritime Regulations in the Shipping Industry*, Liverpool Logistics, Offshore and Marine Centre, Liverpool.

HSE (2022), ALARP - As low as reasonably practicable, Available at: https://www.hse.gov.uk/comah/alarp.htm, [Accessed: 11/07/2022].

HSE (2015a), *The Control of Major Accident Hazards Regulations 2015 No. 483*, Health and Safety Executive, Norwich.

HSE (2015b), *The Control of Major Accident Hazards Regulations 2015 Guidance on Regulations L111 (Third edition) Published 2015*, Health and Safety Executive, Norwich.

HSE (2011), *Buncefield: Why did it happen? The underlying causes of the explosion and fire at the Buncefield oil storage depot, Hemel Hempstead, Hertfordshire on 11 December 2005*, Competent Authority for the Control of Major Accident Hazards.

HSE (2003), *Out of control: Why control systems go wrong and how to prevent failure*, Health and Safety Executive, pp. 5, 30-31.

HSE (2001), *R2P2 Reducing Risks, Protecting People, HSE's decision-making process,* Health and Safety Executive, Her Majesty's Stationery Office, Norwich.

HSE (1974), *Health and Safety at Work etc. Act 1974*, Part 1, Health and Safety Executive. Norwich.

IEC (2010a), *IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 4*, International Electrotechnical Commission.

IEC (2010b), *IEC 61508 Functional safety of electrical/ electronic/programmable electronic safety-related systems Part 3: Software requirements*.

IEC (2010c), *IEC 61508 Functional safety of electrical/ electronic/programmable electronic safety-related systems Part 2: Software requirements*.

IET (2022), Introduction to functional safety. Available at: https://academy.theiet.org/introduction-to-functional-safety. [Accessed: 14/07/2022].

IMO (2019a), *Brief History of IMO*, Accessed at: https://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx, [Accessed: 08/07/2022].

IMO (2019b), *SOLAS,* Accessed at: https://www.imo.org/en/KnowledgeCentre/ConferencesMeetings/Pages/SOLAS.aspx, [Accessed: 06/07/2022].

IMO (2019c), *Autonomous shipping*, Accessed at: http://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx, [Accessed: 08/07/2022].

IMO (2019d), *Meeting Summaries and Schedule,* Accessed at: http://www.imo.org/en/MediaCentre/MeetingSummaries/MSC/Pages/MSC-101st-session.aspx, [Assessed: 08/07/2022].

IMO (2019e), *Formal Safety Assessment*, Accessed as: https://www.imo.org/en/OurWork/Safety/Pages/FormalSafetyAssessment.aspx, [Accessed: 07/07/2022].

IMO (2018), *Revised Guidelines For Formal Safety Assessment for use in the IMO Rule-making Process,* International Maritime Organization, London.

IMO (2017), *Guidelines on Cyber Risk Management*, International Maritime Organization, London.

IMO (2002), *Revised Guidelines For Formal Safety Assessment for use in the IMO Rule-making Process*, International Maritime Organization, London.

IMO (1974), *International Convention for the Safety of Life at Sea (SOLAS), 1974*, International Maritime Organization, London.

Joosten, J. (2010), *Applying Buncefield Recommendations and IEC 61508 and IEC 61511 Standards to Fuel Storage Sites*, Global Product Manager Radar and Safety, Honeywell, Phoenix.

Kaplan, R.S., Norton, D.P. (2007), *Using the balanced scorecard as a strategic management system*, Harvard business review, managing for the long term.

Karnouskos, S. (2011), *Stuxnet Worm Impact on Industrial Cyber-Physical System Security*, SAP Research, Germany.

Kelly, T., Weaver, R. (2004), *The Goal Structuring Notation - A Safety Argument Notation*, Department of Computer Science and Department of Management Studies University of York, York.

Kopia, J., Kompalla, A., Buchmuller, M., Heinemann, B. (2017), *Performance measurement of management system standards using balanced scorecard*, The Bucharest University of Economic Studies, Romania.

Labonté Jones, A., Lerigo-Smith, N. (2018), *Shipping Safety into the Naval Industry*, Shipping Safety into the Marine Industry V3.0, L3 MAPPS Ltd.

Lees, F.P. (2012), *Loss Prevention in the Process Industries - Hazard Identification, Assessment and Control 4th edition*, Butterworth Heinemann.

Loughran, C.G., Pillay, A., Wang, J., Wall, A., Ruxton, T. (2002), *A preliminary study of fishing vessel safety*, Journal of Risk Research 5 (1), 3–21, Taylor & Francis Ltd.

Lozano, J (2019), *Explosion, fire injures 37 at Exxon Mobil refinery in Texas*, Accessed at: https://eu.usatoday.com/story/news/nation/2019/07/31/exxon-mobil-explosion-fire-texas-refinery-injures-37/1883778001, [Accessed: 06/07/2022].

LR (2020), *Rules and Regulations for the Classification of Ships*, Lloyd's Register Group Limited, London.

LR (2016), *Provisional Rules for Software to be used in Naval Ships*, Lloyd's Register Group Limited, London, pp 6.

Mackey. A (2005), *A Practitioners' Report Based on: Shareholder and Stakeholder Approaches to Strategic Performance Measurement Using the Balanced Scorecard*, The Chartered Institute of Management Accountants, London.

MAIB (2021), *Marine Accident Recommendations and Statistics 2020*, Marine Accident Investigation Branch, Southampton.

MAIB (2020a), *Marine Accident Statistics 2019*, Marine Accident Investigation Branch, Southampton.

MAIB (2020b), *MAIB Safety Bulletin 1/2020*, Marine Accident Investigation Branch, Southampton.

MAIB (2019a), *Report on the investigation of the fatal accident to a crew member on board the scallop dredger Olivia Jean (TN35) north-east of Aberdeen, Scotland 28 June 2019*, Marine Accident Investigation Branch, Southampton.

MAIB (2019b), *Report on the investigation of the cargo tank explosion and fire on board the chemical tanker Stolt Groenland Ulsan, Republic of Korea 28 September 2019*, Marine Accident Investigation Branch, Southampton.

Maxwell, H. (2018), *What are the regulatory barriers to autonomous ships?*, Technology Bulletin September 2018, Lloyds Register.

MIIB (2008), *The Buncefield Incident 11 December 2005: The final report of the Major Incident Investigation Board*, Volume 1 HSE Books 2008.

Mitlif, R., Hussein, I. (2022), *Proposal Yager Ranking Function to Solve the Fuzzy Transportation Model via Trapezoidal Fuzzy Number*, Journal of Physics: Conference Series 2322 (2022) 012019, Baghdad.

Mokhtari, K., Ren, J., Roberts, C., Wang, J. (2012), *Decision support framework for risk management on seaports and terminals using fuzzy set theory and evidential reasoning approach*, Expert systems with applications, Volume 39, Issue 5, pp. 5087-5103.

Ndzomga, F. (2020), *The Balanced Scorecard is overrated and outdated. Here is the alternative*, Accessed at: https://fsndzomga.medium.com/the-balanced-scorecard-is-overrated-and-outdated-here-is-the-alternative-3da1ab55bdba, [Accessed: 30/10/2022].

Pomeroy, V., Twomey, B., Smith, R. (2009), *System design and integration*.

Potton, E., Ares, E., Wilson, W. (2017), *Grenfell Tower fire: Response and tackling fire risk in high rise blocks*, House of Commons Library, London.

R2A (2022), SFAIRP not equivalent to ALARP, Accessed at: https://r2a.com.au/sfairp-not-equivalent-to-alarp/, [Accessed: 12/07/2022].

RFF (2010), *Deepwater Drilling: Recommendations for a Safer Future*, Center for Energy Economics and Policy, Washington DC.

Saaty, T. L. (2008), *Decision making with the analytic hierarchy process*, Int. J. Services Sciences, Vol. 1, No. 1, pp. 83–98.

Saaty, T.L. (2003), *Why the Magic Number Seven Plus or Minus Two*, Mathematical and Computer Modelling 38, Elsevier, pp. 233 – 244.

Saaty, T.L. (1983), *A fuzzy extension of Saaty's priority theory*, Fuzzy Sets and Systems 11, pp. 229-241.

Sailor Insight (2016), *UNCLOS: The United Nations Convention On The Law Of The Sea*, Accessed at: https://sailorinsight.com/unclos/, [Accessed: 26/07/2022],

Sheen, J. (1987), *Herald of Free Enterprise Report of Court No. 8074 Formal Investigation,* Department of transport, Her Majesty's Stationery Office, London.

Sii, H. S., Wang, J. (2002), *A design–decision support framework for evaluation of design options/proposals using a composite structure methodology based on the approximate reasoning approach and the evidential reasoning method*, Proc. Instn Mech. Engrs Vol. 217 Part E: J. Process Mechanical Engineering, Liverpool.

Singh, B., Jukes, P., Poblete, B., Wittkower, B. (2010), *20 Years on lessons learned from Piper Alpha. The evolution of concurrent and inherently safe design*, Journal of Loss Prevention in the Process Industries 23 (2010) pp. 936-953.

Smith, D.J., Simpson, K.G.L. (2016), *The Safety Critical Systems Handbook 4th Edition A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition), IEC 61511 (2015 Edition) and Related Guidance*, Elsevier Butterworth-Heinemann.

Stephens, H. W. (1997), *The Texas City Disaster, 1947*, University of Texas Press, Austin.

Sutherland, V.A., Ehrlich, M., Engler, K. Kulinowski, K. (2016), *Investigation report executive summary Drilling rig explosion and fire at the Macondo Well*, U.S. Chemical Safety and Hazard Investigation Board.

UN (1982), *United Nations Convention on the Law of the Sea*, pp. 27-30.

U.S.CSHIB (2015), *Final investigation report Caribbean Petroleum tank terminal explosion and multiple tank fires*, U.S. Chemical Safety and Hazard Investigation Board, Caribbean Petroleum Company, Report No: 2010.02.I.PR., Report No: 2010-10-I-OS.

Van Der Pol, H. (2018), OKR vs Balanced Scorecard with Paul Niven, Accessed at: https://www.perdoo.com/resources/okr-vs-balanced-scorecard/, [Accessed: 31/10/2022].

Voskoglou (n.d.), *M. Use of the Triangular Fuzzy Numbers for Student Assessment (Revised),* Department of Mathematical Sciences, School of Technological Applications, Graduate Technological Educational Institute (T.E.I.) of Western Greece, Patras.

Wang, Y. F., Min, X., Kwai-Sang, C., Xiu, J. F. (2012), *Accident analysis model based on Bayesian Network and Evidential Reasoning approach*, Journal of Loss Prevention in the Process Industries 26 (2013) 10-21 , Elsevier.

Wang, Y. F., Min, X., Mohamed, S. H. (2011a), *Probability analysis of offshore fire by incorporating human and organizational factor*, Ocean Engineering 38 (2011) 2042 - 2055, Elsevier.

Wang, Y., Roohi, S., Hu, X., Xie, M. (2011b), *Investigations of Human Organisation Factors in hazardous vapor accidents*, Journal of Hazardous Materials 191, pp. 69 - 82.

Wilkinson, A. (2019), *Considerations for Industrial Security*, Integrating functional safety and cyber-security September 18th 2019, London, pp - 14.

Wright, T. (2022), *How to Implement the Balanced Scorecard Framework and Examples*, Accessed at: https://www.cascade.app/blog/how-to-implement-the-balanced-scorecard, [Accessed: 31/10/2022].

Yatsalo, B., Korobov, A., Oztaysi, B., Kahraman, C., Martınez, L. (2020), *A general approach to fuzzy TOPSIS based on the concept of fuzzy multicriteria acceptability analysis*, Journal of Intelligent & Fuzzy Systems 38 (2020) 979–995, IOS Press, Moscow.

APPENDICES

Appendix A Barrier Identification Structured Interviews

A.1 Barrier Identification Structured Interview questions

The following is the text included in a document sent to Expert participants of the Barrier Identification Structured Interview Study.

1. Interview details

Interviewer: [REDACTED]

Interviewee:

Interview date/time:

Interview location:

2. Research brief

Project title: A life cycle risk-based approach for implementing functional safety in the marine sector.

The UKCMS has witnessed rapidly increasing sophistication of technology in regard to safety-critical systems, outpacing currently implemented legislation that influences the quality of functional safety practise. In other engineering sectors that have witnessed similar phenomena, such as the rail, automotive, and defence sectors, ‘accepted good practice’ for the implementation of functional safety comes from using the lifecycle risk-based approach provided by IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) SRSs.

The project aims are to:

Identify the barriers to implementing IEC 61508 in the UKCMS.

Holistically consider the options for overcoming the barriers using a migration strategy that tackles said barriers from different perspectives.

Measure the performance of actions for overcoming the barriers, and drawing recommendations for the UK marine sector.

The project objectives are to:

Identify the challenges surrounding (or barriers preventing) IEC 61508s implementation to the UK marine sector.

Determine objectives for overcoming the challenges.

Determine measures for monitoring the performance of objectives.

Estimate values for the measures.

Propose actions for raising the value of low performing measures.

Evaluate the impact and cost effectiveness of actions.

Make recommendations to the UK marine sector based on the results of the actions evaluation (i.e., propose which actions to take in order to facilitate IEC 61508s implementation, migrating from ‘current practise’ to ‘good working practise’ for implementing functional safety).

3. Interview purpose

To gain good quality data to satisfy the first project objective from Experts with knowledge concerning the barriers to IEC 61508s implementation in the UKCMS, or other engineering sectors.

4. Interview questions

Regarding the practical problems of migrating from current practice in engineering sectors with increasing complexity of technology, to conforming to the guidelines set in IEC 61508:

What are the technical issues?

What are the cultural issues?

What are the social issues?

What are the financial issues?

What are the drivers for IEC 61508s implementation?

What are the challenges whilst dealing with cyber security and functional safety simultaneously?

What are the other challenges that the industry is facing that affects the implementation of IEC 61508?

Do you know of any other Experts with knowledge or experience relevant to the research topics?

Do you have any recommendations regarding the research topics, aims, objectives, and methods?

5. Interviewer contact details

Email: [REDACTED]

Mobile phone: [REDACTED]

A.2 Barrier Identification Structured Interview Results

The following is the Expert's consensus regarding the barriers to IEC 61508s implementation to the commercial marine sector. The brief interpretation of the results feature in section 4.3.2.

Technical Barriers

1. The marine sector has a lower technical capability compared to other engineering sectors (fewer SCS compared to sectors that currently conform to IEC 61508.)

2. IEC 61508 is not generic enough for use in all engineering sectors. (There may be issues related to SCS in the marine sector that the standard does not address. Engineers from the process sector originally wrote the standard to manage control systems and protect workers, and manage the safety of automated systems. The marine sector has very different systems to the process sector.)

3. The standard currently is not suitable for assigning SILs to automated systems.

4. Competency issues may arise without specific training for standard conformity.

5. Gathering Safety insurance evidence for high numbers of PC and PLC signals is difficult and time consuming to acquire. (A ship wide system may have up to 20 PCs at the top layer of a hierarchy. Each top layer PC may have multiple second level PCs. Progressively lower PCs will have multiple tributary PCs, PLCs, and machinery. Thousands of signals in real time.)

6. Customers of marine sector systems might not fully specify all safety functions.

7. Difficulties arise when separate stakeholders share the budget to achieve a target SIL. (Industries with highly complex SCS involve many people in systems design, development, operation, maintenance, and decommissioning. IEC 61508 provides guidance for all life cycle stages difficulties arise gathering evidence based assurance data consistently for FSAs from all domains.)

8. It is often difficult to derive value from quantitative risk assessment data for systematic failures.

9. Due to complexity of AI algorithms, hardwire backups are used to relieve reliance on software. How do you assure performance of software?

Cultural Barriers

1. There is a general lack of awareness of IEC 61508 within the marine industry. (The industry such as shipbuilders, system designers, rule makers and class societies is dominated by those qualified primarily in naval architecture, and secondly, in mechanical engineering. A narrow pool of engineers reduces interest, understanding and uptake of IEC 61508.)

2. Poor communication between different engineering sectors. (The marine sector broadly does not recognise solutions to similar engineering problems employed in other sectors.)

3. The marine sector relies heavily on legacy systems and practise. (It is not agile in regard to changing practise. The extensive use of legacy systems and software restrict practise agility. The majority of builders and designers have little appetite to build or design beyond established practices

that use easy to follow and well-defined ‘do this’ type rules. In addition, there is little awareness and no current encouragement from IMO, IACS and national administrations to adopt IEC 61508. Improving Functional safety management-practice is difficult for currently used functional safety systems; IEC 61508 requires use throughout the systems whole lifecycle. It is difficult to justify to marine safety engineers the use of increasingly complex safety systems when old precautions for low frequency hazards worked in the past, for example, why not use a single fire extinguisher for a low frequency fire hazard area despite not lowering risk to ALARP.)

4. Small numbers of accidents in the marine sector results in an underdeveloped safety culture. (Accidents are what drives society’s perception of safety, and insurance. It is difficult to make the argument for IEC 61508s implementation when existing standards and practise yields acceptably safe enough functional safety. In industries that are not, as agile in regard to changing practise, why do more work for what seems to yield the same results? It is a challenge to convince the value of compliance to IEC 61508 to managerial duty holders.)

5. In the marine sector, more automated systems are wanted but require human interaction, therefore; SCS require safety built in. (With humans in the loop, how do you ensure automated safety systems?)

6. Without Expert advice, it is difficult for a company to understand the importance of risk based, life cycle approach to functional safety. (An Expert could break the standard down into smaller manageable parts. In industry, increased dependence on evidence of competency, requires independent assessments required, requires greater amount of time to complete projects waiting for evidence. Culture wants as short delay as possible.)

7. Failing into a safe state is increasingly hard to design with complex software systems. (Traditional safety involved designing ‘inherently safe’ systems. Example, wooden water towers on the top of buildings in America, during a fire they could potentially fail safely and put the out fire. General safety involves reducing risk of a hazard, and include mechanisms for preventing or reducing consequences by failing into a safe state. The term “inherently safer” now used. Example, reducing inventory on a ship that would cause damage or harm upon unintentional release.)

Social Barriers

1. The marine sectors perception of safety mirrors societies. (It improves at thresholds, for example, after a major accident occurs and causes outrage among the public).

2. Customers and external users of SCS broadly assume robust practise when designed, due to small numbers of accidents. (Internally, duty holders may consider functional safety practise without the use of risk-based standards ‘accepted good practise’.)

3. Companies looking to implement IEC 61508 from the beginning of a SCS life cycle look at technology in a different way. (They risk restraining the complexity, or novelty, of technology in order to conform to IEC 61508. Companies may wish to find a trade-off between conformity and novelty in order to avoid technological stagnancy. If a standard restricts a company’s growth, one questions it relevancy.)

4. IEC 61508 does not use the concept of completely failure safe; you must comply with the standard to prove failure safe for specific modes of failure, the standard avoids loose language. (With floods in mind, promises made to do what it takes to make sure it will not happen again for public acceptance. The term completely failure safe is often misused.)

Financial Barriers

1. Shipping companies generally accept some risk of loss of cargo for reduced costs in safety due to insurance.

2. The initial investment required bringing old systems to acceptably safe levels, and the cost of maintaining safety throughout the entire lifecycle is off putting by ship owners. (Financial issues include the cost for training staff, and paying for documentation and insurance evidence gathering. Complying with IEC 61508 increases project completion time. Costs to implement standard, requires initial investment, but pays off in the long term.)

3. GDP and safety costs increase proportionately. (It is difficult to improve safety without growth.)

4. There is a lack of investment to safety as a whole due to lack of understanding in the marine sector. (Lack of understanding, not knowing precisely what hazards arise from failure of E/E/PE systems result in a weak argument for their defence in a cost benefit analysis. How do we know when we have done enough? Extra costs spent to satisfy independent safety auditors. Little financial gain observed when paying for higher SILS.)

5. If IEC 61508 requirements are decided after a contract award, based on risk assessment, then the cost is taken by the builder. (Typically, the shipbuilder/designer proposes a fixed-cost and assumes the financial risk after contract award unless the buyer requests a change. Therefore, if a change is identified after contract award because of risk assessment for example this is at the builders or designers' expense. Hence. Not knowing before contract award what IEC 61508 requirements are needed and the impact this might have on equipment choices is a strong reason for builders and designers not to want to embrace IEC 61508. If they do, they either take a financial risk or raise the fixed cost. With few in the industry aware of IEC 61508, and its benefits, this makes the bid uncompetitive.)

6. Costs for independent analysis for higher SIL safety functions.

7. Other costs may arise for the initial tweak in alignment effort.

Cyber security Barriers

1. Safety managers are reluctant to accept safety measures blindly. (Cyber security usually addressed via 'acceptable means of compliance', risk mitigation measures outside of what a standard calls for, reliance procedures outside of safety framework.

2. Cyber security can undermine HAZAN, as cyber security threats can result in further consequences of hazards. (Cyber security potentially increases hazard consequences and risk for hazards.)

3. Cyber security is a recent ‘shock’ to engineering sectors. (Risks to cyber security are usually ‘worked around’.)

4. Engineers do not want address cyber security risks. (They require different areas of Expertise to tackle. Addressing cyber security risk are often considered ‘not agreeable to the market’.)

5. Plants connected to office IT networks are at risk to cyber-attacks if connected to the internet. (Cyber security becomes more important the more connected a physical system is to an IT system.)

6. Independent cyber security and functional safety Experts may not achieve the target SIL if integration occurs late into a project.

7. Cyber security is way behind functional safety in regard to Expertise. (There is a lot of disagreement in regard to regulations required for cyber security.)

8 The trade-off between security requirements and safety requirements. (A general problem of all engineering sectors.)

9. A system needs in built Cyber security, or cyber security integrated as early as possible to avoid issues during operation.

10. Need to meet requirements for functional safety and cyber security, whilst complying with normative requirements for both.

11. IEC wants functional safety engineers to work with cyber security Experts, but separately.

Regulatory Barriers

1. Without consistency for fundamental terms used by different maritime regulatory frameworks regarding functional safety practise, the different tiers of the regulatory framework cannot agree where the baseline for equivalent level of safety is.

2. Inconsistency between (or lack of) legal definitions for safety-critical systems, and an understanding of accepted good practise for functional safety between different legal frameworks further increases the complexity of deciding where the baseline for equivalent level of safety exists.

3. Sprawling duty holders required for evidence gathering already causes friction for IEC 61508s implementation, increasing numbers of stakeholders as a result of increased automation on ships means increasing evidence gathering procedures.

4. The IMO does not provide a definition for ALARP (just calls for it, same as the HSWa1974). (Given the standard definition of ALARP, no third party without access to the underlying data can assess cost disproportionality.)

5. No general understanding of what acceptable means.

6. Engineers can only claim dangerous failure rates with appropriate rigor. (If a plant complies with IEC 61508 fully, a regulator will not challenge the dangerous failure rate.)

Other Barriers

1. Despite having comparatively less complex technology, the marine sector faces most of the same non-technical issues as other engineering sectors. (Environmental protection and emissions goals).

2. Engineers fear increasing requirements for proven in use arguments when implementing IEC 61508. (This would limit the use of legacy systems. A general challenge when implementing IEC 61508: engineers would prefer to use off the shelf legacy systems where possible. Their ability to do so is limited when using high SILs.)

3. Restrictions in technology to balance conformity may not be feasible.

4. Political changes may potentially cause deregulation, or dilution of standards. (Manufacturers may take advantage and relax functional safety for a market advantage.)

5. Technical staff involved in functional safety may know how to implement IEC 61508, but cannot easily convince managers they need to do it.

6. Using IEC 61508 restricts the use of 'off the shelf' systems without modification for its environment. (It is hard or sometimes costly to ruggedize a system.)

Other drivers

1. There is an inevitable merging of classifications regarding functional safety frameworks.

2. All engineering sectors want a single framework for conform to regarding functional safety. 12. As more people become aware and trained to use IEC 61508, it will become easier to implement sector the standard sector wide.

3. IEC 61508 is a basic safety standard, which is why it has daughter standards for specific sectors. The marine sector may receive a daughter standard of its own in the future.

4. The Ministry of Defence uses rules that are as least as good as statute. The Naval ship software rules states process requirements for systems, engineering systems, software producers and classification. Processes out of scope of the software rules align with early steps of IEC 61508s overall safety life cycle.

5. IEC 61508 edition 3 is in the active development stage and strongly considers cyber security for integration. A breech of cyber security can compromise power or safety of a plant and lead to an accident. Cyber security is getting increased attention by standard bodies.

6. Most sectors are adopting a risk-based approach when implementing functional safety; it would not be difficult to adapt to conform to IEC 61508.

7. New off-the-shelf systems and hardware may be compliant to IEC 61508. 11. Companies can sell Products certified to IEC 61508 at a higher price to gain a market advantage. Effort invested into certification pays off.

8. A HSE inspection requires risks lowered to ALARP (under the Health and Safety at Work etc. Act 1974), which is why IEC 61508 is benchmark for good working practise.

9. When a hazardous accident occurs, a duty holder who can demonstrate compliance to IEC 61508 can discharge duty of care (under The Corporate Manslaughter and Corporate Homicide Act 2007).

10. Big accidents usually have multiple small precursors. Small improvements made and sustained during the lifecycle of a system can help prevent a hazard from occurring.

12. In other engineering sectors, IEC 61508 chosen because it is prescriptive. Engineers like to use annex A, B part 3 as it is well laid out. 14. Older references need updating.

13. It is difficult to develop safety without high levels of reliability proportionate to complexity of technology.

14. Work is required to illustrate that the likelihood of accidents and/or their consequences would reduce, and equipment reliability would increase. This is a benefit to both the regulators, in terms of improving safety, and owners and operators. It is not a benefit to the shipbuilders and designers. Hence, it is the regulators, owners, and operators that need convincing of the benefits.

15. Many industrial companies likely already employ must of the practise required for conformity to IEC 61508. Independent Expert consultancy may be required to tweak and reiterate practise for all life cycle stages, and conduct hazard identification so that hazard data fits the standard model.

16. There may be a significant cost for an initial compliance effort, however many organisations may already employ the underpinning processes for compliance. Recouping of costs occurs in the end due to improved reliance of functional safety.

17. Raising of the cost of products and services due to conformity is unjustified.

18. Engineering sectors with poor insurance evidence gathering methods would benefit greatly by communicating with engineering sectors with good insurance evidence gathering methods.

19. IEC 61508 provides a holistic view of safety-critical systems, and provides answers for companies that ask, “Do we have what I need, when I need it” in regard to functional safety failures.

20. People want complex technology. IEC 61508 facilitates adoption of complex technology for safety systems at accepted good practise within a legal framework.

Appendix B Target Barrier Survey

B.1 Target Barrier Survey participant document

The following is the text from the document sent to Expert participants of the TBS describing how to answer the survey.

Thank you for agreeing to participate with Target barrier survey. This document consists of two parts.

Part 1 includes:

- A brief description of the Target barrier surveys purpose.
- The theory behind the survey's methodology.
- How the results of the survey contribute to my research project.

Part 2 consists of the survey questions.

If you are unclear about any aspect of this document, please refer back to the information sheet and recruitment email for guidance requesting more information and contacting the researcher.

1. Survey purpose brief

The purpose of this survey is to determine the priority of barriers to the implementation of IEC 61508 to the UKCMS.

1.1. Survey method brief

Previously, the researcher conducted structured interviews with Experts to determine the barriers to IEC 61508s implementation in the UKCMS. This survey asks Experts to allocate linguistic terms that best describe the importance of the barriers when comparing their importance to one another. Prior to this, the Experts must allocate a range on a numerical scale from 1 to 9 to each linguistic term. The closer to 9 the highest possible value for where a linguistic terms range resides, the greater the importance that term represents.

1.2. Significance of results brief

The answer to this survey facilitates the use of an AHP that prioritises the barriers within each barrier type bracket, and prioritises the barrier type brackets as well. The next stage of the project involves producing a BSC (BSC) that features objectives to overcome the barriers. Using the results of the AHP, the researcher can justify the number of objectives allocated to overcoming each barrier, or possible exclusion of barriers.

It makes sense to consider the numerical values of the linguistic terms equidistant from one another on a scale, and in logical order (equally important closer to 1 and extremely important closer to 9). Participants are required however to allocate the numerical ranges for linguistic terms in order to account for possible inconsistency between the Experts' personal definitions. The researcher requests details concerning the Expert's career for the verification stage of the project, so that the researcher may compare them against the consistency of opinion-based answers.

For more information regarding the BSC, I recommend reading, “Using the BSC as a Strategic Management System” by Robert S. Kaplan and David P. Norton. An article submitted to the July – August 2007 Harvard Business Review.

For more information regarding fuzzy set AHP, I recommend reading:

“Decision making with the analytic hierarchy process” by Thomas L. Saaty, most recently submitted in the International Journal of Services Sciences, Volume 1 in 2008.

“A Fuzzy Extension of Saaty’s priority theory” written by P.J.M van Laarhoven and W. Pedrycz, an article submitted to Fuzzy Sets and Systems 11 in 1983.

Reading and understanding the above sources are not required for understanding this survey.

2. Target barrier survey

The Target barrier survey consists of three parts:

Details regarding a participant’s qualifications and career experience.

Allocation of numerical values to linguistic terms.

Pare wise comparison of barriers and barrier types to IEC 61508s implementation in the UKCMS.

2.1. Expert details

Please provide the following details regarding your qualifications and career. If referred to in the thesis, the researcher will protect your identity by replacing your name with a pseudonym.

Name:

Age:

Years of experience in a career relevant to the research topics (positions held in the commercial marine sector, or positions that required understanding of IEC 61508):

☐ 0 – 4 ☐ 5 – 9 ☐ 10 – 14 ☐ 15 – 19 ☐ 20+

Highest achieved academic qualification:

☐ School ☐ HND ☐ Bachelors ☐ Masters ☐ PHD

2.2. Allocation of numerical values to linguistic terms

Please provide an upper value, a lower value, and a most probable value for five linguistic terms on a scale between 1 and 9, where the further from 1 a linguistic term resides, the greater the importance the term represents.

Linguistic term	**Term symbol**	**Lower value**	**Most possible value**	**Upper value**
Equal importance	E			

Equal to Weak importance	EW			
Weak importance	W			
Weak to Strong importance	WS			
Strong importance	S			
Strong to Demonstrated importance	SD			
Demonstrated importance	D			
Demonstrated to Extreme importance	DEx			
Extreme importance	Ex			

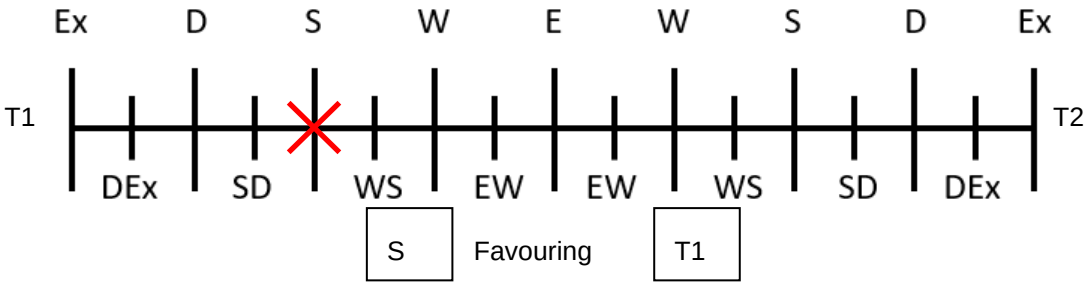
2.3. Barrier profile

The Barrier profile is a list of barriers to IE 61508s implementation, determined via a series of structured interviews with Experts, and a literature review. The profile consists of barriers, represented with a statement, and categorised into a type. Please read the following barriers, then provide pairwise comparisons that express in your opinion which barriers are more, equally, or less important to address. Please also provide pairwise comparisons between the barrier types.

2.3.1. Pairwise comparison of barriers

The following sections to this part of the questionnaire state the barriers; please provide pairwise comparisons between the barriers, using the linguistic term symbols (i.e., E for equal importance, S for strong importance, Ex for extreme importance).

For example, in a comparison between two barriers represented by the symbols T1 and T2:



By inputting S Favouring T1, barrier T1 is strongly more important than barrier T2 in regard to implementing IEC 61508. In order to answer the remainder of the questionnaire, please input the answers that represents your opinion in the text boxes, or clearly marking the pairwise comparison scale using your Word processor. Alternatively, you could print the survey, use a pen to mark the scale, scan your answered survey, and email it back to the researcher if you wish.

Each barrier type has between three and six barriers that represent the consensus among Experts. The following equation describes the relationship between the number of barriers (n) and the number of comparisons required to compare all the barriers in a specific category (C).

$$C = \frac{n(n-1)}{2}$$

At n = 3, C = 3

At n = 6, C = 15

2.3.1.1 Technical barriers

T1 – T6 represent the technical barriers:

T1. Differing technical capabilities in the commercial marine sector compared to the process sector for whom IEC 61508 initially provided guidance.

T2. Lack of competency required for IEC 61508s implementation from within the commercial marine sector.

T3. It is a time consuming process to gather insurance evidence for high numbers of PCs and PLCs on ships.

T4. Low reliance of customers' ability to define all safety functions required by safety-critical systems.

T5. Using IEC 61508 restricts the use of 'off the shelf' systems without modification for its environment, It is hard or sometimes costly to ruggedize a system.

T6. It is very difficult to assign SILs to automated SCS and artificial intelligence, with hardwire back-ups and human interaction, to relieve reliance on software.

Please compare each technical barrier and communicate, by using one of the methods explained before, which is more important to address. C = 15.

B.2 Target Barrier Survey results

B.2.1 Linguistic terms averages

Term symbol	Lower value	Most possible value	Upper value	Crisp value
E	1.00	1.00	1.33	1.11
EW	1.00	1.67	2.33	1.67
W	1.33	2.33	3.33	2.33
WS	2.33	3.33	4.33	3.33
S	3.33	4.00	5.33	4.22
SD	4.33	5.33	6.33	5.33
D	5.33	6.33	7.33	6.33
DEX	6.67	7.67	8.33	7.56
EX	7.67	8.67	9.00	8.44

B.2.2 Barrier weight averages

Technical barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
T1	0.147	0.086	0.122	0.202	0.124	13.61%	0.2154	0
T2	0.338	0.399	0.047	0.065	0.419	25.34%	0.4011	1
T3	0.192	0.247	0.066	0.081	0.131	14.33%	0.2268	0
T4	0.198	0.080	0.300	0.140	0.051	15.38%	0.2435	0
T5	0.063	0.158	0.403	0.096	0.050	15.39%	0.2437	0
T6	0.063	0.030	0.063	0.417	0.225	15.95%	0.2526	1

Cultural barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
C1	0.572	0.333	0.732	0.057	0.231	38.50%	1.4907	2
C2	0.274	0.333	0.191	0.696	0.231	34.51%	1.3362	1
C3	0.154	0.333	0.077	0.248	0.538	27.00%	1.0453	1

Social barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
S1	0.261	0.199	0.213	0.351	0.483	30.15%	0.6522	1
S2	0.298	0.204	0.415	0.092	0.157	23.35%	0.5051	1
S3	0.312	0.394	0.171	0.091	0.069	20.74%	0.4486	0
S4	0.086	0.147	0.065	0.344	0.203	16.89%	0.3654	0
S5	0.043	0.055	0.136	0.122	0.088	8.87%	0.1919	0

Financial barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
F1	0.402	0.120	0.079	0.154	0.362	22.33%	1.1568	1
F2	0.085	0.144	0.040	0.073	0.085	8.53%	0.4419	0
F3	0.161	0.244	0.206	0.242	0.150	20.05%	1.0390	1
F4	0.273	0.187	0.532	0.502	0.266	35.18%	1.8229	2
F5	0.079	0.305	0.144	0.030	0.138	13.91%	0.7209	1

Cyber-security barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
CS1	0.129	0.312	0.045	0.185	0.234	18.09%	0.3834	0
CS2	0.542	0.361	0.119	0.196	0.184	28.02%	0.5938	1
CS3	0.082	0.277	0.254	0.091	0.429	22.67%	0.4804	0
CS4	0.247	0.051	0.582	0.527	0.154	31.22%	0.6615	1

Regulatory barrier weights								
Barrier	**1**	**2**	**3**	**4**	**5**	**Average**	**Weight**	**Number of objectives**
R1	0.197	0.095	0.127	0.312	0.502	24.66%	2.4855	2
R2	0.057	0.222	0.325	0.334	0.087	20.51%	2.0675	2
R3	0.355	0.572	0.062	0.333	0.126	28.97%	2.9205	3
R4	0.391	0.110	0.486	0.020	0.285	25.86%	2.6073	3

Barrier type weights							
Type	**1**	**2**	**3**	**4**	**5**	**Average**	**Number of objectives**
B1	0.115	0.062	0.064	0.023	0.051	6.33%	2
B2	0.183	0.135	0.221	0.125	0.110	15.49%	4
B3	0.118	0.104	0.035	0.062	0.114	8.65%	2
B4	0.132	0.281	0.154	0.250	0.220	20.73%	5
B5	0.094	0.038	0.178	0.068	0.046	8.48%	2
B6	0.358	0.380	0.349	0.471	0.458	40.32%	10

Appendix C Barrier Measures Structured Interviews

C.1 Barrier Measures Structured Interviews document

The following text is from a document sent to the participants of the Barrier Measures Structured Interviews study.

1. Interview details

Interviewer: Edward Shaw. MEng, post-graduate researcher for the Faculty of Engineering and Technology at Liverpool John Moores University.

Interviewee:

Interview date/time:

2. Research brief

Project title: A life cycle risk-based approach for implementing functional safety in the marine sector.

The UKCMS has witnessed rapidly increasing sophistication of technology in regard to safety-critical systems, outpacing currently implemented legislation that influences the quality of functional safety practise. In other engineering sectors that have witnessed similar phenomena, such as the rail, automotive, and defence sectors, 'good working practice' for the implementation of functional safety comes from using the lifecycle, risk-based approach provided by IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) SRSs.

The project aims are to:

1. Identify the barriers to implementing IEC 61508 in the UK marine sector.
2. Holistically consider the options for overcoming the barriers using a migration strategy that tackles said barriers from different perspectives.
3. Measure the performance of actions for overcoming the barriers, and drawing recommendations for the UK marine sector.

The project objectives are to:

1. Identify the barriers preventing IEC 61508s implementation to the UKCMS.
2. Determine objectives for overcoming the challenges.
3. Determine measures for monitoring the performance of objectives.
4. Estimate values for the measures.
5. Propose actions for raising the value of low performing measures.
6. Evaluate the impact and cost effectiveness of actions.
7. Make recommendations to the UKCMS based on the results of the actions evaluation (i.e., propose which actions to take in order to facilitate IEC 61508s implementation, migrating

from ‘current practise’ to ‘good working practise’ for implementing functional safety of safety-critical systems).

3. Interview purpose

The researcher has conducted a series of structured interviews in that past that asked Experts to identify barriers to IEC 61508s implementation in the UK marine sector. Afterwards, the researcher conducted a survey with the same pool of Experts to provide pair-wise comparisons between the barriers. The researcher used a fuzzy variant of the AHP to determine the rank and weights of each barrier. The purpose of this interview is to determine what objectives the migration strategy should include in order to overcome the highest weighted barriers from the AHP.

4. Interview questions

In your opinion, please describe and discuss with the researcher; objectives for overcoming the following barriers, and if possible a means for measuring their progress:

1. Lack of competency required for IEC 61508s implementation from within the commercial marine sector.
2. Assigning SILs to automated SCS and artificial intelligence, with hardwire back-ups and human interaction, to relieve reliance on software.
3. Lack of awareness of IEC 61508, and the significance of a risk based, life cycle approach to functional safety of safety-critical systems.
4. Poor communication between different engineering sectors prevents recognition of solutions to similar challenges the commercial marine sector faces.
5. The commercial marine sector relies heavily on legacy systems and practise, and is not agile to adapt or update.
6. The marine sectors perception of safety mirrors societies, and improves in thresholds rather proportionally to gradually increasing risk because of increasing complexity of technology. Until a major accident occurs, users of SCS broadly assume robust practise when designed.
7. Engineers looking to implement IEC 61508 from the beginning of a SCS life cycle, they risk restraining the complexity or novelty of technology in order to conform to IEC 61508.
8. The initial investment required bringing old systems to acceptably safe levels, and the cost of maintaining safety throughout the entire lifecycle is off putting by ship owners.
9. Typically, a systems designer proposes a fixed-cost and assumes the financial risk after awarding a contract unless the buyer requests a change. If a risk assessment called for a change to a SCS design, this is at the builders or designers’ expense.
10. The costs for independent analysis for higher SIL safety functions and other costs for the initial tweak in alignment effort is off putting by ship owners.
11. Companies typically split the budget to achieve safety functions between different stakeholders, compromising a company’s ability to achieve a target SILs.

12. Cyber security can undermine HAZAN, as cyber-attacks can result in additional causes and consequences of hazards.

13. Indecisiveness regarding the trade-off between security requirements and safety requirements.

14. Without consistency for fundamental terms used by different maritime regulatory frameworks regarding functional safety practise, the different tiers of the maritime regulatory framework cannot agree where the baseline for an equivalent level of safety is.

15. Inclusion of stakeholders relating to increased automation on ships means increasing evidence-gathering procedures.

16. The IMO does not provide a definition for ALARP, given the standard definition of ALARP, no third party without access to the underlying data can assess cost disproportionality.

17. Inconsistent understanding of what acceptable means between the different legal frameworks.

C.2 Barrier Measures Structured Interview results

1. Lack of competency required for IEC 61508s implementation from within the commercial marine sector.

One Expert identified that a lack of understanding of the principles from IEC 61508 would prevent its adoption. Means of overcoming this would involve; training and education, also the advocating of this by regulators.

In the Naval sector, a lack of competency is overcome by ensuring duty holders are well aware of their relevant standards (such as DEFSTAN 00-56). This is due to their customers such as The Royal Navy (RN) demand for use of such standards. These standards need also to comply with those that Commercial Off The Shelf (COTS) systems use. The Naval sector may use in house Experts, and Human Resources staff that logs the training and qualifications of other staff members using a Suitable Qualified Experience Personal (SQEP) Framework. The SQEP framework logs the training and experience of all staff in an organisation. This aligns with the HSE and British Computer Society manual competence 1 and 2 requirements. Line managers may use this framework to send staff on courses, and receive training when needed. The Expert explaining this mentioned there are similar frameworks used in other industries. One limitation however is that IEC 61508s competency requirements are vague.

One of the Experts did not believe that a lack of competency internally within his company (Wartsila) was an issue. He pointed out that only those responsible for systems allocated SILs need to be competent, and that appropriately trained staff and consultation may be imported.

A key objective should be a commercial marine sector focused technical review of compliance with IEC 61508 to define the sector requirements (akin to what IEC 61511/62061 do for other sectors). This will then facilitate the development of knowledge based training which can be used to develop the competency required. The corresponding measure would be implementation of new standard based guidance, regulatory adoption, and commercial availability of the training.

The final Expert iterated the point that to overcome competency issues, companies typically employ competent people to produce and maintain safety-critical systems, or to direct the migration of their practice (using ESC for example).

2. Assigning SILs to automated SCS and artificial intelligence, with hardwire back-ups and human interaction, to relieve reliance on software.

The first Expert did not see this layered approach as a barrier to adopting IEC 61508. Adopting layers of protection is a sound principle for safety, although AI would introduce a level of uncertainty which is discouraged by IEC 61508.

According to Expert 2, the marine sector does not tend to use safety-critical software, but usually opts for hardwired implementation for electrical stops and PLCS (simple system stops such as off buttons. See typical electrical stops in the process sector). Put plainly, ISO 13849 is applied to anything that moves, whilst IEC 61508 is applied to the control systems of things that move. Engineers may be unsure where the use of one standard ends and the next begins. This may be an area that needs further work. Research for how this is done has been conducted in the automatic car industry.

Wartsila uses artificial intelligence to monitor the health of a system. Assigning SILs to said systems is not an issue when the risks are identified. Wartsila is reliant on suppliers of software who are compliant with IEC 61508. The real issue regarding AI comes when trying to define the safety functions, and producing precise documentation to record choices at the concept stage to prove a company did everything they could to design the risks out. One Expert pressed that the marine sector should develop case studies which demonstrate this approach in the context of IEC 61508. The measure therefore would be their adoption in industry as relevant case studies.

The issue when working with AI is that failure rates cannot easily be quantified, and provide great challenges for emerging technology and standards. Conformity to IEC 61508 however allows one to rely on software for safety-critical functions.

3. Lack of awareness of IEC 61508, and the significance of a risk based, life cycle approach to functional safety of safety-critical systems.

A risk based approach to safety is inherent in the UK's Health and Safety work act and associated regulations. A systematic lifecycle based approach to design and development of safety related systems is a sound means for reducing errors introduced by humans in the design and development process of such systems, especially as the systems become more complex, with increased reliance on software etc. One Expert simply stated that appropriate training and education should help.

Another option for improving awareness of IEC 61508 in the marine sector is providing increased publicity for the standard, and the SCS Club (SCSC).

Another Expert believed there is a lack of awareness of IEC 61508 existence at the management, not the technician level (the designers). Unlike SOLAS which gives precise design requirements, ESC standards only provide guidance. Those at top management level may be too busy to educate themselves regarding the implementation of IEC 61508, therefore they are not able to make informed

decisions. The Expert continues by stating that at Wartsila, it is difficult to apply the standard after step 12 of IEC 61508 because they have yet to deliver a compliant system.

One Expert pressed that the writing of a Commercial Marine sector focused version of IEC 61508 (a daughter branch of the standard) expressed as solution for the first objective, would serve as a measure for third objective also.

The final Expert stated that the lack of awareness of IEC 61508 is due to lack of safety discipline, and reluctance to stray from tradition (legacy practice).

4. Poor communication between different engineering sectors prevents recognition of solutions to similar challenges the commercial marine sector faces.

Communication may be facilitated using Cross sector forums, international conferences, and education. Reuse of sound engineering solutions to common problems, rather than reinventing the wheel. The benefit of adopting IEC 61508 is to have available COTS IEC 61508 certified products to be used in safety related systems (rather than producing bespoke solutions).

In order to increase communication between the marine sector and other engineering sectors, there needs to be increased attendance of engineers from the marine sector at SCS focussed conferences and symposiums (see SCSC symposiums). Alternatively, the marine sector could host such conferences for its benefit, and invite innovation from academia.

This issue may manifest as a TUV Rhineland process engineer would be communicating with marine engineers when certifying compliance of their systems. The differences in technology types may cause problems.

This objective would also benefit from the same solution to objective 1 regarding the development of the sectors own standard, with focus on identification of commercial marine focused challenges and development of case studies. The measure therefore would be a number of identified unique challenges and as per 1.

One of the Experts did not see this as an issue, and did not think other sectors did this.

5. The commercial marine sector relies heavily on legacy systems and practise, and is not agile to adapt or update.

Adoption of IEC 61508 would be easier for new products developed for safety related systems. For legacy systems, the concept of ‘proven in use’ can be used as a means to achieve compliance with IEC 61508, with adequate historical in service data, performing as robust statistical data.

The reliance on legacy systems is difficult for the marine sector to rise from. “if it works, why change it?” many would ask. Pressure from within the industry to improve should come from companies competing to sell a better product to its customer.

It is true that ship owners will prefer repetition in regard to practice (to reduce costs when training staff and crew). Designers however would gladly embrace new practice. Ship owners will do the minimum to comply with safety regulations.

Same as with objective 1 with focus on defining practices for legacy systems to confirm adequate risk reduction, management, and lifecycle care. Prior Use and Proven In Use (PU/PIU) cases for the commercial marine sector and its specific "rules". The measure would be a comparison of existing non-compliant systems and new rules for systems considered under new guidance and new PU/PIU approaches.

6. The marine sector’s perception of safety mirrors societies, and improves in thresholds rather proportionally to gradually increasing risk because of increasing complexity of technology. Until a major accident occurs, users of SCS broadly assume robust practise when designed.

The attitude of waiting for major accidents then being pushed to make changes is not a sustainable approach. Adopting a risk based approach would assist with the best use of available resources. Safety culture needs to change, robust practise cannot be assumed rather it needs to be established and followed.

It is a common problem that safety practice improves in thresholds, rather than when new risks are present. The issue is that the cost to ensure the risk of anything happening is always too high. Engineers try to make complex technology as safe as (relatively) simple technology.

One Expert stated again that measures for objective 1 overlap. Clear expectation and understanding of ongoing lifecycle management would not depend on the "trigger event", as other industry sectors include similar requirements in some respects. Ownership and engagement through "personalisation" of approach could serve as an objective 6 specific measure.

Lots of manual back-ups are a costly issue, however it is an issue that is not unique to the marine sector. The premier issue is the regulatory framework.

7. Engineers looking to implement IEC 61508 from the beginning of a SCS life cycle, they risk restraining the complexity or novelty of technology in order to conform to IEC 61508.

Safety engineering does promote simplicity, and use of tried and tested technology. These are sound principles when people’s lives are at risk. Safety engineering also promotes a layered approach (not relying on any single layer for safety protection). The non-safety related functions can be complex and adopt novel technology, the safety related functions that prevent something bad from happening should be much simpler and less novel so that it would work when called upon.

Engineers are less likely to want to reduce innovation for the sake of making a standards implementation easier, or to save money, compared to a project manager. Dyson proves however that innovation can be attractive to customers, however it is “probably a good thing” that IEC 61508 reduced complexity of SCSs.

Some engineers prefer to use technology that is as simple as possible, as long as its compliant with safety regulations. It is preferable to some to limit changes to machinery and systems where possible.

The "restraint" is always the level of understanding of how novel or complex technology can go wrong and this has been exemplified in many cases recently (Boeing 737 MAX). Application and adoption

of novel technology should be risk based which should align with the lifecycle for Safety Related Systems.

8. The initial investment required bringing old systems to acceptably safe levels, and the cost of maintaining safety throughout the entire lifecycle is off putting by ship owners.

The first Expert stated that this is not necessarily associated with IEC 61508. The duty holder (e.g., ship owners) has the responsibility by law to ensure safety. There is a saying “if you think safety is expensive, try and accident”.

There is a trade-off between reassuring modified legacy systems, and manufacturing new ones. In the RN, the typical lifetime of a vessel is 40 years, including a midlife update, due to the reduced availability of parts for old systems.

Wartsila are redesigning engines as part of Wartsila’s realignment efforts for compliance to IEC 61508. Both suppliers and customers need to be compliant to IEC 61508. Barrier 8 therefore seems to be a theoretical issue as customers purchasing compliant systems, will likely also be compliant (IEC 61508 requires compliance for the systems whole lifecycle).

Same as objective one regarding the use of PU/PIU case studies. Managers and engineers may be reluctant to make the initial investments due to lack of studies, and a need to work within economic restraints.

9. Typically, a systems designer proposes a fixed-cost and assumes the financial risk after awarding a contract unless the buyer requests a change. If a risk assessment called for a change to a SCS design, this is at the builders or designers’ expense.

By adopting IEC 61508 safety lifecycle, the hazard identification and risk assessment takes place early on during the lifecycle, requirements are established from that process. There should not be increased financial risk by adopting IEC 61508. However, the contractor must be competent, and understand the costs and resources involved in compliance with IEC 61508 requirements.

Whether or not ship builders and designers take responsibility for costs depends on the type of contract. Negotiations need to be had if SIL requirements are not met. Some companies will not take on safety related contracts.

Wartsila produces systems tailored to specific risk assessments. Ship owners therefore are responsible for operating within the correct conditions.

Objective 9 justifies the role of the lifecycle. The Risk Assessment happens at the start to prevent changes from introducing errors at later stages. The objective should be to understand that early changes (from risk assessment findings) are highlighting application specific needs which may have not been considered by the "off the shelf" budget. Management of variations and clear specification of the process to include the necessary changes is key.

The final Expert confirmed the truth of objective 9, and stated it is “Tied up with culture”.

10. The costs for independent analysis for higher SIL safety functions and other costs for the initial tweak in alignment effort is off putting by ship owners.

The existing practises may not be the most cost effective, adoption of IEC 61508 could bring both increased safety and reduced cost over a long term. By not following a risk based approach, the existing ships may be operating at a higher safety risk, and the resulting accidents could be a lot more costly.

To negate the need for independent analysis of SILs, Ship builders may mandate they do not include safety-critical software (but still incorporate safety related software), in order to keep initial costs down. This is naive however as higher SIL SCSs are more rigorous, and lower SIL SCSs are more open ended (possibly on purpose to get around the need to implement safety measures). Ship builders need more guidance on lifecycle costs from experienced companies to make judgements that better reflect ship builders wishes (to save money).

Wartsila and the rest of the marine sector are in an ‘embryotic stage’ in regard to the implementation of risk based functional safety. Important SIL analysis cannot be avoided, however.

Objective 10 will also benefit from the development of appropriate case studies and sector specific daughter standard.

The final Expert believed the cost for producing and maintaining higher SIL systems is not significantly greater than lower SIL systems.

11. Companies typically split the budget to achieve safety functions between different stakeholders, compromising a company’s ability to achieve a target SILs.

Achieving adequate safety is a requirement by law, and should not be subject to budgetary constraints. Target SILs on different safety functions means better use of budget by putting more effort in areas of higher risk and less effort in areas of negligible risk to achieve an overall biggest risk reduction with the same budget.

Customers need to define the safety functions they require to best ensure that different stakeholders can work towards achieving them. The customer needs to complete the ship level safety assessments, and tag elements of it that are safety related (i.e., the safety signals, the E stops, and alarms). This can be improved with increased involvement or collaboration.

This objective also applies to other industries, and it is effectively managed in many cases. Development of a cross-industry review of IEC61508 with focus on how it applies to the marine sector could clarify this. Measure would be as per objective 4.

12. Cyber security can undermine HAZAN, as cyber-attacks can result in additional causes and consequences of hazards.

The duty holder has the responsibility to ensure safety and compliance with legislation. Additional efforts and burden are not excuses. Security breaches would damage company reputation, could lead to safety risks, and asset damage.

Reducing the risk to cyber security involves reducing connectivity to the internet, and increasing care that crew do not maliciously compromise systems. Use of whitelisted hardware will also help. There is a risk when purchasing hardware from ‘unreliable’ sources (such as eBay) that they may be installed with viruses.

Functional safety and cyber security go hand in hand. Cyber security is considered during a risk assessment at Wartsila. Remote cyber-attacks account for very few hazards in the marine sector. Malicious crew members and human error contribute the most to cyber-attacks (approximately 90% of cyber-attacks according to the Expert).

This is the role of the lifecycle. The Risk Assessment happens at the start to prevent changes from introducing errors at latter stages. The objective should be to understand that early changes (from risk assessment findings) are highlighting application specific needs which may have not been considered on the "off the shelf" budget. Management of variations and clear specification of the process to include the necessary changes is key. Cyber Security is fundamental to HSE, and needs to be taken seriously in any sector.

13. Indecisiveness regarding the trade-off between security requirements and safety requirements.

Both safety and security requirements must be addressed, based on the risk assessments. Security breaches can lead to safety accidents. If a system is not secure, it is not safe.

The decision for how much is spent on security and safety should be made by somebody with experience or understanding in both areas.

This should be risk based and IEC 61508 now includes some guidance on how to approach cyber security risks. The objective is as per 1 with measures and plans as per 4.

This is a challenging issue as both need to be met. Conditional based on companies’ knowledge.

14. Without consistency for fundamental terms used by different maritime regulatory frameworks regarding functional safety practise, the different tiers of the maritime regulatory framework cannot agree where the baseline for an equivalent level of safety is.

There is a need for a consistent set of regulatory frameworks across different tiers. Adopting IEC 61508 can promote consistency.

Inconsistency between fundamental terms used by different legal frameworks is a ‘normal’ issue. Numerical values for safety parameters are required.

Depends on the drivers for regulatory change, and the cost of migration.

15. Inclusion of stakeholders relating to increased automation on ships means increasing evidence-gathering procedures.

Increased automation could reduce errors by manual processes, and free up manpower required for many manual tasks. Many modern systems have automatic logging and reporting facilities in support of evidence gathering.

Increasing automation means increasing reliance on machine learning. This requires new safety measures and evidence gathering techniques.

Increasing numbers of stakeholders introduced by the inclusion of automation on ships can be considered an opportunity, as more people involved with their manufacture and operation means more data may be recorded for future use.

One Expert did not completely agree with this objective unless complexity, the level of evidence gathering, is proportional to the complexity and/or novelty of the system which is the same for non-safety related projects.

Companies can minimise proof by modifying off the shelf products (such as engines). Good practice requires traceability, and FSA.

16. The IMO does not provide a definition for ALARP, given the standard definition of ALARP, no third party without access to the underlying data can assess cost disproportionality.

ALARP is included in the UK legal requirements from Health and Safety at Work etc Act. Refer to HSE website on ALARP.

In the RN, they use a concept known as the Common D Ships matrix. It includes 5 levels of severity verses 5 levels of comparability. It is a qualitative assessment. Different matrixes are used for distinct types of ships, however.

Barrier 16 is considered a consequence of barrier 14.

Same as 1, ALARP as a concept depends on sector specific interpretation of risk, however SFAIRP should apply (actual legal requirement). To "calibrate" risk expectations, a formal bespoke interpretation of the standard must be understood and adopted.

17. Inconsistent understanding of what acceptable means between the different legal frameworks.

In the UK, the legal framework is based on the Health and Safety at Work etc Act. The ALARP principle provided a framework for judging what acceptable risk is.

Look into SFARP, So far as reasonably practicable, harder to meet than ALARP. How would one know when risk is low enough?

It is important to define when ‘safety is acceptable, or done’. There is a need for historical evidence to demonstrate in courts that safety assumptions are solid.

Two Experts suggested that the methods for accomplishing objective 16 are similar to objective 17.

Additional notes made during the interviews include:

- Within an organisation or company, an understanding of functional safety grows organically. Senior management may not understand initially, someone else (with an engineering position) may recognise its necessity.
- The management system needs to grow and develop in order to facilitate FSA(FSA).

- IEC 61508 is used as the benchmark for accepted good practice in regard to management systems.
- Ship builders will generally use other companies to produce and maintain safety-critical systems.
- An effective management system conducts Functional Safety Assessments, and Functional Safety Audits.
    - Audits are for procedures, and are necessary to make sure management systems work.
    - A FS Assessment is a detailed investigation to determine to what degree an organisation complies with the requirements of IEC 61508.
    - A FS Audit involves gathering evidence that a safety-critical system is doing what it is supposed to. It is conducted more frequently than the assessment. This typically involves conducting time checks, delay checks, and other investigations to determine confidence.
    - There are two types of FS Audit: a Routine audit, and a Fitness for purpose audit.
    - The Routine audit is a frequent check to assure the procedures are completed, done correctly, and that errors are recorded.
    - The Fitness for purpose audit tests the quality of procedures, and to facilitate higher auditor capability.
    - For higher SILs, independence is required, in order to avoid a situation synonymous with “a student marking his own homework”.
    - The largest barrier to IEC 61508s implementation in this Expert’s opinion is “getting management on board”.
- As technology improves, the difficulty to make repairs on ships while at sea increases.

One Expert stated: “There is an additional barrier you may want to consider if you have not already done so. I attended the SCS Symposium in York earlier this year and there was much talk of autonomous systems and the application of Artificial Intelligence and Neural Networks. The general feedback from the developing safety community was that there are no current safety standards (including IEC 61508) which can support assurance of such techniques. I suspect future editions of IEC 61508 will need to address machine learning and AI. I do not know whether you would include this within your study or perhaps declare it as a caveat (for future consideration).

Have you considered that it would be good to use pre-certified systems (hardware and or software) rather than invest in expensive safety assurance of COTS? I think too many companies do this purely out of naivety. They either do not engage safety Expert advice or choose to ignore it. That could be a substantial winning recommendation. I doubt if the marketplace could react immediately but if the demand increased from Shipbuilders then it would drive the need for development of off-the-shelf pre-certified marine systems. This is Nirvana I admit but I am sure other industry sectors are more responsive than the marine sector.”

When questioned about process for IEC 61508s inclusion in Lloyds Registers Rules and Regulations for the Classification of ships list of mandated standards for conformity, one Expert stated the following:

“LR can introduce a rule that is not mandated by other organisations. This requires a proposal to one (or more) of our rules’ committees’. These committees consist of industry stakeholders, and they can agree or disagree to include a rule. Each member is independent of LR, and membership is not a commercial undertaking.

Another approach would be to discuss with other class societies (through IACS - International Association of Classification Societies) to reach a common understanding and agreement. IACS could then make representations to IMO (through various groups and committees) to introduce the rule in some code, etc. or agree a UI (Unified Interpretation) to an existing regulation within a code (for example).”

Additional information was acquired from a member of LRs Regulatory Affairs Team. He stated:

“One route to implement IEC61508 would be through IACS. This process would lead the IEC standard through IACS, at which point it may be adopted by all member classification societies.

This is a possible route however this is how it would be done through LR processes, there are three options: Descriptive note, Type approval, and Adoption as ShipRight procedure.

Descriptive notes detail aspects of the fabric or features of the vessel and may include its type, purpose, function and or scope of operation, its materials and or installed equipment and components. They are added at the request of the client and are not directly supported by technical requirements within the Rules. The descriptive note for the installed component or equipment can, if deemed appropriate, refer to an assessment against the IEC standard.

Type approval happens for an existing (series production) component against a standard that is appropriate and that is requested by the client. The type approval certificate then refers to the IEC standard.

A new ShipRight procedure can refer to the IEC standard. The application of the IEC standard may be assigned a notation or descriptive note in the LR Rules. The new notation would go to the Technical Committee for their consideration. The standard is not subject to Technical Committee approval but may be provided to them for information only. ShipRight procedures are not like Rule Changes when it comes to governance.

Some standards can (and are) incorporated in LR Rules but they are prescriptive. The IEC standard is procedural and therefore the process differs. Please note that LR has a ShipRight procedure for Risk Based Design. This is applied to designs that deviate from Rule and Regulation requirements or for novel designs. This may overlap with or run parallel to the IEC standard. A gap analysis may shed some light on that.”

Appendix D Migration Strategy Balanced Scorecard

Vision:	**To mitigate barriers to the implementation of IEC 61508 in the UKCMS**						
Perspectives	**Barrier number**	**Barrier description**	**Objective number**	**Objective description**	**Measure number**	**Measures**	**Notes**
Technical	B.1	Lack of competency required for IEC 61508s implementation from within the commercial marine sector.	O.1	Use of consultation and or in-house Experts.	M.1	Number of consultants and or in-house Experts proportional to required independence for SIL targets of functional safety systems employed in UKCMSs that implement IEC 61508.	Determine independence using BS EN 61508 part 1 section 8 for safety-critical system, then compare against the number of consultants or inhouse Experts employed.
	B.2	Difficulty assigning SILs to automated SCS and artificial intelligence, with hardwire back-ups and human interaction, to relieve reliance on software.	O.2	Recording and development of case studies referring to failure rate of automated SCS and artificial intelligence in the UKCMS.	M.2	Number of case studies and recorded failures relevant to failure of E/E/PE SCS in the UKCMS, and consideration of sources from outside the UKCMS.	Requires measurement of failure records and review of accident reports.
Cultural	B.3	Lack of awareness of IEC 61508, and the significance of a risk based, life cycle approach to functional safety of safety-critical systems.	O.3	Training and education regarding risk based safety and safety life cycles.	M.3	Number of achieved qualifications/certifications relevant to the implementation of IEC 61508 by UKCMS engineers.	List of relevant qualifications and certificates that demonstrate training and education regarding the implementation of IEC 61508.
	B.4	Poor communication between different engineering sectors prevents recognition of solutions to similar	O.4	Increase publicity of IEC 61508 within the UKCMS via increased memberships to the	M.4	Number of staff from management and below that attend SCS Club events from the UKCMS.	Measurement of memberships to the SCSC, record of attendance to events, and use of SCSC

		challenges the commercial marine sector faces.		SCS Club by UKCMS staff and managers.			publications from within the UKCMS.
			O.5	Production of a UKCMS specific daughter standard of IEC 61508.	M.5	Production of a marine sector specific version of IEC 61508 by the International Electrotechnical Commission (IEC) and the British Standards Institute (BSI).	Requires monitoring of efforts made by the IEC, BSI, and other standard and legislation organisations to achieve this.
	B.5	The commercial marine sector relies heavily on legacy systems and practise, and is not agile to adapt or update.	O.6	Pressure to conform to IEC 61508 based on sector internal competition.	M.6	Recording of business signifiers (evidence that suggests improved profits, reputation, reduced failure) from UKCMS companies. A comparison of business signifiers between UKCMS companies that are and are not compliant to IEC 61508.	Requires advertisement or access to data from UKCMS companies.
Social	B.6	The marine sectors perception of safety mirrors societies, and improves in thresholds rather proportionally to gradually increasing risk because of increasing complexity of technology. Until a major accident occurs, users of SCS broadly assume robust practise when designed.	O.7	Training and education regarding risk based safety and safety life cycles to override societal perception.	M.7	Number of achieved qualifications/certifications relevant to risk based safety and the life cycle approach to risk assessment.	Record and categorise achieved qualifications and certifications for UKCMS companies.
	B.7	Engineers looking to implement IEC 61508 from the beginning of a	O.8	Use of COTS technology.	M.8	Number of COTS technology implemented for safety-critical systems.	Tally of COTS implemented by UKCMS per organisation or

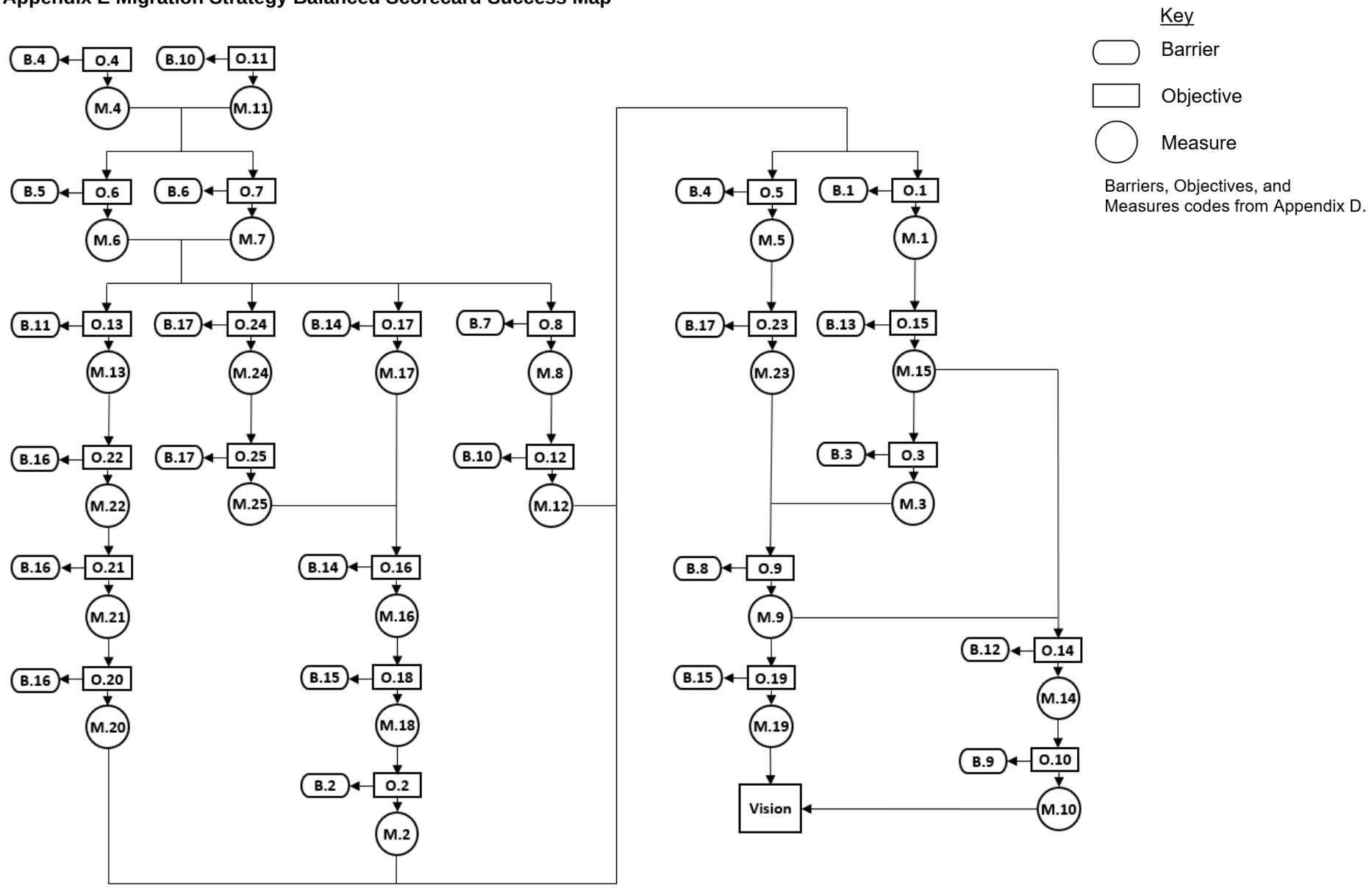
		SCS life cycle, risk restraining the complexity or novelty of technology in order to conform to IEC 61508.					company measured against time.
Financial	B.8	The initial investment required bringing old systems to acceptably safe levels, and the cost of maintaining safety throughout the entire lifecycle is off putting by ship owners.	O.9	IEC 61508 compliance between SCS suppliers and customers.	M.9	Number of customers of UK marine sector suppliers educated on IEC 61508.	Promote requirements for compliancy set by customers to users of this BSC. Promote benefits of compliance to aid in this.
	B.9	Typically, a systems designer proposes a fixed-cost and assumes the financial risk after awarding a contract unless the buyer requests a change. If a risk assessment called for a change to a SCS design, this is at the builders or designers' expense.	O.10	Implementation of tailored risk assessments.	M.10	Number of SCS with risk assessments set using IEC 61508 principles from the earliest stage of the overall safety lifecycle.	Data gathered from companies applying IEC 61508 FSA to systems in the concept, scope definition, and hazard and risk analysis stages of their lifecycle.
	B.10	The costs for independent analysis for higher SIL safety functions and other costs for the initial tweak in alignment effort is off putting by ship owners.	O.11	Provide guidance to ship owners and builders regarding the potential cost of failure of SCS conformity to IEC 61508 reduces.	M.11	Number of ship owners that attend talks and events that educate regarding the cost-benefit of a lifecycle approach to risk assessment.	Relies on representatives from marine sector companies that implement IEC 61508, or suitably qualified consultants that aid implementation efforts to host/speak at talks and events.

			O.12	Recording and development of case studies referring to the failure rates of compliant safety-critical systems.	M.12	Number of recorded and developed case studies referring to the failure rates of compliant safety-critical systems.	Relies on access to UK marine sector failure data, permissions to publish, and investigations regarding the efficacy of IEC 61508s implementation for mitigating past and future failure.
	B.11	Companies typically split the budget to achieve safety functions between different stakeholders, compromising a company's ability to achieve a target SILs.	O.13	Conduct cross industry reviews.	M.13	Number of studies produced that cross reference similar or identical compliant technology from other engineering sectors that exist in the UKCMS.	Requires review of relevant published literature and industry data.
Cyber-security	B.12	Cyber security can undermine HAZAN, as cyber-attacks can result in additional causes and consequences of hazards.	O.14	Consideration of cyber security during each life cycle risk assessment.	M.14	Number of safety cases for E/E/PE SCS in the UKCMS that consider cyber-security during their HAZAN.	Required data gathered during investigation suggested by M.10.
	B.13	Indecisiveness regarding the trade-off between security requirements and safety requirements.	O.15	Employment or consultation of Experts experienced in both safety and security.	M.15	Number of individuals with qualifications/certifications relating to safety and cyber-security involved during HAZAN of E/E/PE SCS in the UKCMS.	Requires access to data concerning individuals' qualifications in UKCMS companies. Internal implementation of this BSC does not require comparison with other companies.
Regulatory	B.14	Without consistency for fundamental terms used by different maritime regulatory frameworks regarding functional	O.16	Consistent language employed by regulatory frameworks.	M.16	Implementation of consistent interpretation of similar terms used between different regulatory frameworks by UKCMS companies.	Requires identification of similar terms, and knowledge of their interpretation by different companies. Comparison

		safety practise, the different tiers of the maritime regulatory framework cannot agree where the baseline for an equivalent level of safety is.					with a common glossary (if none exists, IEC 61508 part 4 provides a glossary).
			O.17	Definitions for quantitative safety parameters.	M.17	Implementation of consistent interpretation of quantitative safety parameters by UKCMS companies.	Investigate quantitative terms used, and their thresholds in each company. Compare these with other companies.
	B.15	Inclusion of stakeholders relating to increased automation on ships means increasing evidence-gathering procedures.	O.18	Employment of safety measures and data gathering techniques tailored for automated safety-critical systems.	M.18	Number of safety measures and data gathering techniques tailored for automated safety-critical systems.	Investigation into safety measures and data gathering related to automated ships. The progress for their writing and current implementation measured against time.
			O.19	Use of modified COTS systems to aid compliance effort.	M.19	Number of COTS technology implemented for safety-critical systems.	Proportion of COTS components used in compliant systems (e.g., entirely comprised of COTS, integrated components, or not used). Number may decrease as implementation of FSA at earlier stages of a systems life cycle increases.
	B.16	The IMO does not provide a definition for ALARP, given the standard definition of	O.20	Implementation of D ships risk classification matrices.	M.20	Number of UK marine sector companies that utilise the D ships risk classification matrix method.	May require adaption of D ships risk classification matrix method for commercial ships.

		ALARP, no third party without access to underlying data can assess cost disproportionality.	O.21	Inclusion of D ships risk classification as part of the LR Rules and Regulations (and consultation to IMO).	M.21	Raising of D ships risk classification matrix method at appropriate IMO or LR plenary session.	Requires attendee representation at an LR plenary session.
			O.22	Education and training in D ships risk classification matrices use within the UKCMS.	M.22	Number of individuals that have read D ships risk classification matrix method Ships Operating Centre Safety Risk Review Leaflet 5.	Awareness of leaflet required. Adaptation and translation of classification matrix leaflet may be required for use outside of Naval sector.
	B.17	Inconsistent understanding of what acceptable means between different legal frameworks.	O.23	Use of SFARP universally in the UKCMS.	M.23	Number of UK marine sector companies that comply to the Health and Safety Work Act 1974.	Verification of HSWa1974s inclusion within standards and legislation abided by UKCMS companies.
			O.24	Definition for acceptable established by the appropriate regulatory duty-holder.	M.24	IMO or LR plenary session that establishes the definition for acceptable to be used by the UKCMS.	Monitor plenary session published minutes and reports.
			O.25	Awareness for definition of acceptable increased within the UKCMS.	M.25	Number of UKCMS companies with awareness of definition of acceptable established by LR or IMO.	May require investigation into UKCMS companies' awareness, or sources for term definitions.

Appendix E Migration Strategy Balanced Scorecard Success Map



Appendix F Measure Performance Assessment

F.1 Measure Performance Assessment participant sheet

The following is the text included in a document sent to participants of the Measure Performance Assessment Study.

Thank you for considering participation in this study. This document describes the purpose for the research, justification for the data collected, and sets questions to gather the desired data.

1. Survey introduction

This section provides a brief description of the project, a description of the data required to progress the project, the method for gathering the data, and how the results will be utilised.

My project aims first to identify the barriers to implementing IEC 61508 in the UKCMS. Afterwards, to consider the options for overcoming said barriers to facilitate migration from current practice for implementing functional safety of safety-critical systems, to guidance set in IEC 61508. Lastly, to measure the performance of actions for overcoming the barriers, and drawing recommendations.

So far I have conducted a study to identify the barriers to implementing IEC 61508. The results yielded a profile of barriers that can be categorised into six types: technical, cultural, societal, financial, regulatory, and those related to cyber security. I then conducted an investigation to determine a number of objectives for overcoming the barriers proportional to their significance. Each objective is represented with a measure that when assessed, indicates the progress of its success.

1.1 Purpose brief

The purpose of this survey is to estimate the progress of all the objectives so far from the perspective of their respective measures, and identify actions which may result in raising each measures value.

Data is accepted from the opinions of individuals with backgrounds, achieved qualifications, and knowledge related to the UKCMS and its regulatory framework, IEC 61508, functional safety, and or cyber security.

1.2 Methodology brief

Participants are asked to:

1. Provide a statement concerning background, achieved qualifications, and knowledge relevant to the topics of the project.
2. Provide scores that represent progress made towards the completion of 25 objectives.
3. Provide their opinion regarding actions/tasks/methods for improving the progress, or achieving the successful completion each objective if/where possible.

These are delivered via the survey laid out in section 2 of this document, and upon completion sent to the researcher via email at: [REDACTED]

1.3 Significance of results

The results represent the last step of a rigorous process to produce a bases from which the researcher can justify suggested actions for UKCMS companies that wish to implement IEC 61508. The actions shall form a migration strategy for the whole UKCMSs migration from current practice for implementing functional safety of safety-critical systems, to accepted good practice. Actions may require internal changes to a company, or a collaborative effort made by the whole sector.

2. Survey questions

This section consists of the three parts of the survey. The survey involves providing a brief statement regarding your background and achieved qualifications relevant to the topics of this project and study. This survey is issued alongside the BSC Documents, the questions in section 2.2 relate to the progress of its objectives. The survey concludes with an invitation to provide opinions regarding methods for progressing the completion of the BSC objectives. **It may save you time by answering the questions in sections 2.2 and 2.3 at the same time.** You do not need to answer any questions you do not wish to answer.

The survey can be completed on your computer, alternatively; it can be printed out, answered on paper, then scanned back onto your computer.

2.1 Participant details

Please provide the requested personal information:

Achieved Qualifications and or background related to the following topics:

- UKCMS, and or UK marine sectors regulatory framework.
- IEC 61508, its daughter standards, and or functional safety of SCS in general.
- Cyber Security in the UKCMS.

2.2 Measures scores

Please read the Balance Scorecard document while answering this section of the survey. Please read each of the Objectives of the BSC, then provide a score from 0 to 10 that reflects your opinion in regard to the progress made towards its completion. 0 being entirely unaccomplished and 10 meaning the objective in question is completely accomplished. The BSC provides a measure for each objective, and notes for each measure to aid determining a score.

2.3 Action suggestions

Please provide a statement that explains any actions, tasks, or methods for progressing the achievement of any of the objectives in the BSC. Please write your answers in the boxes provided. If more space is required, please either adjust the font size, or type in another document or write on another sheet of paper.

F.2 Measure Performance Assessment results

Expert 1

Expert 1 has experience working in both the UKCMS and the Defence Naval sector. Expert 1 has experience complying to IEC 61508 guidelines when implementing functional safety in both sectors, and can therefore provide opinions from an internal and external perspective. The following are their answers to the BSC measures performance survey. This chapter explores the Objective scores and how well the measures represent them, whilst chapter 8 interprets recommendations for improved synthesis of the marine sector and the IEC 61508 guidelines based on the survey answers.

M.1 measures the number of consultants and or in-house Experts proportional to required independence for SIL targets of functional safety systems employed in UKCMSs that implement IEC 61508. Expert 1 explained that a small team of functional safety engineers were recruited against their training, experience, and ability to assess complex software-controlled systems with integrity targets up to SIL2. This team performed independent reviews of the engineering lifecycle development activities. An in-house independent safety engineer reviewed the outputs of the safety activities. These were also subject to scrutiny from external independent safety Experts appointed by the direct customer and in turn by independent safety Experts appointed by their customer.

One drawback was that there was some disagreement between Experts as to the level of independence actually required. The levels of independence were thus often obstructive rather than constructive. Expert 1 seemed satisfied with the number of consultants and in-house Experts employed.

M.2 measures the number of case studies and recorded failures relevant to failure of E/E/PE SCS in the UKCMS, and consideration of sources from outside the UKCMS. Expert 1 stated that empirical evidence from case studies was not forthcoming due to data protection from various navies around the globe. This was a limiting factor in determining SILs which could only be done by analysis of the new system (at concept stage).

As the system preliminary design developed and the requirements started to take shape, the architecture presented unique challenges in use of legacy software with new COTS hardware (COTS was mandated by the customer). SIL 2 thus became more of a qualitative than quantitative target where empirical evidence was lacking. This gave rise to additional development risk in achieving assurance goals. COTS shortfall was made up as much as possible by procurement of good quality COTS, application of IEC 61508-2 and 61511 principles and qualification testing etc.

M.3 measures the number of achieved qualifications/certifications relevant to the implementation of IEC 61508 by UKCMS engineers. Expert 1 stated that application of IEC 61508 was largely new to the development team, who underwent some external training. They also received assistance from the in-house safety team who had experience of IEC 61508, and learnt on-the-job under the guidance of the safety team.

There was some resistance initially until it became apparent why certain documentation and reviews were necessary. This was a long-term development (5 years) thus plenty of time was spent learning and adapting. Safety practice was becoming the norm and fairly well established, although still meeting some resistance particularly where timescales were tight.

M.4 measures the number of staff from management and below that attend SCS Club events from the UKCMS. Expert 1 stated that there was support from management to fund attendance of safety seminars for engineering staff, however this was very much voluntary not mandated (and not always well received by attendees).

M.5 measures the production of a marine sector specific version of IEC 61508 by the International Electrotechnical Commission (IEC) and the British Standards Institute (BSI). Expert 1 stated that the closest requirement to a Marine implementation of IEC 61508 was the Naval Authority Notice (NAN) for Software Integrity applied to naval surface ships and submarines. This was Loosely based on IEC 61508 and made reference to it. This was only partially enforceable; however, it was however good guidance for software contributions to platform-level Hazards and recommended use of HAZOPs.

M.6 records business signifiers (evidence that suggests improved profits, reputation, reduced failure) from UKCMS companies, and compares business signifiers between UKCMS companies that are and are not compliant to IEC 61508. Expert 1 states that legacy systems are largely unsuitable for IEC 61508 compliance where empirical data is unavailable. Software presents additional issues where not previously assured to a particular SIL. Redevelopment against IEC 61508 may be required, which can be prohibitively expensive. For any SIL functions, good architecture is essential to partition safety-related functionality and any quantitative analysis would ideally be carried out from concept/preliminary design.

Use of COTS will always carry additional risk until COTS has been qualified and assured to the standard. Pre-qualified COTS are preferred but not always available. A common (sector-wide) approach would help as it is hard work to make good progress against set timescales currently.

M.7 measures the number of achieved qualifications/certifications relevant to risk based safety and the life cycle approach to risk assessment. Expert 1 states that additional relevant safety training

would benefit social awareness and adoption of safety practices. It still takes time and experience however to win over some who are particularly resistant to safety practice. Keeping lifecycle metrics may help here. If shown that; software bugs for example, are identified and fixed earlier in the lifecycle, that may help to win them over. The later that problems are detected and fixed, the longer it takes and the more expensive it is to rectify generally. Training helps but is not the only thing required.

M.8 measures the number of COTS technology implemented for safety-critical systems. Expert 1 provided a summary of COTS:

COTS shortfall in IEC 61508 compliance (where empirical evidence is unavailable) can somewhat be made up as much as possible by procurement of good quality COTS, application of IEC 61508-2 and 61511 principles and qualification testing etc i.e., good engineering practice. Use of COTS will always carry additional risk until COTS has been qualified and assured to the standard. Pre-qualified COTS are preferred but not always available. A common (sector-wide) approach would help as it is hard work to make good progress against set timescales currently.

If more appropriate market-place COTS solutions were available for the marine sector, that would help a lot.

M.9 measures the number of customers of UK marine sector suppliers educated on IEC 61508. Expert 1 states that developers should take care to select suitable suppliers where possible. Better awareness of suppliers of marine systems and components with IEC 61508 would really help. In the defence sector requirements are flowed down from the MOD to all tiers of suppliers in the supply chain. Often it is the bottom of the chain that lacks awareness of IEC 61508. This may be a supplier of a PC or a level gauge or some other component/system that is required to be part of a safety loop. If that system/component is not already qualified to IEC 61508 then it is very hard to make a suitable safety case without carrying additional risk and/or requiring additional design/architecture to make up for shortfalls.

M.10 measures the number of SCS with risk assessments set using IEC 61508 principles from the earliest stage of the overall safety lifecycle. Expert 1 states that risk management needs to be understood, agreed, and managed collaboratively between suppliers and customers from the project concept. Otherwise, if the supplier needs to make up the shortfall it could be prohibitively expensive leading to concessions that would otherwise not provide a viable safety solution. This may lead to unreasonable limitations on the operation of the safety system. Manual/procedural mitigations may be put in place that are ineffective and lead to an accident through human factors that could otherwise have been avoided. As an achievement this is assessed based on personal experience in the naval marine industry though it may be lower commercially. Effective risk management needs regular and timely review/update to be effective i.e., to ensure the timely action of mitigation measures.

M.11 measures the number of ship owners that attend talks and events that educate regarding the cost-benefit of a lifecycle approach to risk assessment. Expert 1’s opinion is that this is probably the most difficult obstacle to overcome.

They advise ship owners that any software-control/automated system requires safety assurance through an evidence-based argument to ensure its safe operation (avoidance of collision/run-aground/flood/fire etc) and IEC 61508 presents an excellent framework for that. Certainly, with the advent of more automation on-board it makes sense to adopt good safety practice prior to development of such systems. You cannot simply bolt-on safety measures at the end.

Expert 1 point out that defence seems to be leading the way here at present, the commercial sector does not fully appreciate the benefits.

M.12 measures the number of recorded and developed case studies referring to the failure rates of compliant safety-critical systems. Expert 1 states that progress against O.12 is impacted by reluctance from the commercial marine to adhere to evidence-based safety standards, which is often viewed as a prohibitively costly overhead incurring additional developmental risk. A fear is that without that investment in safety, autonomous systems could be developed without adequate safety (and cyber security) measures. Expert 1 has witnessed this reluctance in both the marine and naval sectors. This is due to the limited number of catastrophic events arising from failure of automation/software control. That is likely however to increase as the level of automation increases unless safety practices are adopted from conceptual development of complex control systems and implemented effectively throughout the lifecycle.

M.13 measures the number of studies produced that cross reference similar or identical compliant technology from other engineering sectors that exist in the UKCMS. Expert 1 states that there are concerns here that not only is the budget split across different stakeholders (where they may not be readily understood/even achievable) but also that the budget may have been set incorrectly in the first place, and that a better solution could have been determined with early collaborative engagement with all stakeholders. The marine sector appears to suffer from lack of experience here and may not fully understand how to achieve the best architected solution for platform-wide safety and graceful degradation. There is generally much better established practice in air systems for example. The marine sector could learn a lot from other industries.

M.14 measures the number of safety cases for E/E/PE SCS in the UKCMS that consider cyber-security during their HAZAN. Expert 1 states that like safety measures, cyber security may also be an afterthought if not considered from the design concept. Again, it is hard to fully resolve once the design is started as the later it is implemented in the lifecycle the more costly it is likely to be as components may need to be replaced/redesigned. Key operations will need to be considered and designed into the system for effective cyber security including all stages of the product lifecycle: installation, operation and health monitoring, maintenance/updates etc. Progress is estimated to be low in the commercial marine industry.

M.15 measures the number of individuals with qualifications/certifications relating to safety and cyber-security involved during HAZAN of E/E/PE SCS in the UKCMS. Expert 1 anticipates that cyber security Experts are uncommon in commercial marine, except where serious infringements have occurred or where they are specified as system requirements from design concept. They are commonly included in naval marine systems for new designs but do not necessarily require Expert knowledge unlike safety systems, therefore progress is anticipated to be low.

M.16 monitors the implementation of consistent interpretation of similar terms used between different regulatory frameworks by UKCMS companies. Expert 1 states that consistency of terminology is desirable for easy read-across between different standards however the devil is in the detail. That is where measures, although similar, may have different emphasis between standards. IEC 61508 provides some flexibility but is generally more rigid than other standards/guidance such as RTCA DO-178. It may prove difficult to show compliance with IEC 61508 for a development that originated against RTCA DO-178, say, where there is a higher degree of flexibility in approach.

M.17 monitors the implementation of consistent interpretation of quantitative safety parameters by UKCMS companies. Expert 1 states that as for O.16, IEC 61508 is generally more rigid in its definitions for quantitative safety measures than other safety standards/guidance. That usually means it is easier to apply a SIL to a non-SIL assessment than the other way around. Any concessions carry additional of risk of unacceptance from the approval authority without further work which could be costly and may be entirely at the designer's risk. IEC 61508 may require further work for additional concession here to marry up with other safety standards. It does not readily lend itself to existing (legacy) development where empirical data does not exist. Perhaps a Route 4S is required?

M.18 measures the number of safety measures and data gathering techniques tailored for automated safety-critical systems. Expert 1 states that levels of automation are at present poorly understood by the marine industry, automotive is largely leading the field here. Automation can include machine-learning techniques which may be variable as they are heavily dependent upon algorithmic approach. Data gathering would need to consider such variations. There is much work to do here.

M.19 measures the number of COTS technology implemented for safety-critical systems. Expert 1 states that modified COTS means that the party carrying out modification takes on additional responsibility for qualification of any modified COTS. It then carries some risk that the modified product will not satisfy the certifying approval authority. The extent and type of modification will be subject to hazard risk assessment to ensure that it does not increase risk or introduce any new safety risks. In order to be confident of meeting IEC 61508 required measures most developers will buy COTS that are already IEC 61508 compliant (if available). With increased automation it likely that software safety that will require most of the assurance effort. It is anticipated that there is little progress here.

M.20 measures the number of UK marine sector companies that utilise the D ships risk classification matrix method. Expert 1 states that the D Ships Common RCM was developed with naval surface ships in mind. It rarely applies to naval submarines which normally have a higher level of criticality than ships as they are more likely to sink irrecoverably (particularly under dive) than a naval surface ship which is designed for good stability. It could be that commercial vessels will have different parameters and different operations to naval ships which mean that the criticality is lessened and thus D ships may be too onerous. A similar scheme however could be applied to certain classes of ships where operations and incidents are common. LR should be able to advise on the practicality of such a suggestion.

M.21 monitors progress towards the raising of D ships risk classification matrix method at appropriate IMO or LR plenary session. Expert 1 states that they have attended a session with LR and the Naval Authority before now (circa 2018), so they know that discussions have taken place with regard to the alignment of safety practices (which stemmed from Naval Authority Guidance and Notice for Software Integrity on Naval Surface Ships and Submarines) however they am not up to date with progress which is likely to have been hampered with COVID 19. They recall they were quite interested in potential updates to IEC 61508:2010.

M.22 measures the number of individuals that have read D ships risk classification matrix method Ships Operating Centre Safety Risk Review Leaflet 5. Expert 1 states that besides the UK MOD, LR and safety consultancies working in the marine sector (particularly defence) there is little or no knowledge of D Ships RCM. It would require a roll-out of knowledge, maybe inclusion within an appendix to IEC 61508, bearing in mind that it could need additional work to align it to the requirements of commercial ship classifications and their particular operations which would not normally include any hostile military operations.

M.23 measures Number of UK marine sector companies that comply to the Health and Safety Work Act 1974. Expert 1 asked if UK companies not generally work to ALARP not SFARP? ALARP is the legal norm for the UK. If commercial marine supply internationally then such definitions can vary widely. For example, the definition of SFARP in Australia has no concept of ALARP and Cost Benefit Analysis is rarely used to justify that safety risk is tolerable/acceptable as in the UK. I suspect that qualitative risk is not widely understood in the commercial marine sector beyond the assessment of physical risk as functional risk assessments would normally be carried by suppliers of systems rather than the shipbuilders themselves. Opportunities to roll down safety requirements to system developers for safe operation of complex control systems could thus be missed/overlooked.

M.24 monitors IMO or LR plenary sessions that establishes the definition for acceptable to be used by the UKCMS. Expert 1 states that the definition of acceptable appears to vary widely. Most safety consultancies tend to derive it from Reducing Risks Protecting People (R2P2) Societal Risk where it is deemed acceptable for 1 in 1000 employees to suffer a fatal accident per annum. That is normally set as the risk class A/B boundary in the Risk Class Matrix for Critical (where critical equates to 1 or more deaths). This is not enforced however, and I have seen many variations on this theme often because a matrix has been derived from another standard e.g., MIL-STD-882 (the US military equivalent of UK Def Stan 00-056) where damage to equipment/platform is also taken into account.

M.25 measures the number of UKCMS companies with awareness of definition of acceptable established by LR or IMO. Expert 1 states that It would require discussion forums to engage with commercial Shipbuilders and their suppliers and a roll-out of knowledge, maybe inclusion within an appendix to IEC 61508. It could need additional work to ensure appropriateness to the subject matter.

Appendix G Migration Strategy

Recommendation number	Recommendation description
R.1	Hire enough engineers to satisfy the level of independence required for the systems a given company produces.
R.2	Prepare for disagreement between engineers in regard to required independence levels.
R.3	Engage consultants to initiate mapping against a real life system and start documenting findings.
R.4	Integration of high quality COTS systems that comply to IEC 61508.
R.5	Engage stakeholders to initiate wider spread desire for implementation of IEC 61508, and to collaborate with development of case studies.
R.6	Determine and implement non-financial incentives for engineers to attend functional safety related training and seminars.
R.7	Commitment to IEC 61508 conformity regardless of timescale.
R.8	Determination and implementation of steppingstones between current and accepted good practice.
R.9	Assess necessity to update functional safety capability.
R.10	Place pressure on the UKCMS to demonstrate compliance to IEC 61508.
R.11	Widespread availability for recertified systems
R.12	Measurement of effective risk management.
R.13	Measure the number of ship owners who attend talks and seminars related to accepted good practice for functional safety.
R.14	Monitor how other sectors implement IEC 61508 continuously.
R.15	Increase awareness for accepted best practise regarding cyber-security of E/E/PE systems.

R.16	Development of sector specific daughter standard for IEC 61508, emphasising the use of language compatible with the UKCMS.